erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

Jörg Pohle

Was wir aus der Geschichte der Datenschutzdebatte für die Technikgestaltung lernen können

Sonderpreis

Der vorliegende Beitrag soll in aller Kürze einen Überblick darüber geben, was der Hintergrund meiner Dissertation Datenschutz und Technikgestaltung *(Pohle 2018) ist, also warum ich mich damit beschäftigt habe, was meine Forschungs- und Erkenntnisinteressen sind, um dann zu klären: Was ist, was soll Datenschutz? Oder in der Sprache der Informatik: Was ist das Bedrohungsmodell, das dem Datenschutz zugrunde liegt? Diese Fragestellungen können auf eine lange historische Tradition zurückblicken und wurden sehr stark auch von Personen geprägt, die im FIfF oder im Umfeld des FIfF aktiv waren oder noch aktiv sind. Abschließend will ich kurz meinen Vorschlag für ein Vorgehensmodell mit einem analytischen Framework präsentieren, mit dem man solche sozio-technischen Systeme in der Entwicklung und für die Entwicklung analysiert und dann datenschutzgerecht – was sich nicht unbedingt in Datenschutzrechtskonformität erschöpft – entwerfen, entwickeln, umsetzen und einsetzen kann.*

Zentraler Hintergrund der Arbeit ist die Erkenntnis, dass privacy, surveillance und Datenschutz *essentially contested concepts* sind (zum Konzept siehe Gallie 1956, zur diesbezüglichen Einordnung von *privacy* siehe Mulligan, Koopman und Doty 2016). Weder in der wissenschaftlichen noch in der politischen Debatte gibt es eine Einigung zu unzähligen Aspekten, die grundlegend für das Verständnis der Problemlage und die Entwicklung von Lösungsansätzen sind. Schon auf der Ebene der Bestimmung des Phänomenbereichs gibt es massive Diskrepanzen zwischen den Beschreibungen, den Einordnungen und Erklärungen, die von verschiedener Seite geliefert werden. Während am einen Ende des Spektrums zwischenmenschliche Beziehungen zum Ausgangspunkt der Analyse gemacht werden, richtet sich der Blick am anderen Ende auf die strukturellen Bedingungen der modernen, funktional differenzierten Gesellschaft. Nicht überraschend ist es daher, dass es auch keine Einigung über das Schutzgut gibt: Von individuellen Bedürfnissen oder Interessen wie Privatheit, Vertraulichkeit, Eigentum, Entscheidungsfreiheit oder Persönlichkeitsentfaltung über soziale Konstruktionen wie Menschenwürde, Fairness oder Kommunikationsschutz bis zu gesellschaftlichen oder strukturellen Eigenschaften wie Freiheitsräumen, der Informationsordnung oder der Aufrechterhaltung der funktionalen Differenzierung der Gesellschaft wird alles vertreten. Gleiches gilt für die möglichen Gründe, Auslöser oder Verstärker der Gefährdung der betreffenden Schutzgüter: Ob technische Artefakte wie Daten, Informationen oder gar der Computer selbst, Praktiken wie Überwachung, Veröffentlichung, Verdatung, Missbrauch, Informationsverarbeitung oder -nutzung, Akteurskonstellationen oder deren Eigenschaften wie Machtasymmetrien, oder Phänomene auf der gesellschaftlichen Ebene wie die Digitalisierung aller Lebensbereiche, die globale Vernetzung oder die Industrialisierung der gesellschaftlichen Informationsverarbeitung – alles ist schon einmal als Gefahr oder Gefährder, Risiko oder Risikoquelle identifiziert worden.

Vor diesem Hintergrund überrascht es vielleicht ein wenig, dass die Auseinandersetzung um Datenschutz – gleiches gilt für privacy- oder Privatheitsschutz – in den letzten fünfzig Jahren eine extrem große Zahl von Gesetzen hervorgebracht hat. Die naheliegende Annahme, dass es dabei jeweils zu Einigungen gekommen ist, trügt jedoch, wie etwa der Vortrag von Kirsten Bock und Malte Engeler auf der FIfFKon 2018 mit Blick auf die EU-Datenschutzgrundverordnung gezeigt hat: Obwohl es Einigungen auf einen gemeinsamen Gesetzestext gibt, bleibt die Frage extrem umstritten, was die Einzelregelungen jeweils bedeuten, wie sie also auszulegen sind.

Hinzu kommt an vielen Stellen und immer häufiger, sowohl in der Öffentlichkeit wie in Gesetzen, die Forderung, privacy oder Datenschutz in Technik umzusetzen, ob als *Privacy by Design*, *Datenschutz by Design* oder *Privacy-Enhancing Technologies*. Was ich in meiner Arbeit festgestellt habe, ist, dass auch die Debatten um eine technische Umsetzung des Datenschutzes schon seit mindestens den 1960er Jahren laufen. So zeigt sich etwa, dass die heute verbreitet zu hörende Forderung, dass *privacy* oder Datenschutz schon in frühen Phasen der Technikentwicklung mit einzubeziehen sei, bereits im Jahr 1965 erhoben wurde (Baran 1965) – sehr weit, so scheint es, sind wir damit also noch nicht gekommen.

Forschungs- und Erkenntnisinteresse

Mein Forschungs- und Erkenntnisinteresse hat sehr viel damit zu tun, dass es sich um ein im Wesentlichen ungeordnetes Feld handelt: Ich habe untersucht, wie historisch eine Menge von Problemen konstruiert wurde, Probleme, die je nach Theorieschule oder -strömung wahlweise als *privacy*-, *surveillance*- oder Datenschutzprobleme bezeichnet werden, und wie dann jeweils Antworten, Verfahren und Techniken konstruiert wurden, die diese identifizierten Probleme beseitigen oder vermeiden sollen. Ich habe analysiert, welche Akteure in diesen Theorien und Debatten jeweils betrachtet wurden und werden – und welche nicht –, welche Beziehungen zwischen den Akteuren unterstellt wurden und werden, welche Interessen, Eigenschaften, Kenntnisse oder Fähigkeiten ihnen jeweils zugeschrieben – oder gerade ausgeblendet – wurden und werden, wie deren Informationsverarbeitung und Entscheidungsfindung adressiert wurde und wird, welche Rolle dabei jeweils informationstechnischen Systemen zugeschrieben wurde und wird, und welche Folgen sich daraus ergeben sollen – für Individuen, Gruppen, Organisationen, Institutionen oder die Gesellschaft insgesamt. Darauf aufbauend habe ich untersucht, wie auf der Basis der Problemidentifikation, die eine Konstruktion des Problems ist, dann jeweils identifiziert wird, wie gerade dafür dann passende Lösungen – und dabei vor allem auch Lösungen in Technik – aussehen sollen. Auf der Basis dieser Analysen konnte ich dann ermitteln, was davon aus informatischer Sicht überhaupt oder überhaupt noch haltbar ist, und was daraus für die Gestaltung informationstechnischer Systeme gelernt werden kann.

Seit mehr als fünfzig Jahren beschäftigt sich die Informatik mit diesem Thema. Die ersten dezidiert informatischen Beiträge dazu sind Mitte der 1960er Jahre erschienen (siehe etwa die Beiträge in Rector 1965). Dennoch diskutieren wir immer noch und immer wieder über die gleichen Grundlagen und Grundfragen. Das liegt nicht zuletzt daran, dass es eine relativ schwache theoretische Basis gibt. In der Informatik wird dann sehr gerne einfach irgendetwas – irgendeine Theorie oder auch nur ein Theoriefragment – herausgegriffen, das zum Objekt der technischen Umsetzung gemacht wird. Am Ende sind die Beteiligten ganz stolz darauf, dass sie die Umsetzung beweisen können. Das ist absurd: Angesichts der Vielzahl untereinander umstrittenen Vorstellungen davon, worum es gehen soll, eine Theorie oder einen Ansatz herauszugreifen – beliebig und ohne jede Begründung – und dann stolz zu verkünden, diese seien beweisbar umgesetzt. Informatisch lässt sich das so reformulieren: Wir nummerieren die Theorien und Vorstellungen einfach durch, von 1 bis n. Dann wählt jemand *privacy7* und baut dafür Technik, das heißt eine „*Privacy7*-Enhancing Technology". Aber niemand hinterfragt die Behauptung, dieses System stelle zugleich eine Lösung für *privacy3* oder für *privacy11* dar …

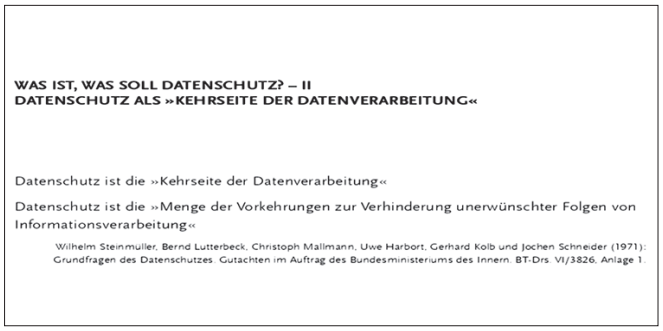
Der Schwerpunkt meiner Arbeit lag dabei auf dem Verständnis von Datenschutz, wie es historisch vor allem in Deutschland und vor allem in den 1970er Jahren im Umfeld der damaligen Rechtsinformatik, oder besser: Rechtskybernetik, konzeptualisiert wurde. Das hatte nicht zuletzt auch einen großen Einfluss auf die ursprüngliche Architektur des Datenschutzrechts. Personen, an die in diesem Zusammenhang zu erinnern lohnt, sind etwa Wilhelm Steinmüller, Adalbert Podlech – beide waren etwa auch Kläger gegen das Volkszählungsgesetz –, Herbert Fiedler oder Klaus Lenk.

Was ist, was soll Datenschutz?

Die wichtigste Erkenntnis der Vorarbeiten aus den 1970er Jahren lautet, dass eine informatisch fundierte Analyse der individuellen und gesellschaftlichen Auswirkungen moderner, automationsgestützter, zunehmend automatisierter und tendenziell industrialisierter Informationsverarbeitung ausgehen muss von den realen Informationsverarbeitungsprozessen, -praxen und -techniken in Organisationen und der Gesellschaft. Und zumindest damals wurde Datenschutz nicht einfach nur als Schutz von Privatheit verstanden, sondern als „Kehrseite von Datenverarbeitung", nämlich als „Menge der Vorkehrungen zur Verhinderung unerwünschter Folgen von Informationsverarbeitung" (Steinmüller u. a. 1971). Dabei handelt es sich um ein dezidiert politisches Programm, formuliert von der Gruppe um Wilhelm Steinmüller 1971 im *Gutachten Grundfragen des Datenschutzes* für das Bundesministerium des Innern. Diese Zielvorstellung geht weit über das hinaus, was heute unter Labels wie *privacy*, *Privatheit* oder *surveillance* diskutiert wird. Es geht um den Schutz von Einzelnen wie von gesellschaftlichen Gruppierungen, es geht aber auch um den Schutz staatlicher oder gesellschaftlicher Institutionen, etwa des Parlaments oder der kommunalen Selbstverwaltung, der Demokratie, des Rechtsstaats oder des Sozialstaats, denn als unerwünscht kann jede Folge von Informationsverarbeitung gelten, die den Zielen der Gesellschaft zuwiderläuft, Zielen, die wir uns als Gesellschaft gesetzt haben, etwa im Grundgesetz, der Europäischen Menschenrechtskonvention oder in der EU-Grundrechtecharta. Es geht, wie Wilhelm Steinmüller es am Ende seines Lebens formulierte, nicht um Privatsphäre, sondern um die gesellschaftliche Kontrolle von Technik (siehe das Video-Interview Rost und Krasemann 2009). Es geht ebenso um Öffentlichkeit; es geht um den Schutz der Öffentlichkeit vor „Verdatung" (Dammann 1974). Es geht, wie die Arbeit zeigt, um die politische Deliberation, es geht um das Funktionieren aller anderen autonomen gesellschaftlichen Bereiche oder Subsysteme, die jeweils eigene Funktionslogiken haben, um die Unterwerfung unter die Funktionslogiken derjenigen, die die Technik, die Technikgestaltung und den Technikeinsatz kontrollieren (dazu zusammenfassend Pohle 2018, S. 249 ff.). Es geht auch nicht nur um personenbezogene Daten, denn es ist keineswegs besser oder wünschenswerter, wenn Grundrechte oder Grundfreiheiten oder Rechtsstaat und Demokratie mit anonymen oder statistischen Daten verletzt werden (ausführlich zum problematischen Umgang mit Personenbezug und Anonymität von Informationen S. 171 ff.). Es geht auch nicht nur um Daten, sondern auch um Prozesse, also organisationseigene Entscheidungsprogramme, oder Interaktions- und Entscheidungsarchitekturen wie User Interfaces, kurz: alles, was der Welt „entnommen" und in Modelle verwandelt wird, die dann in die Technik „gesteckt", also eingeschrieben, werden (früh schon Fiedler 1975, siehe dazu auch den Beitrag von Guagnin & Pohle in Ausgabe 1/2019 der *FIfF-Kommunikation*).

Was ist also das (abstrakte) Bedrohungsmodell, das dem Datenschutz zugrunde liegt? Erstens geht es darum, Informationsmacht unter Kontrolle zu bringen. Informationsmacht erwächst etwa aus der Verstärkung der Fähigkeit zur Kontrolle oder Beeinflussung individueller, kollektiver und institutioneller Betroffener und ihrer Kommunikationen, Entscheidungen und Handlungen (Pohle 2018, S. 247 ff.). Es geht zweitens darum zu verhindern, dass es zu Rationalitätsverschiebungen zugunsten derjenigen kommt,

die die Technik gestalten oder einsetzen (S. 249 f.). Organisationen bedrohen die – die moderne, funktional differenzierte Gesellschaft prägende – Trennung zwischen gesellschaftlichen Subsystemen oder Feldern mit Kontexten und ihren jeweils spezifischen Eigenschaften und Eigenlogiken, weil sie diese ihrer eigenen Organisationslogik unterwerfen (S. 250 f. sowie ausführlich Rost 2008). So produziert etwa Facebook nicht einfach Öffentlichkeit, sondern eine Öffentlichkeit nach Facebooks Vorannahmen und Vorgaben. Und drittens gilt es zu verhindern, dass es zu Kontingenzverlust für Betroffene kommt: indem Organisationen Entscheidungsarchitekturen gestalten und Handlungsmöglichkeiten prästrukturieren (Lenk 1982), indem sie auf der Basis der Vergangenheit, wie sie sich in den zugrunde gelegten Information, d. h. Modellen, widerspiegelt, in der Gegenwart über Zukunft disponieren (Luhmann 1990). Sie fesseln damit an die Vergangenheit, wie sie von den Organisationen selbst erzeugt wurde, und blockieren Möglichkeiten für Betroffene, sich in der Zukunft anders zu entscheiden (so schon früh Podlech 1972).



Datenschutz heißt also, informationell begründete soziale Macht in der Informationsgesellschaft unter Bedingungen zu stellen, sie zu zwingen, sich zu verantworten, und sie damit – wieder oder überhaupt erst einmal – gesellschaftlich verhandelbar zu machen. Die Funktion des Datenschutzes besteht darin, dass kontingente Sozialstrukturen sich auch unter den Bedingungen der zunehmenden „Industrialisierung der gesellschaftlichen Informationsverarbeitung" (Steinmüller 1981) und gegen die überlegene „Strukturierungsmacht" (Rost 2014) von Organisationen reproduzieren können.

Vorgehensmodell und analytisches Framework

Eine allgemeine „Lösung" des Datenschutzproblems kann es ebenso wenig geben wie ein allgemeines, gleichwohl stets passgenaues, Bedrohungsmodell. Das abstrakte Bedrohungsmodell muss immer auf den konkreten Kontext zugeschnitten werden, in dem das zu gestaltende System eingesetzt werden soll, denn konkrete Bedrohungen lassen sich nur anhand konkreter Informationssysteme identifizieren. Daher bedarf es eines prozeduralen Operationalisierungsansatzes, der dieses Zuschneiden leistet, der es erlaubt, darauf basierend konkrete, materielle Anforderungen abzuleiten und für die Systemgestaltung nutzbar zu machen (ausführlich zu Angreifer-, Bedrohungs- und Vorgehensmodell Pohle 2018, S. 257 ff.). Überprüfbarkeit ist dabei nur dann gegeben, wenn die Zwischenprodukte transparent gemacht werden müssen – das sind nachfolgend die Anwendungsbereichsbestimmung, die Akteursanalyse sowie die Interessen-, Zweck- und Machtanalyse.

Im ersten Schritt ist der Anwendungsbereich des zu gestaltenden oder des zu prüfenden Verfahrens oder – im Rahmen von Technikgestaltung oder Technikprüfung – des informationstechnischen Systems festzulegen oder zu bestimmen.

Im zweiten Schritt sind die beteiligten oder zu beteiligenden AkteurInnen zu identifizieren und zu beschreiben. Dazu zählen nicht nur die Organisation und deren MitarbeiterInnen, „Verdatete" (Steinmüller 1988) und eventuelle Dritte, sondern gerade auch relevante Teilgruppen, also etwa Admins oder einfache UserInnen als klassische Typen von MitarbeiterInnen, Gruppen von Betroffenen nach den unterschiedlichen Risiken, denen sie ausgesetzt sind, oder AngreiferInnen nach ihren ökonomischen, politischen oder anderen Interessen. Für diese AkteurInnen ist dabei zu identifizieren, in welchen Rollen sie auftreten. Damit sind nicht nur die gesellschaftlich konstruierten Rollen wie Individuum, Subjekt, Familienmitglied, BürgerIn, KundIn, PatientIn oder MandantIn für Menschen – als Personenkonzepte – oder Behörde, Unternehmen oder Presse für Organisationen gemeint, sondern auch die konkreten Handlungsrollen wie TechnikgestalterIn, Admin, AnbieterIn, NutzerIn, in denen sie jeweils miteinander und mit der Technik interagieren. Anhand dieser Rollen lassen sich dann sowohl gesellschaftlich geprägte Erwartungen und gesellschaftlich konsentierte Interessen identifizieren und zuweisen, also die Freiheits- und Partizipationsversprechen der modernen bürgerlichen Gesellschaft und sogar ihre Strukturschutzprinzipien und -mechanismen, wie auch individuelle oder kollektive Erwartungen und Interessen der jeweiligen AkteurInnen. Anschließend sind die Zwecke zu identifizieren, die die AkteurInnen jeweils verfolgen, gleich ob es interpersonale, politische, ökonomische oder andere Zwecke sind.

Im dritten Schritt sind daher die Interessen und Zwecke zueinander in Beziehung zu setzen und zu analysieren vor dem Hintergrund, in welchem Verhältnis die AkteurInnen zueinander stehen, vor allem in welchem Machtverhältnis, und inwieweit sie voneinander abhängig sind, etwa von der Erbringung einer spezifischen Leistung wie der Bereitstellung einer Kommunikationsinfrastruktur für die Kommunikation mit anderen. In dieser Interessen-, Zweck- und Machtanalyse muss deutlich werden, inwieweit die Interessen und Zwecke der unterschiedlichen AkteurInnen einander entsprechen, kompatibel sind oder einander widersprechen, welche Interessen und Zwecke nur durchgesetzt oder erreicht werden können, wenn andere AkteurInnen kooperieren, von welchen AkteurInnen Kooperation zu erwarten ist und von welchen nicht. Darüber hinaus ist zu analysieren, welche Folgen sich für die Machtbeziehungen zwischen den AkteurInnen ergeben oder ergeben können, wenn AkteurInnen ihre Interessen und Zwecke auch gegen die Interessen und Zwecke anderer AkteurInnen durchzusetzen in der Lage sind. Anschließend sind diese Interessen und Zwecke zu gewichten und zu bewerten, um darauf basierend zwischen den widerstreitenden Interessen und Zwecken abzuwägen. Datenschutz steht dabei konsequent aufseiten der strukturell schwächeren AkteurInnen und schreibt sich die Durchsetzung ihrer Interessen gegen die Interessen der ungleich mächtigeren Organisationen auf die Fahne, und in diesem Sinne sind auch Gewichtung, Bewertung und Abwägung vorzunehmen.

Im Systementwicklungsprozess darf erst an dieser Stelle die eigentliche Zwecksetzung für das zu entwickelnde System vorge-

nommen werden, damit sie selbst zum diskutierbaren Teil der das System definierenden Vorentscheidungen wird. Damit wird zugleich das Problem der Zweckspezifizierung lösbar, also die Frage, wie abstrakt oder konkret, wie weit oder eng der Zweck festzulegen ist. Die Entscheidungsheuristik lautet dann: Je divergenter die Interessen und Zwecke sind, desto konkreter muss der Zweck spezifiziert werden. Je asymmetrischer das Machtverhältnis ist, desto enger muss der Zweck definiert werden.

Die anwendungsbereichsspezifische Bedrohungsanalyse stellt den vierten Schritt dar und dient der Erzeugung des konkreten, anwendungsbezogenen Bedrohungsmodells, indem sie das abstrakte Bedrohungsmodell (das umfassend dargestellt wird in Pohle 2018, S. 260 ff.) vor dem Hintergrund der vorherigen Analysen spezifiziert, und der Ableitung von materiellen wie prozeduralen Anforderungen.

Erst auf dieser Basis lässt sich dann für die identifizierten Bedrohungen entscheiden, wie informationstechnische Lösungen zu gestalten sind, welche existierenden informatischen Artefakte – Frameworks, Module, Codefragmente – dabei für die konkreten Bedrohungen geeignete Lösungen sind und darum ausgewählt werden sollten – und welche nicht –, und welche Anforderungen sich für den Einsatz dieser Systeme ergeben, also etwa auch, welche nicht informatisch lösbaren Anteile der Probleme durch das soziale Umsystem, in das die Informationstechnik jeweils eingebettet ist, gelöst werden müssen.

Literaturverzeichnis

Baran, Paul (1965), „Communications, computers and people". In: Proceedings of the November 30–December 1, 1965, fall joint computer conference, part II: computers: their impact on society. AFIPS '65. New York, NY: ACM. 45–49.

Dammann, Ulrich (1974), „Strukturwandel der Information und Datenschutz". In: Datenverarbeitung im Recht 3 (3/4): 267–301.

Fiedler, Herbert (1975), „Datenschutz und Gesellschaft". In: GI – 4. Jahrestagung, herausgegeben von D. Siefkes. Berlin: GI / Springer. 68–84.

Gallie, Walter Bryce (1956), „Essentially Contested Concepts". In: Proceedings of the Aristotelian Society, New Series, 56: 167–198.

Lenk, Klaus (1982), „Information Technology and Society". In: Microelectronics and Society. For Better or for Worse. A Report to the Club of Rome, herausgegeben von Günter Friedrichs und Adam Schaff. Oxford: The Club of Rome, Pergamon Press. 273–310.

Luhmann, Niklas (1990), „Risiko und Gefahr". In: Soziologische Aufklärung: Konstruktivistische Perspektiven, Band 5. Opladen: Westdeutscher Verlag. 131–168.

Mulligan, Deirdre K., Koopman, Colin und Doty, Nick (2016), „Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy". In: Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences 374 (2083). DOI: 10.1098/rsta.2016.0118.

Podlech, Adalbert (1972), „Verfassungsrechtliche Probleme öffentlicher Informationssysteme". In: Datenverarbeitung im Recht 1: 149–169.

Pohle, Jörg (2018), „Datenschutz und Technikgestaltung: Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung". Dissertation, Mathematisch-Naturwissenschaftliche Fakultät, Humboldt-Universität zu Berlin. DOI: 10.18452/19136. URL: https://edoc.hu-berlin.de/handle/18452/19886.

Rector, Robert W. (Hrsg.) (1965), Proceedings of the November 30–December 1, 1965, fall joint computer conference, part II: computers: their impact on society. AFIPS '65. New York, NY: ACM.

Rost, Martin (2008), „Gegen große Feuer helfen große Gegenfeuer – Datenschutz als Wächter funktionaler Differenzierung". In: vorgänge, Nr. 4: 15–26.

Rost, Martin (2014), „Neun Thesen zum Datenschutz". In: Fundationes I: Geschichte und Theorie des Datenschutzes, herausgegeben von Jörg Pohle und Andrea Knaut. Münster: Monsenstein und Vannerdat. 37–44.

Rost, Martin und Krasemann, Henry (2009), Interview mit Wilhelm Steinmüller. Interviews zur Geschichte und Programmatik des Datenschutzes in Deutschland. URL: https://www.datenschutzzentrum.de/interviews/steinmueller/.

Steinmüller, Wilhelm (1981), „Die Zweite industrielle Revolution hat eben begonnen – Über die Technisierung der geistigen Arbeit". In: Kursbuch 66: 152–188.

Steinmüller, Wilhelm (Hrsg.) (1988), Verdatet und vernetzt. Sozialökologische Handlungsspielräume der Informationsgesellschaft. Frankfurt am Main: Fischer Taschenbuch Verlag.

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

Jörg Pohle

Dr. **Jörg Pohle** ist PostDoc am Alexander von Humboldt Institut für Internet und Gesellschaft in Berlin, wo er das Forschungsprogramm *Daten, Akteure, Infrastrukturen* coleitet und sich unter anderem mit gesellschaftlichen Aushandlungen im Bereich Privacy, Surveillance, IT-Sicherheit und Datenschutz befasst. Sein Forschungsinteresse gilt dem Schnittbereich von Informatik und Recht, dem Feld Informatik und Gesellschaft, der Modellifizierung und ihren gesellschaftlichen Auswirkungen sowie dem Datenschutz durch Technikgestaltung.

Jörg Pohle studierte Rechtswissenschaft, Politikwissenschaft und Informatik in Berlin. Seine Diplomarbeit beschäftigte sich mit der Sicherheit von und dem Sicherheitsdiskurs zu Wahlcomputern. Er promovierte bei Wolfgang Coy an der Humboldt-Universität zu Berlin über Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung.