Jörg Pohle

Die immer noch aktuellen Grundfragen des Datenschutzes

1 Einleitung

Wird der Beginn der Hearings von US-Senat und US-Repräsentantenhaus zum Informationsgebaren von Staat und Privaten als Geburtsstunde der modernen Datenschutzdebatte begriffen,[1] dann begeht diese 2014 ihren 55. Jahrestag.[2] Da verwundert es doch sehr, dass es bis heute keinerlei Einigung gibt – weder in der wissenschaftlichen noch in der politischen Debatte, weder zum Schutzgut noch zur Schutzarchitektur. Allein das Schutzobjekt scheint festzustehen: „personenbezogene Daten", obwohl es durchaus auch Streit um deren Geeignetheit gibt (Schwartz und Solove 2011). Zu einem nicht unerheblichen Umfang liegt das sicherlich an den verschiedenen Interessen und Ideologien, vor allem zwischen den verschiedenen Gruppen der Datenverarbeiter und denjenigen, die sich dem Schutz der Betroffenen verschrieben haben, sowie den Kämpfen zwischen den wissenschaftlichen Disziplinen um die Definitionsmacht und damit mittelbar auch um die Futtertröge mit den Drittmitteln. Ein weiterer und nicht ganz unwesentlicher Grund – und eigentlich eine große Peinlichkeit für „die Wissenschaft" – liegt im Fehlen einer fundierten wissenschaftlichen Auseinandersetzung mit den Arbeiten aus den Anfängen der Datenschutzdebatte, die viele der heutigen Probleme schon in der Frühzeit der automatisierten Informationsverarbeitung untersucht und nicht selten dafür auch heute noch passende Lösungen angeboten haben.

Eine der einflussreichsten und durchaus häufig zitierten – gleichwohl allerdings nur wenig kritisch reflektierten[3] – Arbeiten entstand

1971 unter der Leitung von Wilhelm Steinmüller als Gutachten für das Bundesministerium des Innern: die „Grundfragen des Datenschutzes“ (Steinmüller u. a. 1971). Weil das Gutachten trotz aller notwendigen Kritik bis heute eine der sinnvollsten Zusammenstellungen aus fundierter Analyse des Datenschutzproblems, konsistenter Lösungsarchitektur und stringenter Operationalisierung darstellt,[4] verhilft eine kritische Auseinandersetzung mit diesem Gutachten immer noch zu neuen Erkenntnissen für eine der Informationsgesellschaft des 21. Jahrhunderts angemessene Lösung des Datenschutzproblems. Wilhelm Steinmüllers eigene Auseinandersetzung mit dem Gutachten hält dabei leider nicht, was sie verspricht: „Das informationelle Selbstbestimmungsrecht – Wie es entstand und was man daraus lernen kann“ (Steinmüller 2007).

2 Grundsätze und Vorgehen

Das Gutachten basiere, so Steinmüller in der Rückschau, auf drei Grundsätzen (ebd., 159). Erstens bedürfe es eines realistischen Modells des zu analysierenden Phänomens. Zweitens seien daraus – noch abstrakte – Regeln zu entwickeln, die einer gesellschaftlich akzeptablen Datenverarbeitung zur Umsetzung verhelfen, „dergestalt, dass für die betroffenen Menschen durch die Technik nicht nur kein Schaden entsteht, sondern maximaler Vorteil erwächst.“ Drittens seien diese abstrakten Regeln in widerspruchsfreie rechtliche Formen zu gießen.

Obwohl die Formulierung Steinmüllers das nahezulegen scheint, lässt sich aus den Grundsätzen nicht einfach das für das Gutachten gewählte Vorgehen ableiten. Vor allem haben Wilhelm Steinmüller und seine Koautoren weniger als behauptet versucht, den Datenschutz positiv zu formulieren. Vielmehr sprechen sowohl ihr Vorgehen als auch die für die rechtlichen Anforderungen an die Datenverarbeitung gewählten Formulierungen dafür, dass sie den

Datenschutz – oder genauer: das Datenschutzrecht – im Sinne eines klassischen Abwehrrechts ausgestaltet sehen wollten.

Die Argumentationsstruktur des Gutachtens folgt andererseits – jedenfalls grob – tatsächlich einem Dreischritt: In einem ersten Schritt wird der Stand der gesellschaftlichen Informationsverarbeitung beschrieben, vor allem der durch Organisationen vollzogenen und – fast ausschließlich – der automationsgestützten. Als typische Struktur wird dabei die Phasenorientierung der Informationsverarbeitung identifiziert. Im zweiten Schritt werden die zentralen Risiken beschrieben, die sich aus der aufkommenden Industrialisierung der gesellschaftlichen Informationsverarbeitung insgesamt ergeben. Im dritten Schritt werden dann auf der Basis eines Metamodells der organisierten Informationsverarbeitung – dem Phasenmodell, das sie im ersten Schritt identifiziert haben – Gefahren, die während der einzelnen Phasen für die Grundrechte der Betroffenen entstehen können, analysiert, bewertet und direkt daraus konkrete Schutzanforderungen in Form (öffentlich-)rechtlicher – und dabei vor allem formeller – Regelungen ausformuliert.

3 Zu Grunde gelegte Annahmen

Neben den beschriebenen Grundsätzen und der Annahme einer Phasenorientierung jeder organisierten Informationsverarbeitung liegen dem Gutachten weitere Annahmen zu Grunde. Leider wurden nicht alle davon im Gutachten selbst expliziert.

Eine der Annahmen betrifft den Charakter des Datenschutzes. Aus der Aussage „Datenschutz ist die Kehrseite der Datenverarbeitung“ (Steinmüller u. a. 1971, 34) folgt einerseits, dass sich die Notwendigkeit von Datenschutz nur aus dem spezifischen Charakter der gesellschaftlichen Informationsverarbeitung ableiten lässt, und andererseits, dass Datenschutz so lange gesellschaftlich notwendig

ist, wie es gesellschaftliche Informationsverarbeitung gibt. Daher gilt, dass das Datenschutzproblem im grundsätzlichen Sinne nicht gelöst werden kann, sondern gesellschaftlich vor dem Hintergrund des Standes der Informationsverarbeitung immer neu ausgehandelt werden muss. Diese Aushandlung kann dabei, so folgt eindeutig aus den Ausführungen der Autoren zur Notwendigkeit interdisziplinärer Zusammenarbeit bei der Analyse der gesellschaftlichen Informationsverarbeitung, nicht allein den Juristen überlassen werden, weder damals noch heute oder in Zukunft.

Die zentrale Annahme des Gutachtens ist sicher die der „Unbrauchbarkeit der Privatsphäre" (ebd., 48 ff.). Diese haben sie sicher auch vor den für die Ausarbeitung eines Entwurfs für ein Datenschutzgesetz Verantwortlichen im BMI vertreten, als sie für den Gutachtenauftrag warben. Jedenfalls hat sich auch Herbert Auernhammer, der zuständige Referent, diese Annahme zu eigen gemacht und in seinen „Gedanken zur Datenschutzgesetzgebung" (Auernhammer 1971) lange vor Veröffentlichung des Gutachtens als Begründung für das phasenorientierte Vorgehen der Öffentlichkeit präsentiert. Er argumentiert dabei indirekt: Die beiden konventionellen Ansätze rechtlicher Regelung von individuellen und gesellschaftlichen Gefährdungen – aus der Begriffsdefinition abgeleitete Schutzregeln sowie ein kasuistisches Vorgehen – seien zum Scheitern verurteilt. Einerseits sei die „Privacy-Problematik"[5], also das Problem einer Legaldefinition der zu schützenden Privatsphäre – oder allgemeiner: des zu schützenden Rechtsgutes –, grundsätzlich unentscheidbar. Andererseits sei auch eine kasuistische Inhaltsbestimmung undurchführbar, weil sie „ins Uferlose führen und im übrigen ebenfalls an der Schranke der Relativität der Privatsphäre enden" würde (ebd., 26). Statt dessen bedarf es einer sinnvollen Objektivierung, um die Datenverarbeiter angemessen klar verpflichten zu können. Ohne eine solche Objektivierung wären Datenverarbeiter schlicht nicht in der Lage, ihr eigenes Informationsverhalten so zu steuern, dass die Grundrechte der Betroffenen nicht verletzt werden.[6]

Zu den nicht explizierten Annahmen gehören unter anderem die über den Charakter der Organisationen, die von den Autoren des Gutachtens betrachtet werden, sowie die über den Charakter der Maschine, die in den Organisationen zur Unterstützung oder zur Übernahme von Informationsverarbeitung und Entscheidungsfindung verwendet wird. Die Autoren betrachten ausschließlich rationale Bürokratien im Sinne Max Webers, also Organisationen, die die Prozesse ihrer eigenen Entscheidungsfindung rational vorplanen, die dafür notwendigen Informationsverarbeitungsprozesse geeignet formalisieren und danach funktionieren wie ein Uhrwerk – das Preußische Militär und Siemens als Prototypen, wie Wolfgang Coy auf einer Veranstaltung vor einiger Zeit anmerkte. Zweitens unterstellen die Autoren dem Computer einen ausschließlich instrumentellen Charakter, den er wohl auch Anfang der 1970er Jahre durchaus noch hatte. Spätestens mit dem Erscheinen des PC Anfang der 1980er Jahre hat sich der Computer allerdings zu einer allgemeinen Medien- und Kommunikationsmaschine verändert und ist damit viel mehr als nur ein Werkzeug, das speziell auf einen konkreten Informationsverarbeitungsprozess zugeschnitten ist.

4 Der Informationsbegriff

Im Gegensatz zu fast allen nachfolgenden Generationen von Forschern, die sich an der Formulierung einer Privacy- oder Datenschutztheorie versuchten, verwendeten Wilhelm Steinmüller und seine Mitautoren einen auch heute noch sinnvollen und vor allem interdisziplinär anschlussfähigen Informationsbegriff. Es handelt sich um den Informationsbegriff der Semiotik mit seinen vier Dimensionen Syntax, Semantik, Pragmatik und Sigmatik (Steinmüller u. a. 1971, 42 f.). Der Begriff Datum, der nicht nur das deutsche Datenschutzrecht durchzieht und immer wieder zu abstrusen Anfeindungen einlädt, sei verwendet worden, weil er kompatibel mit dem damals schon eingeführten Begriff Datenschutz gewesen sei,

vor allem aber, damit die Informatiker – was sie seitdem mit steter Regelmäßigkeit trotzdem versuchen – davon absehen, Claude Shannons technischen Informationsbegriff zu Grunde zu legen. Mit Syntax wird dabei die konkrete, meist zeichenmäßige Repräsentation, mit Semantik die Bedeutung und mithin der Kontext, mit Pragmatik der Zweck und mit Sigmatik der Verweis auf die betroffene Person bezeichnet und damit rechtlich regulierbar. Kommunikative Anschlussfähigkeit ist offenkundig garantiert für die moderne Soziologie, die Verwaltungswissenschaft und wenig überraschend auch für die Informatik.

Der unzweifelhaft abstruseste Beitrag zur Debatte um die Definition des zu verwendenden Informationsbegriffs stammt von Marion Albrecht, die in ihrer 2005 veröffentlichten Habilitationsschrift versucht, Gregory Batesons biokybernetischen Informationsbegriff in die Datenschutzdebatte einzuführen (Albers 2005). Batesons Informationsbegriff mit Information als „a difference which makes a difference“ (Bateson 1987, 321) soll bei der Erklärung der biologischen Informationsverarbeitungsprozesse im Gehirn helfen. Für eine rechtliche Regelung der gesellschaftlichen Informationsverarbeitung ist er nicht geeignet. Das liegt daran, dass nach dieser Definition nur das eine Information ist, was neu ist. In dem Augenblick, in dem eine Organisation Verfügung über Informationen erlangt hat, verlieren sie die Eigenschaft, neu zu sein. Sie sind damit entsprechend der Definition auch keine Informationen mehr. Organisationen verarbeiten und nutzen daher keine Informationen im Sinne dieser Definition. Daraus folgt, dass für jede gesetzliche Regelung des Umgangs mit Informationen unabhängig vom Umfang der rechtlichen Anforderungen gilt, dass sie Organisationen nicht bindet und auch nicht binden kann. Gesetzliche Regelungen auf der Basis dieser Informationsdefinition sind daher grundsätzlich für einen Schutz der Betroffenen untauglich.

5 Die verfassungsrechtliche Basis

Wilhelm Steinmüller und seine Koautoren halten eine Konzeption eines Datenschutzrechts ohne verfassungsrechtliches Fundament für keinen gangbaren Weg. Ihr Entwurf soll deshalb auf „zwei Säulen" stehen: den Grundrechten und dem Rechtsstaatsprinzip (Steinmüller u. a. 1971, 60).

Zwar betrachten sie – jedenfalls kursorisch – auch die speziellen Grundrechte, soweit diese auch personenbezogene Informationen betreffen, als zentralen verfassungsrechtlichen Prüfungsmaßstab identifizieren sie jedoch die „freie Entfaltung der Persönlichkeit in Artikel 2 Abs. 1" (ebd., 85). Auf der Basis einer – im Einzelnen durchaus kritikwürdigen – interdisziplinären Argumentation mit Anleihen aus der Kybernetik, der Soziologie und der Rechtswissenschaft versuchen sie zu zeigen, dass Artikel 2 Absatz 1 GG „das Selbstbestimmungsrecht des Bürgers[7] über sein informationelles Personenmodell" schützt (ebd., 88). Damit wird deutlich, dass die verfassungsrechtliche Konzeption des bundesdeutschen Datenschutzrechts historisch weder auf dem allgemeinen Persönlichkeitsrecht aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG fußt, wie es seit dem Volkszählungsurteil auch rückwirkend oft angenommen wird, noch sich fundamental von Ansätzen unterscheidet, die zur gleichen Zeit in den USA diskutiert wurden, wie vor allem seit der Arbeit von James Q. Whitman „The Two Western Cultures of Privacy: Dignity versus Liberty" (Whitman 2004) verbreitet behauptet wird.[8]

Die Art der Bezugnahme auf das Rechtsstaatsprinzip – oder allgemein: die „Grundprinzipien der staatlichen Ordnung" (Steinmüller u. a. 1971, 90) – im Gutachten ist stark kritikwürdig. So werden erstens diese Prinzipien nur in ihren direkten Auswirkungen auf Artikel 2 Absatz 1 GG betrachtet, nicht jedoch auch in ihrem Charakter als gesellschaftliche Instrumente zur Beschränkung struktureller

Informationsmacht. Zweitens wird zwar darauf verwiesen, dass die private Informationsverarbeitung nicht den Rechtsstaatsanforderungen unterliege, die im Laufe der Analyse entwickelte Regelungsarchitektur wird jedoch unterschiedslos auf sowohl die öffentliche wie die private Informationsverarbeitung angewendet.

6 Die Regelungsarchitektur

Zentrales und gleichzeitig Alleinstellungsmerkmal der vorgeschlagenen Datenschutzarchitektur ist nach Steinmüllers eigener Darstellung seine Phasenorientierung, deren Urheber Bernd Lutterbeck gewesen sei und die die quasi transhistorische Grundstruktur jeder Informationsverarbeitung in rationalen (öffentlichen und privaten) Organisationen in der Struktur des Gesetzes widerspiegelt. Entgegen Steinmüllers anekdotenhafter Erzählung handelt es sich beim phasenorientierten Datenschutz jedoch keineswegs um eine Neuerfindung speziell für das Gutachten, sondern um eine Weiterentwicklung früherer – auch Steinmüllerscher – Ansätze. Während in „EDV und Recht – Einführung in die Rechtsinformatik" noch ein Maschinenmodell Pate stand – „input controls", „output controls" (Steinmüller 1970, 88) –, wurde nun das informationsverarbeitende System Organisation Grundlage der Analyse. Folgerichtig wird an das informationelle Handeln der Organisation angeknüpft und Informationsermittlung, Informationserfassung, Informationsspeicherung, Informationsveränderung, Informationsaustausch, Informationsweitergabe an Dritte, Informationsverbund und Informationslöschung als wohlunterscheidbare Phasen identifiziert (Steinmüller u. a. 1971, 57). Ziel ist damit, das informationelle Handeln der Organisationen vermittelt über seine Teilschritte unter rechtliche Kontrolle zu bringen. Dahinter steht offensichtlich die Annahme, dass wenn die Rechte der Betroffenen in jeder Phase des Informationsverarbeitungsprozesses sichergestellt seien, dann seien sie es auch insgesamt. In dieser Zuspitzung widerspricht es jedoch einer

der wesentlichen Eigenschaften komplexer Systeme: Das Ganze ist mehr als die Summe seiner Teile. Für jede organisierte Informationsverarbeitung, die ein komplexes System ist, würde damit gelten: Das Gesamtrisiko für die Rechte der Betroffenen ist größer als die Summe der Risiken, die in den einzelnen Phasen liegen.

Dass die Nutzung der Struktur von Informationsverarbeitungsprozessen zur Analyse und Regelung des Datenschutzproblems auch heute noch ein sinnvolles Vorgehen darstellt, zeigt das weitverbreitete Lob, das Daniel Solove für seine Arbeit „A Taxonomy of Privacy" (Solove 2006) zuteil wurde und wird. Soloves Vorstellung von Informationsverarbeitung ist bedeutend weniger reflektiert als die dem Gutachten zu Grunde liegende. So unterscheidet er etwa nur drei Phasen: „information collection", „information processing" und „information dissemination" (ebd, 488), wobei er behauptet, den Begriff „information processing" der EG-Datenschutzrichtlinie 95/46/EG zu entlehnen (ebd, Fn. 46), die diesen Begriff jedoch offenkundig als Obermenge für alle Phasen verwendet. Auch ist seine Begründung für die konkrete Trennung der Phasen, die er vornimmt, nicht überzeugend. So definiert er, dass „[information processing] concerns how already-collected data is handled" (ebd., 504). Obwohl „information dissemination" offenkundig ein „Umgang" mit bereits gesammelten Informationen ist, betrachtet er sie als eigene Phase.

7 Abschluss und Ausblick

Bis heute ist das inzwischen über 40 Jahre alte Gutachten von 1971 der umfassendste Versuch geblieben, eine fundierte und gleichzeitig auf den Bereich des Datenschutzes beschränkte Analyse vorzulegen, die die gesellschaftliche Informationsverarbeitung als Ausgangspunkt nimmt und nicht nur an der Oberfläche kratzt, um mit den IT-Buzzwords der Saison um sich zu werfen. Die im Gutachten

entwickelte Regelungsarchitektur prägt bis heute das Datenschutzrecht, nicht nur das bundesdeutsche.

Dabei ist das Gutachten keineswegs frei von Fehlern. Vor allem die nicht explizierten Annahmen, die der Analyse des Datenschutzes und der Lösungsarchitektur zu Grunde liegen, stellen ein grundsätzliches Problem dar. Weder handelt es sich bei informationsverarbeitenden Systemen notwendig um rationale Verwaltungen im Sinne Max Webers noch kann dem Computer vorbehaltlos ein instrumenteller Charakter unterstellt werden. Auch die Annahme, dass sich die aus der Informationsverarbeitung ergebenden Grundrechtsgefährdungen verhindern ließen, wenn nur die einzelnen Informationsverarbeitungsphasen grundrechtsschützend gestaltet werden, überzeugt nicht.

Die Phasenorientierung ist zweifellos das bedeutendste Erbe der „Grundfragen des Datenschutzes". Sie ist als analytisches Mittel zur Komplexitätsreduktion sowohl für die Gefahrenanalyse wie die Formulierung angemessener gesetzlicher Regelungen als auch für deren praktische Umsetzung auch weiterhin unverzichtbar. Die Anforderungen, die an die einzelnen Phasen aber auch an die Informationsverarbeitung in ihrer Gesamtheit gestellt werden sollen, müssen dabei ohne Bezugnahme auf konkrete Implementierungsdetails und sinnvollerweise unter Verwendung von Schutzzielen[9] formuliert werden.

Das Gutachten zu lesen und zu verstehen und dabei auch seine Grenzen zu begreifen, ist und bleibt Vorbedingung für jede Analyse, die über das Erreichte hinausgehen will, um einen angemessenen Datenschutz für das 21. Jahrhundert und darüber hinaus zu

entwickeln. Nur dann können wir behaupten, tatsächlich auf den Schultern von Riesen zu stehen.

Anmerkungen

1 Zur Vorgeschichte des Datenschutzes als Begrenzung von Informationsmacht siehe Kai von Lewinskis Arbeit „Geschichte des Datenschutzrechts von 1600 bis 1977“ (von Lewinski 2009).

2 Das erste dieser Hearings war „Freedom of Information and Secrecy in Government“, Hearings before the Subcommittee on Constitutional Rigths of the Senate Committee on the Judiciary, 86th Congress, 1st Session, 1959. Das bekannteste dürfte hingegen das von Cornelius E. Gallagher geleitete Hearing „The Computer and the Invasion of Privacy“, Hearings before a Subcommittee of the House Committee on Government Operations, 89th Congress, 2d Session, 1966, sein.

3 Das könnte durchaus daran liegen, dass die Arbeit zwar häufig zitiert, aber nur selten gelesen wurde (Simkin und Roychowdhury 2003).

4 Das kurz darauf entstandene und durchaus einige Ähnlichkeiten aufweisende Gutachten des U.S. Department of Health, Education, and Welfare „Records, Computers, and the Rights of Citizens“ (HEW 1973) ist weder ähnlich rigoros in seiner Analyse noch kann es nachweisen, dass seine Lösungsvorschläge mehr sind als willkürlich operationalisierte Einzelregelungen. Gleiches gilt für das Gutachten „Modernisierung des Datenschutzrechts“ (Roßnagel, Pfitzmann und Garstka 2001), dem es darüber hinaus deutlich an Widerspruchsfreiheit hinsichtlich Regelungsarchitektur und Einzelregelungen mangelt. Daniel Soloves Arbeit „A Taxonomy of Privacy“ (Solove 2006) ist allem Anschein nach ein strukturelles Übersetzungsplagiat, das angesichts der relativen Unbekanntheit des Gutachtens in der amerikanischen und internationalen Debatte bislang nur mit Lob überschüttet, jedenfalls aber noch keinem Vergleich mit dem Gutachten unterzogen wurde. Andere Arbeiten spielen nicht in der gleichen Liga, viele nicht einmal das gleiche Spiel.

5 Die Wortwahl Auernhammers ist besonders beachtenswert, denn mit dieser Art der Übernahme des Begriffs der „Privacy“ aus der amerikanischen Debatte gesteht er ein, dass es zu diesem Zeitpunkt in der bundesdeutschen Debatte noch nicht einmal eine Einigung über das der Lösung harrende Problem gab. Witzigerweise – oder traurigerweise, je nachdem – hat sich daran bis heute nichts geändert, wie insbesondere die auch derzeit wieder allzu häufig zu hörende

Behauptung untermauert, zentrales – oder gar einziges – Ziel des Datenschutzes sei die Sicherstellung von Vertraulichkeit.

6 Diesen Fehler begeht etwa Helen Nissenbaum in „Privacy as contextual integrity“ (Nissenbaum 2004), obwohl ihre Theorie eigentlich schlicht eine Abwandlung des rollentheoretischen Datenschutzansatzes aus den 1970er Jahren ist, wie er etwa von Paul J. Müller in „Funktionen des Datenschutzes aus soziologischer Sicht“ (Müller 1975) vorgelegt wurde. Während nach der soziologischen Rollentheorie „Kontext“ eine Eigenschaft von „Rolle“ ist, ist „Rolle“ bei Nissenbaum eine Eigenschaft von „Kontext“. Rollen und Rollenzuschreibungen haben dabei einen durchaus objektiven Charakter, während sich Kontexte und die daraus abzuleitenden Anforderungen an Erhebung, Verarbeitung und Nutzung personenbezogener Informationen wenn überhaupt nur hochgradig subjektiv festlegen lassen.

7 Tatsächlich handelt es sich bei Artikel 2 Absatz 1 GG nicht um ein exklusives Bürger- oder Deutschengrundrecht, sondern um ein Jedermann-Grundrecht und also um ein allgemeines Menschenrecht.

8 Zwar wird im Gutachten durchaus Bezug auf die Menschenwürde genommen, Artikel 1 GG wird allerdings „nur Unterstützungswert“ (Steinmüller 1971, ebd.) für die Auslegung von Artikel 2 Absatz 1 GG zugestanden.

9 Siehe dazu die grundlegende Arbeit von Martin Rost und Andreas Pfitzmann „Datenschutz-Schutzziele – revisited“ (Rost und Pfitzmann 2009) und die von dort ausgehenden Weiterentwicklungen. Nicht überzeugend ist dabei allerdings, dass Rost die Schutzziele nicht aus seinen grundsätzlichen – und sehr fundierten – Analysen des Datenschutzproblems wie „Zur Soziologie des Datenschutzes“ (Rost 2013) ableitet, sondern sie schlicht als Kondensat der Erfahrungen der letzten Jahrzehnte mit dem Datenschutzrecht und der Datenschutzpraxis sieht. Dadurch entsteht jedoch ein Zirkelschluss: Problemanalyse und Lösungsansatz, denen die ihnen zu Grunde liegenden Annahmen zu großen Teilen weggebrochen sind, werden als Quelle für die neuen grundlegenden Schutzziele benutzt, aus denen heraus dann wieder einzelne konkrete Anforderungen operationalisiert werden, die am Ende wieder (fast) nur die gleichen Datenschutzmaßnahmen ergeben, die auch jetzt schon in jeder Maßnahmensammlung für die Umsetzung datenschutzrechtlicher Anforderungen zu finden sind.

Literatur

Albers, Marion (2005): Informationelle Selbstbestimmung. Baden-Baden: Nomos.

Auernhammer, Herbert (1971): „Gedanken zur Datenschutzgesetzgebung". In: Öffentliche Verwaltung und Datenverarbeitung, S. 23–27.

Bateson, Gregory (1987): Steps to an Ecology of Mind. Collected Essays in Anthropology, Psychiatry, Evolution, and Epistemology. Northvale: Jason Aronson Inc. Nachdruck. Ursprünglich veröffentlicht: San Franciso: Chandler Pub. Co., 1972.

von Lewinski, Kai (2009): „Geschichte des Datenschutzrechts von 1600 bis 1977". In: Arndt, Felix (Hrsg.): Freiheit – Sicherheit – Öffentlichkeit. 48. Assistententagung Öffentliches Recht. Baden-Baden: Nomos, S. 196–220.

Müller, Paul J. (1975): „Funktionen des Datenschutzes aus soziologischer Sicht". In: Datenverarbeitung im Recht, S. 107–118.

Nissenbaum, Helen (2004): „Privacy as contextual integrity". In: Washington Law Review, S. 101–139.

Rost, Martin (2013): „Zur Soziologie des Datenschutzes". In: Datenschutz und Datensicherheit, S. 85–91.

Rost, Martin und Pfitzmann, Andreas (2009): „Datenschutz-Schutzziele – revisited". In: Datenschutz und Datensicherheit, S. 353–358.

Roßnagel, Alexander; Pfitzmann, Andreas und Garstka, Hansjürgen (2001): Modernisierung des Datenschutzrechts. Gutachten für das Bundesministerium des Innern.

Schwartz, Paul M. und Solove, Daniel J. (2011): „The PII Problem: Privacy and a New Concept of Personally Identifiable Information". In: New York University Law Review, S. 1814–1894.

Simkin, Mikhail V. und Roychowdhury, V. P. (2003): „Read Before You Cite!" In: Complex Systems, S. 269–274.

Solove, Daniel J. (2006): „A Taxonomy of Privacy". In: University of Pennsylvania Law Review, S. 477–560.

Steinmüller, Wilhelm (1970): EDV und Recht – Einführung in die Rechtsinformatik. Berlin: J. Schweitzer Verlag.

Steinmüller, Wilhelm (2007): „Das informationelle Selbstbestimmungsrecht – Wie es entstand und was man daraus lernen kann". In: Recht der Datenverarbeitung, S. 158–161.

Steinmüller, Wilhelm u. a. (1971). Grundfragen des Datenschutzes. Gutachten im Auftrag des Bundesministeriums des Innern, BT-Drs. VI/3826, Anlage 1.

U.S. Department of Health, Education, and Welfare (1973): Records, Computers, and the Rights of Citizens. The Massachusetts Institute of Technology.

Whitman, James Q. (2004): „The Two Western Cultures of Privacy: Dignity versus Liberty". In: The Yale Law Journal, S. 1151–1221.