Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Sommerakademie 2011

„Optimierte Verantwortungslosigkeit“

Eröffnungsrede

Dr. Thilo Weichert

Optimierte Verantwortungslosigkeit – Eine Einführung

Sehr geehrte Damen und Herren,

herzlich willkommen bei der Sommerakademie 2011. Als die erste Sommerakademie vor genau 17 Jahren stattfand, war sie als Forum wichtig, um einen Austausch zwischen Datenschutzbehörden, Zuständigen für den Datenschutz in Wirtschaft und Verwaltung, Wissenschaft und Öffentlichkeit zu ermöglichen. Diese Funktion hat die Sommerakademie heute noch. Doch ihre Bedeutung hat sich gewandelt. Der Austausch unter Interessierten erfolgt heute einfach über elektronische Medien; Veranstaltungen zum Datenschutz gibt es inzwischen zuhauf, die mediale Präsenz des Datenschutzes lässt seit 2008 auch nicht mehr zu wünschen übrig. Was wir aber so dringend wie je benötigen, sind Foren, in denen über den Tag hinaus der digitale Grundrechtsschutz diskutiert wird. Neudeutsch sagt man, wir brauchen weiterhin „think tanks“.

Insofern hat sich die Funktion der Sommerakademie gewandelt. Dies hat zur Folge, dass auch hinsichtlich der Form, bei allem Traditionsbewusstsein, Änderungen nötig sind. Davon gibt es dieses Jahr eine ganz Menge: Nach den Lokalitäten Landtag, Kieler Schloss und Maritim in den vorangegangenen Jahren sind wir ganz in der Nachbarschaft der ULD-Dienststelle und mitten im Herzen von Kiel im Hotel Atlantic gelandet. Sollte heute noch nicht alles organisatorisch rund laufen, so bitten wir um Nachsicht. Es ist vielleicht den vorgenommenen Änderungen zuzuschreiben. Dann haben wir uns vorgenommen, weniger zu referieren und mehr zu diskutieren. Das führt dazu, dass wir dieses Mal zweimal auf dem Podium streiten werden, morgens mit eher überregionalen Themen, nachmittags mehr im Landeskontext und zwischendrin zusätzlich in einem längeren Workshop.

Offensichtlich wurden nur wenige Menschen von der Teilnahme an der heutigen Veranstaltung dadurch abgehalten, dass wir einen (geringen) Teilnahmebeitrag erheben. Der Hintergrund ist die Erhöhung unseres Services: Statt der zu erwerbenden Essensmärkchen gibt es diesmal ein offenes Buffet, das die Mittagspause kulinarisch verfeinert; leider lässt sich dies aber finanziell nicht mehr über die Einnahmen der DATENSCHUTZAKADEMIE abdecken, die auch diesmal die Grundfinanzierung der Sommerakademie sichern. Das bedeutet nicht, dass wir nichts zu verschenken hätten, und ich hoffe, Sie bekommen davon heute wieder viel ab: Erfahrungen, Ideen, Meinungen, Anregungen und vielleicht auch ein wenig Unterhaltung in doppeltem Sinn des Wortes. Alles steht – bei allem Spaß und aller Freude am Informieren und Diskutieren – vor einem ernsten Hintergrund, nämlich die Zukunft der Informationstechnik menschengerecht gestalten zu wollen.

„Optimierte Verantwortung/slosigkeit“ – der Titel der heutigen Veranstaltung – war bzw. ist für Sie vielleicht gewöhnungsbedürftig. Unsere Visualisierung auf der Einladung trägt eventuell ein wenig zum Verständnis unseres Anliegens bei: Wichtige Werte für einen verantwortungsvollen Informationstechnikeinsatz werden weggeworfen und mit Füßen getreten, während ein Geldregen auf eine nicht näher personifizierte lachende Person niedergeht. Ähnlich wie bei der aktuellen Finanzkrise erleben wir auch beim Einsatz von Informationstechnik derzeit eine gewaltige Umverteilung: von Arm nach Reich, von unten nach oben, von öffentlich nach privat. Sicherlich hinkt mein Vergleich. Doch ist es aus meiner Sicht evident, dass starke Umgewichtungen und Veränderungen erfolgen.

Während aber in der Finanzkrise die Frage nach den Verantwortlichen und den Profiteuren diskutiert wird, scheint dies bei der IT noch kein Aufreger zu sein. Vielleicht ist die Aufregung um Rupert Murdochs Abhörskandal ein erstes Indiz, dass Profiteure und Verantwortliche und deren politisch-wirtschaftliche Seilschaften in unserer Medienwelt zum Thema des politischen Diskurses gemacht werden.

Nur am Rande sollen in der heutigen Veranstaltung die positiven Effekte der Informationstechnik auf unsere demokratische und freiheitliche Gesellschaft behandelt werden, die auf der Hand liegen und die sich fast zwangsläufig ergeben. Die Demokratisierung von Information und Kommunikation geht voran und ist ein Treibsatz für die Modernisierung der teilweise noch im Feudalsystem steckenden arabischen Welt. Enthüllungen von z. B. Wikileaks und Doktorplag-Seiten treiben auch in unseren westlichen Ländern den aufklärerischen demokratischen und freiheitlichen Diskurs voran.

Gegenstand der heutigen Diskussionen sollen vielmehr die kritischen Seiten der Entwicklung sein – nämlich die Diffusion von Verantwortung durch den Verlust unserer bisherigen analogen Sicherheiten. Unsere digitale Unsicherheit wird derzeit unter den Stichworten „Cyber Attacks“ und „Cyber Warfare“ diskutiert, also im Hinblick auf die Gefährdung unserer digitalen Infrastruktur durch fremde feindliche oder terroristische Angreifer. Diskutiert wird derzeit außerdem nach einer kritikwürdigen Äußerung des Bundesinnenministers die Frage, inwieweit Nutzende im Netz anonym oder pseudonym unterwegs sein dürfen. Dabei handelt es sich aber nur um zwei Themenbereiche auf der Basis von realen Problemlagen, die sich durch die technischen Umwälzungen ergeben. Bisher bleiben bei vielen dieser Szenarien nicht nur die Angreifer, sondern auch die Abwehrkräfte diffus. Das neue Cyber-Abwehrzentrum soll koordinieren, nicht selbst abwehren. Die bestehenden Verantwortlichkeiten für die Datensicherheit sollen nicht angetastet werden. Und diese waren und bleiben diffus.

Die von der Politik gesetzten Prioritäten bei den digitalen Bedrohungen sind offensichtlich: An erster Stelle stehen die Gefahren für die informationstechnischen Infrastrukturen, dann kommen die ökonomischen Risiken, z. B. durch digitale Wirtschaftsspionage oder durch systematische Verletzung von Urheber- und Markenrechten. Die Sensibilität für die Gefährdung unserer digitalen Grund- und Menschenrechte scheint dagegen noch wenig ausgeprägt. Deren systematische Missachtung und die informationelle Fremdbestimmung der Bevölkerung sind heute an der Tagesordnung und werden immer noch als Kavaliersdelikte behandelt: Die

Beschränkung der Meinungsfreiheit im Netz, die systematische Überwachung und die informationelle Ausbeutung der Nutzenden sind allgegenwärtig, wobei die Angreifer – wenn es sich nicht um eindeutig Kriminelle handelt – oft bekannt sind, ohne dass sie als solche genannt werden: Es sind einerseits global agierende Unternehmen und andererseits staatliche Einrichtungen. Letztere haben nicht nur ihren Sitz in Diktaturen wie China, sondern auch in den USA und potenziell bzw. latent und oft genug real auch in Europa. Die Handelnden können noch immer die Existenz der Menschenrechte im digitalen Raum leugnen und die Verantwortung für deren Verletzung zurückweisen, ohne dass sich hierüber die westeuropäische Politik ernsthaft erregen würde. Es fehlt wohl noch an der Erkenntnis, dass diese Menschenrechte grundlegend sind für die Bewahrung der freiheitlich-demokratischen Ordnung in unserer High-Tech-Informationsgesellschaft.

Dabei verfolgt z. B. die US-Regierung ein m. E. durchsichtiges Kalkül: Das Leugnen und Ignorieren informationeller Selbstbestimmung insbesondere gegenüber europäischen Bürgerinnen und Bürgern bringt politisch wie ökonomisch Nutzen: Die informationelle Ausbeutung – auch in Europa – verschafft US-Unternehmen, die sich an europäisches oder nationales Recht nicht gebunden fühlen – und damit indirekt der US-Gesamtwirtschaft – immer noch Vorteile auf dem Weltmarkt. Zugleich garantiert die Leugnung informationeller Selbstbestimmung als Menschenrecht die sicherheitspolitische Hegemonie der USA, was anschaulich bei den Abkommen mit Europa zu Fluggastdaten oder Bankdaten zur Schau gestellt wird. Der jüngste bekannt gewordene Fall ist die Inanspruchnahme des Zugriffs auf europäische Datenverarbeitungen über den US-Patriot Act, wenn Mutter- oder Tochterunternehmen ihren Sitz in den USA haben. Anscheinend haben die politisch Verantwortlichen in den USA wie auch in Europa noch nicht gemerkt, dass damit an den bürgerrechtlichen Fundamenten von unseren modernen Demokratien gerüttelt wird.

Es geht mir hier nicht um kulturellen Ethnozentrismus oder gar um Anti-Amerikanismus. Es geht mir um Entwicklung einer modernen Verantwortungsethik, die überall – auch hier in Europa und Deutschland – noch in den Kinderschuhen steckt. Ein alltägliches Beispiel unserer „homegrown“ Verantwortungslosigkeit ist die gnadenlose, immer noch ungebremste Internet- und Telefonabzocke – nicht nur, aber vorrangig bei älteren und bei technisch weniger versierten Menschen. Aus unserer Praxis als Datenschutzbehörde könnte ich ihnen zig weitere Fallbeispiele nennen.

Das Thema unserer heutigen Veranstaltung soll sein: Wer ist für was verantwortlich? Wo ist Verantwortlichkeit nötig, wo gerade nicht? Wie, mit welchen rechtlichen, organisatorischen und technischen Mitteln, kann zur Verantwortung gezogen werden?

Die äußerst konservative Antwort des früheren – zweifellos technikaffinen – Bundesinnenministers de Maizière war, die analoge Verantwortlichkeit in die digitale Welt so weit wie irgend möglich fortzuschreiben. Von seinem Nachfolger Friedrich waren noch überhaupt keine ernst zu nehmenden Initiativen zu erkennen. Anders dagegen Signale aus dem Bundesjustiz- und dem -verbraucherministerium; letzteres soll ja heute maßgeblich zu Wort kommen. Vielleicht sind wir Datenschützer zu ungeduldig, aber der Lernprozess geht uns einfach zu langsam, wie er sich z. B. in einer Bundestagsenquete oder in untauglichen Gesetzgebungsversuchen äußert: Wer

meint, die digitale Welt wäre nur eine winzige Modifikation unserer analogen Welt, der ignoriert die zentralen Eigenschaften unserer Informationstechnik: Globalität, beliebige Reproduzierbarkeit, höchstgradige Arbeitsteilung ohne geklärte Verantwortlichkeiten. Was also nicht geht, ist das „Weiter so!“

Was aber ebenso wenig geht, ist ein Ansatz, der von einer mit dem Insiderbegriff „Spackeria“ gekennzeichneten Gruppe vertreten wird: „Everything goes.“ Unter dem Deckmantel der Freiheit des Netzes und der digitalen Selbstbefriedigung wird hingenommen, dass die technisch weniger Versierten rücksichtslos ausgebeutet und entrechtet werden. Damit einher geht eine ökonomische Konzentration, wie wir sie in unserer über 150 Jahre alten kapitalistischen Marktwirtschaft noch nie erlebt haben.

Ansätze für eine informationstechnische Verantwortungsordnung gibt es schon eine ganze Menge. Auf den World Summits on the Information Society in Genf im Dezember 2003 und in Tunis im November 2005 erfolgten erste globale Diskussionen über die Relevanz von Informationstechnik, über deren Risiken und Chancen und erste Versuche einer Verständigung über den Umgang damit. Dass seitdem die globale Diskussion weniger medienwirksam gewesen ist, bedeutet nicht, dass sie nicht weitergeführt wurde. Kaum zu leugnen ist, dass die wichtigsten Impulse für diese Diskussion derzeit von Europa aus gehen. Im Kommissionspapier der EU zur Modernisierung des Datenschutzes wird erstmals der neue Begriff der „accountability“ in den Vordergrund gestellt, also letztlich die Forderung nach einem regulierten Verantwortungsmanagement. Und auch auf nationaler Ebene sind die Forderungen nach einer Modernisierung unseres IT-Rechts angesichts der Gegebenheiten des Internets nicht mehr zu ignorieren.

Lassen Sie mich im Folgenden einige Fragen aufwerfen, die bei dieser nötigen Modernisierung bearbeitet und gelöst werden müssen. Materiell-rechtlich besteht eine zentrale Herausforderung darin, zwischen Transparenz und Informationsansprüchen einerseits und Geheimhaltungs- und Vertraulichkeitsansprüchen andererseits einen technikadäquaten Ausgleich zu finden. Für mich als Datenschützer steht dabei natürlich der Ausgleich zwischen Meinungs- und Informationsfreiheit und dem Schutz der Persönlichkeitsrechte im Vordergrund, wobei die Erwägungen des Bundesverfassungsgerichts zur Schaffung einer digitalen Privatsphäre, also des Grundrechts auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme, noch viel zu kurz gekommen ist.

Prozessual stehen wir vor der Herausforderung, eine Rechtsordnung zu schaffen, die die Zuständigkeiten dorthin verlagert, wo auch die Risiken beherrscht werden können. Dabei müssen die übergriffigen Allzuständigkeitsansprüche mancher US-Behörden ebenso zurückgewiesen werden wie die Unzuständigkeitsausflüchte, wie wir sie immer noch im Umgang mit v. a. US-amerikanischen Datenverarbeitern hier in Europa erleben. Produziert Datenverarbeitung in Europa finanziellen Mehrwert und eine örtliche Beschränkung von Grundrechten, so muss auch eine europäische rechtliche Zuständigkeit gegeben sein – und wo dies noch nicht so ist, muss dies dahin geändert werden.

Ein weiteres zentrales Problem unseres IT-Rechtes besteht darin, dass angesichts der komplexen Arbeitsteilung bei IT-Anwendungen und den dadurch entstehenden Wechselbeziehungen sich alle dem entziehen können, verantwortlich gemacht zu werden. Die einfachste Fallgestaltung ist die der Auftragsdatenverarbeitung, bei der die rechtlich verantwortliche Stelle, der Auftraggeber, sich durch Outsourcing der realen Verantwortung entzieht, und der Auftragnehmer als real Verantwortlicher rechtlich so behandelt wird, als sei er nur der Schwanz, der vom Hund gewedelt wird, obwohl schon längst der Schwanz mit dem Hund wedelt.

Bei komplexeren Systemen, wie sie im E-Government und bei der kommerziellen Internet-Datenverarbeitung immer mehr verbreitet sind, muss ein neuer Rechtsbegriff eingeführt werden: der der Systemverantwortlichkeit. Es ist eine Illusion und eine rechtliche Fiktion, den Bürgermeister einer Gemeinde für die Detailgestaltung der Systeme verantwortlich zu machen, die dessen Bedienstete nutzen. Diese Verantwortung liegt heute faktisch bei koordinierenden Ministerien oder übergreifenden Dienstleistern, in Norddeutschland also z. B. bei Dataport. Insofern hat das Land Mecklenburg-Vorpommern kürzlich mit der Änderung des Landesdatenschutzgesetzes Neuland betreten. Das Land Schleswig-Holstein wird in Kürze mit seiner LDSG-Novellierung dem nacheifern.

Unser IT-Recht kennt bisher nur beschränkt eine Produzenten-, also eine Anbieter- oder Herstellerhaftung. Im Datenschutzrecht ist diese bisher völlig unbekannt. Wir im ULD versuchen diese Verantwortlichkeit über unsere Gütesiegel zumindest über den Markt positiv zur Geltung zu bringen. Damit haben wir aber nur einen ersten Schritt gemacht. Der Verantwortlichkeit für Rechtsverletzungen mit IT aus eigener Produktion sind sich die meisten Bosse der IT-Wirtschaft noch nicht ansatzweise bewusst. So wie wir hinsichtlich der Herstellung und dem Export von Kriegswaffen eine Regulierung haben, müssen auch die Hersteller und Exporteure von grundrechtsverletzenden Überwachungs- und Zensurtechnologien, z. B. in den Iran oder nach China, zur Rechenschaft gezogen werden können.

Ganz ohne Verantwortung bleibt schließlich auch das schwächste Glied in der IT-Produktionskette nicht: der Verbraucher bzw. der User. Er ist verantwortlich für eigengenerierte Inhalte und mitverantwortlich für erzeugte Verkehrsdaten oder für den Einsatz unsicherer Infrastrukturen, etwa eines offenen WLANs. Den Wenigsten ist dies bisher hinreichend klar und bewusst.

Das Gesagte soll zur Einführung in das Thema genügen. In einem Hintergrundtext zur heutigen Veranstaltung haben wir die Themen aus unserer Sicht schon weiter präzisiert. Wichtig ist in jedem Fall nicht nur eine Neudefinition von Verantwortlichkeiten, sondern auch eine neue Festlegung, wie diese Verantwortlichkeiten über staatlich regulierte Verfahren eingeklagt und umgesetzt werden können, über die Gerichtsbarkeit, über die Datenschutzaufsicht, über Sicherheits- und Strafverfolgungsbehörden, über den Verbraucherschutz, über den Markt.

Jetzt sollen aber erst Andere zu Wort kommen, unsere Gäste. Davon haben wir wieder viele eingeladen, mit Kompetenz und Prominenz. Heute Vormittag sind dies Landtagsdirektor Utz Schliesky, Abteilungsleiter Christian Grugel, Buchautor Lars Reppesgaard und Peter Fleischer, Global Privacy Council von Google. Ich wünsche Ihnen viel Spaß und eine gute erkenntnisreiche Diskussion.