Jörg Pohle

Zweckbindung revisited

Einleitung

Das datenschutzrechtliche Prinzip der Zweckbindung steht vermehrt unter Beschuss. So hat etwa der ITK-Verband BITKOM gerade erst öffentlich die Abschaffung der Zweckbindung gefordert.[1] Damit steht der Verband keineswegs allein. Im Rahmen einer schriftlichen Anhörung hatte das BMI erst Ende 2014 gemeinsam mit dem BMWi und dem BMJV unter anderem sehr zielgerichtet gefragt, »welche Bedeutung das Erfordernis der Kompatibilität des geänderten Zwecks einer Datenverarbeitung mit dem Erhebungszweck für bestehende und künftige Geschäftsmodelle sowie für die Rechte und Interessen der Betroffenen habe« und »welche Folgen es für diese Geschäftsmodelle sowie für die Betroffenen hätte, wenn eine mit dem Erhebungszweck unvereinbare Zweckänderung aufgrund überwiegender berechtigter Interessen des Datenverarbeiters (Art. 6 Abs. 1 lit. f DS-GVO-E) ausgeschlossen wäre.« Von wenigen Ausnahmen abgesehen, sind die eingegangenen Stellungnahmen bisher nicht veröffentlicht worden – die Ergebnisse der Anhörung sind jedoch umso sichtbarer: Die Innen- und Justizminister der EU-Mitgliedsländer haben im EU-Rat beschlossen, das Zweckbindungsprinzip auszuhebeln.[2]

Vor diesem Hintergrund soll das Zweckbindungsprinzip als Artefakt[3] einer spezifischen Operationalisierung des Datenschutzes im Recht beleuchtet und eingeordnet werden. Dabei sollen nicht nur schlaglichtartig die Genese dieses Rechtsgrundsatzes und seine historischen Begründungen erörtert, sondern auch einer der ihm zunehmend entgegen gehaltenen zentralen Kritikpunkte widerlegt werden – die vermeintliche Veralterung des Zweckbindungsgrundsatzes aufgrund neuerer technischer Entwicklungen, wie sie etwa unter dem Schlagwort »Big Data« zusammengefasst werden.

Die historischen Konstruktionen des Zweckbindungsgrundsatzes

Informierte Einwilligung und Zweckbindung

Der Grundsatz der Zweckbindung hat die moderne information privacy- und Datenschutzdebatte schon seit ihrem Beginn in den 1960er Jahren begleitet.

Die »Special Committee on Science and Law« der New Yorker Anwaltskammer formulierte im Rahmen einer wissenschaftlichen Untersuchung die Anforderungen, denen eine verantwortbare Verhaltensforschung am Menschen zu genügen habe. Der Kommissionsvorsitzende Oscar M. Ruebhausen und der Präsident der Russell Sage Foundation Orville G. Brim, Jr. veröffentlichten die Untersuchungsergebnisse, die sich dem Spannungsverhältnis zwischen wissenschaftlicher Forschung und der »private personality« widmen, Ende 1965 in der Columbia Law Review.[4]

Als eine der wesentlichen Anforderungen identifizieren sie unter Verweis auf die Ergebnisse des Nürnberger Ärzteprozesses die Notwendigkeit eines »fully informed consent, freely given, of the individual person being examined«.[5] Neben einer Diskussion über die notwendigen Eigenschaften der Einwilligung – explizit oder implizit, informiert, freiwillig – stellen die Autoren fest, dass eine Einwilligung immer nur kontext- und zweckbezogen sein könne mit der Folge einer Kontext- und Zweckbindung für den Umgang mit den erhobenen Informationen:

»Moreover, consent to the revelation of private personality for one purpose, or under one set of circumstances, is not license to publish or use the information so obtained for different purposes or under different conditions.«[6]

Die Einwilligung wirke dabei nicht nur hinsichtlich der Kontext- und Zweckdimension einschränkend, sondern auch »to the methods to be used, the risks to be taken, the degree of information the subject wishes to give or receive, the type of data to be obtained, or the uses to which it may be put.«[7]

Einer sehr ähnlichen Begründung bedient sich fünf Jahre später das Bundesverfassungsgericht im Ehescheidungsakten-Beschluss vom 15. Januar 1970.[8] Auch der damalige Bundesminister der Justiz hatte in seiner Stellungnahme an das Gericht auf den »begrenzten Kundgebungszweck« verwiesen, mit dem »Details aus der ehelichen Intimsphäre« in einem Ehescheidungsverfahren vorgetragen würden, nur darauf beziehe sich der »Wille der Beteiligten«. Diese Beschränkung werde »von der Rechtsordnung durch die Bestimmungen über die Nichtöffentlichkeit der Verhandlung und die Amtsverschwiegenheit entsprechend gesichert.«[9] Das Bundesverfassungsgericht folgt in seinem Beschluss dieser Argumentation und stellt fest, dass »die Offenlegung in bezug auf den Adressatenkreis – das Gericht und die Verfahrensbeteiligten – und in bezug auf den verfolgten Zweck – Herbeiführung der Gerichtsentscheidung – inhaltlich begrenzt« sei. Eine Übersendung der Akten für andere Zwecke sei somit ein Eingriff in das Persönlichkeitsrecht der Ehegatten und ohne ihr Einverständnis nur dann zulässig, wenn sie nach dem Verhältnismäßigkeitsprinzip gerechtfertigt sei.[10] Eine solche Rechtfertigung vermochte das Gericht jedenfalls in Bezug auf die disziplinarische Verfolgung von Dienstvergehen nicht zu erkennen.

Das damit verfolgte Ziel ist offensichtlich: Die Einwilligung soll bedeutungsvoll gemacht werden, indem mit der Zwecksetzung – und der darauf aufbauenden Zweckbindung – eine der wesentlichen Eigenschaften von Information und Informationsverarbeitung der Entscheidungsprärogative der Betroffenen unterworfen wird. Die Zweckbindung ist insoweit ein Artefakt der Ent-

scheidung, die Informationserhebung, -verarbeitung und -nutzung von der Einwilligung der Betroffenen abhängig zu machen.

Phasenorientierung und Zweckbindung

In ihrem 1971 für das Bundesministerium des Innern erstellten und 1972 veröffentlichten Gutachten »Grundfragen des Datenschutzes«,[11] dessen dort entwickelte Regelungsarchitektur bis heute das Datenschutzrecht prägt, nicht nur das bundesdeutsche,[12] beziehen sich Wilhelm Steinmüller et al. explizit auf diese Entscheidung des Bundesverfassungsgerichts und die dort formulierte »Zweckentfremdungsregel«, d. h. das »Verbot, Individualinformationen, die für einen bestimmten Zweck ermittelt sind, einem anderen Zweck zuzuführen.«[13] Damit erweitern sie gleichzeitig den Geltungsbereich des Zweckbindungsgrundsatzes: Nicht nur auf Basis einer Einwilligung erhobene personenbezogene Informationen, sondern alle personenbezogenen Informationen dürften ausschließlich zu dem Zweck verarbeitet werden, zu dem sie erhoben wurden.[14]

Die Autoren knüpfen damit direkt an das von ihnen zugrunde gelegte Informationskonzept an[15] und lösen gleichzeitig elegant das Zeitproblem, das sie mit ihrer phasenorientierten Gestaltung des Datenschutzrechts geschaffen haben.

Dieser Operationalisierungsansatz knüpft an einen »tatsächlichen Prozeß [an]; er geht also von einer (zugleich gesellschaftlichen wie „technischen“) Realität aus.«[16] Dieser Prozess ist die Informationsverarbeitung, die »eine typische Struktur aufweist«: »eine regelmäßige Wiederkehr gleicher Zustände des Prozesses der [Informationsverarbeitung]«.[17] An diesen Prozess – den »Ort des Problems« – und seine einzelnen »Phasen« ließen sich dann rechtliche Anforderungen formulieren.[18] Die im Gutachten formulierten und später ins BDSG übernommenen Anforderungen betreffen jedoch jeweils nur eine Phase, nicht jedoch den Prozess insgesamt.[19] Eine der beiden phasenübergreifenden Konstanten, die den ganzen Prozess rechtlich klammern, ist der Zweck, der vor der Erhebung der Information festgelegt wird und an den die verantwortliche Stelle bis zur Informationslöschung gebunden ist. Die andere Konstante ist der Personenbezug: Solange er besteht, muss er gleich bleiben; seine Aufhebung bietet jedoch eine Möglichkeit zur »Flucht aus dem Datenschutzrecht«.[20]

Beide Konzepte – der Personenbezug von Informationen und die Zweckbindung – lassen sich damit deutlich als Artefakte der jeweils zugrunde liegenden Operationalisierungsentscheidungen identifizieren: Die Wahl des Informationskonzepts der Semiotik bietet mit der sigmatischen Informationsdimension eine rechtliche Anknüpfungsmöglichkeit für die bezeichnete Person und ermöglicht es – jedenfalls grundsätzlich –, zu jedem Zeitpunkt während des Informationsverarbeitungsprozesses rechtlich verbindlich festzustellen, wer Rechte gegenüber der verantwortlichen Stelle wahrnehmen darf und wem gegenüber die verantwortliche Stelle begründungs- und nachweispflichtig ist. Und wenn vor dem Hintergrund einer außerhalb des faktischen Herrschafts- und damit Eingriffsbereichs der Betroffenen individuelle Eingriffsrechte und -möglichkeiten geschaffen werden sollen, erfordert das gerade ein Konzept wie den Personenbezug.

Andererseits wird mit der Operationalisierung des Datenschutzes im Recht über die einzelnen Phasen des Informationsverarbeitungsprozesses ein Zeitproblem erzeugt: Die Dauer des Prozesses muss nicht a priori determiniert sein, auch müssen die einzelnen Phasen zeitlich nicht direkt aneinander anschließen. Weil darüber hinaus grundsätzlich alle Bestandteile des Prozesses variabel sind – technische Verfahren und Datenverarbeitungsmittel, die verarbeitende Stelle,[21] deren innere Organisation und die mit der Verarbeitung betrauten Personen u. v. m. –, existiert gerade keine natürliche Konstante als Prüfanker, von dem aus alle anderen Aspekte zu jedem Zeitpunkt während des Informationsverarbeitungsprozesses abgeleitet bzw. nachträglich überprüft werden können. Ein solcher Prüfanker muss demnach explizit konstruiert und in das Recht eingeschrieben werden. Der Personenbezug ist dabei kein für diesen Zweck geeigneter Prüfanker, denn anhand dessen lassen sich weder die eingesetzten Mittel prüfen noch Erhebungs- und Verwendungskontexte. Personenbezug stellt nur die Verbindung zu den subjektiven Rechten her, während die objektivrechtliche Dimension – die »zweite Säule des Datenschutzrechts«[22] – gerade mit dem Zweckbindungsprinzip adressiert wird.

Kontrollierbarkeit und Zweckbindung

Es ist Bernhard Hoffmanns Verdienst, die erste – und bislang einzige – umfassende Analyse der Rolle des Zweckbindungsgrundsatzes in der rechtlichen Operationalisierung, die der Datenschutz im bundesdeutschen Datenschutzrecht gefunden hat, vorgelegt zu haben.[23] In seiner Betrachtung beschränkt er sich allerdings deutlich auf die Erforderlichkeit des Zweckbindungsprinzips für die »Wahrung des ursprünglichen Erhebungskontexts«[24] und insbesondere für die Schaffung »wohlgeordnete[r], transparente[r] und kontrollierbare[r] Strukturen«.[25] Die Rolle des Zweckbindungsgrundsatzes für die Sicherstellung einer bedeutungsvollen Einwilligung der Betroffenen und die Lösung des Zeitproblems des prozeduralen Datenschutzrechtsansatzes bleiben demgegenüber überraschend ausgeblendet.

Einerseits sind Zwecke strukturbildend, sie definieren Bereiche und damit die Grenzen zwischen den Bereichen, die zur Informationsflusskontrolle genutzt werden können.[26] Andererseits dienen sie der Bestimmung der Menge der für die Zweckerreichung, also innerhalb der Bereiche, funktional äquivalenten Handlungsmöglichkeiten und Mittel.[27] Datenschutzrechtlich handelt es sich dabei um die Bestimmbarkeit der Geeignetheit. Die Setzung von Zwecken trennt dabei den Raum aller überhaupt möglichen Handlungen und Mittel sowie ihrer Wirkungen in erwünschte und unerwünschte.[28] Zugleich eröffnet die Zwecksetzung die Möglichkeit, die grundsätzlich erwünschten Handlungsalternativen und Mittel sinnvoll miteinander vergleichen zu können,[29] so etwa zur Unterscheidung zwischen erforderlichen und nicht erforderlichen Handlungen und Mitteln. Auf dieser Basis kann abschließend die Angemessenheit

der Handlungen und Mittel adressiert werden. Mit der Zweckbindung, der »Gewährleistung einer ausschließlich zweckbestimmten Verwendung«,[30] wird dann Kongruenz von Sollen und Sein sichergestellt.

Das Zweckbindungsprinzip ist demnach Mittel zur Erzeugung von Kontrollierbarkeit der Informationserhebung, -verarbeitung und -nutzung sowie der dabei verwendeten technischen wie nicht-technischen Mittel, indem es wohlgeordnete Organisationsstrukturen und Prozesse erzeugt, die zugleich transparent gemacht werden können – den Organisationen selbst, vor allem jedoch den Betroffenen und den Aufsichtsbehörden.

Zweckbindung ist nicht veraltet

Im Ergebnis stellt sich Zweckbindung nicht notwendigerweise als Teil einer Datenschutz- oder information privacy-Theorie dar, sondern in erster Linie als ein Artefakt spezifischer Operationalisierungen und Umsetzungen im Recht. Sie dient als konzeptionelle und operationale Klammer um den Prozess von Informationserhebung, -verarbeitung und Entscheidungsfindung, indem sie als Konstante in einem dynamischen Umfeld wirkt und damit einen festen Anker für die Prüfung sowohl der Handlungen wie der eingesetzten Mittel bietet. Zugleich stellt sie bei hoheitlichen Informationsverarbeitungsprozessen sicher, dass diese grundsätzlich auf die konkrete behördliche Aufgabe beschränkt und die Anforderungen der zur Erhebung ermächtigenden Rechtsgrundlage gewahrt bleibt.[31]

Zwecksetzung ist dabei entweder Fremd- oder Selbstbindung, Zweckbindung ist dessen überprüfbare Einhaltung. Während der öffentliche Bereich durch Fremdbindung in Form von Zweck- und Aufgabenzuweisung geprägt ist, handelt es sich im nicht-öffentlichen Bereich in der Regel um eine Selbstbindung, also im Grunde eine Ausprägung von Selbstregulierung, dafür jedoch mit Compliance-Garantie.

Darüber hinaus war Zweckbindung schon immer kontrafaktisch. Seit der Erfindung der Schrift vor fast 6.000 Jahren durch die Sumerer speichern alle Datenträger, die die Menschheit je erfunden hat, ausschließlich Zeichen. Moderne Datenverarbeitungssysteme wie Computer sind reine Syntaxverarbeitungsmaschinen – Kontext- und Zweckfreiheit sind oft explizite Technikgestaltungsziele;[32] Kontexte und Zwecke den Systemen (wieder) beizubringen ist alles andere als einfach.[33]

Diese Eigenschaft der Multifunktionalität moderner IT-Systeme ist in der Datenschutzdebatte schon lange bekannt.[34] Zweckbindung war gerade die bewusste normative, aber eben auch kontrafaktische Antwort des Rechts auf moderne, grundsätzlich zweckfrei mögliche Informationsverarbeitung.[35] Demnach können Big-Data- und andere Verfahren moderner Informationsverarbeitung dieses normative Instrument auch nicht »einfach veralten« lassen – im Gegenteil: Gerade seine Fähigkeit zur effektiven Beschränkung der Informationsmacht der Datenverarbeiter macht das Zweckbindungsprinzip bei privaten wie öffentlichen Datenverarbeitern und deren jeweiligen Lobbyisten derart unbeliebt.[36]

Die Zukunft der Zweckbindung

Der Datenschutz adressiert das Problem der gesellschaftlichen Machtverteilung und Machtkontrolle unter den Bedingungen der Industrialisierung der gesellschaftlichen Informationsverarbeitung – vergleichbar zum »Problem des Verfassungsstaates im politischen Bereich und […] der Kontrolle der Produktionsverhältnisse im wirtschaftlichen Bereich«[37] – mit seinen Folgen für Mensch und Gesellschaft, Gruppen und Institutionen.[38] Viele überkommene Operationalisierungen gelten grundsätzlich oder in ihrer Umsetzung im Recht jedoch inzwischen als nicht mehr zeitgemäß, etwa der exzessive Fokus des Rechts auf die individuelle Einwilligung,[39] oder werden zu Recht hinterfragt, etwa die Möglichkeit der Grenzziehung beim Personenbezug von Informationen.[40] Vorschläge für alternative Regelungsansätze existieren, etwa unter Verwendung von Schutzzielen,[41] die seit den 1980er Jahren in der IT-Sicherheit erfolgreich eingesetzt werden. Aber lässt sich damit auch das Zweckbindungsprinzip ersetzen?

Als Alternative zur Nutzung der personenbezogenen Information als Anknüpfungsobjekt des Datenschutzrechts ließe sich etwa – wenn die Anbindung an das Individuum und die Möglichkeit zur Festschreibung von Betroffenenrechte beibehalten werden soll – an das Konzept der personenbezogenen Entscheidung rechtlich anknüpfen. Personenbezogene Entscheidungen seien dabei alle sozial relevanten Entscheidungen über Menschen in vermachteten Verhältnissen. Dies würde vor allem das Problem adressieren, dass Organisationen keineswegs – wie es der derzeitige Datenschutzrechtsansatz unterstellt – Menschen nur auf der Basis von Informationen sortieren, kategorisieren, bewerten und über sie entscheiden, die personenbezogen im Sinne des Datenschutzrechts sind, sondern durchaus auch auf der Basis von Gruppen- oder statistischen Informationen.[42] Über den Anknüpfungspunkt der personenbezogenen Entscheidung wären dann alle Informationen, ob personenbezogen oder nicht, die zur Grundlage dieser Entscheidung gemacht worden sind oder gemacht werden sollen, rechtlich adressierbar.[43]

Doch auch der Fokus des Datenschutzrechts auf die Einwilligung der Betroffenen ist nicht alternativlos. Mit dem das Rechtsstaatsprinzip adaptierenden Prinzip des »Systemdatenschutzes« steht längst ein angemessener Ersatz zur Verfügung:

»Systemdatenschutz heißt dann die Menge der Rechtsregeln, die Vorgänge der Informationserhebung oder der Informationsverarbeitung unabhängig davon, ob im Einzelfall Interessen der Betroffenen berührt sind oder nicht, rechtlich so ordnen, daß die Gesamtheit der rechtlich geregelten Informationsvorgänge keine sozialschädlichen Folgen herbeiführen.«[44]

Im Grunde nichts Neues – mit dem BDSG sind schon immer auch nicht-öffentliche Stellen aus dem Rechtsstaatsprinzip folgenden Anforderungen unterworfen;[45] dieser Ansatz wird inzwischen wieder deutlich lauter vertreten.[46]

Selbst die Phasenorientierung als zentrales Element des derzeitigen Datenschutzrechts und Mittel zur Komplexitätsreduktion für eine Analyse für die von der Informationsverarbeitung ausgehenden Gefahren kann zur Dis-

position gestellt werden. Schon in der EG-Datenschutzrichtlinie 95/46/EG von 1995 war sie nur noch rudimentär vorhanden. Mit den Entwürfen für eine EU-Datenschutzgrundverordnung hat sie weiter an Boden verloren, und mit dem Inkrafttreten der Verordnung würde sie aus dem deutschen Datenschutzrecht wohl einfach verschwinden. Auch der derzeit meistdiskutierte alternative Regelungsansatz, der auf der Verwendung von Schutzzielen basiert,[47] kommt ohne eine Phasenorientierung aus.[48]

Allein für das Zweckbindungsprinzip scheint keine geeignete Alternative in Sicht. Zwar gibt es wie beschrieben Bestrebungen zu seiner Abschaffung, auch wurden schon Abschwächungsvorschläge unterbreitet,[49] ein Vorschlag für einen funktional äquivalenten Ersatz, mit dem die Wahl der Mittel und ihre Verwendung sowohl entschieden wie geprüft werden kann, wurde bislang jedoch nicht vorgelegt. Und gerade diese Eigenschaft ist es, die den zentralen Wert des Zweckbindungsgrundsatzes ausmacht: Die Geeignetheit des Zwecks, ob selbst- oder fremdgesetzt, als Konstante und fester Prüfanker die Kontrollierbarkeit zunehmend komplexer Informationsverarbeitungs- und Entscheidungsprozesse, der beteiligten Akteure, ihrer Handlungen und der eingesetzten Mittel – von Hard- und Software über Algorithmen und Heuristiken bis zu den verwendeten Informationen – herzustellen und zu wahren. Wenn zum Schutz der einzelnen Betroffenen und der Gesellschaft insgesamt vor der strukturell überlegenen Informationsmacht von Organisationen die Ausübung dieser Macht einer Kontrolle unterworfen werden soll, führt am Prinzip der Zweckbindung derzeit kein Weg vorbei.

1 BITKOM (2015). EU-Datenschutzverordnung muss Innovationen ermöglichen. Presseerklärung vom 24.06.2015. url: http://www.bitkom.org/de/presse/8477_82534.aspx.

2 Stefan Krempl und Andreas Wilkens (2015). „EU-Datenschutzreform: Zweckbindung und Datensparsamkeit ausgehebelt“. In: heise online. 15.06.2015. url: http://heise.de/-2690862.

3 Artefakt kann einerseits allgemein etwas Menschengemachtes bezeichnen, andererseits jedoch auch ein – oft störendes – Phänomen, das als Folge von etwas wie der Wahl der Messmethode in der Sozialforschung oder des verwendeten Algorithmus bei der verlustbehafteten Bildkompression auftritt. Hier sollen beide Lesarten zusammengeführt werden: Es wird gezeigt, dass das Zweckbindungsprinzip einerseits Folgeprodukt vorhergehender Operationalisierungsentscheidungen ist, andererseits jedoch explizit Menschenwerk. Ein Beispiel: In einem mehrstöckigen Gebäude sind notwendig Höhenunterschiede zu überwinden. Rampen, Leitern, Treppen oder Lifte sind dafür geeignete Mittel. Dass solche Mittel überhaupt erforderlich sind, ist eine Folge der vorhergehenden Entscheidung, ein mehrstöckiges Gebäude zu bauen. Das gewählte Mittel, etwa der Lift, ist damit ein Artefakt dieser Entscheidung. Und es bleibt auch dann ein Artefakt der Entscheidung, wenn bewiesen werden kann, dass es unter den grundsätzlich geeigneten Mitteln das beste ist.

4 Oscar M. Ruebhausen und Orville G. Brim Jr. (1965). „Privacy and Behavioral Research“. In: Columbia Law Review 65.7, S. 1184–1211.

5 Ruebhausen und Brim 1965, S. 1198.

6 Ruebhausen und Brim 1965, S. 1199.

7 Ruebhausen und Brim 1965, S. 1199.

8 BVerfGE 27, 344. Ehescheidungsakten.

9 BVerfGE 27, 344, 348.

10 BVerfGE 27, 344, 352.

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

12 Vgl. Jörg Pohle (2014a). „Die immer noch aktuellen Grundfragen des Datenschutzes“. In: Wovon – für wen – wozu. Systemdenken wider die Diktatur der Daten. Wilhelm Steinmüller zum Gedächtnis. Hrsg. von Hansjürgen Garstka und Wolfgang Coy. Humboldt-Universität zu Berlin, Hermann von Helmholtz-Zentrum für Kulturtechnik. Berlin, S. 45–58.

13 Steinmüller u. a. 1971, S. 115.

14 Zweckbindung müsse selbst für Informationen gelten, die »um einer öffentlichen – vor allem auch politischen – Wirkung willen ganz bewußt in die Öffentlichkeit« getragen worden seien, so die Datenschutzkommission des Deutschen Juristentages (1974). Grundsätze für eine Regelung des Datenschutzes. Bericht der Datenschutzkommission des Deutschen Juristentages. München: C. H. Beck’sche Verlagsbuchhandlung, S. 27.

15 In ihrem von der Semiotik übernommenen vierdimensionalen Konzept – Syntax, Semantik, Pragmatik und Sigmatik – wird der Zweck gerade über die pragmatische Dimension rechtlich adressierbar, siehe Steinmüller u. a. 1971, S. 42 f.

16 Steinmüller u. a. 1971, S. 54.

17 Steinmüller u. a. 1971, S. 57.

18 Steinmüller u. a. 1971, S. 57.

19 Zu den Hintergründen und zur Kritik siehe Jörg Pohle (i.E.). „Transparenz und Berechenbarkeit vs. Autonomie- und Kontrollverlust: Die Industrialisierung der gesellschaftlichen Informationsverarbeitung und ihre Folgen“. In: Mediale Kontrolle unter Beobachtung.

20 Zum Scheitern der damit verbundenen Erwartung an den Durchbruch datenvermeidender Verfahren siehe Paul Ohm (2010). „Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization“. In: UCLA Law Review 57, S. 1701–1777.

21 Das gilt etwa beim Rückgriff auf Auftragsdatenverarbeiter.

22 Steinmüller u. a. 1971, S. 60.

23 Bernhard Hoffmann (1991). Zweckbindung als Kernpunkt eines prozeduralen Datenschutzansatzes. Baden-Baden: Nomos Verlagsgesellschaft.

24 Hoffmann 1991, S. 127. Das ist Helen Nissenbaums »contextual integrity« avant la lettre, siehe Helen Nissenbaum (2004). „Privacy as contextual integrity“. In: Washington Law Review 79, S. 101–139. Gerade die konzeptionelle Verwandtschaft zwischen den verschiedenen Theorien zu den individuellen und gesellschaftlichen Folgen moderner Informationsverarbeitung wird jedoch in der Forschung bislang weitgehend ignoriert.

25 Hoffmann 1991, S. 26.

26 Hoffmann 1991, S. 25.

27 Hoffmann 1991, S. 81, mit Verweis auf Niklas Luhmann (1964). Funktionen und Folgen formaler Organisation. Berlin: Duncker & Humblot, S. 109.

28 Hoffmann 1991, S. 46.

29 Hoffmann 1991, S. 50.

30 Hoffmann 1991, S. 21.

31 Vgl. BVerfG, Urteil vom 24.04.2013, Rn. 113.

32 Das gilt vor allem für die Hardware, siehe schon Claude E. Shannon (1948). „A Mathematical Theory of Communication“. In: The Bell System Technical Journal 27.3, S. 379–423, S. 379.

33 Vgl. Jörg Pohle (2014b). „Kausalitäten, Korrelationen und Datenschutzrecht“. In:

Fundationes I: Geschichte und Theorie des Datenschutzes. Hrsg. von Jörg Pohle und Andrea Knaut. Münster: Monsenstein und Vannerdat, S. 85–105, Rn. 42 ff.

34 Zusammenfassend Wilhelm Steinmüller (1993). Informationstechnologie und Gesellschaft: Einführung in die angewandte Informatik. Darmstadt: Wissenschaftliche Buchgesellschaft, S. 488 ff. 35 Vgl. Martin Kutscha (1999). „Datenschutz durch Zweckbindung – ein Auslaufmodell?“ In: Zeitschrift für Rechtspolitik 4, S. 156–160. 36 Siehe den Vergleich Chris Hoofnagles zwischen dem Fair Credit Reporting Act von 1970 und heutigen Vorschlägen für die Regulierung von Big Data: Chris Jay Hoofnagle (2013). „How the Fair Credit Reporting Act Regulates Big Data“. In: Future of Privacy Forum Workshop on Big Data and Privacy: Making Ends Meet. 37 Adalbert Podlech (1976). „Gesellschaftstheoretische Grundlage des Datenschutzes“. In: Datenschutz und Datensicherung. Hrsg. von Rüdiger Dierstein, Herbert Fiedler und Arno Schulz. Köln: J. P. Bachem Verlag, S. 311–326, S. 313.

38 Vgl. Pohle i.E.

39 Vgl. Bert-Jaap Koops (2014). „The trouble with European data protection law“. In: International Data Privacy Law 4.4, S. 250–261.

40 Vgl. Paul M. Schwartz und Daniel J. Solove (2011). „The PII Problem: Privacy and a New Concept of Personally Identifiable Information“. In: NYUL Review 86, S. 1814–1894.

41 Vgl. Martin Rost und Katalin Storf (2013). „Zur Konditionierung von Technik und Recht mittels Schutzzielen“. In: Informatik 2013 : Informatik angepasst an Mensch, Organisation und Umwelt. Hrsg. von Matthias Horbach. Bd. 220. Lecture Notes in Informatics. Gesellschaft für Informatik. Bonn, S. 2149–2166.

42 Steinmüller warnte schon früh vor dieser Möglichkeit und verlangte daher, dass auch statistische Informationen dem Datenschutzrecht unterworfen werden, siehe Wilhelm Steinmüller (1971). „Allgemeine Grundsätze zur rechtlichen Regelung des Datenschutzes“. In: Datenschutz – Datensicherung. Hrsg. von Jochen Schneider. Beiträge zur integrierten Datenverarbeitung in der öffentlichen Verwaltung Heft 5. München: Siemens Aktiengesellschaft. Kap. 3, S. 13–17, S. 16.

43 Für die Schwierigkeiten, ein als Gefahrenabwehr wirkendes Schutzrecht ausschließlich auf Verwendungsbeschränkungen zu gründen, und die umfassende Diskussion in den 1960er Jahren dazu, siehe Arthur Raphael Miller (1969). „Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society“. In: Michigan Law Review 67.6, S. 1089–1246.

44 Adalbert Podlech (1982). „Individualdatenschutz – Systemdatenschutz“. In: Beiträge zum Sozialrecht – Festgabe für Grüner. Hrsg. von Klaus Brückner und Gerhard Dalichau. Percha: Verlag R. S. Schulz, S. 451–462, S. 452.

45 Vgl. Pohle 2014a, S. 51 f.

46 Vgl. Gabriela Zanfir (2013). Forgetting about consent. Why the focus should be on „suitable safeguards“ in data protection law. University of Craiova. Faculty of Law und Adminsitrative Sciences.

47 Grundlegend Martin Rost und Andreas Pfitzmann (2009). „Datenschutz-Schutzziele – revisited“. In: Datenschutz und Datensicherheit 33.6, S. 353–358.

48 Vgl. Marit Hansen, Meiko Jensen und Martin Rost (2015). „Protection Goals for Privacy Engineering“. In: 2015 International Workshop on Privacy Engineering (IWPE). IEEE eXplore.

49 Vgl. etwa Martin Eifert (2007). „Zweckvereinbarkeit statt Zweckbindung als Baustein eines modernisierten Datenschutzes“. In: Rechtswissenschaft im Wandel. Hrsg. von Walter Gropp, Martin Lipp und Heinhard Steiger. Tübingen: Mohr Siebeck, S. 139–152.