Martin Rost

Zur Soziologie des Datenschutzes

Dieser Artikel erinnert an den produktiven Diskurs der 1970er Jahre zu Datenschutz und Privatheit, der zu dessen erfolgreicher Institutionalisierung, Verrechtlichung und instruktiver Kommentierung geführt hatte. Nach dieser Würdigung werden Komponenten aktueller Gesellschaftstheorien vorgestellt, die für die anstehende Fortentwicklung des Datenschutzes in der EU nützlich sind. Ein auf Wirkung bedachtes Recht muss den Vorgang der sozialen Konstruktion von „Privatsphäre" sowie die konkreten Bedingungen des Wandels bei ihrer Verteidigung zutreffend erfassen.

1 Problemaufriss

Es waren die gesellschaftstheoretisch orientierten Diskussionen über Datenschutz und Privatheit der 1970er Jahre, in denen die wesentlichen Komponenten des Datenschutzrechts zusammengetragen und kondensiert wurden. So finden sich die wirkmächtigen Grundsätze des Datenschutzes – das Verbot, personenbezogene Informationen für unbestimmt bleibende Zwecke zu erheben, die Zweckbindung der Datenverarbeitung, das Verbot der „sektorenübergreifende Informationskontrolle" oder auch der Direkterhebungsgrundsatz – in einem gesellschaftstheoretisch ausgerichteten Aufsatz bei Podlech (1976a). Man hatte damals insbesondere die Datenbanken der öffentlichen Verwaltung, Sicherheitsbehörden und Sozialversicherungen vor Augen, um deren Auswirkungen auf die Grundrechte zu erörtern. Die Beiträge zeichneten sich dadurch aus, dass sie empirische Befunde gesellschaftstheoretisch, angereichert von der Kybernetik als allgemeiner Steuerungstheorie (vgl. Simitis 1964, Luhmann 1966, Podlech 1967), analysierten und neue rechtliche Anforderungen formulierten. Erste gründliche Vorschläge zur rechtlichen Umhegung des Computers wurden dann im Datenschutzgutachten von 1971 formuliert, das allerdings zunächst weitgehend unbeachtet blieb (Steinmüller et al. 1971). Die Entwicklung eines Datenschutzrechts war auf diese rechtsexternen Impulse zur Problemformulierung mit Vorschlägen für Lösungen angewiesen.[1]

Damals wurden Definitionen zum Datenschutz vorgelegt, deren Bedeutungsumfang man heute vielfach erst wieder mühsam rekonstruieren und zurück gewinnen muss. Datenschutz war schon frühzeitig und klar von Datensicherheit (Backup, Verschlüsselung, Integritätsschutz…) und dem unmittelbaren Schutz der Privatsphäre geschieden: „Danach ist Datenschutz die Gesamtheit der (artifiziellen, gewollten) Restriktionen und Verpflichtungen beim Umgang mit Daten zum Schutz gesellschaftlich anerkannter Zielsetzungen (‚Interessen')." (Fiedler 1976: 182).[2]

Derartige Einsichten, Begründungen und Anforderungen fanden 1979 ihren Niederschlag im Bundesdatenschutzgesetz und 1983 im Volkszählungsurteil, sowie konsolidiert vor allem im BDSG-Kommentar (Simitis 2011) und dem Alternativkommentar des Grundgesetzes (Denninger et al. 1989). Im Alternativkommentar zu den Artikeln 1 und 2, die die für die Begründung des Volkszählungsurteils wesentlichen Argumentationsfiguren enthalten, findet sich die folgende soziologisch ungewöhnlich gehaltvolle Passage: „Privatheit ist keine Sache des isoliert gedachten Individuums, die durch Kommunikation mit anderen, die durch einen Sozialbezug verloren geht. Privatheit ist eine mögliche Eigenschaft des Umgangs mit anderen. Die **Gemeinschaftsbezogenheit** in der Formulierung des Bundesverfassungsgerichts ist daher **Grund des Grundrechtsschutzes** des Art. 2 Abs. 1, nicht Grund der Eingriffsbefugnisse des Staates." (Podlech 1989: 266). (...) „Weil Menschen in Gesellschaftsbezügen stehen, die durch *Machtdifferenzen* bestimmt sind, ist der *Grundrechtsschutz* unentbehrlich, um den Konsens mit der die Gesellschaft formenden Rechtsordnung zu ermöglichen." (Podlech 1989: 273). Der gesellschaftstheoretisch zentrale Bezugspunkt für Datenschutzaktivitäten, der vor dem Datenschutzrecht liegt, weil das Recht bereits eine Reaktion auf den Machtkonflikt darstellt, ist demnach die *Konditionierung asymmetrischer Machtbeziehungen,* – und wir ergänzen die nachfolgenden Ausführungen vorwegnehmend – *die spezifisch zwischen Organisationen und Personen im Kontext einer funktional differenzierten Gesellschaft vorliegen*. Akzeptiert man diesen Ausgangspunkt zur Analyse von Datenschutzkonflikten, dann hat das konzeptionelle Folgen.

1 Vgl. zur Entwicklung des Datenschutzes: Wiederin 2003, Lewinski 2009, Simitis 2011. Ich bedanke mich bei Jörg Pohle für die nimmermüde Bereitschaft zu Diskussionen über Theoriegeschichte des Datenschutzes sowie bei Kirsten Bock, Dr. Michael Schack und Wolfgang Zimmermann für die kritische, cokonstruktive Durchsicht dieses Beitrags.

2 Fiedler warnt in seinen weiteren Ausführungen zudem davor, dass der Computer nicht zum „Sündenbock von in Wahrheit sozialen Konflikten" gemacht werden sollte. Was sicher auch für die Rede über „die Risiken des Internet" gilt.

Martin Rost

Mitarbeiter im Referat „Systemdatenschutz" beim Unabhängigen Landeszentrum für Datenschutz (ULD) in Kiel.

E-Mail: martin.rost@datenschutzzentrum.de

Eine dieser Folgen besteht darin, dass die „informationelle Selbstbestimmung" des Individuums sich nicht trivialliberal gedacht durch monadische Isolierung noch am ehesten einstellen kann und sich eines anthropologischen Bedürfnisses nach Privatheit verdankt.[3] Solche Konstrukte bilden keinen angemessenen Ausgangspunkt für die Begründung von Datenschutz. Denn faktisch kann sich Selbstbestimmbarkeit erst dann einstellen, wenn die Machtkonstellationen, denen eine Person in der Gesellschaft ausgesetzt ist, unter wirksamen Bedingungen steht.. Die Gesellschaft mit ihren Organisationen ist immer schon vorher da. Selbstbestimmung kann nur angestrebtes Ziel nicht aber bezugslos-axiomatischer Ausgangspunkt sein.

Geht es stattdessen um die Konditionierung von Macht und um Handlungsalternativen derjenigen, die sich auf der schwachen Seite der Asymmetrie befinden, so können weder die Selbstregulation auf Seiten der Organisationen noch die „Einwilligung" als die wichtigsten Regelungskomponenten des Datenschutzrechts herhalten.[4] Etwa mit der Idee, dass sich gerade in der Einwilligung als einseitig vorgegebenem Vertrag die Souveränität des Einzelnen besonders deutlich manifestiere.[5] Das überschätzt die Macht der Person und verschleiert die Macht der Organisationen. Sobald Organisationen etabliert sind, verfolgen sie Eigeninteressen und haben weder an Märkten, Demokratie und Gewaltenteilung noch an freien Diskursen Interesse.

Vielmehr muss zunächst die Frage beantwortet sein, wer tatsächlich empirisch ermittelbar die Macht über die reale Ausgestaltung von personenbezogenen Verfahren und wer die größeren Chance im Abwälzen von Risiken hat, so dass zunächst immer infrage steht, ob auf der schwächeren Seite überhaupt *Handlungsalternativen* bestehen. Der Hinweis auf ein Privatrechtsverhältnis reicht keinesfalls aus, um die Behauptung, es handele sich allein deshalb um ein symmetrisches Machtverhältnis zu stützen.[6]

Der heutige Problemdruck, den Datenschutz fortentwickeln zu müssen, ist aufgrund der Machtfülle auf Seiten der IT nutzenden Organisationen zweifelsfrei enorm.[7] Man darf vermuten, dass dieser Problemdruck des Unterlaufens der Grundrechte insbesondere durch die Polizei in den 1970er Jahren jedoch nicht geringer war. Damals waren in Deutschland, in einer historisch einmaligen Konstellation, die Erinnerungen an Nazidiktatur und Stalinismus noch hellwach und es standen die zeitgenössischen Provokationen des Rechtsstaates durch Aktivitäten der DDR sowie insbesondere durch die RAF-Anschläge vor Augen. Die Anschläge – sowie nicht zu vergessen: die hohen Sicherheitsanforderungen beim Betrieb von Atomkraftmeilern und bei den Auseinandersetzungen etwa zu den Vorhaben um Brokdorf, Wackersdorf usw. – verschafften den staatlichen Sicherheitsbehörden die Legitimation, um die längst auf einen Anwendungsfall wartenden neuen technischen Handlungsoptionen zur Rasterfahndung auf Basis zentraler Datenbanken mit bis dahin unbekannter Wirksamkeit zu nutzen. Entsprechend klare Maßstäbe für gelingenden Datenschutz wurden seitens der Datenschützer der 1. Generation genannt: „Eine Datenschutzregelung ist nur so gut, wie sie das Problem der Geheimdienste regelt. (...) Kann man es als die Hauptaufgabe des Datenschutzes bezeichnen, einen Gesellschaftszustand zu verhindern, in dem ein Bürger nicht wissen kann, wer wann was zu welchem Zweck über ihn weiß, so ist einer der Hauptregelungsgebiete des Datenschutzes der Geheimdienstbereich." (Podlech 1976a: 32)

In dieser konfliktgeladenen Situation kamen 1979 ein Bundesdatenschutzgesetz[8] und 1983 ein weitsichtiges Urteil zustande. Diese erzeugten einen zunehmend wirksameren Schutz der Grundrechte der Bürger, insbesondere im öffentlichen Bereich. Bis zum Aufkommen der massenhaften Nutzung des Internet spätestens 1995.[9]

Mit der Nutzung des Internet sind Organisationen weltweit in der Lage, aber strukturell auch gezwungen, die Informationsverarbeitung von Personendaten nicht nur zu technisieren, sondern zu industrialisieren. Die Grundlage dieser noch einmal beschleunigten Industrialisierung bilden per Internet und Mobilfunk vernetzte Rechner sowie ubiquitäre Sensorik. Entscheidend ist, dass mit dem Begriff der Industrialisierung mehr als nur Technisierung gemeint ist, nämlich die vorausliegende Standardisierung von Arbeitsteilung mit der Folge organisationsnützig gebildeter und dann technisiert bearbeitbarer Normfälle. Es sind die Organisationen, die die Technikentwicklung bestimmen und mit Motiven aufladen.

Historisch betrachtet geht die Industrialisierung organisierter Produktions- und Geschäftsprozesse mit einer Explikation latenter sozialer Konflikte einher; seien diese Konflikte gesellschaftlicher Art entlang von Arbeit und Kapital, wie bekanntlich Marx/Engels darlegten, oder ökologischer Art (vgl. Radkau 2011). Und das weltweit, worauf das Recht bislang nicht reagieren kann (vgl. Spieker 2012: 719). Trotz manifester Konflikte können die Industrialisierungspioniere deshalb noch eine zeitlang mit ganz außerordentlich hohen Gewinnen rechnen, bis die Regulierung struktureller Konflikte einsetzt, zu denen politische Aktivitäten und nationale rechtsstaatliche Mittel bereitstehen oder entwickelt werden müssen.[10] Zugleich können Organisationen heute kontrollierter denn je Vorstellungen und Argumentationsmuster manipulieren mit dem Ziel, ihre Einzelinteressen als Allgemeininteressen erscheinen zu lassen.[11] Der wesentliche Unterschied der Si-

3 So aber Capurro et al. 2012.

4 Siehe dazu den Beitrag von Kamp / Rost in diesem Heft.

5 So aber Buchner 2006.

6 Die Schwierigkeiten im Datenschutzrecht, sinnvolle Regelungen aus dem öffentlichen Bereich auch im privaten Bereich zu nutzen, sind Schwierigkeiten, die sich aus dem Zuschnitt des Rechts und dessen Begründungszusammenhang, nicht aber aus der Andersartigkeit des Konflikts oder des Regelungsgegenstands ergeben.

7 Neuerdings werden Datenschutzkonflikte auch wieder als Machtkonflikte thematisiert, vgl. z.B. http://www.zeit.de/2012/46/Deutsches-Datenschutzgesetz-Spiekermann/seite-1.

8 Die empirische Untersuchung von Liedtke legt den Verdacht nahe, dass das BDSG mit seinen besten Regelungskomponenten nur deshalb zustande kam, weil seitens der Industrie einer bestimmten Ausschusssitzung nicht genügend Aufmerksamkeit geschenkt wurde (vgl. Liedtke 1980). Aktuelle Thesen zum Datenschutzrecht finden sich bspw. bei Dix (2012), kritisch: Hoeren (2011), abschätzig: Schneider (2011).

9 Der deutsche Datenschutz-Jurist Podlech weist in einem Interview darauf hin, dass mit dem Aufkommen des Internet ein genuin neues Datenschutzrecht geschrieben werden muss, das zu schreiben er sich in den 1990ern aber nicht mehr in der Lage sah (Podlech 2009).

10 Der Industrietheoretiker Karl Marx formulierte eine solche Phase bekanntlich als die der „ursprünglichen Akkumulation des Kapitals". Heute denkt man dabei konkret vornehmlich an die einseitige Ausbeutung der Internet-Allmende und die Enteignung von IT-Geräten insbesondere durch facebook, google, amazon, apple, IBM oder Microsoft, die ihrerseits von staatlichen Behörden in Dienst genommen werden (können) (vgl. Adamnek 2011). Zur Illustration der Macht und Gewinne am Beispiel von facebook und google: Spiegel 2011/49, 2012/19, 2012/43 sowie zur datenschutzrechtlichen Analyse Weichert 2012.

11 So tragen Menschen heute freiwillig und begeistert Überwachungssensorik in Form mobiler devices wie das iPhone oder Android-Handies bei sich, die neben der jederzeitigen Lokalisierung auch die Überwachung der Inhalte von Kommunikationen oder Informationsverarbeitungen erlauben, bis hin zum Vorausahnen möglicher Bedürfnisse der Nutzer. So die Aufgabenstellung des

tuation des Datenschutzes in den 1970er Jahren zu der Situation heute lässt sich klar mit zwei Punkten markieren:

a) Es gibt eine *Datenschutzaufsicht*. Die Aufgabe dieser Aufsicht besteht im Prüfen von Organisationen. Skandalöse Formen der Datenverarbeitung werden öffentlich angeprangert (vgl. Schaar 2007). Seit Anfang 2000 sehen sich Datenschützer außerdem in der Lage, Beratungen und Auditierungen von Verfahren oder Komponenten durchzuführen.[12]

b) *Technik* kann auch einen *Beitrag zur Sicherung von Privatheit* leisten. Anfang der 1990er setzten verstärkt Bestrebungen ein, aktiv gestaltenden Einfluss im Sinne einer „Technikgestaltung durch Recht" (vgl. Roßnagel 1993) zu nehmen. Computer können Personen Schutz vor nicht legitimen Zugriffen durch Organisationen bieten, wenn Computer tatsächlich der Verfügungskontrolle des nutzenden Eigentümers unterliegen. Dies war die grundlegende Einsicht bei der Entwicklung der Privacy-Enhancing-Technologies („PET").[13] Zur Mitte 2000 fand PET im Konzept des „user-controlled identity-management" eine erste technische Konsolidierung (vgl. Hansen 2008, Pfitzmann / Hansen 2010). Der rechtliche Absicherungsanker wurde 2008 über das „Integritätsurteil" des Bundesverfassungsgerichts gesetzt. Und um 2010 herum war mit den „neuen Schutzzielen" (Rost / Pfitzmann 2009) und deren Einarbeitung in ein „Standard-Datenschutzmodell" ein systematischer Rahmen für standardisierbare Prüf- und Beratungstätigkeiten der Datenschutz-Aufsichtsbehörden gefunden (vgl. Rost 2012).

PET macht anonyme oder verkettungssichere Kommunikation über das Internet möglich und gibt technische Lösungen für Probleme an die Hand, die eine moderne Gesellschaft mit dem Internet als universeller Verkettungsmaschine an neuralgischen Stellen hat. So ist gesicherte Anonymität unabdingbar etwa für die Möglichkeit von korrekten Preisvergleichen auf Märkten, für freie politische Wahlen für die Filterung wissenschaftlicher Beiträge oder damit Menschen Hilfe auch in sozial besonders prekären Situation erhalten.[14]

Die mit der Internetnutzung massenhaft gemachte Erfahrungen, dass private PCs Angriffen von Hackern ausgesetzt sind, hat zu einer Perspektivverschiebung des Datenschutzfokus geführt: Nicht mehr eine grundschutzgerechte Gestaltung der personenbezogenen Verfahren in Organisationen, sondern die private Abwehr von Angriffen auf den eigenen PC mit dessen wertvollen Datenbeständen oder den besonders komfortablen Möglichkeiten des sicheren Einkaufens und Bankings, schiebt sich paradigmatisch dominant vor Augen. Selbst viele Datenschützer sehen sich kaum mehr in der Lage, sinnvoll zwischen Datenschutz, Privatheitsschutz (privacy) und Datensicherheit zu unterscheiden. Entsprechend unberechenbar können Stellungnahmen sogar von Datenschutz-Aufsichtsbehörden ausfallen.

Das „Privatheitsparadox" besteht deshalb nicht darin, dass Personen Smartphones bei sich tragen oder Dienste wie Facebook und Google nutzen, obwohl sie wissen, dass sie dadurch in historisch bislang unbekannter Perfektion bespitzelt und fremdbestimmt werden.[15] Dass Personen mit Organisationen interagieren, die Personen existentiell gefährlich werden können und denen sie sich trotzdem ausliefern (müssen), gehört zum schlichten Alltagswissen spätestens seit der Schule. Die Leistungen „gefährlicher" Organisationen, etwa des Staates, der Banken und Versicherungen, der Energieunternehmen und Kommunikationsdienstleister sind ganz ohne Zweifel existentiell unverzichtbar. Wenn man dem Begriff „Privatheitsparadox" einen Sinn abgewinnen möchte dann stattdessen dafür, dass von einem nur individualisierten „Schutz von Privatheit" keine hinreichende Schutzwirkung für Personen gegenüber Organisationen ausgeht.[16] Es geht selbst dann keine Schutzwirkung aus, wenn Organisationen nur mit anonymisierten Daten rechnen, die für die einzelne Personen zunächst kein Risiko darstellen, daraus jedoch Personentypologien und Scoringmodelle generiert werden, die den realen Person als Personenschemata zur Grundlage der Datenverarbeitung und Kommunikationen übergestülpt werden. Die datenschutzrechtlich maßgebliche Frage ist, ob diese Personenschemata mit den Konzepten vom Bürger, Kunden, Individuum kompatibel sind.

Privatheit kann deshalb nur entstehen, wenn Organisationen personenbezogene Daten ausschließlich auf Fairness bedacht eng zweckbestimmt und vor allem sektorenspezifisch erheben und verarbeiten. Wieder lohnt ein Blick in die Diskussionen der 1970er Jahre. Denn auch diese Einsicht, dass Privatheit erst aus Datenschutz entsteht, lag bereits vor.[17] Da stellte der Soziologe Paul J. Müller fest, der frühzeitig über Erfahrungen mit der computergestützten Auswertung von Massendaten in den USA verfügte, dass „die Privatsphäre das *Ergebnis selektiver Informationsweitergabe an verschiedene Instanzen*. ist. (...) die Vorstellung einer Schneckenhaus-Privatsphäre als Zielvorstellung – obwohl selbst nur als defensiv gedacht – schützt gerade das nicht, was sie zu schützen meint: die Autonomie der Individuen." (Müller 1975: 107). Knapp 30 Jahre später lautet der Befund zur Schutzwirkung des Privatssphären-Konzepts: „(...) dass die Figur einer impermeablen Sphäre ein Mythos ist und dass Bürgerinnen und Bürger eine solche Sphäre weder haben noch brauchen, weil sich die Zulässigkeit staatlicher Informationseingriffe ausnahmslos nach dem Zweck beurteilt, dem der Eingriff dient, und nicht nach der Sphäre, aus der die Information stammt (...)". (Wiederin 2003: 53) An dieses Reflexionsniveau zum Datenschutz gilt es wieder anzuschließen, um Datenschutz im erweiterten Kontext einer Internet basierten Industrialisierung der Datenverarbeitung weiter entwickeln zu können.

Nachfolgend wird mit Hilfe der Theorie sozialer Systeme nach Luhmann verständlich, wie es in der Moderne zum Datenschutzkonflikt kam, wie er sich seitdem wach hält und was unter „sozialer Konstruktion von Privatheit" zu verstehen ist. Dadurch wird deutlich, warum die Datenschützer der ersten Generation den Datenschutzkonflikt noch nicht auch theoretisch hinreichend scharf stellen konnten. Anschließend wird vorgeschlagen, die Schutzziele des Datenschutzes als Zielvorgaben für eine industrialisierte Datenverarbeitung zu nutzen, wobei deren Umsetzung die Voraussetzung dafür ist, dass die „Geltungsanforderungen an eine vernünftige Rede" (Habermas) auch bei technisch vermittelter Kommunikation einlösbar werden. Dadurch entsteht ein zum

Netzdienstes „google now" auf Android-Basis (zu den Nutzerzahlen: BVDW 2012). Man fühlt sich, selbst ohne polemische Absicht, an die Vision von Horst Herold, dem Präsidenten des BKA zwischen 1971 und 1981, erinnert, wonach die Polizei durch gute IT-Unterstützung noch vor dem Täter am Tatort sein könnte.

12 Erfahrungsbericht zum europäischen Datenschutzgütesiegel EuroPrise siehe Meissner 2011.

13 Es ist an John Borkings „Identity Protector" zu erinnern.

14 Der Aufwand zur Herstellung von Anonymität ist erheblich, weil Nutzer insbesondere vor denjenigen Organisationen zu schützen sind, die Anonymität als Programm oder Dienstleistung herzustellen versprechen (vgl. Rost 2003).

15 So aber Buchmann 2012: 8

16 So bereits formuliert von Wiederin 2003: 55.

17 Widersprechend: Gräf 1993.

Persönlichkeitsrecht komplementärer, genuin soziologischer Begründungszusammenhang für Datenschutz.

2 Soziale Systeme

Die deutsche Soziologie institutionalisierte sich Ende des 19. Jahrhunderts erfolgreich durch die Stabilisierung eines wissenschaftlichen Diskurses entlang der Differenz von „Gemeinschaft und Gesellschaft" (Tönnies 2010). Der zeitgenössische französische Beitrag zur Konstitution der Soziologie bestand im methodischen Postulat, dass das Soziale als eine „Realität sui generis" systemisch zu analysieren und „Soziales nur durch Soziales" zu erklären sei (Durkheim 1992). Wesentlich an diesen beiden Konzepten ist die Distanzierung von Spekulationen über „den Menschen", der mit überhistorischen, biologischen und psychischen Bedürfnissen ausgestattet wird, die sich für beliebige Verwendungszwecke dann wieder aus „dem Menschen" heraus zaubern lassen. Die moderne Soziologie unterscheidet drei Sozialsystemtypen, nämlich Interaktionssysteme, Organisationssysteme und Funktionssysteme. Und sie kann auf die Vorstellung verzichten, dass es Menschen sind, die Sozialsysteme bilden (vgl. Luhmann 1999). Soziale Systeme erzeugen als Realität sui generis ihre eigenen Komponenten in einer fortlaufenden Unterscheidung zwischen System und Umwelt mit systemeigenen Mitteln. Diese „autopoietisch" reproduzierten Komponenten des Sozialen sind Kommunikationen.[18]

Für eine Theorie des Datenschutzes ist diese Unterscheidung von drei Sozialsystemtypen deshalb bedeutsam, weil damit drei unterschiedliche Inklusions-/ Exklusionsmuster für „Personen"[19] und ihre Verpflichtung auf Rollen verbunden sind. Mit dieser Differenzierung sieht man sich bspw. in der Lage, systematisch die Achtung der Privatsphäre eines Mitarbeiters oder eines Kunden durch ein Unternehmen von der Achtung der Privatsphäre eines Kindes durch die Eltern oder von Mitarbeitern durch den Arbeitgeber zu unterscheiden. Luhmann zeichnet nach, wie die Umstellung der Sozialsystemstruktur, von stratifizierter Struktur auf funktionale Differenzierung in verschiedene Funktionssysteme (Politik, Recht, Wirtschaft, Kunst), mit der Ausbildung moderner Konzepte der Individualität einhergeht (Luhmann 1989: 195f). Es entstanden Personenkonzepte, die man heute als Bürger, Kunden, Nutzer, Patienten/ Petenten/ Mandanten/ Klienten, Menschen, Individuum und Subjekt bezeichnet. Diese Personenkonzepte sind mit Imaginationen und Versprechen für „Freiheit" und dem Anspruch auf rollenbezogenen „Respekt" aufgeladen, die sich aus den Funktionssystemen der Gesellschaft ableiten. Dazu gleich noch etwas mehr.

Organisationen konkretisieren diese Personenkonzepte in zunehmend industrialisierten Formen und reduzieren mit den dabei eigennützig gebildeten Normfällen die Freiheitsgrade der Personen. Die Personenkonzepte sind anspruchsvoll, weshalb deren Explikation im Zuge der Industrialisierung personenbezogener Verfahren konfliktgeladen ist. Der Bürger gilt einerseits als der Souverän des Staates, andererseits ist er dem staatlichen Gewaltmonopol und den Gesetzen und Verfahren unterworfen. Der Kunde gilt als freier Nutzen-/Kosten-Optimierer, dessen entsprechend rationale Präferenzen durch verführerische Werbung und Verhandlungstricks beeinflusst werden dürfen, auf emotionale Wirkungen abzielende Fremdbestimmung gilt als legitim. Oder: Der Mensch gilt als vernunftbegabt und sich seiner Interessen bewusst, aber als triebgeleitet. Und bei Organisationsmitgliedern wie dem Soldaten als „Bürger in Uniform", darf man es noch weniger genau wissen wollen, wie es um deren Souveränität als freier Bürger einer Gesellschaft steht, das als Mitglied einer Organisation in den Tod geschickt wird darf.

Knapp formuliert: Datenschutz nimmt heute die modernen Konzepte vom Bürger, Kunden und selbstbestimmten Individuum auf und reproduziert diese Figuren entlang der permanent reproduzierten Differenz von Funktionssystemen und Organisationssystemen. Datenschutz institutionalisierte sich im Zuge der Verarbeitung personenbezogener Daten, in denen diese Personenkonzepte von Organisationen typisiert, standardisiert, technisiert und automatisiert bearbeitbar wurden.

2.1 Interaktionssysteme

Interaktionssysteme reproduzieren sich anhand von Kommunikationen unter (Fern-)Anwesenden. Das Konzept der Privatheit greift im Umfeld von Interaktionssystemen in Form von „Gemeinschaft" kaum. Vielmehr gelten insbesondere Familien als Bereiche, in denen man privat sein darf, Privatheit auslebt und in seinen Ambivalenzen authentisch und somit besonders schutzlos gegenüber Fremdbestimmungen ist (vgl. Wiederin 2003: 39f). Entsprechend sind solche Vorstellungen, die die Konstitution des Sozialen ausschließlich aus den willkürlich „gewollten" Interaktionen zwischen anwesenden Menschen entstehen lassen, zu unterkomplex für die Konstitution einer modernen Weltgesellschaft. Interaktionstheorien bekommen mit ihren begrifflichen Mitteln deshalb auch das Datenschutzproblem gar nicht hinreichend scharf gestellt in den Blick. Wenn Privatpersonen einander formal auf Augenhöhe begegnen und keine strukturell bedeutsame Machtasymmetrie besteht, spielt Datenschutz keine Rolle.

Gleichwohl ist es jedoch vorwiegend dieser Sozialsystemtypus, der in sozialwissenschaftlich inspirierten Überlegungen zum Datenschutz die Basis für Erwägungen bildet. Das gilt für die eingangs zitierten, besten Passagen der soziologischen Argumentation bspw. von Podlech ebenso wie für die Argumentation des Bundesverfassungsgerichts (vgl. Becker 1996). In einer aktuellen Studie zu „Privacy im Internet" stellen die Autoren (Ochs / Löw 2012) unter Berufung auf Solove (2006) zunächst einmal fest, dass zur Bestimmung von Privatheit zwar viele politologische und philosophische Texte insbesondere der liberalen Tradition, aber keine überzeugend ausgearbeiteten sozialwissenschaftlichen Konzepte und Begrifflichkeiten vorliegen[20] Um trotzdem weiter über Privatheit forschen zu können, bearbeiten sie ohne nennenswertes Ergebnis die Differenz von privat/öffentlich und ziehen dann vor allem mit Simmel und Goffman zwei soziologische Klassiker zu Rate, die als Interaktionstheoretiker vornehmlich die Wechselwirkungen von Menschen untereinander untersuchen. Man kann von diesen Autoren viel über privates Leben, aber nichts über Datenschutz lernen. Zum Schluss versammelt die Studie zwar einen durchaus problembewussten Katalog mit Anforderungen, der sich aber, methodisch wenig überraschend, nicht aus der Analyse der Meinungen über Privatheit ableiten

18 Zur Einführung in die soziologische Systemtheorie siehe Kneer/Nassehi 1999. Zu Datenschutz und Funktionssysteme: Rost 2008.

19 Zum Konzept der Person siehe Luhmann 1995 sowie insbesondere Fuchs 2007.

20 „Die begriffliche Erfassung des Privatlebens macht notorische Schwierigkeiten". (Wiedern 2003: 50)

lässt und zudem diese Anforderungen nicht hinreichend konkret und spezifisch zugespitzt adressieren kann. Für eine moderne Theorie des Datenschutzes ist die Analyse von Interaktionssystemen insofern vorerst wenig instruktiv.

2.2 Funktionssysteme

Funktionssysteme der Gesellschaft reproduzieren sich entlang „symbolisch generalisierter Kommunikationsmedien", die binäre Schematismen ausgebildet haben. So hält das Medium Geld, in die Form von Preisen gebracht, die fortlaufende Unterscheidung von Zahlungen/Nichtzahlung auf Märkten im ökonomischen System aufrecht. Gesetze und Verordnungen entscheiden über Recht/Nichtrecht im Rechtsystem, politische Programme über politische Macht/Nichtmacht im Politiksystem, beide Systeme sind im Konzept der Gewaltenteilung aufeinander bezogen. Und Theorien und Methoden entscheiden über wahre/falsche Aussagen im Wissenschaftssystem. Strukturell ist entscheidend, dass diese Funktionssysteme nur jeweils sich selbst reproduzieren, aber nicht auf die anderen Sozialsysteme durchgreifen. Diese Funktionssysteme verfügen dabei über systemintern geformte Risikoquellen: Märkte (Wirtschaft), Demokratie und Gewaltenteilung (Politik und Recht) und selbstregulativ-freie Diskurse (Wissenschaft und Kunst). Die Geschlossenheit der Systeme ist ein wesentliches Charakteristikum der „funktionalen Differenzierung".

Für Datenschutz ist das Verständnis der funktionalen Differenzierung der Systeme deshalb wichtig, weil es zu verstehen hilft, dass der Kauf von Wählerstimmen in einer Demokratie oder von Entscheidungen auf gesetzlicher Grundlage dysfunktional ist. Und wenn dies trotzdem geschieht, wird das als ein nicht akzeptables Problem formulierbar. Und: Funktionssysteme bilden die übergeordnete Nomenklatur, an der sich die Formulierung spezifischer Zwecke von Datenverarbeitung ausrichten kann.

Zum zweiten wird die Entstehung von Individualität durch Funktionssysteme für Datenschutz verstehbar. Personen sind nur situativ-punktuell sozial gekoppelt, etwa durch den Akt der Zahlung oder durch die Akzeptanz und Beachtung gesetzlicher Regelung im Straßenverkehr oder durch die Akzeptanz oder geäußerte Zweifel an einem Argument oder einer Beobachtung. Man spricht nicht, man zahlt. Gesellschaftliche Funktionssysteme erzeugen punktuell eine enorme Fülle an Anregungen, Anforderungen, Themen, Aktivitätsmustern, Schemata, Skripte, die durch ihre bloße Kombinatorik auf Personen eine individualisierende Wirkung entfalten (vgl. Luhmann 1993). Es entsteht zugleich der Zwang für Personen, sich an den Märkten für Produkte zu orientieren, in den politischen Programmen die eigenen Interessen wiederzuerkennen oder mit widerstreitenden wissenschaftlichen Expertisen Kindererziehung, Ernährungs- oder Gesundheitsstrategien zu bewältigen.[21] Die moderne Gesellschaft erzeugt mit ihren Funktionssystemen massenhaft einen „Zwang zur Individualisierung" (vgl. Meutert 2002). Sie fordert Personen „informationelle Selbstbestimmung" als digital anschlussfähiges Selbstmanagement strukturell ab. Selbstbestimmung muss nicht erst „der Gesellschaft" irgendwie abgerungen werden, wie noch der Anarchismus oder Liberalismus des 19. Jahrhunderts argumentierte (vgl. Rössler 2001), sondern den Organisationen.

Organisationen versuchen stets, die Risiken des Marktes, der Demokratie und Gewaltenteilung sowie der freien ästhetischen und wissenschaftlichen Diskurse, kurz: der funktionalen Differenzierung, zu minimieren und auf schwächere Risikonehmer, und das sind Einzelpersonen, abzuwälzen. Konventioneller formuliert: Wirtschaftsunternehmen neigen *strukturell gezwungen* – und das ist keine Frage von Moral oder persönlicher Integrität des Führungspersonals –, zur Monopolbildung, staatliche Organisationen zur Dominanz der Exekutive, Wissenschaftsinstitute zur Verödung von Diskursen. Und je mehr effektive Technik dafür eingesetzt wird, desto effektiver funktioniert die Risikoabwälzung auf Personen.

2.3 Organisationssystem und Industrialisierung

Organisationssysteme reproduzieren sich anhand von Kommunikationen über Entscheidungen, insbesondere auch über Entscheidungen zu Mitgliedschaften von Personen. Sie sind von den drei Sozialsystemtypen die einzigen, die adressierbar sind. Deshalb können Organisationen Erwartungen bzw. Anforderungen an Adressen, also an andere Organisationen und Personen, formulieren. Die gesellschaftliche Funktion von Organisationssystemen besteht darin, Arbeit zu organisieren und bei gesellschaftlicher Arbeitsteilung Motive (Geld) bereit zu stellen, so dass auch unattraktive, nicht unmittelbar zur Befriedung führende aber gesellschaftlich notwendige (Teil-) Arbeiten zuverlässig ausgeführt werden. Diese Arbeiten kristallisieren über Konditional- und Zweck-Programme zu Ereignisabfolgen aus, die von Techniken unterstützt werden, die sinnfällig als „Industrieprozesse" ausgeprägt sind. Industrialisierung ist gekennzeichnet durch Standardisierung und Modularisierung, Technisierung und letztlich Automatisierung von Prozessen.

In Bezug auf Datenschutz führt die Industrialisierung der Erhebung und Verarbeitung von personenbezogenen Daten zur Typisierung von Personenmodellen. Organisationen müssen mit der Automatisierung „die Karten auf den Tisch legen", wie sie es denn nun tatsächlich und konkret mit dem Bürger, dem Kunden, dem Patienten, dem Individuum bei personenbezogenen Verfahren halten.[22] Und Automatisierung offenbart Verwertungsinteressen, die nicht an Fairness orientiert durchgesetzt werden. Das gilt nicht nur für Privatorganisationen, sondern auch für den Staat.[23]

Es ist dabei zu konstatieren, dass die synthetische Leistung von Organisationen zugleich gesellschaftlich unverzichtbar ist. Diese funktionale Trennung von differenzierten Sozialsystemen, für deren Zusammenwirken es keinen Masterplan gibt, heben Organisationen auf. Organisationssysteme regulieren das Zusammenwirken der Sozialsysteme. Sie leisten insofern den wesentlichen Beitrag zur gesellschaftlichen Synthese (vgl. Lieckweg 2001). Für den Datenschutz hat das zur Folge, dass es immer nur darum gehen kann, einen kompromissbehafteten Arbeitspunkt im Ver-

21 Facebook und google bieten nicht nur eine Kommunikationsplattform bzw. ein Portfolio hoch-interessanter Netzdienstleistungen, sondern sie lassen eine Strategie des „technisch gestützten Life-Managements" (Christian Krause) erahnen.

22 Ausführlicher zur Industrialisierung der Personenschemata: Rost 2012a.

23 Zwar mögen die Verfahren bspw. im Meldewesen oder Personenstandswesen grundrechtlich einwandfrei ausgerichtet sein und bspw. nur wirklich erforderliche Datenfelder enthalten. Doch der jederzeitige Zugriff auf Bürger und deren Profilierungen im Sicherheitsfalle kann, im Umweg über privat vorgehaltene Datenbestände, mit anderen Mitteln als einer Recherche in einer Meldedatenbank geschehen, Stichwort: Strafrechtsverfolgung bei facebook. Es gibt insofern keinen Anlass für Entwarnung bzgl. der staatlichen Überwachungsaktivitäten, sie werden heute auch privat finanziert (vgl. Kamp 2007).

hältnis zwischen ebenso gefährlichen wie unverzichtbaren Organisationen und Personen zu finden.

Diese Notwendigkeit zur Synthese verführt im täglichen Geschäft Organisationen natürlich, nicht nur regelkonform mit ihren Optionen umzugehen. Organisationen kommen auf die Idee – eine solche „Idee" drängt sich strukturell schlicht auf – bspw. als „wissenschaftlich" ausgeflaggte Gutachten zu kaufen, um sie für politische Zwecke in einem Gerichtsverfahren einzusetzen. Aber das wird, wie bereits angedeutet, erst auf dem Niveau funktionaler Differenzierung zum Problem und thematisierbar. Das permanente Risiko der Aufhebung von getrennten Funktionsvorgängen durch Organisationen beschreibt die latente Problemlage moderner Gesellschaften, zu deren Bearbeitung sich Datenschutz herausgebildet hat. Datenschutz soll genau die Kurzschlüsse bei funktionalen Trennungen verhindern. Sinnfällig werden solche „Pathologien" im Umgang der Organisationen mit Personen.

2.4 Kriterien vernünftiger Kommunikation

In der „Theorie des kommunikativen Handelns" weist Jürgen Habermas „Geltungsanforderungen für eine vernünftige Rede" aus (Habermas 1981). Diese Theorie besagt, wiederum nur knapp angedeutet, dass bei einer Kommunikation immer zumindest drei Geltungsansprüche gestellt werden: Nämlich dass das Kommunizierte sachlich wahr ist, dass es den zutreffenden sozialen Rollenbezug beachtet und dass es etwas mit dem Sagenden selbst im Sinne der Wahrhaftigkeit zu tun hat. Wenn der Verdacht entsteht, dass diese Geltungsansprüche zu Unrecht unterstellt werden – also dass etwas falsch dargestellt wird oder gelogen wurde –, dann setzen kommunikative Reparaturaktivitäten ein: Man lässt sich das Gesagte erläutern, versucht unaufgedeckte Interessen oder Logikbrüche zu ergründen. Wichtig an dieser Figur ist der Aspekt, dass Kommunikationen strukturelle Anforderungen beinhalten, so dass Kommunikationen überhaupt stattfinden, aufhören und wieder neue Kommunikationen entstehen, die als sinnvoll oder gar als vernünftig gelten können.

Nun der Schwenk zum Datenschutz und den technisch-organisatorischen Maßnahmen: Kommuniziert wird heute auf der Basis von Kommunikationstechniken (Telefon, Brief, E-Mail, Datenbanken, PC, Web-Server, Router, Kommunikationsprotokolle, Verzeichnisdienste, Betriebssysteme, Glasfaser usw. usw.). Die Technik darf die oben genannten Anforderungen nicht unterlaufen, damit Kommunikation qualitativ als gelungen wahrnehmbar wird. Die Kommunikationstechniken und die für deren Betrieb notwendigen Organisationen müssen die Mitteilung transportieren und die Daten verarbeiten, ohne dadurch semantisch Einfluss zu nehmen. Und ob dies hinreichend der Fall ist, muss sowohl für die Organisationen selber als auch für die Betroffenen und die Aufsichtsinstanzen, als die Vertreter des gesellschaftlichen Allgemeininteresses, kontrollierbar sein. Nur unter diesen Bedingungen können die Ansprüche an eine vernünftige Rede gelten und etwaige Reparaturstrategien durchgeführt werden.

Dass über die Geltungsanforderungen an eine vernünftige Rede hinaus gehende Anforderungen auch an die verwendete Kommunikationstechnik zu stellen sind, konnte Habermas Ende der 1970er Jahre noch nicht hinreichend klar formulieren, so wie es aufgrund der Erfahrungen mit dem Internet heute möglich ist. Die These lautet, dass die sechs „elementaren Schutzziele" des Datenschutzes – nämlich die Sicherung der Verfügbarkeit, Integrität und Vertraulichkeit, der Transparenz, Intervenierbarkeit und Nicht-Verkettbarkeit – die wesentlichen datenschutzrechtlichen Anforderungen der Transparenz, der Zweckbindung, Erforderlichkeit und Datensparsamkeit sowie der Umsetzung von Betroffenenrechten systematisch verdichten und operationalisieren (vgl. Rost / Pfitzmann 2009, Rost / Bock 2011).. Sie formulieren damit die Anforderungen an Organisationen, die diese bei der Nutzung von Technik für personenbezogene Verfahren erfüllen müssen, damit gesellschaftlich notwendige Kommunikation gelingen kann (vgl. Rost 2012a).

Mit dieser Perspektive wird ein Begründungszusammenhang für Datenschutz freigelegt, der nicht wie bislang ausschließlich auf das Persönlichkeitsrecht bzw. Grundrechte des Einzelnen sondern auf die Kompatibilität der von Organisationen genutzten Verfahren mit den qualitativen Anforderungen an gelingende Kommunikation abstellt.

3 Fazit

Die Industrialisierung der personenbezogenen Verfahren in den Organisationen gefährdet das bisherige „Erfolgsmodell" der funktionalen Differenzierung in Funktionssysteme der Wirtschaft, Politik, Recht und Wissenschaft. Es ist dieses Setup der Funktionssysteme, das die Konzepte der „informationellen Selbstbestimmung", „Individualität", „Freiheit" oder „Privatssphäre" von Personen, als Bürger, Kunde, Patient, Individuum, konstituiert. Deshalb muss Datenschutz normativ, operativ und strategisch so ausgerichtet sein, dass er Funktionssysteme stärkt und den durchindustrialisiert agierenden Organisationen die Umsetzung von Schutzzielen abringt. Andernfalls wälzen Organisationen die sozialen Risiken der heutigen ökonomisch dominierten Weltgesellschaft faktisch unbegrenzt auf Personen ab, mit der Folge, dass Privatorganisationen sich anschicken, sich für allzuständig auszugeben und „in sich" Gesellschaft zu simulieren. Das bedeutete eine Regression der gesellschaftlichen Sozialstruktur wieder auf eine nur stratifizierte Stufe.

Die in den 1970er Jahren kondensierten Grundsätze der Datenverarbeitung und datenschutzrechtlichen Anforderungen an Organisationen haben deshalb nichts von ihrer Berechtigung und Aktualität verloren. Schutzziele verdichten, systematisieren und standardisieren diese Anforderungen und geben diesen eine methodisch und operativ zugängliche Form. Dadurch genügen sie den operativen Anforderungen durchindustrialisierter Organisationen in einer funktional-differenzierten Risikogesellschaft.

Literatur

Adamnek, Sascha, 2011: Die facebook-Falle, Heyne-Verlag.

Becker, Ulrich, 1996: Das Menschenbild des Grundgesetzes in der Rechtsprechung des Bundesverfassungsgerichts, Berlin: Duncker & Humblot.

Buchmann, Johannes (Hrsg.), 2012: > Internet Privacy – Eine multidisziplinäre Bestandsaufnahme, acatech Deutsche Akademie der Technikwissenschaften.

Buchner, Benedikt, 2006: Informationelle Selbstbestimmung im Privatrecht, Tübingen, Mohr Siebeck.

BVDW 2012: Mediascope 2012 – Fokus Mobile.

Capurro, R. / Eldred, M. / Nagel, D., 2012: IT And Privacy From An Ethical Perspective – Digital Whoness: Identity, Privacy And Freedom In The Cyberworld, in: Buchmann, Johannes (Hrsg.), 2012: Internet Privacy: 63-142.

Denninger, Erhard / Ridder, Helmut / Simon, Helmut / Stein, Ekkehart, 1989: Kommentar zum Grundgesetz für die Bundesrpublik Deutschland, Band 1, Luchterhand.

Dix, Alexander, 2012: Thesen auf dem DJT 2012: 70f.

Durkheim, Emile, 1984: Regeln der soziologischen Methode, Frankfurt: Suhrkamp (erstmals erschienen: 1895).

Fiedler, Herbert, 1976: Datenschutz und Gesellschaft, in: Steinmüller, Wilhelm (Hrsg.), 1976: Informationsrecht und Informationspolitik, München, Wien, R. Oldenbourg-Verlag: 179.

Fuchs, Peter, 2007: Das Maß aller Dinge – Eine Abhandlung zur Metaphysik des Menschen, 1. Auflage, Velbrück.

Gräf, Lorenz, 1993: Privatheit und Datenschutz, Dissertation an der philosophischen Fakultät der Universität Köln.

Habermas, Jürgen, 1981: Theorie des kommunikativen Handelns – Band 1: Handlungsrationalität und gesellschaftliche Rationalisierung, Band 2: Zur Kritik der funktionalistischen Vernunft –, Frankfurt am Main, Suhrkamp.

Hansen, Marit, 2008: Marrying Transparency Tools with User-Controlled Identity Management; in: Fischer-Hübner et. al., 2008: The Future of Identity in the Information Society, Springer US: 199-220.

Hansen, Marit; Pfitzmann, Andreas, 2010: A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability.

Hoeren, Thomas, 2011: „Wenn Sterne kollabieren", in: „Zeitschrift für Datenschutz" 2011, Nr. 4: Editorial

Kamp, Meike, 2007: Unternehmen – Hilfsbeamte der Sicherheits- und Finanzbehörden? Vortrag auf der Sommerakademie 2007 (verfügbar unter www.datenschutzzentrum.de).

Kneer, Georg / Nassehi, Armin, 2000: Niklas Luhmanns Theorie sozialer Systeme, 4. Auflage, UTB.

Lewinski, Kai, 2009: Geschichte des Datenschutzrechts von 1600 bis 1977; in: 48. Assistententagung Öffentliches Recht: Freiheit Sicherheit Öffentlichkeit, Nomos.

Liedtke, Werner, 1980: Das Bundesdatenschutzgesetz – Eine Fallstudie zum Gesetzgebungsprozess, Dissertation an der LMU München.

Lieckweg, Tanja, 2001: Strukturelle Kopplung von Funktionssystemen „über" Organisation, in: Soziale Systeme – Zeitschrift für soziologische Theorie, Jahrgang 7, Heft 2: 267-289.

Luhmann, Niklas, 1965: Grundrechte als Institution: Ein Beitrag zur politischen Soziologie, Berlin, Duncker & Humblot.

Luhmann, Niklas, 1966: Recht und Automation in der öffentlichen Verwaltung.

Luhmann, Niklas, 1993: Individuum, Individualität, Individualismus; in: Gesellschaftsstruktur und Semantik, Band 3, Frankfurt am Main: Suhrkamp.

Luhmann, Niklas, 1995: Die Form Person, in: Soziologische Aufklärung. Band 6, Opladen, Westdeutscher Verlag: S. 142-154.

Luhmann, Niklas, 1999: Gesellschaft der Gesellschaft, Frankfurt am Main: Suhrkamp.

Lutterbeck, Bernd, 2009: Interview, www.maroki.de/pub/video/lutterbeck/start_video_lutterbeck.html

Meissner, Sebastian, 2011: Datenschutzgütesiegel als vertrauensbildende Maßnahme am Beispiel des europäischen EuroPrise-Zeichens, in: Bogendorfer, R. J. (Hrsg.), 2011: Datenschutzgespräche 2011, Jan Sramek Verlag.

Meuter, Norbert, 2002: Müssen Individuen individuell sein?; in: Straub, Jürgen / Renn, Joachim (Hrsg.): Transitorische Identität – Der Prozesscharakter des modernen Selbst, Frankfurt, New York: Campus: 187-210.

Müller, Paul J., 1975: Funktionen des Datenschutzes aus soziologischer Sicht; in: Datenverarbeitung im Recht 1975: 107ff.

Ochs, Carsten / Löw, Martina: Unfaire Informationspraktiken: Internet Privacy aus sozialwissenschaftlicher Perspektive; in: Buchmann, Johannes (Hrsg.), 2012: Internet Privacy: 15-62.

Podlech, Adalbert, 1967: Anforderungen der Kybernetik an die Rechtswissenschaft; in: Recht und Politik: 84-87.

Podlech, Adalbert, 1976; Gesellschaftstheoretische Grundlage des Datenschutzes, in: Dierstein, Rüdiger / Fiedler, Herbert / Schulz, Arno (Hrsg.), Datenschutz und Datensicherung, Köln 1976: 311-326.

Podlech, Adalbert 1976a: Aufgaben und Problematik des Datenschutzes, in: Datenverarbeitung im Recht 5: 23-39.

Podlech, Adalbert, 1982: Individualdatenschutz – Systemdatenschutz, in: Brückner, K. / Dalichau, G. (Hrsg.), 1982: Beiträge zum Sozialrecht, Festgabe für Hans Grüner, Percha:: 451-462.

Podlech, Adalbert, 1989: Die Grundrechte, Art. 2 Abs.1: in: Denninger et al..

Podlech, Adalbert, 2008: Interview, www.maroki.de/pub/video/podlech/start_video_podlech.html

Roßnagel, Alexander, 2012: Nutzerschutz, 1. Auflage, Baden-Baden, Nomos.

Rössler, Beate, 2001: Der Wert des Privaten, Frankfurt am Main: Suhrkamp.

Radkau, Joachim, 2011: Die Ära der Ökologie – Eine Weltgeschichte, Tübingen, C.H. Beck.

Rost, Martin, 2003: Über die Funktionalität von Anonymität für die bürgerliche Gesellschaft; in: Bäumler, Helmut / von Mutius. Albert (Hrsg.), 2003: Anonymität im Internet, Braunschweig / Wiesbaden: Viewg: 62-72.

Rost, Martin, 2008: Gegen grosse Feuer helfen große Gegenfeuer, Datenschutz als Wächter funktionaler Differenzierung; in: Vorgänge, Heft 4/2008, Nr. 184: 15-25.

Rost, Martin / Pfitzmann, Andreas, 2009: Datenschutz-Schutzziele – revisited; in: DuD – Datenschutz und Datensicherheit, 33. Jahrgang, Heft 6, Juli 2009: 353-358.

Rost, Martin / Bock, Kirsten, 2011: Privacy By Design und die Neuen Schutzziele – Grundsätze, Ziele und Anforderungen; in: DuD – Datenschutz und Datensicherheit, 35. Jahrgang, Heft 1: 30-35.

Rost, Martin, 2012: Standardisierte Datenschutzmodellierung; in: DuD – Datenschutz und Datensicherheit, 36. Jahrgang, Heft 6: 433-438.

Rost, Martin, 2012a: Faire, beherrschbare und sichere Verfahren, in: Kersten, Heinrich. / Peters, Falk / Wolfenstetter, Klaus-Dieter (Hrsg.), 2012: Innovativer Datenschutz, Berlin, Duncker & Humblot.

Roßnagel, Alexander, 1993: Rechtswissenschaftliche Technikfolgenforschung – Umrisse einer Forschungsdisziplin, Baden-Baden, Nomos-Verlag.

Schaar, Peter, 2007: Das Ende der Privatsphäre – Der Weg in die Überwachungsgesellschaft, München, Bertelsmann.

Solove, Daniel J., 2006: A Taxonomy of Privacy, University of Pennsylvania Law Review, Vol. 154, No. 3: 477-560.

Schneider, Jochen, 2011: Hemmnis für einen modernen Datenschutz: Das Verbotsprinzip; in: Anwaltsblatt 2011/ 04.

Simitis, Spiros, 1964: Rechtliche Anwendungsmöglichkeiten kybernetischer Systeme; in: Helmar, Frank (Hrsg.), 1964: Kybernetische Maschinen, Frankfurt am Main: 351-367.

Simitis, Spiros, 2011: Bundesdatenschutzgesetz, 7. Auflage, Nomos.

Spiecker gen. Döhmann, Indra, 2012: Die Durchsetzung datenschutzrechtlicher Mindestanforderungen bei Facebook und anderen sozialen Netzwerken; in: Kommunikation & Recht, Nr. 11/ 2012: 717-725

Steinmüller, W. / Lutterbeck, B. / Mallmann, C. / Harbort, U. / Kolb, G. / Schneider, J., 1971: Grundfragen des Datenschutzes – Gutachten im Auftrag des Bundesinnenministeriums, Drucksache VI/3826.

Tönnies, Ferdinand, 2010: Gemeinschaft und Gesellschaft, Kessinger Publishing (erstmals erschienen: 1887).

Weichert, Thilo, 2012: Datenschutzverstoß als Geschäftsmodell – der Fall Facebook; in: DuD 2012/10: 716-721.

Wiederin, Ewald, 2003: Der grundrechtliche Schutz der Privatssphäre: Eine Entwicklungsgeschichte; in: Peissl, Walter, 2003: Privacy – Ein Grundrecht mit Ablaufdatum? Wien, Verlag der österreichischen Akademie der Wissenschaften.