Kommunikation & Recht

K&R 1/2010

Univ.-Prof. Dr. Dirk Heckmann, Passau/Friedrichshafen*

Vertrauen in virtuellen Räumen?

Rechtssichere Internetnutzung zwischen Fake und Faszinosum

Eine der ganz wesentlichen Botschaften des 4. Nationalen IT-Gipfels am 8. 12. 2009 in Stuttgart ging von Bundesinnenminister Thomas de Maizière aus: Eine freiheitliche Gesellschaft braucht freie und sichere Kommunikation im Internet. Das hierfür unabdingbare Vertrauen muss zurückgewonnen und erhalten werden. Verantwortlich dafür sind Staat, Wirtschaft und Gesellschaft gleichermaßen. Dem stimmt der Autor dieses Beitrages, selbst Mitglied der Gipfelarbeitsgruppe 9 (E-Justice), zu.

I. Einleitung

Am 29. 3. 2009 starb Maurice Jarre, der für seine Filmmusik vielfach für den Oscar nominiert wurde und ihn auch 3 Mal erhielt, u. a. für Doctor Shivago. Zu seinen weniger bekannten Werken zählt die Musik zu dem Film „Die Fälschung" nach dem gleichnamigen Roman von Nicolas Born, verfilmt 1981 von Volker Schlöndorff. Darin geht es um die Geschichte eines Kriegsreporters, der im Libanon „angesichts der Kriegsspielereien der verschiedenen Parteien, der Kulissenhaftigkeit und der gleichzeitigen Realität der Panzer und der Kriegsgreuel an der Beschreibung dieser Kriegswirklichkeit persönlich und beruflich zu scheitern meint. Es ist ein Roman über das Schreiben und über das Verhältnis von Wirklichkeit und ihrer Beschreibung"[1]. Der Regisseur Volker Schlöndorff soll dazu gesagt haben: „Es geht nicht um den Krieg, sondern um den Mann, der darüber berichten soll. Er erwartet Tod und Grauen, findet aber das Leben. Denn die Wirklichkeit ist immer anders, wenn man sie miterlebt, als wenn man nur darüber informiert wird."[2]

Dieses (Spannungs-) Verhältnis von Fiktion (oder in moderner Diktion: Fake) und Realität, insbesondere in ihrer Vermittlung durch konventionelle und neue Medien wie das Internet, hat auch eine juristische Dimension. Die Ausgangsfrage lautet: Wem oder worin kann ich vertrauen in einer zunehmend virtuellen, unbegreifbaren[3] Welt? Welche Rolle spielt hier das Recht? Wie sehr verändert das Internet die gesellschaftliche Realität, die es eigentlich nur abbilden sollte? Dieses Thema ist nicht neu. Seit Jahrzehnten befasst sich auch die Rechtswissenschaft mit Vertrauensschutz und Rechtsschein. Schon in den ersten Semestern des Jurastudiums befasst man sich etwa mit dem guten Glauben in die Richtigkeit des Grundbuchs oder mit Haftungsfragen, wenn man einen Vertrag mit einem Minderjährigen abgeschlossen hat, den man für geschäftsfähig hielt. Ganz bewusst wurde auch das Eingangsbeispiel aus dem Bereich konventioneller Medien gewählt: Krieg ist ein komplexes Geschehen, dem auch in der Realität ein Moment der Täuschung innewohnt; das ist auch für die Kriegsberichterstattung eine große Herausforderung. Welche Rolle nimmt hier der Reporter ein, der kaum eine kritische Distanz wahren kann, wenn er Teil des Geschehens ist?[4] Um noch einmal Volker Schlöndorff zu zitieren: „Wirklichkeit ist immer anders, wenn man sie miterlebt, als wenn man nur darüber informiert wird." Das Internet ist die größte Informationsquelle des jungen 21. Jahrhunderts. Im Folgenden soll an einigen Alltagsbeispielen gezeigt werden, wie das Internet das Dilemma der Ungewissheit sinnlicher Wahrnehmung verschärft, nicht zuletzt, weil sich kaum jemand der Faszination seiner Funktionen und Fähigkeiten entziehen kann.

II. Vertrauen in virtuellen Räumen: eine empirische Betrachtung

1. Vorbemerkung

Zweifellos verlagert sich zunehmend ein erheblicher Teil unserer privaten, sozialen und beruflichen Sphäre in das Internet: sei es dass wir dort Freundschaften pflegen, Einkäufe tätigen, unseren Alltag organisieren oder am öffentlichen Leben teilnehmen. Wir tun dies, weil die angebotene Technologie allerlei Vorteile verspricht: das weltweite Netz erweitert unseren sozialen Nahraum, vereinfacht den Alltag und unterstützt auf spielerische Weise die Lösung von Problemen[5]. Genannt seien beispielhaft 4 Anwendungsfelder: soziale Netzwerke (2.), Bewertungsportale (3.), Online-Shops (4.) und Verwaltungshandeln im virtuellen Raum (5.).

2. Vertrauen in sozialen Netzwerken

Der Mensch ist ein Gemeinschaftswesen. Das ist nicht nur eine banale Alltagserfahrung, sondern entspricht auch dem Menschenbild des „gemeinschaftsgebundenen Individuums", welches das BVerfG seit jeher seiner Rechtsprechung zugrunde legt[6]. Das setzt sich im Internet fort.

---

* Der Beitrag beruht auf der Antrittsvorlesung, die der Autor anläßlich seiner (nebenamtlichen) Berufung als Leiter des Center for IT-Compliance and Trust im Deutsche Telekom Institute for Connected Cities am 10. 9. 2009 an der Zeppelin University in Friedrichshafen gehalten hat. Mehr über den Autor erfahren Sie auf S. VIII.

1 So die wertende Zusammenfassung über die Romanvorlage im Online-Lexikon Wikipedia, siehe http://de.wikipedia.org/wiki/Die_Fälschung_(Roman).

2 Zitat nach Wikipedia, http://de.wikipedia.org/wiki/Die_F%C3%A4lschung#cite_note-0.

3 Den Aspekt der – buchstäblichen – (Un-)Begreifbarkeit von informationstechnischen Vorgängen betont das BVerfG in seiner Wahlcomputer-Entscheidung (Urt. v. 3. 3. 2009, K&R 2009, 255); vgl. hierzu *Heckmann*, DuD 2009, 656 ff., 659 sowie ders., jurisPR-ITR 6/2009, Anm. 2.

4 Hierzu statt Vieler *Korte/Tonn* (Hrsg.): Kriegskorrespondenten. Deutungsinstanzen in der Mediengesellschaft, 2007.

5 Die wir – zum Teil – ohne diese Technik allerdings gar nicht erst hätten.

6 „Das Menschenbild des Grundgesetzes ist nicht das eines isolierten souveränen Individuums; das Grundgesetz hat vielmehr die Spannung Indivi-

Was die Clique noch in der Jugend früherer Generationen war, ist nun der virtuelle Freundeskreis auf studiVZ, schülerVZ oder Facebook. Während man sich damals aber mit 3 Freunden und 10-20 guten Bekannten begnügte, müssen es heute schon weit mehr als 100 Freunde sein, mit denen man im sozialen Netzwerk vernetzt ist. Der Unterschied ist aber nicht nur quantitativ. Immerhin kannte man seine damaligen Freunde noch höchstpersönlich. Freundschaften, die heute im Internet gepflegt werden, sind eben buchstäblich virtuell.

Genau genommen muss man natürlich 2 Erscheinungsformen unterscheiden: Zum einen die Fortsetzung realer Freundschaften mit Hilfe der web 2.0-Funktionen des sozialen Netzwerks, zum anderen die spielerische Interaktion auf der Plattform. Im ersten Fall dient das Internet als willkommenes Medium in einer globalisierten, beschleunigten Welt, deren Bedürfnisse mit konventionellen Medien wie Briefpost, Papierdokumenten und Telefon nicht ausreichend befriedigt werden können. Der zweite Fall beschreibt das Phänomen, das schon vor einigen Jahren abschätzig als Spaßgesellschaft[7] bezeichnet wurde, im Grunde aber eine weitere Facette menschlicher Charaktere offenlegt: Es geht um Eitelkeit, Geltungsdrang oder einfach nur Zerstreuung[8].

Das Problem – auch in rechtlicher Hinsicht – ist nun, dass die an rechtlichen Anforderungen ausgestaltete Portaltechnologie nicht zwischen diesen beiden Erscheinungsformen unterscheidet. So entspricht es zwar den Anforderungen des Datenschutzes und des Schutzes von digitaler Persönlichkeit und Privatsphäre, dass jeder Nutzer beim Anlegen und Verwalten seines Nutzerkontos Einstellungen vornehmen kann, um im Rahmen informationeller Selbstbestimmung zu entscheiden, welche Daten von jedermann und welche einschränkend nur von den vernetzten Freunden wahrgenommen werden können[9]. Nur unterscheidet die Portalsoftware nicht nach Art und Hintergrund der Freundschaft. Wer per Mausklick der Kategorie „Freund" zugeordnet wird, hat Einblick in alle private Fotoalben, Profildaten wie politische Ausrichtung oder Beziehungsstatus sowie alle Einträge auf der Pinnwand. Das gilt dann für die „beste Freundin" genauso wie für flüchtige, buchstäblich virtuelle Bekanntschaften. Dies dürfte nicht allen Nutzern hinreichend deutlich sein. Es ist deshalb fraglich, ob die Freigabe solcher Daten auf der Grundlage einer ausreichenden informierten Einwilligung erfolgt.

Die Situation verschärft sich bei sog. Fake-Accounts[10]: So dürfte der Prozentsatz derer, die in den in sozialen Netzwerken angelegten Nutzerkonten nicht jene Person abbilden, die als Kontoinhaber nach außen erscheint, recht groß sein. Und nicht minder zahlreich dürften jene Nutzer sein, die den Angaben in solchen Nutzerprofilen Glauben schenken. Das liegt in der Natur der Sache. Anders als in anonymen Internetdiskussionsforen oder in Chat-Räumen steht in sozialen Netzwerken nicht die Nachricht im Vordergrund, sondern die Person. Deshalb sollte bei der Einrichtung des Nutzerkontos auch kein fiktiver Benutzername angelegt werden. Solche sozialen Netzwerke zielen auf echte personenbezogene Daten. Das ist besonders augenfällig bei Portalen wie stayfriends, deren Ziel es ist, alte Schulfreunde wieder zusammen zu bringen – sinnigerweise kann man hier nur mit den geläufigen Echtdaten suchen.

Dieses Prinzip gilt aber für studiVZ oder Facebook ganz ähnlich. Der Portalbetreiber kann nicht verhindern, dass diese Funktion missbraucht wird. Das heißt, er könnte das Risiko zwar schon minimieren, wenn er bei der Registrierung andere Authentifizierungsmechanismen einsetzen würde. Exemplarisch seien die digitale Signatur, die eID oder gar biometrische Daten genannt, wie sie über den elektronischen Personalausweis ab 2010 faktisch zur Verfügung stehen und zum Zwecke einer eindeutigen Zuordnung verwendet werden könnten[11]. Das aber widerspräche dem Geschäftsmodell des Portalbetreibers, der auf die spontane, leichthändige Preisgabe von Nutzerdaten angewiesen ist. Augenscheinlich wurden 85 Millionen Euro für studiVZ bezahlt – für eine bloße Datenbank[12].

Wie verträgt sich die dahinter stehende Geschäftsidee mit Überlegungen, die Nutzer mehr als rechtlich notwendig auf die Gefahren unüberlegter Datenpreisgabe oder nicht vertrauenswürdiger Nutzer hinzuweisen? Und was hinzukommt: Möchte der Nutzer sozialer Netzwerke überhaupt eine solche Formalisierung? Nähme permanentes Misstrauen nicht die Lust am Netzwerkeln? Man stelle sich vor, die Registrierung in sozialen Netzwerken bekäme den Charme eines Einwohnermeldeverfahrens. Grob vereinfachend kann man das Phänomen webbasierter sozialer Netzwerke mit einer Risikosportart[13] vergleichen: Die Verletzungsgefahr ist nicht ausgeschlossen, wird aber mehr oder weniger unterbunden oder verdrängt. Das ist Lifestyle.

Erste Zwischenerkenntnis:

Soziale Netzwerke stellen als hochbrisante Sammlung von Profildaten datenschutzrechtlich jegliche Volkszählung in den Schatten. Das Datenschutzrecht schützt den Einzelnen nicht vor freiwilliger Datenpreisgabe. Die Nutzung dieser vermeintlich kostenfreien Portale mit ihren komfortablen Funktionen bezahlt man mit seinen persönlichen Daten. Auf diese Weise wird unwillkürlich ein Teil der Privatsphäre auf Server mächtiger Anbieter verlagert und von dort einer unbestimmten Zahl von Nutzern zur Verfügung gestellt. Hier ist gesundes Misstrauen angebracht, weil einmal online gestellte Daten angesichts unüberschaubarer Kopien und Cash-Suchfunktionen faktisch nicht rückholbar sind. Eine interessengerechte Regulierung solcher Datenflüsse kann redlicherweise kaum vom Portalbetreiber erwartet werden, dessen Geschäftsmodell dem Grundsatz der Datensparsamkeit diametral entgegen steht. Dem Einzelnen kann deshalb nur empfohlen werden, entweder seinen sogenannten Freundeskreis oder Art und Umfang seiner Profildaten zu überdenken[14]. Das Internet vergisst nichts[15].

---

duum – Gemeinschaft im Sinne der Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person entschieden, ohne dabei deren Eigenwert anzutasten", so BVerfGE 30, 20; 45, 228.

7 Hierzu (aus sozialwissenschaftlicher Perspektive) *Gerhard Schulze*, Die Erlebnisgesellschaft. Kultursoziologie der Gegenwart, 1992.

8 Wer hat mehr Freunde? Zeigen meine Fotoalben Urlaubsmotive von den Malediven oder aus dem Bayerischen Wald? Liegt mein persönliches Profil im Trend?

9 Hierzu *Hohmann-Dennhardt*, RDV 2008, 1 ff.; Heckmann, jurisPR-ITR 1/2008, Anm. 5.

10 Zur Einrichtung eines Mitgliedskontos unter falschen Personalien bei eBay vgl. KG Beschl. v. 22. 7. 2009 – 1 Ss 181/09, m. Anm. von *Maisch/Seidl*; jurisPR-ITR 22/2009, Anm. 3. Zur Verantwortlichkeit für Benutzerkonten im Internet BGH, 11. 3. 2009 – I ZR 114/06, K&R 2009, 401 sowie *Hecht*, K&R 2009, 462 ff.

11 Hierzu *Heckmann*, DuD 2009, 656 ff.; *Roßnagel*, DÖV 2009, 301.

12 So die Zeitschrift FOCUS, vgl. http://www.focus.de/finanzen/news/studivz_aid_121976.html.

13 Zum Aspekt der Selbstgefährdung aus polizeirechtlicher Sicht vgl. *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, 6. Aufl. 2005, Rn. 401 ff.; *Heckmann*, in: Becker/Heckmann/Kempen/Manssen, Öffentliches Recht in Bayern, 4. Aufl. 2008, Teil 3 Rn. 103 ff.

14 Keine „Selbstentblößung" im Internet, vgl. ZRP 2009, 160.

15 Hierzu *Heckmann*, vorgänge 184 (2008), 20, 27 f.

3. Vertrauen in Bewertungsportalen

Ein zweites Beispiel bieten die stark verbreiteten Bewertungsportale. So wie es soziale Netzwerke für jede Zielgruppe gibt, lässt sich auch alles oder jeder bewerten: ob Hotels auf holidaycheck, lokale Dienstleister auf qype, Professoren auf meinprof oder Lehrer auf spickmich[16]. Bewertet wird jeder, der Leistungen gegenüber Dritten erbringt, die insbesondere auch deshalb ein Interesse an dieser Bewertung haben, weil sie ihre Kaufentscheidung oder die Inanspruchnahme einer Dienstleistung an der Erfahrung anderer Kunden ausrichten[17].

Auch das gab es schon in früheren Zeiten (als sogenannte Mund-Propaganda), in denen solches Kundenfeedback aber lokal und auf bestimmte Sachbereiche begrenzt blieb. Das hat sich mit dem Internet erheblich verändert. Die Mitgestaltung von Portalinhalten im web 2.0 durch sogenannten „user generated content"[18] hat generell eine Demokratisierung[19] der Netzgesellschaft zur Folge, sie wird zur Jekami-Gesellschaft: Jeder kann mitmachen. Das Geschäftsmodell geht in dieser Win-win-Situation auf und unterscheidet sich auch von den sozialen Netzwerken. Der Portalbetreiber stellt eine komfortable, für jeden Laien handhabbare Bewertungssoftware zur Verfügung, natürlich kostenlos. Seine Bemühungen werden entlohnt durch eine Vielzahl von Nutzern, die sich auf diesem Portal einfinden, um Bewertungen abzugeben oder zu lesen. Finanziert wird dies durch Werbung, die sich zielgruppenorientiert mit geringen Streuverlusten schalten lässt. Im Gegensatz zu sozialen Netzwerken erfolgt die Bewertung in anonymisierter oder zumindest pseudonymisierter Form. Im Vordergrund steht nicht die Person, sondern die Information. Das erscheint im Wesentlichen datenschutzkonform[20]. Das rechtliche Problem liegt hier an anderer Stelle, nämlich im Ehrenschutz[21]. So sinnvoll Bewertungsportale auch sein mögen – immerhin erzeugen sie Transparenz im Dienstleistungssektor und dienen letztlich der Qualitätssicherung – erscheint das zugrunde liegende Leitbild, nämlich das eines besonnenen und sachlich-distanzierten Bewerters, diskussionswürdig. Nicht selten werden Bewertungen im Kontext emotionaler Befangenheit und aus heterogenen Motiven abgegeben. Dies gilt besonders für die Bewertung von Professoren und Lehrern, bei denen es zum Rollentausch kommt, vom Prüfer zum Geprüften[22]. Was hier spickmich.de, das Portal zur Bewertung von Lehrern, betrifft, hat vor kurzem der BGH mit einem höchstrichterlich typischen „Ja, aber!" entschieden[23]: Lehrer dürfen online, auch anonym, bewertet werden, wenn bestimmte Verfahrensvorkehrungen getroffen werden. Unzulässig bleiben Schmähkritik oder gar beleidigende Äußerungen, erforderlich ist die Möglichkeit zur Gegenäußerung etc. Auch und gerade anonyme Bewertungen unterfallen der grundrechtlich gesicherten Meinungsfreiheit. Dagegen wäre nichts einzuwenden, wenn die Grenze zwischen bloßer Kritik und Schmähkritik hinreichend bestimmt wäre[24].

Hier zeigt sich ein weiteres Mal das Vertrauensdilemma[25]: Bewertungsportale erhalten ihre hohe, grundrechtssichernde Legitimität aus dem Gedanken eines erweiterten Verbraucherschutzes. Kritische, negative Bewertungen werden nicht um ihrer selbst willen abgegeben, sondern als Information künftiger Nutzer bzw. Leistungsempfänger, die ihr Verhalten im Wettbewerb unterschiedlicher Anbieter auch an solchen Erfahrungen ausrichten. Das setzt aber die Vertrauenswürdigkeit der Bewertung voraus. Woran erkennt man die Validität solcher Informationen? Nicht immer weisen plumpe Formulierungen darauf hin, dass der Bewerter böse Absichten hegt, vielleicht als Konkurrent ein Produkt schlecht macht oder als Anbieter die eigene Leistung über den grünen Klee lobt. Das geht heute viel subtiler. Mittlerweile befassen sich Agenturen schwerpunktmäßig mit täuschend echt wirkenden Fake-Bewertungen und beeinflussen so den Wettbewerb. Erst vor kurzem kam heraus, dass auch die Bahn Forenbeiträge aus PR-Zwecken gefälscht hat, um das eigene Image aufzubessern[26]. Vielleicht hätte man dieses Geld direkt in den DB-Service investieren sollen.

Zweite Zwischenerkenntnis:

Bewertungsportale gelten heute als basisdemokratisches Instrument der Leistungsbewertung und Qualitätskontrolle. Ihre Grundfunktionalität, der quasi anonyme Zugriff auf vorformulierte Bewertungskriterien, sichert die kritische Masse und gewährleistet in Über-/Unterordnungsverhältnissen Repressionsfreiheit. Grundrechtlich sind auch anonyme Bewertungen durch die Meinungsäußerungsfreiheit geschützt. Gleichwohl löst die Anonymität den Verantwortungszusammenhang und entwertet die Produkt- oder Dienstleistungsbewertung. Ohne Blick auf die Person des Bewerters und die Umstände der konkreten Bewertung bleiben Motiv und Kompetenz unklar. Für den Nutzer solcher Bewertungsportale, der diese als Entscheidungsgrundlage ansieht, stellt sich die Frage der Gewichtung solcher Informationen für die eigene Entscheidung. Als Lackmustest gilt: Ist das Risiko hinnehmbar, dass sich das zugrunde gelegte Bewertungsergebnis als nicht valide erweisen könnte? Ein gesundes Misstrauen ist angebracht. Schon die Existenz solcher Bewertungsportale mag aber eine qualitätssteigernde Warnfunktion gegenüber den Leistungserbringern begründen.

4. Vertrauen in Online-Shops

Ein drittes Anwendungsfeld bieten die Online-Shops[27]. Neben den neuen web 2.0-Portalen sind nach wie vor die klassischen Webshops im Bereich des E-Commerce eine Triebfeder der Internetentwicklung und eine wichtige Grundlage der Internetnutzung für jedermann. Was sie von sozialen Netzwerken und Bewertungsportalen unterscheidet, ist ihr expliziter rechtsgeschäftlicher Charakter. Während man bei Bewertungen anonym bleiben darf und in sozialen Netzwerken seine wahre Identität zumindest

16 Hierzu *Ballhausen/Roggenkamp*, K&R 2008, 407.
17 *Janal*, NJW 2006, 870.
18 Hierzu grundlegend *Heckmann*, in: jurisPK Internetrecht, 2. Aufl. 2009, Kap 1.7 Rn. 145 ff. (Allgemeines und Haftung); Kap. 1.11 Rn. 6 ff. (Datenschutz).
19 *Kollman/Häsel*, Web 2.0 – Trends und Technologien im Kontext der Net Economy, 2007, S. 53 ff.; für den Bereich des E-Governments dezidiert *Boehme-Neßler*, NVwZ 2001, 374, 378; *Roggenkamp*, Web 2.0 Plattformen im kommunalen E-Government, 2010, im Erscheinen.
20 Zu Einzelheiten zur Schutzbedürftigkeit persönlicher Daten von Funktionsträgern wie Lehrern siehe *Heckmann*, in: jurisPK-Internetrecht (Fn. 19), Kap. 1.7 Rn. 201 ff. m. w. N.; *ders.*, jurisPR-ITR 1/2008, Anm. 5; eher kritisch *Ladeur*, JZ 2009, 966; vgl. auch *Pfeifer/Kamp*, ZUM 2009, 185 mit dem interessanten Ansatz, die Grundsätze der Produktkritik auf personenbezogene Bewertungsplattformen wie spickmich.de zu übertragen.
21 *Heckmann*, juris PraxisReport IT-Recht 1/2008 Anm. 5; ders., juris PraxisReport IT-Recht 11/2007 Anm. 5.
22 So auch *Dix*, DuD 2006, 330.
23 BGH, 23. 6. 2009 – VI ZR 196/08, K&R 2009, 565 ff. m. Anm. *Roggenkamp*.
24 Hierzu Braun, jurisPR-ITR 11/2007 Anm. 4; *Ballhausen/Roggenkamp* K&R 2008, 407.
25 Näher *Heckmann*, vorgänge 184 (2008), 20 ff.
26 http://www.spiegel.de/wirtschaft/0,1518,627353,00.html.
27 Zu den typischen Rechtsfragen *Heckmann*, in: jurisPK-Internetrecht (Fn. 19), Kap. 4.2.

problemlos verbergen kann, ist dies im E-Commerce nur sehr bedingt möglich und sinnvoll. Für den Leistungsaustausch bedarf es zumindest gewisser Grunddaten mit hoher Verlässlichkeit, zum Beispiel die Lieferadresse oder eine Bankverbindung. Damit ist nicht gesagt, dass jeder Vertragspartner alle Daten selbst ermitteln muss, solange Leistung und Gegenleistung interessengerecht ausgetauscht werden. Das ist im realen Leben nicht anders bei Bargeschäften des täglichen Lebens, bei denen sich der Kunde im Supermarkt auch nicht identifiziert. Im Internet können Intermediäre als Zahlungsvermittler zwischengeschaltet werden und entfallen beim Download digitaler Güter auch Adressdaten. Im Regelfall werden Online-Geschäfte auf einer hinreichend sicheren Datenbasis abgewickelt. Das geschieht so erfolgreich, dass der E-Commerce zu einer bedeutenden Säule im Handel und Dienstleistungssektor avanciert ist[28].

Das Problem besteht hier darin, unter diesen durchaus bereichernden Angeboten des Wachstumsmarktes E-Commerce die schwarzen Schafe herauszufinden. Wieder geht es um Vertrauensbildung zwischen Fake und Faszinosum. Wer kennt das nicht? Man sucht einen bestimmten Gegenstand, etwa ein originelles Geschenk, und Google verweist auf ein Webangebot des bislang unbekannten Anbieters „www.XYZ.com“. Man ist fasziniert von der Produktpalette, vielleicht auch vom innovativen Webauftritt – aber kann man dieser ausländischen Firma „vertrauen? Das wäre sicher kein Problem bei Lieferung auf Rechnung mit garantiertem Rückgaberecht. Aber was ist bei Vorkasse? Schließlich weiß auch der Verkäufer nicht, ob er es mit einem zahlungsfähigen und zahlungswilligen Kunden zu tun hat.

Es ist nicht verwunderlich, dass dieses Anwendungsfeld des web 1.0 rechtlich weitaus besser durchdrungen ist als die sozialen Netzwerke und Bewertungsportale aus dem web 2.0. Das europäische und nationale Verbraucherschutzrecht fordert transparente Webshopsysteme mit klarer Anbieterkennzeichnung, begründet Informationspflichten und Widerrufsrechte[29] und verbessert inzwischen auch die grenzüberschreitende Rechtsdurchsetzung, etwa durch die small-claims-Verordnung[30] zur elektronischen Erhebung kleiner Forderungen, wie sie bei Internetgeschäften typisch sind. Ein anderes Beispiel: Kürzlich hat der Europäische Gerichtshof klar gestellt, dass man nicht automatisch Wertersatz leisten muss, wenn man eine Sache innerhalb der Widerrufsfrist nutzt[31]. Ganz praktisch bei Gegenständen, die man nur kurzfristig braucht, wie etwa online bestellten Brautkleidern. Man könnte diese Liste verlängern. Auffällig ist allemal, dass sich der Gesetzgeber beim Schutz materieller Ansprüche leichter tut als beim Datenschutz oder Ehrenschutz[32]. Das ist freilich nicht internettypisch. Auch im realen Raum hat es lange, zu lange gedauert, bis Phänomene wie Mobbing oder Stalking gesetzliche Regelungen erfahren haben.

Dritte Zwischenerkenntnis:

Der Vertrauensschutz im E-Commerce ist verhältnismäßig gut ausgeprägt. Insbesondere Fernabsatzgeschäfte zwischen Unternehmern und Verbrauchern sind gesetzlich stark reguliert; die Interessen des Kunden, nicht von dem „großen Unbekannten“ übervorteilt zu werden, werden angemessen berücksichtigt. Das gilt zumindest für klassische Konsumgüter, die das Erscheinungsbild des E-Commerce bislang prägen. Wie sich das bei neuartigen Online-Geschäften wie Beratungsdienstleistungen, Online-Spielen oder im Bereich der Telemedienarbeit gestalten wird, bleibt abzuwarten. Hier darf insbesondere das Betrugspotential[33] nicht unterschätzt werden.

5. Verwaltungshandeln im virtuellen Raum

Als letztes Anwendungsfeld soll hier der Bereich des E-Government angesprochen werden. Auch wenn die Online-Praxis deutscher Behörden weit hinter den Ankündigungen der E-Government-Projekte zurückbleibt[34] (typisches Beispiel ist die seit Jahren angekündigte elektronische Gesundheitskarte[35]), werden bereits heute zahlreiche Verwaltungsdienstleistungen webbasiert erbracht: von den mehr oder weniger aktuellen und vollständigen Informationen auf den Behördenseiten über die elektronische Kommunikation bis hin zu rechtsverbindlichen Online-Anträgen und Online-Rechtsbehelfen[36]. Und der Modernisierungsdruck auf Staat und Verwaltung wächst: Die EU-Dienstleistungsrichtlinie fordert die Schaffung einheitlicher Ansprechpartner, über die Bürger und Unternehmen in transparenten und effizienten elektronischen Verfahren alle Formalitäten zur behördlichen Behandlung einer Dienstleistungstätigkeit abwickeln können[37]. Umsetzungsfrist ist bereits der 28. 12. 2009 – wahrscheinlich wird Deutschland diese Richtlinienfrist nicht einhalten[38]. Worum es aber im vorliegenden Kontext geht:

Welches Vertrauen kann – und soll – der Bürger in die elektronische Verwaltung und in den IT-Staat setzen?[39] Hier geht es weniger um die Themen Anonymität, Legalität und Lauterkeit behördlichen Verhaltens als vielmehr um die Funktionsfähigkeit eines Verwaltungsapparates, der schon in konventionellen Verfahren nicht immer durch Effizienz glänzte und nun in komplexen IT-Strukturen vollends überfordert sein könnte. Beispielhaft genannt sei eine der Datenpannen, die es im letzten Jahr auf Platz 1 der Tagesschau geschafft haben. Es mag ein besonderer Fall gewesen sein, als tausende von Meldedaten in Schleswig-Holstein frei im Netz einsehbar waren[40]. Die Behörde

28 So ist Deutschland die „führende E-Commerce Nation“ in Europa. Im Jahr 2008 kauften private Verbraucher im Internet Waren im Wert von über 13 Milliarden Euro, was einem Plus von 19 % im Vergleich zum Jahr 2007 entspricht, vgl. *Heckmann*, in: jurisPK-Internetrecht (Fn. 19), Kap. 4.1 Rn. 1 ff. m. w. N.

29 Hierzu *Heckmann*, in: jurisPK-Internetrecht (Fn. 19), Kap 4.1 Rn. 75 ff.

30 Verordnung (EG) Nr. 861/2007 des Europäischen Parlaments und des Rates v. 12. 12. 2007 zur Einführung eines europäischen Verfahrens für geringfügige Forderungen.

31 EuGH, Urt. v. 3. 9. 2009 – C-489/07, NJW 2009, 3015; hierzu *Lapp*, jurisPR-ITR 19/2009, Anm. 2.

32 Ähnlich *Pfeifer/Kamp*, ZUM 2009, 185.

33 Hierzu allgemein *Heckmann*, in: jurisPK Internetrecht (Fn. 19), Kap. 8 Rn. 60 ff., 90 ff.

34 Das liegt nicht nur an fehlenden Angeboten, sondern auch an einer geringen Nachfrage; hierzu *Schaeff*, Wenig los im virtuellen Rathaus, Kommune 21, 12/2009, S. 12 („weniger als ein Viertel der Bürger nutzt E-Government-Angebote der öffentlichen Hand“).

35 Zum aktuellen Stand *Pitschas*, NZS 2009, 177.

36 Vgl. hierzu den Überblick von *Heckmann*, in: jurisPK-Internetrecht (Fn. 19), Kap. 5 Rn. 1 ff.

37 Siehe die Übersicht von Schmitz/Prell, NVwZ 2009, 1 ff. und die Kommentierung von *Schlachter/Ohler*, Europäische Dienstleistungsrichtline, 2008 sowie *Heckmann*, in: jurisPK-Internetrecht (Fn. 19), Kap. 5 Rn. 433 ff.

38 Bemerkenswert ist, dass sich mittlerweile innerhalb der mittelständischen IT-Wirtschaft eine Initiative gebildet hat, welche diese Entwicklungsverzögerung durch eine privatwirtschaftliche Lösung der Verwaltungsberatung abfedern könnte. Vgl. zu den Plänen zur Errichtung einer Deutschen Verwaltungsagentur, über die Bürger und Unternehmen alle elektronischen Verwaltungsdienstleistungen abwickeln können, *Heckmann*, in: jurisPK-Internetrecht (Fn. 19), Kap. 5 Rn. 35 f.

39 Hierzu detaillierter *Heckmann*, vorgänge 184 (2008), 20 ff.

40 http://www.focus.de/digital/internet/datenschutz-vertrauliche-meldedaten-im-internet_aid_313198.html; zum erforderlichen Datenschutz im Meldewesen bei Einschaltung privater IT-Dienstleister *Heckmann/Braun*, BayVBl. 2009, 581.

hatte das voreingestellte Passwort nicht geändert, die IT-Firma hatte das Musterpasswort auf ihrer Homepage veröffentlicht. Kollektiver Dilettantismus kann man das nennen – vertrauenswürdiger Umgang mit IT sieht anders aus.

Es ist in den letzten Jahren aber auch auffällig, dass Bund und Länder verstärkt neue Technologien zur Gefahrenabwehr und Kriminalitätsbekämpfung einsetzen. So erhofft man sich Fahndungserfolge durch automatisierte Kfz-Kennzeichenerfassung, Prävention durch Vorratsdatenspeicherung oder die Verhinderung terroristischer Anschläge durch Online-Durchsuchung. Die Liste ließe sich verlängern. Kein einziges dieser Gesetze war verfassungskonform[41]. Nun könnte man meinen, das läge nur daran, dass das BVerfG Freiheit und Sicherheit anders abgrenzt als die Regierungen in Bund und Ländern. Aber es geht weiter. Auch in anderen Konstellationen korrigiert Karlsruhe den IT-Einsatz. So wurde bekanntlich kürzlich der Einsatz von Wahlcomputern gestoppt, weil die bei der Bundestagswahl eingesetzte Technik Sicherheitsanforderungen nicht genügte[42]. Hier bekommt man den Eindruck, dass die Politik schlecht beraten ist, wenn es um die schlichte Frage geht, ob denn die vorgesehene Technologie überhaupt so funktioniert, wie dies zur Gesetzesanwendung erforderlich ist. Das betrifft auch das sogenannte Zugangserschwerungsgesetz[43]. Keine Frage: Die Bekämpfung des Handels mit kinderpornografischen Inhalten ist ein hehres Ziel – nur sind die politisch auserkorenen Mittel schlicht ungeeignet. Mittlerweile hat Bundespräsident Köhler – vorbehaltlich der Prüfung weiterer Stellungnahmen der Bundesregierung – die Ausfertigung des Gesetzes verweigert[44]. Dies dürfte der Bundesregierung entgegenkommen, nachdem im Koalitionsvertrag zwischen CDU, CSU und FDP ohnehin vereinbart wurde, das bereits beschlossene Gesetz ein Jahr lang nicht anzuwenden, da man stattdessen ein Vorgehen nach dem Motto „löschen statt sperren" testen wolle[45].

So medienwirksam diese Themen waren, so still und leise hielt die Informationstechnologie in Form des Art. 91 c GG Einzug ins Grundgesetz: im Zuge der Föderalismusreform II kurz vor der Sommerpause, und das von der Fachwelt und Öffentlichkeit praktisch unbemerkt[46]. Statt eines transparenten Wettbewerbs um die besten Ideen für einen kooperativen IT-Staat wurde hinter verschlossener Tür ausgehandelt, unter welchen Bedingungen die Bundesländer IT-Kompetenzen an den Bund abtreten[47]. Keine Frage: Das Ergebnis kann sich sehen lassen, die Staatsvertragslösung erscheint als tragfähige Lösung für die IT-Zusammenarbeit von Bund und Ländern.[48] Indes ist aber auch das Procedere letztlich eine Frage des Vertrauens: Wie viel Transparenz und Bürgernähe vertragen Verfassungsänderungen, wenn zugleich heterogene Länderinteressen betroffen sind?

III. Vertrauen in virtuellen Räumen: eine dogmatische Betrachtung

1. Das Recht als bedingt tauglicher Vertrauensgarant

Die Nutzung neuer Technologien und insbesondere des Internet wirft in unterschiedlicher Weise die Vertrauensfrage auf: ausgelöst durch Sorglosigkeit und Missbrauch seitens der IT-Nutzer, oder auch durch die Unbeholfenheit des Staates bei der Regulierung. Die Frage ist aber: Welche Rolle spielt hier das Recht? Kann es in unsicherer Situation unser Vertrauen stärken? Ist das nicht sogar das primäre Ziel rechtlicher Regeln? So beschrieb es der große Rechtssoziologe Niklas Luhmann[49]: „Mit Hilfe des Rechts sollen Erwartungen auf Zeit festgeschrieben und für den Fall, dass die Erwartungen nicht erfüllt werden, enttäuschungsfest gemacht werden." Diese Aussage beschreibt nicht nur die Funktion des Rechts und das Prinzip der Rechtssicherheit, sie kann auch fruchtbar gemacht werden, wenn es um das Verhältnis von Rechtssicherheit und IT-Sicherheit[50] geht. Im Prinzip ist die Entwicklungsgeschichte der Informationstechnologie eine Geschichte voller Erwartungen und Enttäuschungen. Der Einsatz von IT ist nicht selten mit der Erwartung verbunden, Arbeitsabläufe effizienter, aber auch sicherer, stabiler und damit vorhersehbar zu gestalten. Maschinen ersetzen menschliches Handeln (nicht nur, aber) auch deshalb, weil sie im Prinzip genau das tun, was man von ihnen (im Rahmen ihrer Programmierung) erwartet. Wie aber geht man mit der ernüchternden Erkenntnis um, dass besonders komplexe Netzwerktechnologien (wie das Internet und seine webbasierten Applikationen) verletzlich, angreifbar und eben unsicher sind?[51] Wie macht man IT-Unsicherheit enttäuschungsfest?

Das geht nur sehr bedingt durch rechtliche Regelungen. Denn einerseits ist das Recht im IT-Bereich regelmäßig „zu spät dran". Es soll technische Neuerungen regulieren, die es zum Zeitpunkt der Normsetzung noch nicht gibt, bzw. deren Fernwirkungen auf Gesellschaft und Umwelt noch nicht vorherzusehen sind[52]. Das Recht benötigt Erfahrung mit zu regulierenden Techniken und Prozessen, um deren Folgen (etwa Technikversagen) und damit den Regulierungsauftrag beurteilen zu können. Diese Zeit ist dem Recht bei der rasanten Technologieentwicklung häufig nicht mehr gegeben. Ist eine neue Technik reguliert, spielt sie in der Praxis häufig nur noch eine untergeordnete Rolle und ist schon im Begriff, von neuen Techniken abgelöst zu werden[53]. Insoweit gilt es schon bei der Entwicklung neuer Technologien, deren zukünftige Rechtskonformität und Vertrauenswürdigkeit – in Form einer juristischen Modellierung – sicherzustellen. Dabei sollten sich Zertifikate nicht auf konkrete Produkte beschränken. Wir brauchen vielleicht eine Art IT-Verfahrensakkreditierung.

41 BVerfG, 11. 3. 2008 – 1 BvR 2074/05, NJW 2008, 1505 (Automatisierte Erfassung von Kfz-Kennzeichen); BVerfG, 11. 3. 2008 – 1 BvR 256/08, K&R 2008, 291 (teilweise Aussetzung der Regelungen zur Vorratsdatenspeicherung), BVerfG, 27. 2. 2008 – 1 BvR 370/07, DÖV 2008, 459 (Online-Durchsuchung).

42 BVerfG, 3. 3. 2009 – 2 BvC 3/07, 2 BvC 4/07, K&R 2009, 255; hierzu *Heckmann*, jurisPR-ITR 6/2009, Anm. 2.

43 Hierzu *Heckmann*, in: jurisPK Internetrecht (Fn. 19), Kap. 8 Rn. 56 ff.; *Höhne/Dienst*, jurisPR-ITR 13/2009, Anm. 6; *Schnabel*, JZ 2009, 996.

44 http://www.faz.net/s/Rub594835B672714A1DB1A121534F010EE1/Doc~EC081605504E244BDBFBEFE0DE84E8096~ATpl~Ecommon~Scontent.html.

45 „Wachstum. Bildung. Zusammenhalt", Koalitionsvertrag zwischen CDU, CSU und FDP, 17. Legislaturperiode, S. 106.

46 Zur Entstehungsgeschichte des Art. 91 c GG vgl. auch *Schallbruch/Städler*, CR 2009, 619; *Braun/Albrecht*, jurisAnwZert-ITR 23/2009, Anm. 3; *Siegel*, NVwZ 2009, 1128 sowie umfassend *Heckmann/Braun*, Stellungnahme zur Vorbereitung der Öffentlichen Anhörung des Rechtsausschusses des Bundestages und des Finanzausschusses des Bundesrates am 4. 5. 2009.

47 Öffentliche Anhörung des Rechtsausschusses des Bundestages und des Finanzausschusses des Bundesrates am 4. 5. 2009.

48 Hierzu und zur Kritik an den Vorgängerentwürfen *Heckmann*, K&R 2009, 1 ff.

49 *Luhmann*, Das Recht der Gesellschaft, 1993, S. 124, zitiert nach *Hesse*, Einführung in die Rechtssoziologie, 2004, S. 49.

50 Hierzu ausführlich *Heckmann*, Die elektronische Verwaltung zwischen IT-Sicherheit und Rechtssicherheit, in: Hill/Schliesky, Herausforderung e-Government, 2009, S. 131 ff.

51 Dazu *Heckmann*, vorgänge 184 (2008), 20 ff.

52 Hierzu näher *Roßnagel*, Innovation als Gegenstand der Rechtswissenschaft, in: Hof/Wegenroth (Hrsg.), Innovationsforschung – Ansätze, Methoden, Grenzen und Perspektiven, 2007, S. 9, 13 ff.

53 *Roßnagel*, Innovation als Gegenstand der Rechtswissenschaft, in: Hof/Wegenroth (Hrsg.), Innovationsforschung – Ansätze, Methoden, Grenzen und Perspektiven, 2007, S. 9, 13 ff.

Das ist eine Aufgabe, die freilich nicht der Gesetzgeber leisten kann, sondern in erster Linie hoch spezialisierte IT-Juristen aus der Wissenschaft bewältigen müssen.

Zudem ist ein weiteres, viel grundlegenderes, Dilemma festzustellen: Recht ist nicht nur Vertrauensgarant, sondern bedarf als komplexes System selbst des Vertrauens[54], das es im Umgang mit hochkomplexen technischen Systemen aber in der Bevölkerung immer weniger erfährt. Geht man davon aus, dass Recht das Vertrauen stärkt, in komplexen Systemen zu agieren (nach Luhmann: „Vertrauen als Mechanismus zur Reduktion sozialer Komplexität“[55]), steht man vor dem Problem, dass (IT-)Recht selbst ein hochkomplexes System ist, das teilweise nur noch von Experten durchschaut wird. Zudem: Das Recht kann sich jederzeit ändern. Es ist korrumpierbar, teilweise unklar und Gegenstand von Kontroversen. Weil aber das Recht die Aufgabe hat, Vertrauen zu stabilisieren, wird das Vertrauen auf das Recht zu einem Problem. Das Recht hat den Auftrag, normativ unsere Zuversicht in das Funktionieren von IT-Abläufen, Leistungsversprechen und Zuständen zu stabilisieren. Hierfür muss das IT-Recht einfacher werden. Zugestanden: Komplexe Sachverhalte lassen sich nur schwerlich durch einfache Regelungen bewältigen. Zumindest in Teilen muss das Vertrauen in die (IT-) Rechtsordnung aber durch eine Reduktion normativer Komplexität gestärkt werden. Einfach ist dies aufgrund widerstreitender politischer Interessen zugegebener Maßen nicht. Auch das BVerfG trägt nicht immer zu einer Vereinfachung IT-rechtlicher Regelungsstrukturen bei, wenn es den Gesetzgeber mit regelungstechnisch kaum umsetzbaren Vorgaben konfrontiert[56].

Man sollte sich nicht zu viel vom Recht als Vertrauensgaranten versprechen. Gerade im Hinblick auf technische Innovationen ergibt sich ein Dilemma. Lässt man technologischen Innovationen freien Lauf, dann bleiben Rechtspositionen auf der Strecke, zum Beispiel: das Urheberrecht (siehe Google Books)[57], Persönlichkeitsrechte wie das Recht am eigenen Bild (Beispiel Google Street View)[58] oder auch das Datenschutzrecht in der Faszination der neuen sozialen Netzwerke[59]. Reguliert man wiederum durch präventive Gebote oder Verbote, dann würde sich manche Innovation nicht entfalten – zumindest unterbliebe auch manche Investition. Cloud Computing: Hochinnovativ, aber wahrscheinlich datenschutzrechtlich bedenklich! RFID-Tags? Früh gescheitert im Einsatz durch die Metro-Gruppe![60] Oder die Domainvergabe: Hätten sich Internetadressen so rasant verbreitet, wenn man diese statt bei einem Provider bei einer staatlichen Domainverwaltungsbehörde hätte beantragen müssen?

Gerade der Einfluss von Recht auf Innovationen im IT-Bereich, d. h. dessen hemmende und fördernde Wirkung, unterliegt noch unzureichender Steuerung. Zweifellos muss Recht nach dem geltenden marktwirtschaftlichen Grundverständnis Anreize für Innovationen setzen[61]. Doch wie? Sicherlich, indem es Freiräume für Kreativität und Initiative schafft und staatliche Nichtinterventionen garantiert, ohne Technikvertrauen in der Bevölkerung und Rechtssicherheit zu gefährden. Dieser Spagat ist indes kaum zu schaffen. Vor dem Hintergrund der auch sozialen Komplexität der Gesellschaft im 21. Jahrhundert fällt es schwer, im IT-Bereich genau zu bestimmen, wann Recht Innovationen als gerechtfertigte Schranke und wann als unnötiges Hemmnis entgegentritt. Auch typische rechtliche Steuerungsinstrumente versagen zunehmend. Ein Beispiel: Wurden Innovationen etwa durch das Urheber- und Patentrecht von der Rechtsordnung belohnt, werden nun die Belohnten durch den rechtsmissbräuchlichen Einsatz von Technik um die Früchte ihrer Arbeit gebracht (Bsp.: Filesharing)[62].

Innovationen lassen sich durch Recht grundsätzlich auch aktiv – mittels Regulierung – fördern. Im IT-Bereich freilich ist diese Art der Innovationspolitik bislang gescheitert. Marktbildung durch Administration ist zwar in vielen Lebensbereichen ein gutes Rezept: Man denke an das Umweltrecht, in dem durch gesetzgeberische Restriktionen und Förderpolitik ein Markt für Umwelttechnologieanbieter geschaffen wurde[63]. Die IT-Wirtschaft hat indes gesetzlich verordnete Techniken – man denke an die digitale Signatur – bislang nicht genutzt. Die verordnete Implementierung von Chiptechniken (elektronischer Personalausweis, Gesundheitskarte usw.) könnte zwar mehr Akzeptanz erfahren. Dennoch: Gesetzlich oktroyierte Innovationen werden sich in der IT-Landschaft regelmäßig nicht durchsetzen. Die IT-Welt, die sich (noch) durch Sachverstand, bedingungslose Kreativität, spielerisches Forschen und Programmieren, ohne Blick auf eine Marktposition des entstehenden Produkts, auszeichnet, verträgt kaum staatliche Einmischung.

2. Vertrauensbedürftigkeit elektronischer Prozesse

Ist das Recht also kaum in der Lage, technische Innovationen zu steuern und Vertrauen in virtuellen Räumen zu gewährleisten, steht die Vertrauensbedürftigkeit elektronischer Prozesse doch außer Frage. Wie groß dieser Bedarf ist, zeigt eine Aussage des Bundesbeauftragten für die Informationstechnik, Beus, wenn er formuliert[64]: „Wenn die Bürgerinnen und Bürger kein Vertrauen in die IT sowie die eGovernment- und eBusiness-Angebote haben, werden sie die Dienstleistungs- und Partizipationsangebote nicht nutzen. Für die nächste eGovernment-Generation wird dies eine der wichtigsten Herausforderungen sein: das Vertrauen der Bürgerinnen und Bürger herzustellen.“ In ähnlicher Weise erklärte Bundesinnenminister de Maizière die Vertrauensbildung zu einem Hauptthema der künftigen IT-Politik.

Wie aber stellt man dieses Vertrauen her? Dazu müssen wir zunächst die vertrauenshemmenden Ursachen ermit-

54 Ähnlich *Towfigh*, Komplexität und Normenklarheit, in: Reprints of the Max Planck Institute for Research on Collective Goods 2008/22, S. 37 ff.
55 *Luhmann*, Vertrauen, 4. Aufl. 2000.
56 Etwa was den erforderlichen Schutz des Kernbereichs privater Lebensgestaltung im Falle eines „Lauscheingriffs“ betrifft, BVerfG, 3. 3. 2004 – 1 BvR 2378/98, NJW 2004, 999; hierzu mit leichter Kritik *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, 6. Aufl. 2005, Rn. 619 ff.
57 Hierzu *Kubis*, ZUM 2006, 370; zum Google Book Settlement, *Adolphsen/Mutz*, GRUR Int 2009, 789.
58 Vgl. *Ott*, MMR 2009, 158.
59 Hierzu *Bauer*, MMR 2008, 435.
60 Die Metro Gruppe ist seit langem „Vorreiter“ beim Einsatz von RFID-Technologien (vgl. http://www.metrogroup.de/servlet/PB/menu/1155070_l1/index.htm). Hierfür wurde die Metro Gruppe bereits im Jahr 2003 mit dem Big Brother Award des FoeBuD e. V. „ausgezeichnet“ (http://www.bigbrotherawards.de/2003/.cop).
61 *Roßnagel*, Innovation als Gegenstand der Rechtswissenschaft, in: Hof/Wegenroth (Hrsg.), Innovationsforschung – Ansätze, Methoden, Grenzen und Perspektiven, 2007, S. 9 ff.
62 Allerdings werden zunehmend Stimmen laut, die eine „Neubewertung“ des geistigen Eigentums fordern, vgl. etwa *Seipenbusch*, MMR 2009, 293.
63 Hierzu *Roßnagel*, Ansätze zu einer rechtlichen Steuerung des technischen Wandels, in: Marburger (Hrsg.), Jahrbuch des Umwelt- und Technikrechts, 1994, S. 425 ff.; allgemein *Hoffmann-Riem*, Rechtswissenschaftliche Innovationsforschung als Reaktion auf gesellschaftlichen Innovationsbedarf, in: Eifert/Hoffmann-Riem (Hrsg.), Innovation und rechtliche Regulierung, 2002, S. 26 ff.
64 http://www.bmi.bund.de/SharedDocs/Interviews/DE/2009/06/interview_beus_kammer.html?nn=109590.

teln und die liegen letztlich in den Eigenschaften elektronischer Prozesse[65]: fehlende „Sichtbarkeit", „Unmerklichkeit"; Komplexität und Fernwirkungen; Fehleranfälligkeit; Manipulierbarkeit; partielle Gegenläufigkeit der Interessen. Aus alledem folgt: IT ist kaum beherrschbar, wenn überhaupt, dann von Experten, also solchen Fachleuten, für die elektronische Prozesse beruflicher und vielleicht auch privater Alltag sind. Ganz anders die vielen Nutzer. Hier ergibt sich das sog. Pilot-Passagier-Dilemma: Um von A nach B zu fliegen, genügt es, wenn man ein Ticket kaufen kann und sich notfalls beim Anschnallen helfen lässt. Niemand käme auf die Idee, wochenlang am Flugsimulator zu üben. Denn die Rollen sind verteilt: Hier der Pilot, dort der Passagier. Der einfache IT-Nutzer hat hingegen die Rolle eines Passagiers, aber die Rechte eines Piloten. Er kann mit seinem Rechner machen was er will. Das wäre auch problemlos, wenn es nur um private Briefe oder Computerspiele ginge. Es geht aber um mehr, der Internetnutzer ist quasi Teil des Netzwerkes und beeinflusst auch die IT-Sicherheit mit Folgen für Dritte. Die Schaffung von „user generated content" in web 2.0-Applikationen, die Nutzung des elektronischen Personalausweises mit seiner eID oder die Beteiligung an der elektronischen Kommunikation, z. B. mit Weiterleitung virenverseuchter E-Mails: All dies hebt die IT-Nutzung aus der Privatsphäre in den Gemeinschaftsraum Internet. Und begründet Verantwortung.

Das ist es, worum es bei der Vertrauensbedürftigkeit eigentlich geht: die IT-Kompetenz der Nutzer. IT-Systeme dürfen nicht einfach als Fernseher oder Mikrowellengeräte betrachtet werden, die man nur an- und ausstellen müsste. In globalen und vernetzten Systemen sind die Nutzer gleichsam Teil des Systems und brauchen deshalb jene Kompetenz, die ein funktionsgerechtes und nicht schädliches Agieren erfordert. Der Durchschnittsnutzer hat diese Kompetenz nicht. Sein Wissen erschöpft sich in bloßem Anwendungswissen, Zusammenhänge und Wirkungen bleiben oft im Dunkeln. Deshalb verstärken sich auch Fehleranfälligkeit und Manipulierbarkeit. Und was hinzukommt: Die IT-Anbieter haben nicht immer das Interesse, dass die Nutzer informiert und kritisch mit ihrer IT umgehen. So erfordert das Geschäftsmodell eines sozialen Netzwerks, dass die Nutzer möglichst viele Daten preisgeben. Deshalb sind die Default-Einstellungen auch oft nicht auf Datensparsamkeit ausgelegt.

Gefordert ist eine konzertierte Aktion für ein IT-Entwicklungskonzept, das „nur" 4 Eigenschaften erfüllen muss: kreativ, intelligent, verantwortungsbewusst, ideologiefrei. Erinnert sei erneut an das Zitat von Volker Schlöndorff[66]: „Denn die Wirklichkeit ist immer anders, wenn man sie miterlebt, als wenn man nur darüber informiert wird." Dies gilt auch im vorliegenden Zusammenhang: das eigene Erleben von IT, ihren Funktionen und Wirkungen. Dafür ist die eigene IT-Kompetenz der Nutzer zwingend notwendig, denn sonst sind sie abhängig von Dritten, die ihnen das erklären, was sie gerade selbst tun. Wie aber soll man dann noch unterscheiden zwischen Fake und Faszinosum?

IV. Fazit: Auf dem Weg in eine neue Vertrauenskultur (Vertrauensschutz als Magna Charta der Internetgesellschaft)

Was wir letztlich brauchen, ist eine neue Vertrauenskultur, auch und gerade auf dem Weg in einen IT-Staat mit seiner Internetgesellschaft. Zu dieser Vertrauenskultur könnte unter anderem die selbstkritische Prüfung beitragen, ob eine Technologie wirklich „reif" ist. Bananensoftware, die beim Kunden reift, gehört zumindest nicht in die staatlichen Produktpaletten. Es bedarf bei aller Rasanz der globalen IT-Entwicklung einer Entschleunigung: Qualität vor Tempo. Dann hat auch der Nutzer noch eine Chance zu lernen. Notwendig ist weiter mehr Ehrlichkeit: Der Gesetzgeber sollte sich in seinen Begründungen zur Einführung neuer Technologien nicht darauf beschränken, ein „höchstes IT-Sicherheitsniveau" zu proklamieren, sondern sich vielmehr mit Bedenken auseinandersetzen und aufzeigen, wie man mit der unvermeidbaren Unsicherheit umgeht[67]. Dazu zählt dann auch die Aufklärung über Risiken, ein „doppelter Boden" gegen Datenverlust oder der Appell zur permanenten Selbstkontrolle. Und allemal: Transparenz aller Prozesse sowie die Rekonstruktion des virtuellen Raums: vom Second Life zum First Life. Das Internet muss vergessen lernen[68]. Technische Steuerung mit menschlichem Antlitz.

V. Epilog

Als Maurice Jarre am 29. 3. 2009 starb, gab es ganz angemessen eine Vielzahl von Nachrufen in allen großen Zeitungen. Schon wenige Stunden nach der Todesnachricht erschienen die ersten Nachrufe in den Internetausgaben der großen Tageszeitungen, unter anderem im britischen Guardian oder der Washington Post. Nachdem ein Nachruf – zumal auf einen großen Künstler – selbst wie eine Kunstgattung behandelt wird, galt es natürlich, die passenden Worte zu dem Verstorbenen zu finden, etwa mit einem passenden einleitenden Zitat. Und so wurde Maurice Jarre mit den Worten zitiert: „Man könnte sagen, mein Leben ist ein einziger langer Soundtrack gewesen. Wenn ich sterbe, wird in meinem Kopf ein letzter Walzer spielen, den nur ich hören kann."

Auf dieser Grundlage ließ sich der eine oder andere sehr persönlich gehaltene Nachruf formulieren, der dann in den Printausgaben nachhaltig in die Welt gesetzt wurde. Dummerweise stammte dieses Zitat nicht von Maurice Jarre, sondern von einem irischen Studenten, der diese Sätze wenige Augenblicke zuvor dem Wikipedia-Eintrag über Jarre zugefügt hatte. Er betrachtete diesen Fake als Bestandteil seiner Soziologie-Arbeit, in der er nachweisen wollte, wie leichtgläubig selbst seriöse Journalisten auf Internetquellen vertrauen, wenn die Recherchezeit knapp bemessen ist und das Rechercheergebnis plausibel erscheint[69]. Erst als der Student einen Monat nach der Veröffentlichung dieses Experiment offen legte, reagierte die Weltpresse – wortlos, amüsiert, pikiert. Wikipedia hatte das Falschzitat übrigens aus formalen Gründen bereits am Folgetag gelöscht, da waren die Nachrufschreiber bereits mit neuen Themen befasst.

Man sieht: nicht einmal den alten Medien kann man vertrauen, weder in Kriegs- noch in Friedenszeiten, mag es um Leben oder Tod gehen. Wir alle sind aufgerufen, ab und zu etwas zu zweifeln, im wahren Leben und in virtuellen Räumen – auch wenn das bei faszinierenden Internettechnologien schwer fällt.

---

65 Näher hierzu *Heckmann*, vorgänge 184 (2008), 20 ff.

66 Zitat nach Wikipedia, http://de.wikipedia.org/wiki/Die_F%C3%A4lschung#cite_note-0.

67 Hierzu *Heckmann*, DuD 2009, 656 ff.

68 Hierzu *Ito*, Identität und Privatsphäre in einer globalisierten Gemeinschaft, http://90.146.8.18/de/archiv_files/20021/2002_252.pdf.

69 Vgl. Hierzu den Bericht von n24, http://www.n24.de/news/newsitem_5047141.html.