DAS INFORMATIONELLE SELBSTBESTIMMUNGSRECHT AUF DEM PRÜFSTAND

7 Schritte auf dem Weg zu einem zukunftsfähigen Datenschutz

Notizen für das 5. Datenschutzkolloquium der SCHUFA[*]

Berlin, 28. September 2010

von Bernd Lutterbeck[†]

[*] Diesem Papier liegt ein Essay zugrunde, der im Wettbewerb *Zwischen Liberalität und Paternalismus – Wo fördert, wo beschränkt der* Datenschutz Bürgerrechte? ausgezeichnet wurde: «Komplexe Kontexte – Einfache Regeln» (Lutterbeck 2010)

[†] Dr. iur., Prof. emeritus an der Technischen Universität Berlin

Inhalt

Living a normal American life, one cannot avoid disclosing to strangers a tremendous amount of personal information that will find its way into publicly accessible, readily searchable databases; and so one's privacy, or much of it, is blown.
Richter Robert C. Posner (2008)

1
Das ISR ist kein Naturgesetz

Das Informationelle Selbstbestimmungsrecht (ISR) ist eine Erfindung aus dem Jahr 1972[1] und kein Naturgesetz.

Es ist äußerst schwierig, solche Erfindungen in die Rechtsordnung einzupassen. Sie sind daher selten.

1983 hat das Bundesverfassungsgericht das ISR in seinem Volkszählungsurteil (BVerfGE 65, S.1 ff) zur Verfassungsdoktrin erhoben und mit einer Art neuem Grundrecht geadelt. Inzwischen ist das ISR auch von der ganz übereinstimmenden juristischen Lehre übernommen worden und Bestandteil einer ausgefeilten Grundrechtsdogmatik, an der auch der Gesetzgeber nicht vorbeikommen kann.

Namhafte Rechtswissenschaftler haben diese Doktrin in letzter Zeit heftig kritisiert (Bull 2009; Ladeur 2009). Es ist die Rede von einer «juristischen Fehlkonstruktion». Die Kritik ist berechtigt: Die Einpassung des ISR in die Rechtsordnung ist misslungen. Die ganz hM in Wissenschaft und Praxis verwechselt Naturgesetze mit Erfindungen.

Die Dampfmaschine ist gewiss eine der größten Erfindungen der Menschheit. Aber es gibt kein Gesetz, nach dem die Menschen auf alle Ewigkeit Dampfmaschinen betreiben müssen.

---

[1] An dieser Erfindung war Bernd Lutterbeck als einer der drei Hauptautoren beteiligt (Steinmüller/Lutterbeck/Mallmann 1972). Das Wort ISR findet sich erstmals auf S. 93 der Bundestags-Drucksache. Das Bundesverfassungsgericht hat dann später die Formulierung übernommen, mit der A. Podlech aus Darmstadt unsere Erfindung logisch präzisiert hat. Einzelheiten der Rezeptionsgeschichte des ISR finden sich bei Ishii/Lutterbeck/Pallas (2008, S. 10-12)
In den 40 Jahren seit unserer Erfindung habe ich es ausdrücklich vermieden, mich öffentlich bzw. wissenschaftlich zu dieser Erfindung zu äußern. 1979 habe ich eine Ausnahme gemacht: Schon damals habe ich die sich abzeichende hM für ihr aus meiner Sicht fehlerhaftes Verständnis des Datenschutzes kritisiert und ihr «gravierende Versäumnisse» vorgehalten, Näheres bei Ishii/Lutterbeck/Pallas (2008, S. 40-42)

2
There is no thing as privacy as such

Das Datenschutzgutachten von Wilhelm Steinmüller, Bernd Lutterbeck und Christoph Mallmann, eben diese «Patentschrift» von 1972, enthält eine Art wissenschaftliche Blaupause für das bis heute gültige deutsche Datenschutzkonzept. Kern dieses Konzepts ist eine auch heute noch zutreffende Einsicht: Es gibt *d i e* «Privatsphäre» nicht, sie verhält sich relativ zu den Bedürfnissen jeweiliger Menschen, aber auch relativ zu Zeit und Ort. Was A zu seiner «Privatsphäre» zählt, muss B noch lange nicht dazu zählen.

Man nehme das Beispiel Google StreetView: Mein fünfgeschossiges Wohnhaus in 12159 Berlin, Handjerystr. 17 wird durch den neuen Google-Dienst im Internet für Jedermann sichtbar. Ich finde den Dienst nützlich. Schon der Gedanke, dass StreetView meine «Privatsphäre» oder gar meine Menschenwürde verletzten könnte, scheint mir geradezu abwegig. Ich kann mir aber sehr wohl vorstellen, dass ein bis zwei von 16 Mietparteien das Ganze völlig anders sehen. Ihr denkbarer Widerspruch würde dazu führen, dass das Haus Handjerystr. 17 verpixelt wird. An ein und demselben Gegenstand könnte also sowohl ein Interesse an Offenheit wie auch Geheimhaltung bestehen. Welches Verständnis von «Privatsphäre» ist richtig bzw. legitim, welches nicht? Wie lassen sich legitime und nicht-legitime Interessen am Gleichen unterscheiden – trennscharf, wie man aus verfassungsrechtlichen Gründen fordern muss? Angenommen die 14 hätten ein «besseres», legitimes Interesse. Dürften die dann Google auf «Ent-Pixelung» verklagen? Macht die Tatsache einen Unterschied, dass andere Suchmaschinen Angebote ermöglichen, die StreetView gleichen oder gar übertreffen [zB Microsoft's Bing]?

Dieses Beispiel belegt zwei prinzipielle konzeptionelle Probleme im Umgang mit der «Privatsphäre»:

1. Es gibt nur einen einzigen Bereich, in dem die Vorstellung einer »Privatsphäre» unstreitig ist – in der deutschen wie zB der anglo-amerikanischen Rechtsordnung: «Privatheit beginnt an der verrammelten Wohnungstür, keinen Schritt früher» (Seibt 2010). Einer der führenden Rechtswissenschaftler der USA, James Whitman aus Yale, drückt den juristischen Gehalt dieser Sicht so aus: «For Americans, the right to privacy is, at its metaphoric core, a right to hide behind the walls of one's home…» (Whitman 2004, S. 1202).
   An allen sonstigen Fällen ist begriffsnotwendig die Öffentlichkeit beteiligt. Schon den Hausflur teile ich mit meinen Mitbewohnern.

2. Es ist ein herausragendes sprachliches Problem, wie man die verschiedenen Sachverhalte bezeichnen soll. Schon im Datenschutzgutachten von 1972 hatten sich die Autoren entschieden, das Wort *Privatsphäre* nur mit Anführungs-

zeichen zu benutzen. Das sollte ausdrücken: Es gibt die «Privatsphäre» nicht. Gleichzeitig ist es Tatsache, dass in unser Umgangssprache und den Reden der meisten Politiker und Wissenschaftler, damals wie heute, unverdrossen von «den Bedrohungen der Privatsphäre» die Rede ist.

«Privatsphäre» mag als Ausdruck für den journalistischen, politischen, auch wissenschaftlichen Alltagsgebrauch ausreichen. Als juristisches Konzept, das vor allem die Abgrenzung der Fallkonstellationen leisten müsste, ist es ungeeignet. Schon 1972 musste man alle von Rechtswissenschaft und Rechtspraxis entwickelten dogmatischen Ansätze als gescheitert bezeichnen. Deswegen hatten sich die Autoren entschieden, ein völlig neues Recht zu erfinden, das mit den deutschen Vorstellungen von Privatheit brach und auf keinen Fall irgendwelche sprachlichen Anklänge an «Privatsphäre» und das Persönlichkeitsrecht hatte: das Informationelle Selbstbestimmungsrecht.

Das «Ende der Privatsphäre» war also schon 1972 unabdingbare Vorraussetzung für die juristische Erfindung des Informationellen Selbstbestimmungsrechts.

Knapp 40 Jahre später findet sich unsere seinerzeitige Überschrift vom «Ende der Privatsphäre» in markanten Äußerungen führender amerikanischer Internet-Unternehmer (natürlich gibt es keinen irgendwie gearteten Zusammenhang). Scott McNealy, CEO von SUN, provoziert schon 1999 mit dem Satz «You have zero privacy anyway. Get over it». Beide Ansichten scheinen sich in einem Punkt zu gleichen: Es ist nicht wichtig und weiterführend, die mit dem Internet für die Menschen verbundenen Probleme mit dem Begriff «Privatsphäre» in Verbindung zu bringen.

Man darf diese Einsichten nicht missverstehen: Dass etwas kein Problem der «Privatsphäre» ist, heisst nicht, dass es sich nicht um ein gesellschaftliches Problem, vielleicht sogar um ein gravierendes, handelt. Das Datenschutzgutachten von 1972 ist ein Gutachten, das diese Sicht der Dinge auf einigen hundert Seiten ausbreitet. Viele Jahre später hat James Whitman diese konzeptionelle Sicht so auf den Begriff gebracht (Whitman 2004, S. 1221):

> *Of course we are all free to plead for a different kind of law—in Europe or in the United States. But pleading for privacy as such is not the way to do it. There is no such thing as privacy as such [Hervorhebung im Original]. The battle, if it is to be fought, will have to be fought over more fundamental values than that.*

Dieser letzte Satz spricht ein Grundproblem der öffentlichen, politischen und juristischen Diskussion um den Datenschutz in Deutschland an: Man streitet sich um Marginalien, nicht um die wirklich wichtigen Dinge. Die «Privatsphäre» trägt man in diesem Disput wie eine Monstranz vor sich her – sie glitzert in der Sonne, aber nicht mehr.

Die Konsequenz dieser Sicht ist bitter und scheinbar paradox für alle, die nach einfachen Lösungen suchen: Es gibt kein überzeugendes juristisches Konzept zum Schutz der «Privatsphäre», weil es die eine «Privatsphäre» schlechterdings nicht gibt.

3
Meine Daten – Deine Daten

Man stelle sich die folgende Situation vor, die sich so viele Male hier und anderswo ereignen dürfte: Jemand will einen Führerschein. Hierzu wird er eine bestimmte Menge an Daten bei der Behörde einreichen. Die muss seine Identität überprüfen und das Ergebnis irgendwo festhalten. Die Behörde wird wissen wollen, ob dieser jemand, berechtigt ist, Autos, die ja nicht ganz ungefährlich sind, zu führen und ob er seinen Führerschein ganz oder vorübergehend verloren hat, zB weil er betrunken Auto gefahren ist. Dann muss er auch noch die Gebühr bezahlen, ein Zahlungsvorgang, der bei der Behörde als auch bei den Kreditunternehmen Spuren hinterlässt. Unser Jemand sagt nun «Ich will das nicht. Ich will meinen Führerschein, ohne diese ganzen Daten von mir preiszugeben.» Wahrscheinlich würde die Behörde auf der ganzen Welt antworten «Tut uns leid. Dann eben kein Führerschein.» Fälle dieser Art sind verallgemeinerbar: Man denke an Lebensversicherungen, Bank-Kredite und Kreditkarten (SCHUFA), Arbeitsverhältnisse und all die Zertifikate in Institutionen der Ausbildung.

Ein Eremit hätte es einfach. Der braucht keinen Führerschein. Alle anderen Menschen brauchen ihn entweder selber oder sind auf andere Menschen mit Führerschein angewiesen, die sie mit den nötigen Dienstleistungen und Waren versorgen. Diesen Grundsachverhalt unseres Lebens spricht Richter Posner in dem Eingangszitat dieses Beitrags an: Die Sozialität unseres Lebens ist normal. Die Grundeinstellung, die Default-Regel, ist daher Öffentlichkeit, nicht Privatheit.

Die Menschen haben längst gelernt, mit diesem Gemisch von ganz privaten, teils privaten, teilweise öffentlichen und ganz öffentlichen Belangen umzugehen. Richter Posner hat schon 1978 zwischen «ultimativen» und eher «instrumentellen» Werten unterschieden (1978, S. 394). Es mag in Einzelfällen Werte geben, in denen Daten ganz prinzipiell als eigene schützenswert sind. In den USA mögen das Daten zB über die Nacktheit bei Frauen in ganz bestimmten Kontexten sein. Schon beim Einsatz detaillierter Kontrollen (einschließlich sog. Körperscanner) etwa an Flughäfen, legen die Menschen eine ganz nüchterne Messlatte an, indem sie Kosten und Nutzen gegeneinander abwägen. Das eigene Recht an den Daten, ein ISR, nutzt ja nichts, wenn gleichzeitig andere Menschen unter dem Schutz ihres ISR das Flugzeug in die Luft sprengen wollen: «Privacy is the terrorist‘s best friend…» (Posner 2008, S. 251). Diese differenzierte Einstellung der Menschen zum Datenschutz belegen zB Meinungsumfragen, die in den USA, Kanada und der Europäischen Union in den letzten Jahren publiziert wurden (Nachweise bei Lutterbeck 2010).

Die wie in Erz gegossene Figur des ISR verhindert einen gelassenen Umgang mit den meisten Situationen des Alltags und zwingt den Gesetzgeber in die unerbittliche Logik des ISR: Er muss Ausnahmen von der Regel definieren. Weil fast jede Situati-

on des Alltags eine solche Ausnahme darstellt, muss er Gesetz um Gesetz erlassen, um den «Herrn» der Daten in sein Recht einzusetzen. Das ISR verkommt so immer häufiger zu einem Mittel symbolischer Politik und die Bürger glauben nicht, dass sie ein «Eigentumsrecht» an ihren Daten haben, das sie in praktisch keinem Fall realisieren können. Zur Erläuterung wieder StreetView als Beispiel: In der Logik des ISR wäre der Anblick meines Hauses in Berlin, Handjerystr. 17 ein Datum, das mir gehört. Wieso kann eine Mietpartei, die das anders sieht, mein Datum zu ihrem machen? Das ginge eigentlich nur, wenn es eine Regel gibt, die den Konflikt über zwei völlig gleich geartete und gleichwertige ISR's auflöst. Eine solche Regel wird bisher von niemanden behauptet. Dann aber ist das Ergebnis «Entpixelung» willkürlich. Karl-Heinz Ladeur zieht aus all diesen Argumenten das folgende juristische Fazit:

> *In der Fassung, in der das Recht heute in der datenschutzrechtlichen Literatur verbreitet ist, hat es jede Bestimmbarkeit verloren. Es erschöpft sich in einem unberechenbaren Recht auf subjektive Willkür. Gegenstand dieser Willkür ist die Inanspruchnahme von individueller Selbstbestimmung über die soziale Wirkung von Information. Die „informationelle Selbstbestimmung" wird in einer zirkulären Wendung von jeder „Sache" abgelöst und selbst zum Schutzgut stilisiert. [Ladeur 2009, S. 49; Hervorhebungen von KHL]*

Die Kritik ist harsch, aber berechtigt. Die Entscheidung kann wie bei StreetView häufig nur willkürlich sein und richtet sich im Zweifel danach, wer gerade über die politische Mehrheit verfügt. In meinem Wettbewerbsbeitrag, der diesem Paper zugrunde liegt, habe ich diese nötige Kritik so ausgedrückt:

> *Die Daten sind dabei immer nur Mittel für den Zweck, sich kommunikativ zu verwirklichen. Datenschutz ist folglich nicht Selbstzweck, er will die Spielräume für Leben erhalten und vergrößern – aber er ist nicht das Leben selber. Deshalb ist der Trade-off, der sich empirisch für zahlreiche Kontexte nachweisen lässt, folgerichtig und rational: Mal ist der Schutz personenbezogener Daten für die Menschen besonders wichtig, mal ist er es nicht. [Lutterbeck 2010]*

Meine Kritik geht also noch einen Schritt weiter als die von Ladeur: Die im Datenschutz herrschende Meinung hat den Menschen, den sie mit dem ISR schützen will, zu Gunsten ihrer Dogmatik aus dem Blick verloren. Sie rettet sich in längst veraltete paternalistische Gestaltungskonzepte.

4
ISR – revisited

Das ISR, nimmt man es wörtlich, hat sich überholt. Seine dogmatische Umsetzung, die einer strengen juristischen Logik folgt, «…läuft darauf hinaus, allgemein über die soziale Wirkung von Informationen zu entscheiden» (Ladeur 2009, S. 50). In die immer nötige Abwägung der Interessen fließt schon immer das höherwertige Interesse der Menschen an ihrer Menschenwürde ein – mag das widerstreitende Interesse noch so wichtig, hochrangig und neuartig sein.

Das ISR ist, so wie es sich in der Praxis darstellt, nicht mehr zu retten. Der gedankliche Ansatz, mit dem dem die im Datenschutz herrschende Meinung die Probleme angeht und abarbeitet, ist widersinnig, absurd und innovationsfeindlich.

Eine Figur des Verfassungsrechts kann man nicht dadurch verändern oder verbessern, dass man sie verwirft. Möglich ist allein, sie auf ihren Wirkungskern zu reduzieren und über die Etablierung dieses Kerns die Funktionsbedingungen unter heutigen und künftigen Verhältnissen zu klären. Notwendig ist daher eine teleologische Reduktion des ISR. Ausgangspunkt muss das Datenschutzgutachten von 1972 sein, von dem das Bundesverfassungsgericht ja die Figur des ISR übernommen hat.

Das ISR war immer als juristische Erfindung konzipiert, die die Neuheit einer völlig neuen Technologie zum Gegenstand hatte – die Datenverarbeitung – und eine völlig neue Wissenschaft, die diese Technologie erklären konnte – aus damaliger Sicht die Kybernetik.

Die «Patentschrift», die [aus politischen Gründen] erst ein Jahr nach Abgabe publiziert wurde, ist nicht frei von Widersprüchen und Zeitgeistigem. Mit dem Wissen und der Erfahrung von heute lassen sich der Schrift vier zukunftsfähige Grundgedanken entnehmen:

1. Ein neues Recht darf nicht über eine Privatsphäre oder ein Persönlichkeitsrecht konzipiert werden. Deshalb lautet die auch heute noch bedeutsame Überschrift «Ende der Privatsphäre» (S. 53). Das ISR muss entsprechend aus der deutschen Tradition des Persönlichkeitsrechts herausgelöst werden.

2. Mit juristischen Methoden lässt sich über das Neue, das zu regeln ist, nichts aussagen (S. 86). Man muss also das zu findende neue Recht mit anderen als rechtswissenschaftlichen Wissensdomänen zusammen bringen. Aus heutiger Sicht wären dies vor allem die Informatik und die Institutionenökonomik.

3. Die «Patentschrift» unterstellt und akzeptiert eine Rangordnung der Probleme: Zuerst kommt die Datenverarbeitung als Mittel zur Modernisierung der Gesellschaft, der Datenschutz unterstützt diese Modernisierung, ist ihre «Kehrseite» (S. 34) und nicht Selbstzweck.

Insbesondere der dritte Punkt bereitet der Schrift Schwierigkeiten, die etwas hilflos von «Datenschutz im engeren Sinne» und «Datenschutz im weiteren Sinne» spricht (S. 44). Mit aller Vorsicht kann man diesem systematischen Argument einen weiteren Grundgedanken entnehmen:

4. Muss muss unterschiedliche Arten des Datenschutzes unterscheiden.

Unser Datenschutzgutachten ist eine Antwort auf die gewachsene Komplexität der Gesellschaft des Jahres 1971. Der Staat mit seinen Institutionen, aber auch die Wirtschaft, verfügten aus unserer Sicht nicht über die technischen Mittel, um diese Komplexität beherrschbar zu machen. Deswegen müssten all diese Institutionen verstärkt Datenverarbeitung einsetzen. Als nötige «Kehrseite» seien die Interessen der Menschen juristisch auf eine neue Stufe zu heben. Das sollte unser Datenschutz im engeren und weiteren Sinne leisten. Unser Problem war also, zugespitzt formuliert, weniger die Schwäche des Bürgers, sondern die Schwäche des Staates und anderer gesellschaftlicher Institutionen.[2] Nach der Publikation des Datenschutzgutachtens haben einige seiner Teile ein Eigenleben entfaltet, ua weil sie durch den Gesetzgeber des ersten BDSG von 1977 unmittelbar umgesetzt werden konnten. Auch die seit den siebziger Jahren anschwellende Diskussion (Stichwort Orwell und sein Großer Bruder) hat mit den Einsichten von 1971 ziemlich wenig zu tun. Der Gedanke von vorrangiger technischer Entwicklung und «Kehrseite» ist völlig verloren gegangen.

Heute kommt es darauf an, das Telos dieser «Kehrseite» neu zu bestimmen. Durch welche Muster, Instrumentarien, sowie rechtlichen, technischen und anderen Instrumente ist die Entfaltung der Menschen entsprechend ihrer Menschenwürde bestmöglich gewährleistet? Das ISR war eine ganz vernünftige Antwort für das Jahr 1971. Sein Ziel aber, die Datenverarbeitung zu fördern, ist im ganzen Ausmaß erreicht. Stattdessen ist eine Situation zu erfassen, in der durch den ubiqutitären Einsatz der IKT viele Zentren, viele Akteure, national wie international, ein zunächst unbekanntes Geschehen durch ihr kooperatives Zusammenwirken zu einem Ergebnis führen.

Man nehme als Beispiel das sog. Smart Grid. Grids sind intelligente Stromnetze, die alle Akteure des Strommarktes und die Netzes kommunikativ miteinander in Beziehung setzen – national, regional, und international. Regulierungsrahmen ist das Energie-Wirtschaftsgesetz, das «eine wirklich vollständig modellierte Abstraktion des realen Energiemarktes» enthält und eine Steigerung der Energieeffizienz durch den Einsatz von IKT beabsichtigt: Energieversorger, Automobilhersteller, Anbieter regene-

---

[2] In diese Richtung auch Posner (1978, Fn 31): «The increase in governmental surveillance and the refinement of surveillance techniques are better viewed as responses to the growth in urbanization, income, and mobility – developments that have weakened governmental control by reducing the information that government has about people: by, in short, increasing privacy».

rativer Energien und Nutzer müssen eine Lösung für ein hochgradig komplexes und deshalb im Einzelnen noch nicht verstandenes Geschehen finden.

Die Vertreter der alten Datenschutzschule müssen geradezu reflexhaft nach einem «Energiegeheimnis» rufen (so klassisch Roßnagel/Jandt 2010, S. 38) – dabei ist das Szenario, für das ein solches Geheimnis gelten könnte, noch nicht einmal in Umrissen bekannt. «Das gute alte Amtsgeheimnis» als Vorbild für den Energiemarkt der Zukunft – viele unser Nachbarn in der Europäischen Union dürften diese deutschen Überlegungen in Erstaunen versetzen.

Man kann aber auch der Auffassung sein, dass es etwas Neues gibt, das 1971 noch nicht bekannt war und versuchen, das Neue zu erfassen. Am ehesten gerecht dürfte diesem Anspruch eine kleine Forschungsgruppe am Karlsruher Institut für Technologie werden, die sich ua mit Datenschutzfragen von sog. Smart Grids beschäftigt.[3] Anders als bei den "üblichen" Vertretern der alten Datenschutzschule wird hier das paradigmatisch Neue erkannt: Entgegen der zentralen Grundannahme des "alten" Datenschutzes müssen wir heute und viel mehr noch in Zukunft von einer hochgradig dezentralen und dynamischen organisierten Datenverarbeitung ausgehen, die eben nicht mehr auf klar definierten «Systemen» geschieht. Entsprechend gibt es auch nicht das eine Instrument, die eine Regelung, notabene das Gesetz, mit der sich die Wirkungen beherrschen lassen. Dieser Befund wiederum erfordert, grundlegende Fragen vollkommen neu zu stellen. Zu deren Beantwortung wird man heute vor allem auch auf informatisches und institutionenökonomisches Wissen zurückgreifen müssen, um das Neue und die sich daraus ergebenden Implikationen für das Recht wirklich zu erfassen. Schnelle Antworten darf man von einem solchen Vorgehen nicht erwarten. Sehr wohl aber fundierte.

Umgesetzt in die heutige wissenschaftliche und sprachliche Denkwelt heisst dies: Das Telos, die «Kehrseite» ist nicht mehr das ISR. «Kehrseite» der technischen Entwicklung ist vielmehr der Kooperationsmechanismus, mit dessen Hilfe sich ein multizentristisches Geschehen bewältigen lässt. In meinem Essay behandle ich diesen Mechanismus unter dem Thema «Crowing Out-Effekt».

Im Ergebnis bleibt aber doch ein widersprüchlicher oder auch zwiespältiger Eindruck bei der Lektüre des Datenschutzgutachtens. Heute, Jahrzehnte später, ist mir klar, wo unser Fehler lag. Er lässt sich mit Hilfe meines nächstens Schrittes 5 ein wenig einkreisen: Die Rechtsvergleichung bringt ihn zu Tage.

---

[3] Forschungsgruppe Energieinformationsrecht und Neue Rechtsinformatik am Karlsruhe Institut für Technologie, http://compliance.zar.kit.edu/. Die Forschungsgruppe hat im Sommer 2010 eigene Empfehlungen zum Datenschutz im Smart Grid publiziert. Ich bedanke mich bei Herrn Dr. iur. Oliver Raabe und Dr.-Ing Frank Pallas, die sich die Zeit genommen haben, mir einige Probleme von Smart Grids in Mails zu erklären. Oliver Raabe ist Leiter der Forschungsgruppe, Frank Pallas bearbeitet dort als wissenschaftlicher Mitarbeiter Probleme im Spannungsfeld von Datenschutz und IT-Sicherheit.

5
Über den Tellerrand blicken: Die 2 Kulturen des Datenschutzes

Wenn «privacy» oder die «Privatsphäre» wirklich ein universelles Menschenrecht ist, warum gibt es dann fundamentale Unterschiede in einzelnen Rechtskulturen? Am deutlichsten sichtbar werden diese Unterschiede in den Streitigkeiten um den Datenschutz, die den transatlantischen Dialog seit Mitte der siebziger Jahre begleiten. Warum muss es zu einem jahrelangen, teilweise erbitterten Streit um Fluggastdaten oder den Umgang mit Bankdaten bei der Installierung von SWIFT kommen? Was unterscheidet die USA und Europa, speziell Deutschland natürlich? Könnten die Streitigkeiten mit den amerikanischen Unternehmen Google und Facebook ihre Ursache in einem prinzipiell unterschiedlichen Verständnis von Datenschutz haben?

«Anders als die Europäer haben die USA keine Sensilibität gegenüber dem Datenschutz, sie haben es einfach nicht verstanden», lautet eine gängige, auch von Wissenschaftlern reproduzierte Auffassung.[4] Ist diese Auffassung auch empirisch zutreffend? «Nein, das ist Quatsch [hogwash]», meint James Whitman, der die vielleicht bedeutendste rechtsvergleichende Untersuchung über den Datenschutz in Deutschland, Europa und den USA vorgelegt hat:

> *In particular, we will not do justice to our transatlantic conflicts if we begin by declaring that American privacy law has "failed" while European privacy law has "succeeded." That is hogwash. What we must acknowledge, instead, is that there are, on the two sides of the Atlantic, two different cultures of privacy, which are home to different intuitive sensibilities, and which have produced two significantly different laws of privacy. [Whitman 2004, S. 1160]*

Whitman bringt den wesentlichen Unterschied beider Kulturen schon in seiner Überschrift auf den Punkt: «Dignity versus liberty». Zwar gäbe es keine absoluten Differenzen zwischen beiden Rechtskulturen, sondern immer nur relative. Der Geist aber, aus dem sich die jeweiligen Vorstellungen speisen, sei diametral verschieden:

> *American privacy law is a body caught in the gravitational orbit of liberty values, while European law is caught in the orbit of dignity. [S. 1163]*

---

[4] Diese Sicht spiegeln auch die Kommentierungen zum BDSG: «In vielen Bereichen, etwa auch im Arbeitsrecht, weisen die USA kein Datenschutzniveau auf, das man nach unseren Maßstäben als angemessen ansehen kann», Däubler (2010) § 4b N. 15 BDSG; «Die einzelnen Regelungen [der Safe Harbour Grundsätze] sind allerdings gerade an besonders kritischen Stellen weit davon entfernt, den Ansprüchen des BDSG und der EG-Datenschutzrichtlinie zu genügen», Simitis (2006) § 4b N. 73 BDSG; zurückhaltender Gola/Schomerus (2010) § 4b N. 15 BDSG.

Kontinentale «privacy protections» sind danach Rechte, unser Bild in der Öffentlichkeit zu kontrollieren – Rechte, die garantieren, dass die anderen uns so sehen, wie wir das wünschen. Es sind «rights to one's image, name, and reputation, and what Germans call the right to informational self-determination» (S. 1161). Das ISR ist also in Whitman's Sicht ein Recht, mit dem wir Deutsche letztlich unsere Ehre verteidigen. Whitman leitet dieses Recht aus der spezifisch europäischen Geschichte des Kampfes zwischen Adel und unteren Schichten her. Ehre sei ursprünglich ein Privileg des Adels gewesen, nur dieser durfte sich – weil satisfaktionsfähig – duellieren, um seine Ehre zu verteidigen. «Privacy» sei etwas für die besseren Stände gewesen. Die aufstrebenden neuen Schichten wollten das auch haben und so den Abbau alter Hierarchien demonstrieren. Das kontinentale Recht hat dann die existierenden «privacy protections to noncelebrities and nonroyals» ausgedehnt» (S. 1170). Nicht ohne Bosheit kommentiert Whitman (S. 1171): «Continental privacy law is (…) "society" privacy for everybody.»

Die Vorstellung einer irgendwie gearteten «Ehre», die zu verteidigen ist, ist der amerikanischen Kultur fremd. Auch diese «privacy»-Kultur ist im 17. Jahrhundert entstanden und hat ein auch heute noch gelebtes Recht hervorgebracht, that «always tends to imagine the home as the primary defense, and the state as the primary enemy» (S. 1215). Notabene muss dieses amerikanische «right of privacy» umso schwächer werden, je weiter sich die betroffene Person von seinem «home» entfernt (S.1194). Dies erklärt zB, warum der Arbeitnehmerdatenschutz in den USA von allen Beteiligten als weniger wichtig angesehen wird. Dies erklärt auch, warum es Amerikanern, Wissenschaftlern ebenso wie den Durchschnittsamerikanern, geradezu abwegig erscheint, Probleme des Credit Reporting mit den entsprechenden Scorings unter dem Gesichtspunkt des Persönlichkeitsschutzes abzuhandeln. Im Kern geht es der amerikanischen Kultur immer um ihre Freiheit gegenüber dem Staat:

> *Freedom of expression is a value of constitutional magnitude in the United States, whereas the protection of personal honor is not, which means that freedom of expression almost always wins out. (Whitman 2004, S. 1196)*

Whitman geht ausführlich auf die spezifisch deutschen Vorstellungen zur Privatheit und Persönlichkeitsrechten ein:

> *German law of personality is a law of freedom—the law of the Inner Space, in which . . . [humans] develop freely and self-responsibly their personalities (Eberle (2002) zit. nach Whitman 2004, S. 1180).*
> *Where Americans often think of "freedom" as opposed primarily to tyranny, nineteenth-century Germans often thought of "freedom" as opposed primarily to determinism (Whitman 2004, S. 1181).*

In unserem Datenschutzgutachten haben wir ausführlich und eindringlich davor gewarnt, die spezifisch deutschen Vorstellungen von Persönlichkeitsrechten für das neu

zu schaffende Datenschutzrecht zu übernehmen. Wir haben das aber mit einer Rechtsfigur getan, eben dem ISR, die die von Whitman so treffend beschriebenen Vorstellungen von Ehre und deutschem «inner space» sprachlich auch noch für die neue Zeit der Datenverarbeitung weiter fortpflanzten. Das musste wohl schief gehen.[5] Zumindest hätte das Problem also eine andere sprachliche Form finden müssen, um nachhaltig erfolgreich zu sein. Ob das aber den deutschen Hang zur Dogmatisierung gebremst hätte, mag man bezweifeln.

James Whitman, der sich als Rechtsvergleicher naturgemäß auch in der deutschen juristischen Literatur recht gut auskennt, macht den Unterschied zwischen der deutschen und der amerikanischen Kultur an einem Zitat aus einem Aufsatz des Urheberrechtlers Löffler (1959, S. 1) deutlich : Es gebe, so Löffler, ein unvermeidbares Spannungsverhältnis zwischen einem Goethe – «Persönlichkeit als „höchstes Glück der Erdenkinder» – und den Vorstellungen von Präsident Thomas Jefferson, «nach dem die Pressefreiheit unverzichtbare Voraussetzung jeder freiheitlichen Staatsordnung» sei.

Das ist also ist der Unterschied: Hier Persönlichkeit und Ehre, da Freiheit. Ich vermute, dass sich die vielen Millionen Menschen, die sich zB in Facebook oder in den Suchmaschinen bewegen, längst für Jefferson entschieden haben und gegen Goethe. Dann hätte man einen weiteren Grund gefunden für die schon sichtbare Patina am deutschen Datenschutzrecht. Das müsste man aber genauer empirisch belegen.

Man kann es sehr krass auf den Punkt bringen: Die europäischen, vor allem aber deutschen Vorstellungen von «privacy» interessieren Amerikaner einfach nicht. Sie beziehen sich in amerikanischer Sicht nicht auf Werte, die für eine demokratische Gesellschaft besonders wichtig sind.

---

[5] Wir haben uns auch in einem weiteren Punkt geirrt. Wir dachten, dass es im amerikanischen Recht ein umfassendes «Right of privacy» gibt. Die Quelle, die man hier allgemein zitiert, haben wir genannt, aber nie gelesen. Der entsprechende Aufsatz von Waren und Brandeis aus dem Jahr 1890 ist die meist zitierte juristische Quelle der amerikanischen Literatur. Bis heute hält sich in der deutschen, aber auch teilweise amerikanischen Literatur die Meinung, dass die Autoren damit ein spezifisch amerikanisches Rechtsinstitut begründet hätten, das seit 1890 seinen Siegeszug um die Welt angetreten habe. Das Gegenteil ist der Fall, wie Whitman nachweist. Die beiden Autoren hätten eine europäische, vor allem deutsche, Vorstellung übernommen und teilweise abgeschrieben. In der Praxis habe ihre so häufig zitierte Sicht nie eine Bedeutung erhalten: «In fact, it is best to think of the Warren and Brandeis tort not as a great American innovation, but as an unsuccessful continental transplant» (S.1204).
Auch für die USA gibt es also einen überraschenden Befund. Das Right of privacy ist äußerst populär zumindest in der juristischen Literatur (vgl Prosser 1960), während es in der Praxis überwiegend abgelehnt wird. Ohne die Gründe wirklich zu kennen, sind die Autoren des Datenschutzgutachtens deshalb schon 1971 insoweit mehr als vorsichtig mit dem leuchtenden Vorbild USA umgegangen. Hier hatten wir, aus Versehen, recht.

6
Denkverbote auflösen!

Die Situation im deutschen Datenschutz ist verfahren. Seit mindestens 10 Jahren wird eine Modernisierung des Datenschutzes angemahnt (vgl. zB das sog. «Professoren-Gutachten» von Rossnagel/PfitzmannGarstka 2001) – vergeblich, wie man heute weiß.[6] Die durch die ubiquitäre Nutzung des Internets entstandenen Probleme lassen vielerorts eine Art Endzeitstimmung aufkommen, etwa wenn der Deutsche Anwaltsverein seine Mitglieder zu einer Fortbildung über das Thema «Ist der Datenschutz noch zu retten?» aufruft.[7] Die deutschen Datenschutzbeauftragten stehen da nicht nach: Am 18.März 2010 beschliessen sie «Eckpunkte für ein modernes Datenschutzrecht für das 21. Jahrhundert» (Konferenz der Datenschutzbeauftragten 2010), ihr Kieler Kollege Thilo Weichert prescht im August 2010 mit der Idee eines «Codex Digitalis» vor. Dieser Codex soll «den Persönlichkeitsschutz optimieren».[8]

Keiner der bekannt gewordenen Ansätze löst die hier benannten Probleme. Es ist vielleicht zu viel verlangt, von den beteiligten Akteuren in der Praxis Einsichten in die prinzipiellen, d. h. nicht behebbaren Mängel des herrschenden Datenschutzkonzepts zu erwarten. Die Wissenschaft aber hat es leichter, ua, weil sie eine überreiche amerikanische Datenschutzliteratur mit zu Rate ziehen kann. Sie sollte sich hüten, jetzt eine Grundsatzdebatte über «privacy as such», das ISR als solches, den Menschen in der digitalen Gesellschaft oder irgendeinen anderen philosophischen Disput vom Zaun zu brechen. Der Ertrag dürfte gering sein und nur weiter die Bücherregale und Festplatten füllen. Vor allem besteht die große Gefahr, dass nutzlose ideologische Debatten die Kräfte dezimieren und binden. In meinem Essay «Komplexe Kontexte – Einfache Regeln» (Lutterbeck 2010) mache ich zwei pragmatische Vorschläge, diesem Problem zu begegnen:

1. Es ist zwischen zwei, ganz unterschiedlichen, Typen von Datenschutz zu unterscheiden: einem institutionellen und einem emergenten Datenschutz.[9]

---

[6] Die in Fachkreisen übliche Kennzeichnung als «Professoren-Gutachten» gibt vielleicht einen ersten Hinweis darauf, warum das Gutachten nie irgendeine praktische Bedeutung bekommen hat. Ebenso wie bei unserem Datenschutzgutachten war auch hier der Bundesinnenminister Auftraggeber. Es hätte daher nahe gelegen, das Gutachten von 1971 im Lichte der neuen Zeit neu zu denken. Diese Herausforderung haben die Gutachter des Jahres 2001 nicht angenommen.

[7] DAV_Forum Datenschutz am 27. Oktober 2010 in Berlin

[8] https://www.datenschutzzentrum.de/presse/d20100830-sommerakademie-grundrechtsschutz.htm

[9] In meinem Essay benutze ich noch das Wort «sozialer» Datenschutz. Wegen der zu Missverständnissen aufrufenden Nähe zum «Sozialdatenschutz» habe ich den Begriff aufgegeben. Das Wort «Emergenz» bezeichnet recht gut den evolutionären Charakter dieses Typs von Datenschutz. Diesen Hinweis verdanke ich einer Mail von Hern Dr. Pallas aus Karlsruhe (vgl. Fn 3)

Dadurch lässt sich das Denkverbot, welches das ISR in der Dogmatik des Verfassungsrechts in der Praxis auslöst, geschmeidig umgehen.

2. Es ist ein «Regelungs-Set» zu definieren, das ca. 80-90% des Alltags der Informationsverarbeitung abbildet.
   Diese Regelungen müssen in Bilder oder Piktogramme umgesetzt werden, die auf eine einzige Webseite (nicht Website) passen.
   Das Regelungs-Set definiert das generische Datenschutzinstrumentarium der Zukunft: Es gilt unabhängig von den Anordnungen einzelner Rechtsordnungen.

Den Unterschied beider Datenschutz-Typen habe ich in meinem Essay so benannt:

> *Der klassische institutionelle Datenschutz kennt den Menschen nur als «Betroffener», für den sozialen [emergenten] Datenschutz sind die Menschen Subjekte, die die Wissensordnung der Zukunft bauen. Im institutionellen Datenschutz spielen Rechtsregeln die alles entscheidende Rolle, beim sozialen [emergenten] sind es soziale Normen. Die größte Herausforderung für den Datenschutz liegt in dem neuerdings so genannten «Institutionendesign», der beide Typen aufeinander beziehen muss. Datenschutz wird sich dann zu einer Disziplin über die Kooperation von Menschen in einer vernetzten Welt entwickeln.*

Es bestätigt sich also die systematische Einsicht aus dem Datenschutzgutachten von 1971 – wenn auch auf eine Weise, die ausserhalb unser damaligen Vorstellungswelt liegt. Der zweite Typ Datenschutz, von uns 1971 «Datenschutz im weiteren Sinne» genannt, ist ein Typ, der nicht auf Rechtsregeln basiert, sondern fast ausschließlich auf sozialen Normen als Regelungsmechanismus. Diese Feststellung gilt für alle modernen sozialen Netzwerke wie zB Facebook, Yahoo, Twitter etc. Diese sozialen Normen machen unter Umständen – also nicht in jedem Falle – rechtliche Regelungen entbehrlich. Die moderne Rechtstheorie, die sich in Sonderheit ökonomischer Motivationstheorien bedient, weiß, dass solche Mechanismen rechtlichen Ansätzen unter Umständen – nur unter Umständen – überlegen sind (Benkler 2010). Gleichzeitig legen diese empirisch recht gut gesicherten Einsichten eine Entlastung des klassischen institutionellen Datenschutzes nahe. Wo Menschen sich selber um ihre Belange kümmern, braucht es kein Recht. Deswegen ist der praktische Rat von Bruno Frey, einem der wichtigsten Ökonomen auf der Welt, auch für den deutschen Juristen erwägenswert:

> *Achte darauf, nicht zu sehr zu intervenieren in das, was Menschen erreichen wollen. Lass sie in Ruh´ und gib ihnen die Chance, ihre intrinsische Motivation so weit wie eben möglich an den Tag zu legen! (Frey 2008)*

Für ein endgültiges Urteil ist es vielleicht noch zu früh: Man muss mehr praktische Erfahrungen mit diesen neuen Ansätzen sammeln. Solche praktischen Einsichten kann mein zweiter Vorschlag beflügeln. Die einfachen Regeln, die zu finden sind, sind gerade nicht identisch mit dem, was die Konferenz der Datenschutzbeauftragten «Vereinfachung und bessere Lesbarkeit des Gesetzes» nennt. Streng genommen handelt es sich auch gar nicht um Recht, sondern um Regelungen, die aus den einzelnen nationalen Gesetzen aggregiert werden, gewissermaßen die Essenz des Datenschutzes. Das sind zB die Privacy Settings von Facebook. Für diesen Typ von neuen Regeln habe ich den Begriff «Generisches Recht» geprägt. Es scheint, dass dieser Begriff vor allem in der Informatik auf fruchtbaren Boden fallen könnte (vgl. meine zusammen mit anderen erstellte neue Arbeit über «Software als Institution», Orwat 2009).

Ein solches neues Set von Regelungen müsste einigermaßen zügig erstellt werden können. Das Set ist vor allem auch eine Forderung von Systementwicklern und Systemadministratoren, denn man wird nicht jeden Informatiker in ein Jurastudium schicken wollen.

Die Aufhebung der Denkverbote macht vieles leichter: Man muss sich eine (Datenschutz-)Welt ohne (Datenschutz-)Recht vorstellen können.

7
Unterschiede wahrnehmen!

Über den Begriff «Emergenter Datenschutz» muss man sicher nochmals nachdenken. Er ist aus der Not geboren, zwei verschiedene Typen von Datenschutz zu unterscheiden, die zunächst nichts miteinander zu tun haben. Datenschutz bei Facebook ist etwas ganz anderes als ein Datenschutzproblem etwa mit der SCHUFA. Irgendwie scheint es aber doch Verbindungen zwischen den beiden Typen zu geben. Diese Unklarheit muss zumindest Rechtswissenschaftler umtreiben – einerlei, in welcher Rechtskultur sie erzogen wurden. Der in Berkeley lehrende Robert Post beginnt einen Aufsatz über «Three concepts of privacy» mit einem Eingeständnis des Nicht-Wissens. Die Konzepte seien teilweise sogar inkompatibel:

> *Privacy is a value so complex, so entangled in competing and contradictionary dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefuly adressed at all.*
> *Robert Post (2001, S. 2087)*

Die Überschrift des Aufsatzes scheint mir wesentlich. Es geht um völlig unterschiedliche Konzepte, nicht um bloße Auffassungsunterschiede zum Gleichen. Mein Begriff «Emergenz», soll darauf hinweisen, dass zB in sog. sozialen Netzwerken Menschen nach gemeinsamen sozialen Normen («shared norms») kommunizieren und, wegen der Netzwerkeffekte, dadurch neue, d.h. bisher unbekannte, gemeinsame Normen herausbilden. Wie in jedem evolutionären Prozess sind diese Normen nicht voraussehbar. Es ist schwierig bis unmöglich, vielleicht sogar kontraproduktiv, diesen evolutionären Prozess etwa durch rechtliche Regeln steuern zu wollen. In diesem Konzept ist der einzelne Mensch durch seine Einbettung in soziale Normensysteme gekennzeichnet, die er notwendig mit anderen teilt. In dem anderen Konzept definiert der einzelne Mensch sich gerade unabhängig von solchen Normensystemen («privacy as freedom»). Dieses Konzept betont die Differenz zu anderen Menschen, jenes die Gemeinsamkeit.

Wenn man solche Unterschiede für nebensächlich hält oder im Bereich rechtstheoretischer Oberseminare verortet, droht Konfusion. Wenn auch der Gesetzgeber sich davon anstecken lässt, schlägt die Konfusion rasch in praktische Desaster um. Man nehme als Beispiel eine Vorschrift aus dem Entwurf eines neuen Arbeitnehmer-Datenschutzgesetzes vom August 2010:

> *§ 32 Datenerhebung vor Begründung eines Beschäftigungsverhältnisses*
> (6) *Beschäftigtendaten sind unmittelbar bei dem Beschäftigten zu erheben. Wenn der Arbeitgeber den Beschäftigten vor der Erhebung hierauf hingewiesen hat, darf der Arbeitgeber allgemein zugängliche Daten ohne Mitwirkung des Beschäftigten erheben, es sei denn, dass das schutzwürd-*

> *ige Interesse des Beschäftigten an dem Ausschluss der Erhebung das berechtigte Interesse des Arbeitgebers überwiegt. Bei Daten aus sozialen Netzwerken, die der elektronischen Kommunikation dienen, überwiegt das schutzwürdige Interesse des Beschäftigten; dies gilt nicht für soziale Netzwerke, die zur Darstellung der beruflichen Qualifikation ihrer Mitglieder bestimmt sind.*

Ich interessiere mich für die Stelle «Privacy and Intellectual Property Team Lead, User Operations», die bei Facebook am 31. August 2010 ausgeschrieben ist. Benutze ich damit ein Netzwerk, das der «*elektronischen Kommunikation dient*» oder ein Netzwerk zur «*Darstellung der beruflichen Qualifikation*»? Und sonst? Man darf mich googeln, aber nicht bei Facebook nachschauen? Was ist mit *<123people>*?[10] Wo beziehen die die Daten über mich her und all die Fotos? Lauter berufliche Details, die aber nicht aus einem Netzwerk zur «*Darstellung der beruflichen Qualifikation*» *stammen* können. Sind *<linkedin>* und *<xing>* wirklich völlig andere Typen von Netzwerken?[11]

Ist § 32 BDSG_E vielleicht nur eine *«Lex Facebook»*, mit dem der Gesetzgeber seine Handlungsfähigkeit beweisen will? Vielleicht sollte er sich einfach die Mühe machen, Marc Zuckerberg zu lesen und zu verstehen, statt ihn sofort mit dem Label *«Für den Facebook-Chef ist Privatsphäre nicht mehr zeitgemäß»* in die Ecke des Rechtsbrechers zu stellen. Zuckerberg sagt nämlich etwas ganz anderes, durchaus im Einklang nicht nur mit der amerikanischen Rechtstheorie:[12]

> *When I got started in my dorm room at Harvard, the question a lot of people asked was 'why would I want to put any information on the Internet at all? Why would I want to have a website?'*
>
> *And then in the last 5 or 6 years, blogging has taken off in a huge way and all these different services that have people sharing all this information. People have really gotten comfortable not only sharing more information*

---

[10] <http://www.123people.de/s/bernd+lutterbeck>; eine Chance, unerkannt zu bleiben, besteht wohl nur dann, wenn man pseudonym kommuniziert. So ergibt eine Recherche unter meinem Pseudonym «Herbert Narwal» null Treffer zur Person BL, <http://www.123people.de/s/herbert+narwal>

[11] Einer meiner früheren studentischen Tutoren, den ich um eine Bewertung von § 32 BDSG_E gebeten habe, schreibt mir am 1.9.2010: «Ich habe xing und Google übrigens eher als hilfreiche Werkzeuge bei der Bewerbung empfunden. Und die Sekretärin, die meine Bewerbung entgegen genommen hat, war auch im studiVZ. Man kann halbe Organigramme über die Firma der Wahl malen, wenn man die auffindbaren Daten außerhalb der Pressemitteilungen nur richtig zu verknüpfen weiß. Es gibt da eine gewisse Symmetrie...Habe ich gegen das neue BDSG verstoßen? Wie sieht es mit Arbeitgeberdatenschutz aus? ;)»

[12] heise online v.10.01.2010 14:01; die Meldung bezieht sich auf «Mike Arrington interrogates Mark Zuckerberg», Video-Interview v. 8.1.2010, http://www.ustream.tv/recorded/3848950

and different kinds, but more openly and with more people. That social norm is just something that has evolved over time.

…We view it as our role in the system to constantly be innovating and be updating what our system is to reflect what the current social norms are. [Hervorhebung BL]

Diese Behauptungen treffen ohne Zweifel zu: Wo soziale Normen evolvieren und die Interessen der Beteiligten steuern, hat «privacy» als Regulierungsansatz ausgedient. Natürlich gibt es außerhalb dieser durch Normen regulierten Bereiche noch andere Felder menschlicher Handlungen, die weiterhin von Rechtsregeln bedient werden. Der Gesetzgeber, aber auch die Datenschutzbeauftragten, müssen akzeptieren: Wo soziale Normen funktionieren, ist der Eingriff des Gesetzgebers [und der Datenschutzbeauftragten] im Zweifel kontraproduktiv (so die Kernaussage meines Essays, Lutterbeck 2010).

Die unter deutschen Datenschützern sich abzeichnende Mehrheitsmeinung müsste diese Auffassung entschieden ablehnen. Eine besonders weit reichende Forderung hat der Datenschutzbeauftragte von Schleswig-Holstein,Thilo Weichert, am 30. August 2010 erhoben (Weichert 2010):

Unsere ersten Überlegungen zum Titel der heutigen Veranstaltung waren „Codex digitalis universalis". Bei der weiteren Planung wurde uns schnell klar, dass wir zunächst kleine, nationale Brötchen backen müssen. Aber unser Anspruch und unser Ziel bleiben eindeutig, eine freiheitliche und demokratische Weltrechtsordnung zu erreichen. So wichtig es nach dem zweiten Weltkrieg war, sich im Rahmen der UNO auf *eine – analoge – Menschenrechtscharta zu einigen, so dringend ist es heute, eine universelle Grundrechtsordnung für die digitale Welt anzustreben.*

Forderungen nach einem «Weltrecht» hat es immer wieder mal gegeben, mehr als «Law in the books» ist daraus nicht geworden. Das ist gut so: Ein Weltrecht könnte als Recht nur funktionieren, wenn es die Freiheit vieler einschränkt. Eine «demokratische Weltrechtsordnung» mit einem Datenschutz nach deutschem Gusto wäre für die Mehrzahl der Menschen und Staaten eher ein Alptraum. Man kann sicher sein, dass sich zB die USA, wie in Schritt 5 ausgeführt, einem solchen Experiment nicht aussetzen werden. Denn Datenschutz ist nach überwiegender Meinung kein universelles Menschenrecht. Sollen deutsche Datenschützer vorgeben, welche Demokratie gut ist und welche nicht? Deutschland als Datenschutz-Sheriff für den Rest der Welt? Nein, dieser Weg ist falsch, völlig falsch. Fürs Erste reicht es völlig aus, wenn die deutschen Datenschützer ihre Bemühungen vom Geruch der «Willkür» (Ladeur) befreien.

8
Der nächste Schritt:
Einfache Regeln zu Bildern machen!

In meinem Essay habe ich den Typ von Regelungen so umschrieben:

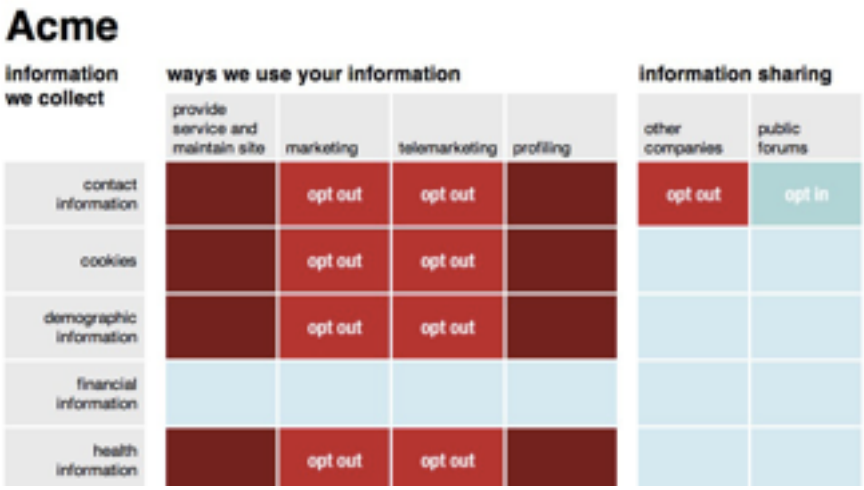
> *Je einfacher die Regeln, umso größer die Wahrscheinlichkeit, dass man sie ernst nimmt. Deshalb hat sich ein neuer Typ von Regelungen herausgebildet, den ich «generisches Recht» genannt habe. Vorbild sind «Creative Commons (CC)-Lizenzen», die es Millionen von Menschen in der ganzen Welt ermöglichen, ihre Urheberrechte im Netz wahrzunehmen – unabhängig von den Anordnungen jeweiliger nationaler Rechtsordnungen. Ein anderes Beispiel sind die «Privacy Settings» von Facebook. Die «Settings» sind so etwas wie die Essenz des Datenschutzes. Denn die Regelungen, die durch Software eingestellt werden, müssen ja für Menschen in unterschiedlichen Jurisdiktionen gelten und vor allem verständlich sein. Am Besten, sie passen – ohne Scrollen und durch Graphiken selbsterklärend – übersichtlich auf eine einzige Webseite. So wird der einzelne Mensch zum Regulator seiner Verhältnisse. Er verwendet wie selbstverständlich «CC-Lizenzen», ohne je eine Stunde Urheberrecht gehört zu haben und im Zweifel ohne Kenntnis seines nationalen Rechts. Dass erst politischer und sozialer Druck zu diesen neuen «Settings» geführt hat, zeigt, dass der Staat und seine Datenschutzbeauftragten im digitalen Zeitalter mitnichten entbehrlich sin*

Diese CC-Lizenzen haben es geschafft, die hoch komplizierte Materie des Urheberrechts auf die überschaubare Menge von vier Elementen zu reduzieren. Aufgrund ihrer einsichtigen Piktogramme werden sie inzwischen auf der ganzen Welt als – generisches – Urheberrecht akzeptiert:

License Conditions, creativecommons.org

Im März 2010, als ich meinen Essay eingereicht habe, war diese Überlegung vielleicht noch neu. Fast gleichzeitig hat die internationale Fachgemeinschaft gleichartige, schon viel praktischere, Vorschläge veröffentlicht (zB Raskin 2010 für die Mozilla Foundation). Zwei Denkansätze setzen diese Regulierungsidee des Essays schon recht gut um:

- Der Nutrition Label Approach von Kelley/Cesca/Bresee/Cranor (2010), der an der Carnegie Mellon University entwickelt wurde:



Vorbild für den Regelset sind hier Label, die auf diversen Verpackungen, aber auch zB Kühlschränken eine verlässliche und klare Botschaft für den Verbraucher enthalten.

- Privacy Rulesets von Cooper/Morris/Newland (2010), die für die Bürgerrechtsorganisation «Center for Democracy & Technology» entwickelt wurden:[13]

SHARING				SECONDARY USE			RETENTION		
Internal	Affiliates	Unrelated companies	Public	Contextual	Customization	Marketing or Profiling	No	Short	Long
	e.g. Flickr to Yahoo			The data may only be used for the purpose of completing the current interaction	The data may be used to customize, personalize, or otherwise tailor the current interaction	Profiling involves the creation of a collection of information about an invidual and applies to profiles created for any purpose other than customization (e.g. For research, to sell to other organizations)	Baseline 35 days for the purposes of maintenance, security etc.		
None of the sharing attributes are mutually exclusive				None of the secondary use attributes are mutually exclusive			The rentention attributes are mutually exclusive		

[13] Die Tabelle habe ich aus dem Text von Cooper/Morris/Newland erstellt

Der Vorschlag konzentriert sich also auf drei Elemente mit 11 Attributen. Hierin wird die Nähe zum Creative Commons-Ansatz schon deutlicher, allerdings fehlt die visuelle Botschaft. Naturgemäß ersetzt dieses Konzept nicht die jeweils nötige Einwilligung oder den informed consent.

Diese Sets erlauben wie die CC-Lizenzen sehr unterschiedliche Nutzer-Präferenzen. Sie reichen von
Least permissive (sharing = internal; secondary use = contextual; retention = no)
zu
Most permissive (sharing = internal + affiliates + unrelated companies; secondary use = contextual + customization + marketing–or–profiling; retention = no).

Die Rulesets erfüllen einige Forderungen, die ich aufgestellt habe, schon recht gut:

1. Die Regeln müssen generisch sein.
2. Die Regeln müssen sprachlich einfache, auf eine zentrale Botschaft reduzierte Begrifflichkeiten enthalten. Im Beispiel sind es drei eingängige Worte oder Wortverbindungen.
3. Einfache ikonografische, deshalb selbst erklärende Botschaften müssen den Regelungsgehalt repräsentieren.
4. Die Regeln müssen Instrumente der Nutzer/Verbraucher/Kunden etc. sein: Sie alleine steuern das gewünschte Ergebnis.
5. Wie ein «Nutrition Label» muss jede Site eine solche tabellarische Übersicht enthalten.
6. Der Gesetzgeber mag solche Tabellen anordnen, eine darüber hinaus gehende Aufgabe hat er insoweit nicht.

Dieser Vorschlag setzt die entscheidende Botschaft meines Essays um: Er ist nicht paternalistisch und überlässt es den einzelnen Menschen zu entscheiden, was für sie gut ist. Der Gesetzgeber ist weiterhin für die Rahmensetzung verantwortlich – mehr muss er in einer sozialen Marktwirtschaft auch nicht tun. Auf diese Weise lassen die generischen Regeln Bereiche menschlicher Kreativität, aber auch Verantwortung neu entstehen. Der Rechtswissenschaftler Lawrence Lessig, der geistige Urheber der CC-Lizenzen, hat diesen Bereiche einmal als «lawyer-free-zone» bezeichnet, Räume also, in denen die alleinige Definitionsmacht der Juristen erklärtermaßen gebrochen ist (noch immer grundlegend die erste Auflage seines Buches «Code and other Laws of Cyberspace», Lessig 1999).[14] Und dieser Raum ist für alle Menschen auf der Welt

[14] Man sollte den Hintersinn solcher Bemerkungen nicht übersehen. Denn schließlich ist Lessig einer der angesehensten Juristen der USA an einer der besten Rechtsfakultäten (Harvard)

gleich – eben weil generische Regeln gelten. Natürlich wird es weiterhin Streit geben – vielleicht in 20 % aller Fälle. Der muss dann vor den jeweiligen nationalen Gerichten nach jeweils geltenden Recht entschieden werden. Man darf gespannt sein, wie sich das jeweilige nationale Recht auf die durch solche Rulesets geänderten Vorgehensweisen der Menschen einstellen wird.

Mein Vorschlag ist ganz praktisch und in überschaubarer Zeit zu realisieren: Die Wirtschaft mit ihren Institutionen möge ein Forschungsprojekt ins Leben rufen, in dem Juristen, Informatiker und vor allem Designer den Creative Commons Ansatz für den deutschen Datenschutz in eine Handvoll Piktogramme umsetzen. Sie wird sich verpflichten, die Anwendung der neu entstandenen Rulesets flächendeckend umzusetzen.

Da sich diese Sets, wie in meinem Essay beschrieben, evolutionär weiterentwickeln werden, darf man auf die Vernunft und die Fantasie der beteiligten Menschen und Institutionen hoffen. Das Ergebnis lässt sich wie bei jedem evolutionären Prozess nicht vorhersagen. Man muss aber vielleicht kein Prophet sein, wenn man erwartet, dass mit diesem Ansatz auch viele der Probleme im institutionellen Datenschutz lösbar werden, bzw. sich erledigen.

Es bleibt das Problem «Goethe oder Jefferson». Hier muss ich wohl Prophet sein. Ich denke, wie gesagt, dass Jefferson siegen wird. Hierfür lohnt es sich, die Mahnung von James Whitman (2004, S. 1221) nochmals zur Kenntnis zu nehmen:

> *The battle will have to be fought over more fundamental values than (privacy as such).*

Quellenverzeichnis

(Stand: 1. September 2010)

Bizer, Johann (2007): Sieben Regeln des Datenschutzes, in: Datenschutz und Datensicherheit 31 (2007) 5, S. 350-356

Bull, Hans Peter (2009), Informationelle Selbstbestimmung – Vision oder Illusion?, MohrSiebeck: Tübingen

Cooper, Alissa, Morris, John, Newland, Erica (2010): Privacy Rulesets: A User-Empowering Approach to Privacy on the Web, W3C Privacy Workshop July 13-14, 2010, http://www.w3.org/2010/api-privacy-ws/papers/privacy-ws-12.html

Däubler, Wolfgang, Klebe, Thomas, Wedde, Peter, Weichert, Thilo (2010): Bundedatenschutzgesetz. Kompaktkommentar, 3. Aufl., Bund Verlag: Frankfurt [zit. nach Bearbeiter]

Frey, Bruno (2008): Motivation crowding theory - a new approach to behaviour, in: Behavioural Economics and Public Policy. Roundtable Proceedings, Melbourne, 8.-9. August 2007. Australian Government Productivity Commission, S. 37-54, online unter http://www.bsfrey.ch/articles/D_201_08.pdf

Gavison, Ruth (1980): Privacy and the Limits of Law, Yale Law Review Vol. 89 No. 3, S. 421-471

Gola, Peter, Schomerus, Rudolf [Bearbeiter] (2010): Bundedatenschutzgesetz. Kommentar, Beck: München

Ishii, Kei, Lutterbeck, Bernd, Pallas, Frank (2008): Forking, Scratching und Re-Merging. Ein informatischer Blick auf die Rechtsinformatik, Bericht Nr. 2008-4 der Fakultät für Elektrotechnik und Informatik der TU Berlin, Fakultätsdruckerei: Berlin, online unter http://ig.cs.tu-berlin/ma/bl/ap

Kelley, Patrick Gage, Lucian, Cesca, Bresee, Joanna, Cranor Lorrie Faith (2010): Standardizing privacy notices: an online study of the nutrition label approach, Proceedings of the 28th international conference on Human factors in computing systems 2010, Atlanta, Georgia, USA April 10 - 15, 2010, S. 1573-1582 [Slides auf der Webseite http://cups.cs.cmu.edu/privacyLabel]

Konferenz der Datenschutzbeauftragten (2010): Eckpunkte für ein modernes Datenschutzrecht für das 21. Jahrhundert v. 18.3.2010, http://www.baden-wuerttemberg.datenschutz.de

Ladeur, Karl-Heinz (2009): Das Recht auf informationelle Selbstbestimmung: Eine juristische Fehlkonstruktion?, in: Die Öffentliche Verwaltung 2009, S. 45-55

Lessig, Lawrence (1999): Code and other laws of cyberspace, Basic Books: New York

Löffler, Joachim (1959): Persönlichkeitsschutz und Meinungsfreiheit, in: NJW 1959, S. 1-6

Lutterbeck, Bernd (2010): Komplexe Kontexte – Einfache Regeln, Wettbewerbsbeitrag für den Wettbewerb *Zwischen Liberalität und Paternalismus – Wo fördert, wo beschränkt der* Datenschutz Bürgerrechte?, hg. SCHUFA AG … (Eine mit Anmerkungen und einem Literaturverzeichnis versehene Version findet sich unter http://lutterbeck.org/2.html)

Nissenbaum, Helen F. (2010): Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford Law Books, Stanford University Press: Stanford

Orwat, Carsten (2009): Software als Institution und ihre Gestaltbarkeit, Beitrag für das Informatik Spektrum von einem Autorenkollektiv (u.a. Bernd Lutterbeck) unter der Federführung von Carsten Orwat, Karlsruhe Institute of Technology (KIT), published online bei Springer-Verlag DOI 10.1007/s00287-009-0404-z vom 16 December 2009, zur Publikation in Informatik Spektrum Heft 4/2010

Pallas, Frank (2008), Simple Regeln für komplexe Strukturen: Was die Informatik von der NIÖ [Neue Institutionelle Ökonomik] lernen kann, Diskussionspapier zum Workshop "Software als Institution", Karlsruhe Institute of Technology, 12. Dezember 2008, http://ig.cs.tu-berlin.de/ma/fp/ap

Posner, Richard (1978) A.: The Right of Privacy, Georgia Law Review Vol. 12 No. 3, S. 393-422 [http://digitalcommons.law.uga.edu/lectures_pre_arch_lectures_sibley/22]

Posner, Richard A. (2008): Privacy, Surveillance, and Law, The University of Chicago Law Review Vol. 75, S. 245-260

Post, Robert C. (1989): The Social Foundations of Privacy: Community and Self in the Common Law Tort, in: California Law review Vol 77 N. 5, S. 957-1010

Post, Robert C. (2001): Three Concepts of Privacy, Georgetown Law Journal Vol.89 (2000-2001), S. 2087-2098

Prosser, William L. (1960): Privacy, California Law Review Vol. 48 (1960) No. 3, S. 363-423

Raskin, Aza (2010): Privacy: A Pictographic Approach Submitted on behalf of Mozilla für das W3-Konsortium, W3C Workshop on Privacy for Advanced Web APIs 12/13 July 2010, London, http://www.w3.org/2010/api-privacy-ws/papers/privacy-ws-22.txt

Roßnagel, Alexander, Pfitzmann, Andreas, Garstka, Hansjürgen (2001): Modernisierung des Datenschutzes. Gutachten im Auftrag des Bundesministeriums des Innern, Selbstverlag des Bundesministeriums des Innern: Berlin

Roßnagel, Alexander; Jandt, Silke (2010): Datenschutzfragen eines Energieinformationsnetzes, Alcatel-Lucent Stiftung, Stiftungsreihe 88, Stuttgart, http://www.stiftungaktuell.de/files/sr88_newise_datenschutz_gesamt.pdf

Martin Rost, Andreas Pfitzmann (2009): Datenschutz-Schutzziele – revisited, in: Datenschutz und Datensicherheit 33 (2009) 6, S. 353 - 358

Nimmer, Melville B. (1954): The Right of Publicity, Law and Contemporary Problems Vol. 19 (1954), S. 203-223

Seibt, Gustav (2010): Blicke in den Vorgarten. Was ist privat und was öffentlich? Zum Streit um Googles Street View, in: Süddeutsche Zeitung v. 14.8.2010

Simitis, Spiros (Hg.) (2006): Bundesdatenschutzgesetz, 6. Aufl., Nomos: Baden-Baden

Spiekermann, Sarah, Pallas, Frank (2006): Technology Paternalism – wider implications of ubiquitous computing, in: Poiesis & Praxis Vol. 4 No. 1 (march 2006), S. 6-18

Steinmüller, Wilhelm; Lutterbeck, Bernd; Mallmann, Christoph (1972): Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministers des Innern, Anlage 1 der Bundestagsdrucksache VI/3826 vom 7. September 1972, Deutscher Bundestag: Bonn.

Warren, Samuel & Brandeis, Louis D. (1890), The Right to Privacy, Harvard Law Review Vol. 4 Iss 5 , S. 193-220

Weichert, Thilo (2010): „Codex digitalis“- Optimierter Persönlichkeitsschutz – digital und vernetzt, Begrüssungsrede zur Sommerakademie am 30. August 2010 in Kiel, abrufbar unter www.datenschutzzentrum.de/sommerakademie/2010/

Whitman, James Q. (2004), The Two Western Cultures of Privacy: Dignity Versus Liberty, Yale Law Journal Vol. 113, S. 1151-1221