- Es gilt das gesprochene Wort -

Keynote

Dr. Otto Schily, Bundesminister des Innern a.D.

Potsdamer Konferenz für Nationale Cyber-Sicherheit

Freitag, 12. Juni 2015, 13.00 Uhr

Potsdam, Hasso-Plattner-Institut

Die Bedeutung des Internets für die Zukunft der rechtsstaatlichen Ordnung

Zunächst darf ich Sie zu der Konferenz für Nationale Cyber-Sicherheit beglückwünschen, deren Themen nicht zuletzt im Blick auf die jüngsten Ereignisse aktueller denn je sind. Die Attacken auf Informationsnetze und Datenbestände nehmen auf bedrohliche Weise zu. Die Tatsache, dass es nach Presseberichten Angreifern gelungen ist, so tief in das Informationsnetzwerk des Bundestages einzudringen, dass möglicherweise das gesamte Computer-Netzwerk des Bundestages nicht mehr gegen den Angriff verteidigt werden kann und vollständig neu aufgebaut werden muss, ist höchst alarmierend. Wenn nicht einmal das Informationsnetzwerk des höchsten Staatsorgans, des Parlaments, vor massiven Angriffen dieser Art geschützt ist, stellt sich schon die Frage, ob und gegebenenfalls welche Versäumnisse bei den Schutzvorkehrungen für die Integrität des Informationsnetzwerks zu beklagen sind.

Wir nennen bekanntlich die sich immer rascher ausbreitende digitalisierte Informations- und Kommunikationstechnik – IuK – eine Querschnitts-Technik, weil sie nahezu alle Lebensbereiche durchdringt, angefangen von der privaten Lebensführung, über die Steuerung und Überwachung

wirtschaftlicher und technischer Prozesse bis hin zur Vernetzung politischer und administrativer Arbeitsfelder. Und wie jede Technik hat IuK ihre Licht- und Schattenseiten, ist Segen und Fluch zugleich. Ob sie ein Segen ist, hängt wesentlich auch davon ab, ob sie dem Einzelnen, dem Staat, der Wirtschaft und den kulturellen Institutionen mehr Sicherheit bietet oder eher existenzbedrohende Gefährdungspotentiale zeitigt.

Wie wir mit dem Thema umgehen, hängt nicht zuletzt von unserem Verständnis des Verhältnisses zwischen staatlicher Verantwortung und Behauptung der individuellen Freiheit ab.

Nach meinem Verständnis ist zentraler Orientierungspunkt für das Verhältnis von individueller Freiheit und staatlicher Verantwortung Art. 1 des Grundgesetzes, mit dem sich der Staat in die Pflicht nimmt, die Würde des Menschen zu achten, zugleich aber auch die Würde des Menschen zu schützen. Achtung der Freiheit des Menschen und Sorge für seine Sicherheit sind also in einen engen Zusammenhang gestellt. Die Würde des Menschen wird dadurch gewahrt, dass der Staat sie achtet, aber auch im Rahmen der rechtsstaatlichen Ordnung gegen Angriffe verteidigt.

Neue Herausforderungen für die bestehende Rechtsordnung

Die durch den Staat und seine Institutionen verbürgte Verfassungs- und Rechtsordnung ist zunächst einmal ein Normengefüge, das aber auf die Observanz der Bürgerinnen und Bürger, der Repräsentanten der gesellschaftlichen Formationen und Organisationen sowie der Vertreter der staatlichen Institutionen angewiesen ist. Die Befolgung der von der Rechtsordnung gesetzten Normen erzwingt der Staat durch Sanktionen unterschiedlichster Art. Das verleitet zu dem Irrtum, die Geltung von Normen sei darauf zurückzuführen, dass bei Nichteinhaltung Sanktionen verhängt werden können. Die soziale Wirklichkeit sieht aber anders aus.

Die Rechtsordnung kann nur funktionieren, wenn jedenfalls die übergroße Mehrheit sich rechtstreu verhält, ohne dass es einer wie immer gearteten staatlichen Sanktion bedarf. Daher ist eine Rechtsordnung in der sozialen Wirklichkeit das Konzertieren der sich in einem kommunikativen Prozess ständig verändernden und erneuernden Gefühle und Verhaltensweisen der Menschen, temperiert durch Sitten und Gewohnheiten, aber auch durch die Wertbindungen und Moralvorstellungen der Menschen. Im lateinischen Wort Konsens kommt das sehr gut zum Ausdruck, Recht ist in erster Linie Konsens, Zusammenfühlen. Demokratie gehört hierzulande zu diesem Konsens, die demokratische Verfassung ist der Grundkonsens.

Man spricht auch von der Akzeptanz von Vorschriften und Gesetzen; fehlt es an dieser, entstehen die bekannten Vollzugsdefizite, die sich häufig nicht durch Sanktionen beheben lassen. Die Notwendigkeit und Wirksamkeit von Sanktionen im Einzelfall bestreite ich gewiss nicht, aber auch der durch Sanktionen erzwungene oder jedenfalls stimulierte Konsens bleibt ein Konsens, ohne den das Recht sich in Staub auflösen würde.

Nun stellt sich die Frage: Verändert sich der sich im allgemeinen Rechtsverständnis manifestierende Konsens durch die modernen Kommunikationsformen im Internet, im World Wide Web, in den so genannten sozialen Netzwerken? Untergräbt die Digitalisierung der Kommunikationsformen im Internet den Rechtsstaat oder bestärken die durch das Internet möglich gewordenen interaktiven Kommunikationsformen den Konsens im Sinne einer Festigung der Rechtsordnung? Ist das Internet ein rechtsfreier Raum? Kann die Einhaltung der bestehenden rechtlichen Gebote und Verbote im Internet durchgesetzt werden oder herrscht dort Anarchie?

Welche Mittel darf der Staat - oder der Staatenbund EU oder die internationale Staatengemeinschaft - zur Kontrolle des Internet einsetzen, ohne die Freiheitsrechte des Einzelnen anzutasten? Wie kann und darf der Staat seine Funktionen im Internet wahrnehmen, um Angriffe auf die Sicherheit seiner Bürgerinnen und Bürger abzuwehren und die Verletzung schutzwürdiger Interessen zu verhindern? Ist der Staat im Internet ohnmächtig, während die Macht großer Player im Internet wie Google, Facebook u.a. überhandnimmt?

Welche neuen Herausforderungen ergeben sich für den Staat bei der Bekämpfung von Straftaten im Internet und durch das Internet? Welche völkerrechtlichen Vereinbarungen sind erforderlich, um einem sich abzeichnenden oder schon subversiv begonnenen Cyber-War zuvorzukommen?

Das Internet mit inzwischen Milliarden von Nutzern und die mobile Kommunikation mit ebenfalls Milliarden von Mobiltelefonen weltweit haben Dimensionen angenommen, die die Beantwortung dieser Fragen als sehr dringlich erscheinen lassen. Die sehr weitreichende Vernetzung von lebenswichtigen Infrastrukturen, die Abhängigkeit der Wirtschaft, der Verwaltung, der staatlichen Institutionen und des privaten Sektors von sicherer Datenverarbeitung, Datenspeicherung und Datenkommunikation machen Angriffe gegen die Integrität von Computersystemen und die Verlässlichkeit von Informations- und Kommunikationssystemen durch kriminelle oder terroristische Gruppen, Einzeltäter oder durch Akteure in einem „grauen“ Cyber-Krieg zu einer sehr ernsthaften und umfassenden Bedrohung.

Weil IuK diesen hohen Durchdringungsgrad erreicht hat, der in Zukunft weiter zunehmen wird, hat die Frage der Verlässlichkeit und Sicherheit der IuK-Strukturen einen besonders hohen Rang. Das gilt vor allem des-

halb, weil IuK mittlerweile nicht nur Teil der Infrastruktur allgemein, sondern der so genannten „Kritischen Infrastruktur“ geworden ist.

Cybersicherheit als gemeinsame Aufgabe von Staat und Wirtschaft

Wie jede Technik hat die fortschreitende digitalisierte IuK ihre spezifischen Risiken in technischer Hinsicht. Es liegt in der Natur der Sache, dass wir, indem wir uns auf die digitalisierten Strukturen und Prozesse einlassen, damit auch unweigerlich die Risiken in Kauf nehmen. Deshalb sagt das BSI auch zu Recht, es gehe nicht mehr um Risikovermeidung, sondern nur um Risikominimierung. Das gilt im Prinzip für jede Technik, beispielsweise für den Autoverkehr, die Chemie-Industrie und den Energiebereich. Die Risiken zu minimieren ist zuallererst Aufgabe der IuK-Wirtschaft und der Wissenschaft und Forschung, aber auch in gewissem Umfang Verantwortung des Staates. Um die notwendigen technischen und organisatorischen Schutzvorkehrungen zur Minimierung technischen Risiken müssen sich Anbieter und Nutzer von Informations- und Kommunikationstechnik in erster Linie selbst kümmern, der Staat kann jedoch dazu Hilfestellung leisten. Der Staat ist aber unter Umständen auch dazu berufen, im Allgemeininteresse bestimmte technische Mindeststandards festzusetzen, die eingehalten werden müssen. Im Übrigen ist der Staat aber auch selbst Anbieter und Nutzer von IuK, insofern erweitert sich seine Verantwortung auch in diese Richtung. Deshalb hat die Bundesregierung unabhängig von den politischen Konstellationen stets großen Wert auf eine enge Kooperation von Staat und Wirtschaft zur Verbesserung der Cybersicherheit gelegt. Diese Kooperation sollte aber deutlich verstärkt werden. Mitunter muss man leider den Eindruck gewinnen, dass Cybersicherheit bei der Festlegung von Prioritäten noch nicht den ihr gebührenden Rang erhält. So enthält die soeben verkündete Strategie der EU-Kommission zum Digitalen Binnenmarkt kaum Nen-

nenswertes in dieser Richtung. Günther Oettinger beklagt zu Recht wie viele andere, dass Deutschland und Europa insgesamt in der digitalisierten IuK-Wirtschaft sowohl in technischer als auch in wirtschaftlicher Hinsicht gegenüber den USA weit zurückgeblieben sind. Warum setzen wir nicht darauf, auf dem Gebiet der Sicherung von digitalisierten IuK-Strukturen unsere Wettbewerbsnachteile gegenüber den USA jedenfalls in gewissem Umfang aufzuholen?

Herausbildung neuer Kriminalitätsformen

Eine weitaus stärkere Verantwortung trifft den Staat hinsichtlich der polizeilichen Gefahrenabwehr und der Strafverfolgung im Bereich der IuK. IuK kann ebenso wie andere Techniken zu kriminellen Zwecken missbraucht werden. Die Verhinderung des kriminellen Missbrauchs der IuK ist in erster Linie Aufgabe des Staates und der internationalen Staatengemeinschaft. Kriminellen Missbrauch beispielsweise des Internets zu unterbinden, ist aber zugleich auch unsere gemeinsame gesamtgesellschaftliche Verantwortung. Angesichts der Spannweite der Informationsnetze ist der Staat nicht zuletzt auf die Mitwirkung der Netzanbieter angewiesen. Notfalls muss der Staat durch gesetzliche Vorschriften dafür sorgen, dass diese Mitwirkung sichergestellt ist.

IuK-Technik ist in erheblichem Umfang ein Instrument global agierender terroristischer Gruppen und der Organisierten Kriminalität. Über das Internet wird terroristische Propaganda verbreitet, das Internet dient terroristischen und kriminellen Organisationen zur Verbrechensvorbereitung und Verbrechensausführung, es dient aber auch zur Begehung minderschwerer Straftaten wie Betrug oder Urheberrechtsverletzungen. Weil IuK aber als Querschnittstechnik und auf Grund seiner Komplexität enorme Angriffsflächen bietet, haben sich völlig neue Kriminalitätsformen herausgebildet, die unter der Bezeichnung „CIA-Delikte“ (in diesem Fall

„Confidentiality, Integrity und Availability“) zusammengefasst werden. Diese neuen Kriminalitätsformen richten sich auch gegen die bereits erwähnten kritischen Infrastrukturen und sind damit ein hochgradiger Gefahrenherd. Die kriminellen Attacken unterscheiden sich nach ihrem Modus Operandi. Die Sicherheitsbehörden beobachten seit geraumer Zeit eine Verlagerung der Bedrohungsszenarien von ungezielten Angriffen mittels SPAM, Viren, Würmern, Trojanern, Drive-by-Downloads gegen unspezifische Zielgruppen auf gezielte Angriffe – Spionage und Sabotage – gegen spezielle Zielgruppen mittels Social Engineering und Trojanern sowie skalpellartigen Angriffen, durch Sabotage spezieller IT-Systeme (und Infrastrukturen) mit großem Schadensausmaß. Diese bedürfen komplexer und langwieriger Vorbereitung, nutzen die so genannte Zero-Verwundbarkeit aus und verwenden gefälschte Zertifikate.

Deutschland ist Angriffen aus dem Cyber-Raum besonders zur Ausspähung von Know-how ausgesetzt. Die Zielbereiche sind Politik, Militär, Wirtschaft, Wissenschaft und Forschung. Akteure sind fremde Nachrichtendienste, Organisationen anderer Staaten, „private Beschaffer“ und Konkurrenten. Die Gefährdungslage hat sich – soweit ich das unter Zuhilfenahme des Lageberichts des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) und sonstigen Informationen beurteilen kann – in den zurückliegenden Jahren eher verschärft. Auf Einzelheiten muss ich nicht eingehen, dazu haben Sie sicherlich im Verlauf der Konferenz schon viel gehört.

Besonders besorgniserregend ist die Tatsache, dass nach dem jüngsten Lagebericht des BSI immer noch erhebliche Sicherheitslücken in großer Zahl entdeckt werden und meist zu so genannten Zero-Day-Angriffen ausgenutzt werden, das heißt die Schwachstellen werden bereits am Tag ihres Bekanntwerdens angegriffen. Ebenso besorgniserregend ist die weitere Feststellung des BSI, dass die Detektion von Schadpro-

grammen immer schwieriger wird, nicht nur wegen der großen Anzahl neuer Schadprogramme. Auch wird ein Schadprogramm nicht wie früher über die Dauer von vielen Monaten genutzt sondern nur noch wenige Tage verwendet, bevor es durch eine neue Variante, die nicht mehr von Viren-Schutzprogrammen diagnostiziert wird, ersetzt wird. Die übliche Detektion von Schadprogrammen anhand von Signaturen und Prüfsummen wird dadurch immer schwieriger, die Hersteller von Viren-Schutzprogrammen haben große Probleme, die Vielzahl unterschiedlicher Schadprogramme zu orten und Erkennungssignaturen zu erstellen. Dass sogar ein Unternehmen wie Kaspersky, dessen Kerngeschäfte AntiVirus-Programme und Internet Security sind, nach neuesten Meldungen von einem Trojaner ausspioniert wurde, ist wahrlich ein Alarmzeichen.
Ganz allgemein ist Gefahrenabwehr immer ein Wettlauf zwischen der Erfindungsgabe krimineller Einzeltäter oder krimineller Gruppen auf der einen Seite und der Perfektionierung der Schutzvorkehrungen auf der anderen Seite. Weil sich Informations- und Kommunikationstechnik in einem rasanten Tempo weiterentwickelt und sich durch extrem kurze Innovationszyklen auszeichnet, ergeben sich unausweichlich auch immer wieder neue Sicherheitslücken.

Strafverfolgung durch internationale Zusammenarbeit

Eine wirksame Bekämpfung des Terrorismus und der Organisierten Kriminalität erfordert daher effiziente Methoden der staatlichen Sicherheitsinstitutionen im Rahmen der Rechtsordnung und im Zusammenwirken mit der Wirtschaft. Dazu gehört auch, die Sicherheitsbehörden mit der Befugnis auszustatten, sich Zugang zu den Informationskanälen und Datenbeständen terroristischer Gruppen und der Organisierten Kriminalität zu verschaffen, um deren Planungen rechtzeitig aufzudecken und zu verhindern.

Dass die Sicherheits- und Justizbehörden des Staates die Vorbereitung und Begehung von Straftaten, die im Internet oder anderen modernen Kommunikationsformen stattfindet, nach besten Kräften vereiteln oder jedenfalls im Rahmen des rechtsstaatlichen Regelwerks strafrechtlich ahnden müssen, kann ebenso wenig ernsthaft in Frage gestellt werden wie das Recht und die Pflicht der Sicherheitsbehörden, die Spuren, die terroristische Gruppen oder kriminelle Organisationen im Internet oder anderen modernen Kommunikationsformen hinterlassen, zur möglichst raschen und umfassenden Aufklärung von Verbrechen zu nutzen, zumal diese Aufklärung nicht selten zugleich die Voraussetzung schafft, Nachfolgetaten zu verhindern, also die Bedingungen für die Abwehr schwerster terroristischer oder sonstiger Verbrechen zu verbessern.

Soweit es um die Abwehr von Angriffen auf IuK-Systeme, Datenwege und Datenbestände geht, haben strafrechtliche Sanktionen und die entsprechenden Strafrechtsnormen nur sekundäre Bedeutung. Wir sollten aber gleichwohl die Bedeutung von strafrechtlichen Ermittlungen nicht unterschätzen, die aber in hohem Maße auf internationale Kooperation angewiesen sind. Jüngsten Medienberichten zufolge ist es einer durch Europol koordinierten Aktion der Polizeien in Großbritannien, Italien, Spanien, Polen, Belgien und Georgien gelungen, eine internationale Bande von Cyberkriminellen zu zerschlagen.

Entscheidend für die Sicherung und Härtung der IuK-Systeme sind jedoch technische und organisatorische Vorkehrungen. Deren Erfolg hängt sehr wesentlich von einer engen Zusammenarbeit zwischen staatlichen Institutionen und der Wirtschaft ab, insbesondere auch im europäischen und internationalen Rahmen. Die Zahl der internationalen Organisationen, die auf diesem Feld tätig sind, erinnern an den Satz von Karl Kraus: „Wenn ich nicht wüsste, was alles möglich ist, würde ich staunen, was es alles gibt.“: EU-Aktionsplan zum Schutz kritischer Infrastrukturen, EU-

US-AG Cyber-Security, Meridian-Prozess seit 2005, Kooperation BSI und BKA mit FBI, bilaterale und multilaterale AGs zu Norms of State Behavior/VBSM [„vertrauens- und sicherheitsbildende Maßnahmen“], NATO, G 8, OSZE, Vereinte Nationen, die vom BSI begründete Sicherheits-Allianz, der Internet Security Summit in München usw. usf.

Dass der Staat seine eigenen Datenbestände und Kommunikationswege vor Angriffen schützt und dass er sich um die redundante Sicherung von kritischen Infrastrukturen, die sich zum überwiegenden Teil in privatwirtschaftlicher Hand befinden, in enger Zusammenarbeit mit der Wirtschaft durch eine Reihe von abgestimmten technischen und organisatorischen Maßnahmen kümmert, hat meines Wissens noch nicht zu ernsthaften Auseinandersetzungen mit der Internet Community geführt.

Konflikte ergeben sich erst dann, wenn es sich um die strafrechtliche Aufklärung und präventiv-polizeiliche Verhinderung von Straftaten im Internet handelt und nicht um Angriffe auf die Integrität von IuK-Strukturen handelt. Freilich ist die Abgrenzung dieser beiden Bereiche nicht immer ganz einfach, denn eine Urheberrechtsverletzung ist zwar eine Straftat im Internet aber unter Umständen auch ein rechtswidriger und strafbarer Angriff auf einen Datenbestand. Besonders argwöhnisch und misstrauisch reagiert die Internet Community jedoch außerdem, wenn der Staat sich selbst die Leistungsfähigkeit des Internets für neue Überwachungs- und Kontrollmöglichkeiten zunutze macht, um Straftaten besser aufklären und vorbeugen zu können.

Ängste vor staatlicher Überwachung weit verbreitet

Zur Illustrierung der Konfliktfelder mit der Internet Community einige wenige Beispiele:

Der sexuelle Missbrauch von Kindern und die Verbreitung von so genannter Kinderpornografie gehört zu den abscheulichsten Verbrechen, derer sich Menschen schuldig machen. Der Rechtsstaat muss daher alle nur denkbaren Mittel aufbieten, um diese Verbrechen zu verhindern und aufzuklären. In diesem Sinne war es folgerichtig, dem Staat die Befugnis zuzuordnen, Webseiten mit pornographischem Inhalt zu sperren, wenn deren rasche Löschung aus organisatorischen oder verfahrensrechtlichen Gründen nicht erreichbar ist. Dagegen erhob sich ein Sturm der Entrüstung, der in dem Vorwurf gipfelte, die Meinungs- und Informationsfreiheit sei bedroht, es werde Zensur im Internet eingeführt. Im Bundestag wurde eine Petition eingebracht, für die über 60.000 Unterschriften gesammelt wurden. Die Politik ließ sich davon zunächst nicht beeindrucken. Zur Sperrung von Kinderpornografie-Seiten im Internet schloss die Bundesregierung am 17. April 2009 einen Vertrag mit fünf großen Internetprovidern. Internetangebote sollten von ihnen nach einer täglich aktualisierten Liste des Bundeskriminalamts (BKA) blockiert werden. Mit dem Gesetz zur Bekämpfung der Kinderpornografie in Kommunikationsnetzen (Zugangserschwerungsgesetz) sollten Provider in Deutschland verpflichtet werden, den Zugang zu vom Bundeskriminalamt vorgegebenen Webseiten mit strafbaren Inhalten zu erschweren. Die Internetanbieter sollten laut dem Gesetz verpflichtet werden, die vom Bundeskriminalamt erstellten Sperrlisten geheim zu halten. Entsprechend einer nachträglichen Änderung des Gesetzentwurfs unter Federführung der damaligen Justizministerin Brigitte Zypries sollten Zugriffsversuche auf diese Seiten auch zeitgleich protokolliert und zu Strafverfolgungszwecken genutzt

werden können. Gesperrt werden sollten gemäß § 8a Abs. 1 des Gesetzentwurfes Webseiten, die Kinderpornografie enthalten oder mit einem Hyperlink auf diese verwiesen. Später, im April 2011, machte die Bundesregierung – nunmehr in der Verantwortung der neuen Justizministerin Leutheusser-Schnarrenberger eine Kehrtwende und beantragte, das bereits beschlossene, aber nie angewendete Gesetz aufheben zu lassen. Die endgültige Aufhebung erfolgte am 1. Dezember 2011 durch Beschluss des Bundestages.

Die Abkehr von der Zugangserschwerung durch Sperrung von Webseiten mit kinderpornografischem Material wurde damit begründet, dass die Löschung dieser Webseiten die bessere Alternative sei.

An diesem Vorgang ist mehreres bemerkenswert: Ein beschlossenes Gesetz wird einfach nicht angewendet, weil es einem neuen Koalitionspartner, der FDP, nicht gefiel. Für die Festigung des rechtsstaatlichen Konsenses ist so etwas nicht gerade förderlich. Das Druckpotential der Internetgemeinde, mit dem sie politische Entscheidungen beeinflussen kann, hat offenbar zugenommen. Es wird eine Maßnahme – die Löschung von Webseiten – als Alternative ausgegeben, die keine echte Alternative sondern nur eine zusätzliche – sicherlich die effizientere – Möglichkeit ist, aber die Sperrung, wenn die Löschung nicht erreichbar ist, nicht überflüssig macht. Und – was das Schlimmste ist – der Staat lässt sich den Vorwurf gefallen, die Verhinderung des Zugangs von kinderpornografischen Webseiten sei Zensur, die ja nach dem Grundgesetz nicht stattfinden darf.

Ein zweites Beispiel ist die Vorratsdatenspeicherung: Die Analyse von Kommunikationsdaten unterschiedlicher Art ist ein wichtiges Element erfolgreicher polizeilicher Gefahrenabwehr und der Aufklärung von Straftaten. Die Urheber der Anschläge auf die Madrider Vorortzüge im März 2004 konnten durch Auswertung von Telekommunikationsdaten ermittelt

werden. Im Jahre 2000 konnte die Ausführung eines Sprengstoff-Attentats auf den Straßburger Weihnachtsmarkt durch Zugriff auf Kommunikationsdaten verhindert werden. Auch in zahlreichen anderen Fällen hat die Auswertung von Kommunikationsdaten entscheidend dazu beigetragen, Verbrechen aufzuklären und zu verhindern sowie die Strukturen terroristischer Gruppen oder krimineller Organisationen aufzudecken. Voraussetzung für die Auswertung von Kommunikationsdaten ist logischerweise, dass sie gespeichert wurden. Eine solche Speicherung wird von Anbietern von Kommunikationsleistungen zu Abrechnungszwecken vorgenommen. Auf diese gespeicherten Daten konnten die Sicherheitsbehörden seit jeher bei Vorliegen eines Verdachtes zur Gefahrenabwehr und zur Strafverfolgung zugreifen, ohne dass das irgendjemand in Wallung gebracht hat. Jedoch ist die Frist zur Speicherung von Kommunikationsdaten zu Abrechnungszwecken auf drei Monate begrenzt. Deshalb hat man sich auf EU-Ebene in der Justiz- und Innenministerkonferenz darauf geeinigt, Telekommunikationsanbieter zu verpflichten, Verkehrsdaten ihrer Kunden, Standortdaten und eindeutige Geräteidentifikationen für einen längeren Zeitraum zu speichern (Mindestspeicherfrist 6 Monate), damit Polizei und Nachrichtendienste darauf zugreifen können. Die Speicherverpflichtung wurde auf Verkehrsdaten erweitert, die nicht zu Abrechnungszwecken gespeichert werden müssen (z.B. bei Flatrate- und Prepaid-Tarifen, eingehenden Verbindungen, Handystandorten, IP-Adressen, Email-Verbindungsdaten). Die entsprechende EU-Richtlinie wurde zunächst in Deutschland im „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ in nationales Recht übertragen. Dieses Gesetz wurde mit einer Entscheidung des Bundesverfassungsgerichts vom 2. März 2010 leider aufgehoben. Das Bundesverfassungsgericht hielt eine Vorratsdatenspeicherung allerdings

für grundsätzlich mit dem Grundgesetz vereinbar; im Hinblick auf das Telekommunikationsgeheimnis der betroffenen Bürger müsse aber gewährleistet sein, dass die Daten nur dezentral gespeichert und mit besonderen Maßnahmen gesichert würden und die unmittelbare Nutzung der Daten durch Behörden müsse auf genau spezifizierte Fälle schwerster Kriminalität und schwerer Gefahren beschränkt bleiben; diesen Anforderungen werde das angegriffene Gesetz nicht gerecht. Gegen eine mittelbare Nutzung, wie sie z. B. für eine Anschlussermittlung über eine IP-Adresse notwendig ist, bestehen nach Auffassung des Bundesverfassungsgerichts bei allen Straftaten, in bestimmten Fällen sogar bei Ordnungswidrigkeiten, ohnehin keine Bedenken.

Auch der EuGH hat in seiner Entscheidung vom 8. April 2014 ausdrücklich im Grundsatz anerkannt, dass „die Vorratsspeicherung der Daten angesichts der wachsenden Bedeutung elektronischer Kommunikationsmittel die nach dieser Richtlinie auf Vorrat zu speichernden Daten den für die Strafverfolgung zuständigen nationalen Behörden zusätzliche Möglichkeiten zur Aufklärung schwerer Straftaten bieten und insoweit daher ein nützliches Mittel für strafrechtliche Ermittlungen darstellen.“ Bei Beachtung der Hinweise des EuGH und des BVerfG sollte auch in Deutschland eine Vorratsdatenspeicherung, die für die Kriminalitätsbekämpfung unerlässlich ist, ermöglicht werden. Es ist zu begrüßen, dass Justizminister Heiko Maas dazu einen Gesetzesvorschlag eingebracht hat. Ängste vor staatlicher Überwachung sind bedauerlicherweise weit verbreitet und werden von bestimmten Medien auch gern immer wieder angefacht. Dabei wird geflissentlich übergangen, dass ein Zugriff seitens der Sicherheitsbehörden auf Kommunikationsdaten, die zu Abrechnungszwecken gespeichert werden, schon in der Vergangenheit möglich und zulässig war, ohne dass sich irgendjemand darüber aufgeregt hat. Weitaus schlimmer ist, dass die Gegner der Vorratsdatenspeicherung in

obsessiver Weise sich selbst und anderen den Unsinn einreden, die gespeicherten Daten seien in ihrer Gesamtheit dem wahllosen und willkürlichen Zugriff der Sicherheitsbehörden ausgesetzt. In Wahrheit dient die Vorratsdatenspeicherung als notwendige präventiv-polizeiliche Maßnahme nur dazu, dass die Kommunikationsdaten nach einer angemessenen Frist schlicht und einfach noch vorhanden sind, um im konkreten Einzelfall dem Verdacht gegen eine bestimmte Person oder eine Gruppe nachzugehen.

Als drittes Beispiel will ich kurz das Urheberrecht ansprechen. Der Urheberrechtsschutz ist vorwiegend im Zivilrecht verankert. Die internationale Rechtsvereinheitlichung durch entsprechende Abkommen auf diesem Gebiet hat schon seit vielen Jahrzehnten große Fortschritte aufzuweisen. Mittlerweile werden diese zivilrechtlichen Abkommen durch sanktions- und strafrechtliche Regelungen ergänzt. Hinzuweisen ist u.a. auf die Richtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, in der die für digitale Güter relevanten Rechte des Urhebers im Hinblick auf typische Pirateriehandlungen im Internet definiert werden.

Gescheitert am breiten und gut organisierten Widerstand zahlloser Gruppen aus der Internet Community ist jedoch das Anti-Counterfeiting Trade Agreement, kurz ACTA, (zu Deutsch Anti-Produktpiraterie-Handelsabkommen), ein multilaterales Handelsabkommen auf völkerrechtlicher Ebene, mit dem die teilnehmenden Nationen bzw. Staatenbünde internationale Standards im Kampf gegen Produktpiraterie und Urheberrechtsverletzungen festlegen wollten. Obwohl das Abkommen bereits von vielen Staaten und der EU unterzeichnet worden ist, lehnte es das EU-Parlament mit großer Mehrheit am 4. Juli 2012 ab, sodass es jedenfalls in der EU nicht in Kraft treten kann. Bisher hat auch kein Einzelstaat das Abkommen ratifiziert. Inzwischen sind wohl aber einige Be-

stimmungen aus diesem Abkommen in das Comprehensive Economic and Trade Agreement, kurz CETA genannt, aufgenommen worden.
Soweit ich das ohne Prüfung der Einzelheiten beurteilen kann, ist die Kritik an dem ACTA-Abkommen in vielen Punkten durchaus berechtigt. Das Scheitern des Abkommens sollte aber nicht dazu führen, den Urheberrechtsschutz und den Schutz vor Produktpiraterie im Internet vollständig aufzugeben. Die Frage ist freilich, ob das Internet auf Grund seiner Gegebenheiten mit der Durchsetzung von Urheberrechten und dem Schutz vor Produktpiraterie noch kompatibel ist. Michael Seemann hat in einem provokativen Beitrag in SPIEGEL ONLINE die generelle Abschaffung des Urheberrechts gefordert, weil sonst die Freiheit des Internets abhanden komme. Er verweist darauf, dass das Internet in seinem innersten Kern fast ausschließlich aus Kopieroperationen besteht; hinter allem, was man im Internet tue, stehe ein Kopiervorgang, das so genannte Filesharing sei in Wirklichkeit keine spezielle Anwendung im Internet, sondern das Internet sei prinzipiell Filesharing. Man habe die Wahl zwischen freiem, d.h. weitgehend unkontrolliertem Internet, oder Urheberrecht - das freie Internet sei wichtiger, also solle man das Urheberrecht einfach abschaffen.

Spannungsfeld zwischen Freiheitsverlangen und Sicherheitsbedürfnis

Hier wird ein Dilemma erkennbar: Können wir das Entgleiten des Internet in einen rechtsfreien Raum nur dadurch verhindern, dass wir eine automatisierte Regeldurchsetzung installieren? Haben automatisierte Sanktionen bei einer Normverletzung im Internet totalitären Charakter oder sind sie eine wünschenswerte Verbesserung der Effizienz des Rechtsschutzes? Oder sind wir an dieser Stelle bei einem unauflöslichen Widerspruch zwischen dem Freiheitsanspruch im Internet auf der einen

Seite und dem Interesse des Staates an der Durchsetzung des Rechts angekommen?

Möglicherweise ist dieser Widerspruch nicht nur partieller, sondern genereller Natur. Ein Spannungsfeld zwischen Freiheitsverlangen und Sicherheitsbedürfnis, der rechtliche Regelungen erfordert, kennen wir aber nicht nur im virtuellen Cyber-Raum sondern auch in der realen Alltagswelt unseres Rechtswesens. Den Umgang mit diesem Spannungsverhältnis nennen wir Güterabwägung, die besonders schwierig wird, wenn es sich um gleichrangige Grundrechte handelt.

Das führt uns zu einem vierten Beispiel, der Wahrung des Datenschutzes im Cyber-Raum. Professor Ulrich Sieber hat in seinem hochinteressanten Gutachten zum 69. Juristentag im Jahre 2012 dazu folgendes ausgeführt: *„Die zunehmende Erfassung, Speicherung und Verknüpfung von personenbezogenen Daten führte seit den 1960er Jahren zu einer neuen rechtlichen Problemstellung der Informationsgesellschaft, die sich mit dem Aufkommen des Internets und der sozialen Dienste dramatisch verschärfte. Das Recht hat auf diese neuen Herausforderungen mit national unterschiedlichen informationsspezifischen Regelungen reagiert, die im globalen Netz mit seinen mächtigen privaten Akteuren heute allerdings nicht mehr durchsetzbar erscheinen. Das – auch in anderen Bereichen deutliche – Vollzugsdefizit des Nationalstaats wird in keinem anderen Bereich des Informationsrechts von den privaten so deutlich vorgeführt wie hier, wenn z.B. die zuständige deutsche Ministerin für den Fall der Nichteinhaltung von Datenschutzvorschriften vergeblich mit der Beendigung ihres Facebook-Accounts droht.“*

Sieber sieht zu Recht die Ursache für diese Probleme hauptsächlich in den abweichenden nationalstaatlichen Vorschriften und den diesen zugrundeliegenden unterschiedlichen Grundpositionen. Diese Grundpositionen sind wieder durch konträre massive wirtschaftliche Interessen be-

stimmt. Darauf ist zurückzuführen, dass innerhalb Europas die Harmonisierung des zivil- und verwaltungsrechtlichen Datenschutzrechtes bis zu einem gewissen Grade erreicht worden ist, während, wie Sieber schreibt, dies im Verhältnis zu den US-amerikanischen Regelungen nicht gelungen ist, die ein weitgehendes „data mining“ bei einzelnen Unternehmen zulassen und dadurch Werbeeinnahmen in Höhe von Milliardensummen ermöglichen.

Vor diesem Hintergrund ist zu verstehen, dass der Juristentag zu diesem Thema die Forderung erhoben hat, die Anwendbarkeit europäischen und nationalen Datenschutzrechts sollte nicht vom Sitz des datenverarbeitenden Unternehmens abhängen, sondern – wie im Entwurf der EU-Datenschutz-VO vorgesehen – davon, auf welche Märkte Diensteanbieter ihr Angebot ausrichten. Europäisches und nationales Datenschutzrecht soll anwendbar sein, wenn ein Angebot sich an Nutzer in europäischen Märkten wendet, unabhängig davon, ob Diensteanbieter ihren Sitz in Drittstaaten haben. Unklar bleibt dabei, ob sich eine Ausrichtung eines Angebots auf einen bestimmten Markt mit der erforderlichen Bestimmtheit überhaupt feststellen lässt.

Auffallend ist, dass das „data mining“ und darüber hinaus das „behavioral tracking“ die Internet Community kaum aufregt. Dieselben Personen, die eine nahezu paranoide Furcht vor angeblicher staatlicher Überwachung durch die Vorratsdatenspeicherung befällt, exponieren sich bedenkenlos in den so genannten sozialen Netzen wie Facebook, YouTube, Google, Twitter, LinkedIn und Xing, um nur einige zu nennen, und geben diesen Unternehmen Daten privatester Natur zum „data mining“ preis.

Für den Datenschutz im Internet bestehen ohnehin „systemische Risiken“, auf die ein andere Gutachter des Juristentages, Professor Gerald

Spindler, hinweist: „Die globale und jederzeitige Verfügbarkeit von Daten ermöglicht Verkoppelungen von isoliert harmlosen Daten, etwa Lokalisierungs- und Zahlungsdaten, zu persönlichen Profilen, so dass quasi ‚systemische Risiken' durch die Kombination von Informationen entstehen können. Aber auch Metasuchmaschinen, insbesondere Personensuchmaschinen, erlauben die Herstellung derartiger Profile und Informationen aus den verschiedensten, oftmals frei zugänglichen Quellen."

Keine Anonymität bei aktiver Nutzung des Internets

Damit sind bei einem fünften Beispiel oder Problemfeld angelangt. Wie sieht es mit dem Schutz der Persönlichkeitsrechte im Internet aus? Endet das vom Bundesverfassungsgericht entwickelte Recht auf informationelle Selbstbestimmung im Internet? Ob zu dem Recht auf informationelle Selbstbestimmung auch das Recht auf Anonymität im Internet gehört, ist strittig. Eine allumfassende, anlasslose Identifizierung der User im Internet, wie sie von manchen als „Klarnamenpflicht" gefordert wird, die die Verfolgung von Rechtsverletzungen im Einzelfall gewiss erleichtern würde, halten viele mit unseren verfassungsrechtlichen Grundsätzen für kaum vereinbar. Eine Einschränkung der Anonymität ist aber notwendig bei Rechtsverstößen, z.B. Urheberrechts- oder Markenrechtsverletzungen oder bei Angriffen gegen die Ehre und das Ansehen einer Person. Das setzt aber die Identifizierbarkeit des Täters voraus. Zuzustimmen ist daher der Feststellung des diesjährigen Juristentages, ein „Recht auf anonyme Internetnutzung" sei nicht anzuerkennen, bei aktiver Nutzung des Internets mit eigenen Beiträgen dürfe der Nutzer nicht anonym bleiben, sondern müsse im Rahmen einer Verwendung von Pseudonymen zumindest identifizierbar sein, nur dann ließen sich Rechtsverstöße wirksam verfolgen, und deshalb sollten Internetdienste den Klarnamen und die Internetverbindung ihrer Nutzer registrieren. In diesem

Zusammenhang muss allen entschieden widersprochen werden, die meinen, „der Rechtsstaat muss Internet-Pöbeleien aushalten“. Der Rechtsstaat muss sich auch im Internet bei anonymen Angriffen gegen die Ehre und die Integrität von Menschen behaupten und den Angreifer identifizieren können.

Es ist wahrlich kein Zivilisationsfortschritt, dass in unübersehbar vielen Fällen anonym die wüstesten und schamlosesten, zutiefst ehrverletzenden Beschimpfungen ins Netz gestellt werden, ohne dass deren Urheber Sanktionen befürchten müssen. Freilich gibt es keine scharfe Grenze zwischen von der Meinungsfreiheit noch gedeckter scharfer Polemik und rechtlich zu ahndender Ehrverletzung und stets wird eine Güterabwägung zwischen Meinungsäußerungsfreiheit und Persönlichkeitsschutz geboten sein. In den Rahmen dieser Güterabwägung gehört die Berücksichtigung der Tatsache, dass angesichts des nahezu unbegrenzten Verbreitungsgrades von Äußerungen im Netz die Folgen von Persönlichkeitsverletzungen besonders schwerwiegend sein können.

Gerald Spindler bezeichnet übrigens in dem bereits erwähnten Gutachten das Internet „als neuen hybriden Raum von Privatsphäre und Öffentlichkeit“ - in diesem Raum verschwimme die Grenze zwischen Individual- und Massenkommunikation, deshalb hat er in seine insgesamt 40 Thesen die Forderung aufgenommen, für das Internet als neuem Medium, das zwischen Individual- und Massenkommunikation steht, ein „Internet-Grundrecht“ im Sinne eines ähnlichen der Presse und dem Rundfunk zustehenden Institutsgrundrechts (Art. 5 Abs.1 Satz 2 GG) anzuerkennen, wobei Datenschutz und Meinungsfreiheit in eine Balance zu bringen seien. Der Juristentag hat sich jedoch dieser Forderung nicht angeschlossen und befand, ein besonderes Grundrecht „der freien Internetnutzung“ sei nicht erforderlich, vielmehr sei eine angemessene freiheitli-

che Nutzung des Internets ausreichend durch die Grundrechte in Art.5 GG und Art.10 EMRK garantiert.
In einem weiteren Beschluss beharrte der Juristentag darauf, dass die von der Rechtsprechung zum Spannungsverhältnis von Persönlichkeitsrecht und Kommunikationsrechten entwickelte Sphärentheorie (Intim-, Privat-, Sozial- und Öffentlichkeitssphäre) grundsätzlich auch auf Internetveröffentlichungen anzuwenden sei und einen flexiblen Ausgleich von Konflikten erlaube.
Welche Schlussfolgerungen können wir aus den verschiedenen Konfliktfeldern ziehen? Sind die Konflikte zwischen Usern auf der einen Seite und den staatlichen Institutionen gewissermaßen systemimmanent und vorgegeben? Oder lassen sich diese Konflikte eingrenzen und im demokratischen Diskurs auflösen? Solange wir uns einig sind, dass auch im virtuellen Cyber-Raum die rechtsstaatlichen Grundprinzipien gewahrt bleiben müssen, sollte das gelingen.

Die eigentliche Gefahr geht nicht von rechtsstaatlich kontrollierten Sicherheitsbehörden aus

Ohnehin sollte sich die Internet Community eingestehen, dass Freiheitsrechte im Internet oder durch das Internet nicht durch rechtsstaatlich kontrollierte Sicherheitsbehörden bedroht sind, sondern dass die wirklichen Bedrohungen aus anderen Richtungen stammen:

- zuallererst durch Terrorismus und organisierte Kriminalität,
- zum Zweiten durch autoritäre und totalitäre Regime und drittens
- durch die Ausübung wirtschaftlicher Übermacht.

Welche Gefahren sich auftun, wenn autoritäre und totalitäre Regimes die Kontrollhoheit über das Internet gewinnen, bedarf wohl keiner näheren Begründung. Daher wehren sich die westlichen Staaten unter der Füh-

rung der USA zu Recht dagegen, der Internationalen Telekommunikationsunion (ITU), einer UN-Organisation, in der im Wesentlichen nur Regierungen das Sagen haben, die Verantwortung für das Internet zu übertragen.

Gefahren für Rechtsstaat und Demokratie ergeben sich aber nicht zuletzt durch Konzentrationen wirtschaftlicher und politischer Macht in Gestalt der großen Internet-Konzerne wie Google, Facebook, WhatsApp u.a. Gegenüber diesen Machtzusammenballungen versagen offenkundig die Instrumente des Kartellrechts und des Steuerrechts.

Internet könnte demokratischen Dialog erschweren

Im Blick auf das spannungsreiche Verhältnis zwischen Rechtsstaat und Internet Community will ich zum Schluss noch eine grundsätzliche Frage ansprechen, die uns auf meine Eingangsbemerkungen zurückführt, in denen ich versucht habe darzustellen, dass die Konsensbildung in einer rechtsstaatlichen verfassten Gesellschaft die Anerkennung der Würde des Individuums aber zugleich voraussetzt, um in der sozialen, politischen und kulturellen Interaktion zu einem rechtlichen Einvernehmen zu gelangen. Meine Zweifel sind gewachsen, ob das Internet diese Interaktion bestärkt und nicht eher schwächt.

Francis Heylighen, ein belgischer Kybernetiker, hält das Internet und seine Nutzer für einen Superorganismus. Die „Räuber“-Parteien alias Piraten-Parteien begeistern sich für Schwarm-Intelligenz, mit der politische Entscheidungen vermeintlich optimiert werden sollen. Abgesehen davon, dass bei den Piraten die „Schwarm-Intelligenz“ nicht gerade Triumphe feiert, verfehlt diese Sichtweise, die Menschen mit dem Internet einem angeblichen Superorganismus einzuverleiben, das Wesen des Menschen in seiner dreifaltigen körperlichen, seelischen und geistigen Gestalt. Die wunderschönen Bewegungen eines Herings- oder Vogel-

schwarms sind in ihrer Eleganz sicherlich außergewöhnlich faszinierend und eines der Zeichen für die in der Tierwelt waltende ehrfurchtgebietende Weisheit. Wir Menschen haben uns aber aus einem Gruppenverband emanzipiert. Das verleiht uns die Fähigkeit zum Konsens in Freiheit. Die Gruppenentleerungen, die das Internet bisweilen in Gestalt von sogenannten Shitstorms hervorbringt, können wohl kaum als geeignete Ausdrucksform in einem demokratischen Dialog gelten.

So nutzbringend auf der einen Seite das Internet gewiss ist, so müssen wir uns auf der anderen Seite immer bewusst bleiben, dass das Internet Realität nur simuliert. Wer sich in der virtuellen Welt des Internet verirrt, verliert leicht den Boden unter den Füßen und bastelt sich eine zweite Nebenwelt (second life) zusammen, in der eine Realitätsprüfung nicht mehr stattfindet und in der sich Machtfantasien in der Seele einnisten, die die Verhaltensmuster in der realen Welt auf sehr negative Weise beeinflussen können. Das Internet kann uns zudem, wenn wir uns dagegen nicht zur Wehr setzen, seelisch-geistig in gewissem Umfang gefangen nehmen, nicht zuletzt deshalb, weil wir im Internet Adressat gewaltiger ökonomischer Interessen sind.

Roland Benedikter, Professor an der Stanford University in den USA, sieht die gesellschaftliche Entwicklung durch drei große Kulturtendenzen im Überschneidungsfeld zwischen Technologie, Medien und Kulturkonsum charakterisiert:

1. Die menschliche Aufmerksamkeit wird im Sinne einer „Aufmerksamkeitsökonomie“, des weltweit am schnellsten wachsenden Wirtschaftszweiges, zum wichtigsten Rohstoff und zur meistgehandelten Ware des 21. Jahrhunderts,
2. Die Technologie wird „nach-industriell“ und gelange damit zu einem neuen Grad gesellschaftlicher und anthropologischer Wirksamkeit, sie werde von einem Faktor gesellschaftlicher Entwicklung zu einer

allpräsenten kulturellen Grundlage, auf der alles aufbaut und die alles durchdringt, und sie erreiche in dieser Weise die Dimension eines eigenständigen, im Prinzip nicht mehr vom gesellschaftlichen Konsens abhängigen Systemfaktors.

3. Transhumanismus wird zur global leitenden Ideologie der Verbindung von Aufmerksamkeit, Technologie und Kulturkonsum.

Die Thesen Roland Benedikters korrespondieren in auffälliger Weise mit denen des russischen Wissenschaftlers Sergej Katretschko, der dem durch das Internet hervorgebrachten Cyberspace einen besonderen ontologischen Status – also Seinsqualität – zuschreibt in Form einer „virtuellen Realität“, die er in Beziehung zu einer „energetischen Realität“ setzt. Abgesehen von dem besonderen ontologischen Status der vermeintlichen „virtuellen Realität“ des Cyberspace konstatiert Katretschko eine Transformation des menschlichen Bewusstseins im Internet. Der Mensch im Cyberspace sei nicht mehr derselbe Mensch, der er in der Struktur der modernen westlichen parlamentarischen Demokratie war, so Katretschko. Das klassische Individuum der Neuzeit und der Aufklärung, das sich durch seine Rechte und Freiheiten auszeichne, verschwinde, und an seine Stelle komme das „Dividuum“, das eine Art offene multiple Persönlichkeitsstruktur darstellt. Diese Entwicklung münde schließlich in einem Übergang vom klassischen individuellen Bewusstsein zu einem überindividuellen postrationalen Gruppenbewusstsein. Was Katretschko bei seinen Betrachtungen in der Eile übersehen hat, ist die Tatsache, dass wir jedenfalls bisher eine „multiple Persönlichkeitsstruktur“ als psychische Erkrankung eingestuft haben. Dann heißt die These von Katretschko im Klartext, dass die Menschen durch den Aufenthalt in der virtuellen Cyberwelt durch „Transformation des Bewusstseins“ psychisch ernsthaft erkranken, für die in einem Rechtsstaat erforderliche Konsens-

bildung und für die Menschheitsentwicklung insgesamt eine wahrlich wenig erfreuliche Perspektive.

Der Rechtsstaat ist zur Konsensbildung und Wahrung des in der Rechtsordnung enthaltenen Konsenses schließlich auf urteilsfähige und den Grundwerten wohlgesonnene Bürgerinnen und Bürger angewiesen. Dass jedenfalls der überdosierte Aufenthalt im Cyberraum das Urteilsvermögen eher deutlich verschlechtert und die Konsensfähigkeit beschädigt, hat Manfred Spitzer in seinem Buch „Digitale Demenz“ eindrucksvoll nachgewiesen.

Technik, das ist immer wieder gesagt worden, ist nicht von vornherein gut oder böse. Es kommt darauf an, wie wir mit der Technik umgehen. Das gilt auch für das Internet, in dem wir ja z.B. expressis verbis gutartige und bösartige Bots unterscheiden. Das Internet vermittelt als Wissensportal den bequemen Zugang zu wertvollen Ressourcen. Ohne den Zugang zu Wikipedia über das Internet und durch bloßes Nachschlagen in meinem veralteten Brockhaus wäre mir die Ausarbeitung meines Vortrags erheblich schwerer gefallen. Entscheidend bleibt jedoch, dass wir als Menschen die Technik beherrschen und nicht umgekehrt die Technik die Menschen zum Herrscher über den Menschen wird. Dazu gehört auch Datensparsamkeit und „Kommunikations-Fasten“. Die digitalisierte IuK einschließlich Internet ist ohne jeden Zweifel ein großer zivilisatorischer Fortschritt, vergleichbar mit der Erfindung des Buchdrucks oder der Telefonie. Das Internet wird von freiheitsfeindlichen autoritären Regimen gefürchtet, aber es kann auch der Unterdrückung von Freiheitsbewegungen dienen.

In dieser Ambivalenz müssen wir versuchen, die richtige Orientierung zu finden.