Jörg Pohle

PERSONAL DATA NOT FOUND:
Personenbezogene Entscheidungen als überfällige Neuausrichtung im Datenschutz

Bei privacy, Privatheit, Privatsphäre, surveillance und Datenschutz handelt es sich unzweifelhaft um essentially contested concepts.[1] Alles an ihnen scheint umstritten, jeder Aspekt umkämpft: Das beginnt schon beim verwendeten Bezeichner, wie die vorstehende Aufzählung zeigt, und geht weiter über den Phänomenbereich und das Schutzgut, den Grund oder die Gründe für dessen Gefährdung sowie das Schutzregime. Eines jedoch scheint für alle Beteiligten sicher zu sein: Das Problem dreht sich irgendwie um personenbezogene Informationen.[2]

Vor dem Hintergrund der Entwicklung, die in den letzten Jahren sowohl die Geschäftsmodelle wie die Technik erfahren haben – von Big Data über Recommender Systems und Predictive Policing bis hin zum Internet of Things –, stellt sich die Frage, ob diese angenommene Selbstverständlichkeit, über personenbezogene Informationen – personenbezogene Daten in der Sprache des Datenschutzrechts[3] – sprechen zu müssen, noch haltbar ist.

Die Antwort darauf lautet – und der Beitrag wird dies zu belegen suchen – nein. Nicht personenbezogene Informationen, sondern personenbezogene Entscheidungen durch Organisationen in strukturell vermachteten Informationsbeziehungen sind zum Anknüpfungspunkt von Datenschutztheorie und Datenschutzrecht zu machen.

Ein Beispiel in vier Fällen

Zur Beantwortung der Frage, ob personenbezogene Informationen ein geeigneter Anknüpfungspunkt für eine Theorie zur Erklärung oder das Recht zur Lösung der oben angedeuteten Probleme im Zusammenhang mit moderner Informationsverarbeitung und Entscheidungsfindung sind, soll folgendes Beispiel dienen: Google entscheidet über Alice. Die Entscheidung, von der hier die Rede ist, kann sich etwa darauf beziehen, welche Informationen Alice als Antwort auf ihre Suchanfrage präsentiert werden und welche nicht, in welcher Reihenfolge die Suchergebnisse angeordnet werden oder welche Werbung dazu jeweils gezeigt wird.[4] Google selbst ist, soviel ist sicher, eine Organisation. Die hier betrachteten Informationsverarbeitungen und Entscheidungsfindungen liegen bei Google nicht in der Hand von Mitarbeiterinnen und Mitarbeitern, sondern sind – jedenfalls so weitgehend wie nur irgend möglich – industrialisiert.[5]

Dieses Beispiel soll nun anhand von vier Fällen analysiert werden.

Im ersten Fall verarbeitet Google personenbezogene Informationen über Alice und trifft die Entscheidungen über Alice auf Basis dieser Informationen. Alice' privacy oder Privatheit ist mindestens tangiert, eventuell – das ist je nach Theorie unterschiedlich – ist sie auch verletzt, jedenfalls aber fällt dieser Sachverhalt unzweifelhaft unter das deutsche und europäische Datenschutzrecht.

Im zweiten Fall trifft Google die Entscheidungen über Alice auf der Basis von Informationen über Bob, die Google zu diesem Zweck verarbeitet. Diese Situation kann etwa eintreten, wenn Alice Bobs Computer nutzt, und Google die Informationen daher als Informationen über Bob verarbeitet, oder wenn Google die Informationen aus anderen Gründen der falschen Person, nämlich

Bob, zuweist. In diesem Fall ist sicher Bobs privacy oder Privatheit betroffen und möglicherweise auch verletzt, aber jedenfalls nicht die von Alice. Die Informationsverarbeitung unterfällt immer noch dem Datenschutzrecht, denn es werden personenbezogene Informationen verarbeitet und genutzt, aber nur Bob hat Betroffenenrechte gegenüber Google, etwa nach §§ 33 ff. BDSG, und Google hat datenschutzrechtliche Pflichten nur gegenüber Bob (und natürlich gegenüber Aufsichtsbehörden), nicht aber gegenüber Alice.

Im dritten Fall basieren Googles Entscheidungen über Alice auf rein statistischen, mithin also nicht personenbezogenen Informationen. Dabei ist unerheblich, was die Basis der statistischen Informationen ist – sie können von vornherein nach § 3a Satz 1 BDSG anonym erhoben oder nach § 3a Satz 2 BDSG nachträglich anonymisiert worden sein und sie können auf Alices Aktivitäten basieren oder auf Aktivitäten von vielen Menschen, die dann zu einer generalisierten Person kondensiert wurden –, denn spätestens mit der nicht wieder aufhebbaren Anonymisierung entfällt „mangels Personenbezug die Anwendbarkeit des Gesetzes ohnehin".[6] Und auch privacy oder Privatheit von Individuen sind nicht oder nicht mehr betroffen.[7]

Im vierten Fall trifft Google die Entscheidungen über Alice auf der Basis von Informationen, die sich Google einfach ausgedacht hat oder die schlicht reine Sachinformationen sind, etwa Informationen über das Wetter. Wieder handelt es sich nicht um einen privacy- oder privatheitsbezogenen oder dem Datenschutzrecht unterfallenden Sachverhalt.

In allen vier Fällen ist klar, dass die Beziehung zwischen Alice und Google von einer strukturellen Machtimbalance zugunsten Googles geprägt ist: Google entscheidet nach selbst gesetzten – und dabei nicht unbedingt in sich konsistenten oder auf Dauer gestellten – Maßstäben darüber, was Alice über sich selbst, die Gesellschaft, ja die Welt – oder womöglich auch nur über das Internet – wissen oder zumindest finden kann. Dennoch handelt es sich nur im ersten Fall – jedenfalls ausweislich aller privacy-, Privatheits- und Privatsphäretheorien – um ein privacy-, Privatheits- und Privatsphäreproblem für Alice und – von einer Ausnahme im Telemediengesetz abgesehen[8] – einen Fall des Datenschutzrechts.[9]

Das alles heißt aber nichts anderes, als dass Entscheidungen über Menschen in vermachteten Beziehungen nur dann problematisiert werden, wenn diese auf der Basis von Informationen über diese Menschen getroffen werden. Warum sollte es aber substantiell einen Unterschied markieren, dass Google – oder irgendeine andere (informations-)mächtige Organisation – Entscheidungen über Menschen auf der Basis von Informationen über andere Menschen – oder Gruppen oder ganze Bevölkerungen oder das Wetter – trifft als auf der Basis von Informationen über die Menschen selbst, über die Google entscheidet? Was ist dieser Unterschied, der als privacy, Privatheit oder Privatsphäre bezeichnet wird, und was macht ihn schützenswert und geschützt durch das Recht? Keine der existierenden Theorien versucht auch nur, darauf eine Antwort zu geben.[10] Und wenn sie es täte, dann müsste sie wohl sicher scheitern.

Woher kommt die Fixierung auf personenbezogene Informationen?

Die erste Frage, die sich in diesem Zusammenhang stellt, ist die nach dem geschichtlichen Hintergrund der Fixierung der gesamten Debatte wie aller gesetzlichen Regelungsregime auf personenbezogene Informationen. Eine umfassende Analyse der wissenschaftlichen Arbeiten, die im Laufe der privacy-, Privatheits- und Datenschutzdebatte die Richtung der Diskussion beeinflussten, ergibt, dass diese Fixierung wohl drei Ursachen hat: Die erste liegt in einem Übersetzungsplagiat aus dem Urheberrecht, die zweite in der Übernahme der informierten Einwilligung aus dem Bereich medizinischer Eingriffe und die dritte in einer Fehlvorstellung darüber, wie rationale Bürokratien im Weberschen Sinne rationale Entscheidungen treffen.

…aus dem Urheberrecht

Obwohl Hans-Heinrich Maass schon vor Jahrzehnten darauf hingewiesen hat,[11] dass sich Samuel D. Warren und Louis D. Brandeis in ihrer bekannten Arbeit „The Right to Privacy"[12] ziemlich frei bei Josef Kohler und seinem Werk „Das Autorrecht"[13] – vor allem für die Konstruktion ihrer Argumentationsstruktur – bedienten, ohne es zu zitieren, sind dieser Zusammenhang und die daraus resultierenden Folgen für das right to privacy bisher nicht wissenschaftlich untersucht.[14]

Kohler argumentiert in seiner Arbeit, dass aus dem von ihm als schon im Römischen Recht durch die actio iniuriarum, die auch Warren und Brandeis als historischen Bezugspunkt verwenden,[15] als geschützt angesehenen „Individualrecht" Autorinnen und Autoren das Recht erwachse, „daß ein Jeder alleiniger Herr ist, zu bestimmen, welche Aeußerungen und Kundgebungen er in das Publikum tragen will und welche nicht".[16] Diese Formulierung, die sich auch bei Warren und Brandeis als „determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others" findet,[17] ist eng gebunden an den betrachteten Phänomenbereich und den zugrunde gelegten Sachverhalt – sowohl bei Kohler wie auch bei Warren und Brandeis. In dem Bereich, den Kohler betrachtet, geht es um die Frage, wer das Recht habe zu entscheiden, ob ein Werk – die „Aeußerungen und Kundgebungen" – mit dem Akt der Veröffentlichung einer unbeschränkten Öffentlichkeit zugänglich gemacht werden soll. Während der Angreifer hier ein Verlag ist, der das Werk ohne Zustimmung der Autorin oder des Autors publiziert, ist es im Falle Warren und Brandeis' die Presse, die „the sacred precincts of private and domestic life"[18] ans Licht der Öffentlichkeit zerrt.

In beiden Fällen ist es demnach der Akt dieser Weitergabe – ob an eine oder mehrere andere Personen oder an eine unbeschränkte Öffentlichkeit –, der einen Eingriff darstellt und damit zugleich zum konstitutiven Element des Konzeptes oder der Theorie gemacht wird, nicht jedoch eine oder mehrere Entscheidungen, die – ob auf der Basis der veröffentlichten Informationen oder nicht – über die Betroffenen getroffen werden. Privacy ist damit von Warren und Brandeis, indem sie sich

im Urheberrecht bedienten, an den ihm zugrunde liegenden Vorgang gebunden worden: ein Etwas, das aus dem „Innersten“ der oder des Betroffenen kommt, und für das die Entscheidung über deren Verbreitung an ein Publikum auch in die Hände dieser Betroffenen gelegt werden soll.

…aus dem medizinischen Bereich

Eine zweite historische Grundlage hat die Fixierung auf personenbezogene Informationen in der spezifischen Konstruktion der informierten Einwilligung, wie sie von Oscar M. Ruebhausen und Orville G. Brim, Jr., aus der Medizinethik übernommen wurde.[19] Diese Arbeit, in der sich die Autoren unter anderem explizit auf die Ergebnisse des Nürnberger Ärzteprozesses bezogen, wurde in der zweiten Hälfte der 1960er und der ersten Hälfte der 1970er Jahre breit rezipiert, wenn es darum ging, welche Anforderungen an eine informierte Einwilligung zu stellen seien.

Der eigentliche Untersuchungsgegenstand der Arbeit war die Verhaltensforschung und die Frage, welche Informationen und welche Zusicherungen den Beforschten über die Erhebung, Speicherung und Verwendung der Informationen, die im Rahmen der Forschung anfallen, gegeben werden müssten.[20] Einer der wesentlichen Hintergründe ist natürlich, dass grundsätzlich davon ausgegangen werden kann, dass die Beforschten sich eher beforschen lassen und dabei wahrheitsgemäß antworten würden, wenn sie Vertrauen in die Integrität der Forscherinnen und Forscher und in die Vertraulichkeit ihrer gemachten Angaben haben.[21]

Auch hier geht es also wieder nicht darum, ob Entscheidungen über die Betroffenen getroffen werden und von wem, sondern – neben der Zweckbindung[22] – vor allem um die Frage einer eventuellen Weitergabe von Informationen aus dem Innenleben der Betroffenen, der private personality.

…von der Unterstellung eines fehlverstandenen Rationalismus

Eine dritte Ursache, die die Fixierung auf personenbezogene Informationen erklärt, liegt in einer weitverbreiteten Zuschreibung von Eigenschaften an einen bestimmten Akteur, der Entscheidungen über Menschen – und Dinge – trifft: die moderne Organisation.[23] In der Frühphase der modernen privacy- und Datenschutzdebatte werden solche Organisationen fast durchgängig als rationale Bürokratien im Weberschen Sinne verstanden, „die die Prozesse ihrer eigenen Entscheidungsfindung rational vorplanen, die dafür notwendigen Informationsverarbeitungsprozesse geeignet formalisieren und danach funktionieren wie ein Uhrwerk“.[24] Einer der wenigen, der offenlegt, wie sehr seine Konzeption von einer solchen zugeschriebenen, spezifischen Rationalität des Datenverarbeiters abhängig ist, ist Christoph Mallmann: „die Datenverarbeitung in der öffentlichen Verwaltung erfolgt zweckrational im Sinne Max Webers.“[25]

Dieser modernen Bürokratie wird also zugeschrieben, dass sie ihre rationalen Entscheidungen über Menschen in rationaler Weise treffen würde – und das heißt, auf der Basis von Informationen über diese Menschen,[26] und zwar möglichst vielen Informationen.[27] Sehr deutlich wird dies in Wilhelm Steinmüllers Annahme über das „unausgesprochene Ziel aller technokratisch ausgerichteten ADV“, der automationsunterstützten Datenverarbeitung: „Alle Daten über alle Betroffenen werden nur einmal erfaßt, einmal gespeichert, einmal gelöscht – »Minimierung der Datenmenge« –; alle Daten werden möglichst häufig verarbeitet und weitergegeben sowie möglichst vielen Benutzern zur Auswertung überlassen – »Maximierung der Datenflüsse und DV-Leistung« […]“[28]

Vor diesem Hintergrund wird dann verständlich, warum – trotz der schon seinerzeit, wenn auch selten, geäußerten Kritik[29] – es damals als zugleich notwendig wie hinreichend angesehen wurde, den „Informationshaushalt“ (Adalbert Podlech) der Organisationen zu regulieren,[30] um deren Produktion von Entscheidungen unter Kontrolle zu bringen. Es bleibt aber zu konstatieren, dass sich die Unterstellung, rationale Organisationen würden Entscheidungen über Menschen nur auf der Basis von personenbezogenen Informationen über diese Menschen treffen, inzwischen als nicht mehr haltbar herausgestellt hat.[31] Daher überrascht es durchaus, dass es bis heute – von einigen wenigen Ausführungen zum „Institutionaldatenschutz“[32] abgesehen – keine einzige privacy- oder Datenschutztheorie gibt, die ohne eine Anknüpfung an personenbezogene Informationen auskommt, obwohl diese (Selbst-)Beschränkung auf personenbezogene Informationen gerade nicht schon in der Analyse des Problems von Informationsmacht zwischen Organisation auf der einen und Individuen und Gruppen auf der anderen Seite selbst angelegt ist.[33]

Damit ist festzustellen, dass es zwar historische Zusammenhänge gibt, die die Fixierung auf personenbezogene Informationen erklären, um eine hinreichende Begründung handelt es sich dabei jedoch nicht. Wo sich in der Vergangenheit die Bezugnahme auf personenbezogene Informationen wissenschaftlich rechtfertigen musste, geschah dies ausschließlich in der Auseinandersetzung mit konkurrierenden Ansätzen wie etwa der Sphärentheorie oder der Privat-öffentlich-Dichotomie,[34] die zugleich jeweils nur eine Beschränkung des Anwendungsbereiches der jeweiligen privacy- und Datenschutztheorien auf Teilmengen von personenbezogenen Informationen forderten, etwa auf bestimmte Datenkategorien.

Folgen der Selbstbeschränkung auf personenbezogene Informationen

Die zweite zentrale Frage, der sich diese Arbeit annimmt, ist die nach den Folgen, die diese konzeptionelle Selbstbeschränkung für den Schutz von Betroffenen wie Alice in den oben beschriebenen und allen vergleichbaren Fällen hat.

Die offensichtliche Folge dieser Fixierung auf personenbezogene Informationen als Schutzobjekt entspricht dem, was Kuhn als Selbstisolierung von wissenschaftlichen Disziplinen oder Communities beschrieben hat: Das zugrunde liegende gesellschaftliche Problem – das Machtproblem und das Problem der Entscheidung über Menschen – kann schlicht nicht beschrieben werden „in terms of the conceptual and instrumental tools the [privacy, Einfügung des Autors] paradigm provides.“[35] Mit die-

ser Fixierung reproduziert sich zugleich – auf der gesellschaftlichen Ebene – die Schließung des Diskursraumes.[36]

Personenbezogene Informationen sind als Bezugspunkt und Schutzobjekt des Rechts aus informatischer, soziologischer wie rechtlicher Sicht ungeeignet, insoweit es für Organisationen möglich ist, individuelle Diskriminierung auch auf der Basis anonymer oder statistischer Informationen vorzunehmen. Das gilt gerade auch für strukturell vermachtete Verhältnisse wie die zwischen Organisationen und ihrem Klientel. Sowohl aus der Außenperspektive wie aus der Perspektive von Alice ist es gleich, ob Google – oder irgendeine andere (informations-) mächtige Organisation – Entscheidungen über sie auf der Basis von Informationen über sie oder über andere Menschen trifft. Auch kann Alice – sowohl nach der derzeitigen Datenschutzrechtslage wie nach allen privacy-Theorien – nicht einmal feststellen, auf welcher Basis Google über sie entscheidet, solange es sich dabei nicht um personenbezogene Informationen über sie selbst handelt, denn Google ist ihr darüber nicht begründungspflichtig. Statt dessen perpetuiert und zementiert sich damit Googles Informationsmacht über Alice.

Die Entscheidung, Alice – und alle anderen Betroffenen – im vermachteten Verhältnis zu Organisationen nur dann zu schützen, wenn die Organisation ihre Macht unter Verwendung personenbezogener Informationen über Alice ausübt, ist sowohl arbiträr wie am eigentlichen Problem vorbeigehend.[37] Alice wird der Macht der Organisation gerade immer dann schutzlos ausgeliefert, wenn es der Organisation gelingt, ihre Machtbasis, nämlich Informationen, erfolgreich zu tarnen: Eine jede Theorie, die personenbezogene Informationen und deren Erhebung, Speicherung, Verarbeitung und Verwendung falsch als das Problem selbst ausweist, erklärt damit zugleich die Erhebung, Speicherung, Verarbeitung und Verwendung anderer als personenbezogener Informationen für unproblematisch. Die Nicht-Verarbeitung personenbezogener Informationen, die (Selbst-)„Beschränkung“ von Organisationen auf die Verarbeitung anonymer oder anonymisierter Informationen, die Möglichkeiten zum „Selbstdatenschutz“ – dies alles sind nur Placebos zur Beruhigung der Betroffenen[38] und zur Sicherstellung der gesellschaftlichen Akzeptanz einer „universellen Verdatung aller Lebensbereiche“.[39] Es ist darum auch kein Wunder, wenn der Schutz von Betroffenen vor der „überlegen standardisierenden Strukturierungsmacht von Organisationen“,[40] den privacy- und Datenschutztheorien zu verfolgen vorgeben,[41] inzwischen häufig nicht mehr als privacy- oder Datenschutzproblem, sondern als Verbraucher_innenschutz- oder Kartellrechtsproblem betrachtet wird – und betrachtet werden muss, weil sich privacy- und Datenschutztheorien einer Auseinandersetzung damit verweigern.

Personenbezogene Entscheidungen als passenderer Anknüpfungspunkt

Die dritte Frage, die sich in diesem Zusammenhang stellt, ist nun offensichtlich: Welcher Anknüpfungspunkt ist besser geeignet als das Konzept der personenbezogenen Informationen, um in vermachteten Informationsbeziehungen wie in den oben beschriebenen und allen vergleichbaren Fällen den Schutz von Betroffenen wie Alice sicherzustellen? Aus dem Vorstehenden lässt sich bereits ersehen, wie dieser Ansatz aussehen kann, um den Datenschutz und das Datenschutzrecht vom Kopf auf die Füße zu stellen.

Sicher ist, dass eine Datenschutztheorie für sich in Anspruch nehmen sollte, die strukturellen Machtasymmetrien, die mit der und durch die Industrialisierung der gesellschaftlichen Informationsverarbeitung erzeugt, verstärkt oder verfestigt werden,[42] als solche zu problematisieren, unabhängig davon, ob sich die verarbeiteten Informationen auf Individuen, Gruppen, Organisationen, Sachen oder selbst Konzepte beziehen. Aber auch wenn sie das nicht versucht, muss sie zumindest die Klasse von Problemen adressieren, die entstehen, wenn in solchen vermachteten Verhältnissen sozial, politisch und ökonomisch mächtige Akteure Entscheidungen über Menschen treffen und diese Akteure dann in der Lage sind, diese Entscheidungen den Menschen zu oktroyieren. Die individuelle Betroffenheit, die offensichtlich in der von der liberalen Ideologie geprägten Vorstellung der bürgerlichen Gesellschaft nachgewiesen werden muss, damit ein gesellschaftliches Problem politisch wie rechtlich adressierbar wird – wenn auch eben nur in der Form einer individuellen Betroffenheit –, entsteht gerade aus sozial relevanten personenbezogenen Entscheidungen in strukturell vermachteten Informationsbeziehungen. Über diesen Anknüpfungspunkt der personenbezogenen Entscheidung wären dann auch alle Informationen, die zur Grundlage dieser Entscheidung gemacht worden sind oder gemacht werden sollen, und nicht nur die personenbezogenen, rechtlich adressierbar.[43]

Mit einer derart gestalteten Anknüpfung an automationsgestützte personenbezogene Entscheidungen in strukturell vermachteten Verhältnissen lassen sich nicht nur die historischen Fehlübernahmen aus Gegenstandsbereichen, die mit Entscheidungsfindung nichts zu tun haben, korrigieren, sondern es erlaubt auch, ein weiteres – weitgehend in Vergessenheit geratenes – Problem zu adressieren: Schon die Diskussionen in den privacy-Anhörungen in beiden Kammern des United States Congress in den 1960er Jahren zeigten, dass die Regulierung von Nutzungen – und dazu gehören auch Entscheidungen – allein nicht ausreicht.[44] Der Grund dafür ist offenkundig: Die Entscheidungen sind selbst „Produkt“ der Informationen und ihrer Verarbeitung, wobei die Informationen wiederum „Produkt“ der zugrunde gelegten Modellannahmen sind.[45] Daraus folgt dann aber zwingend, dass eine Anknüpfung an automationsgestützte personenbezogene Entscheidungen gerade nicht zu einer erneuten Selbstbeschränkung führen darf – hier nun als Selbstbeschränkung auf die Entscheidung –, sondern die Produktion der Entscheidung und deren Bedingungen zum Gegenstand von Theorie und Regulierung machen muss.

Wenn also das Ziel des Datenschutzes nicht einfach sein soll, mit überkommenen Regelungsinstrumenten individuelle Befindlichkeiten zu schützen, sondern die Freiheitsräume – als die Bedingungen der Möglichkeit zur Freiheitsausübung – von strukturell und informationell Schwächeren unter den Bedingungen der Industrialisierung der gesellschaftlichen Informationsverar-

beitung und gegen die überlegen standardisierende Strukturierungsmacht von Organisationen zu schützen, indem die Modellifizierungs- und Entscheidungsmacht von Organisationen mit ihren Folgen für Individuen und Gesellschaft, für Rechtsstaat, Sozialstaat und Demokratie und für die Freiheitsversprechen der bürgerlichen Gesellschaft wirksam beschränkt wird, dann gilt es, dafür die passenden Konzepte, Anknüpfungspunkte und Instrumente auszuwählen. Dazu muss eine Umstellung vorgenommen werden, denn nicht einfach die personenbezogenen Informationen, sondern die personenbezogenen Entscheidungen sind es, die durch das Datenschutzrecht unter Bedingungen zu stellen sind. Das gilt es zum Thema einer informierten Datenschutzdebatte zu machen, bevor das Problem – dann wiederum nur einseitig – als Verbraucher_innenschutz- oder Kartellrechtsproblem endet.

1 Siehe dazu Walter Bryce Gallie. „Essentially Contested Concepts“. In: Proceedings of the Aristotelian Society. New Series 56 (1956), S. 167–198. Ich bedanke mich bei Michael Plöse und Martin Rost für die kritische Durchsicht dieses Beitrags und die sehr produktiven Diskussionen zu Datenschutztheorie und Datenschutzrecht.

2 Auch an dieser Stelle gibt es genug Raum für Streit, etwa zum Begriff und zum zugrunde gelegten Informationskonzept, zur Frage, welche Rolle genau personenbezogene Informationen in diesem Zusammenhang spielen – etwa ob sie Schutzgut oder nur rechtlicher Anknüpfungspunkt sind –, ob alle Informationen oder nur „private“ – im Gegensatz zu „öffentlichen“ – oder nur „sensitive“ – im Gegensatz zu „nicht-sensitiven“ – eingeschlossen werden und ob sich „personenbezogen“ nur auf Menschen oder auch auf Gruppen oder Organisationen – in der Sprache des Rechts: juristische Personen – bezieht.

3 Siehe § 3 Abs. 1 BDSG. Über den Bezeichner „Daten“ ist schon genug geschrieben worden, es handelt sich aber klar um einen Informationsbegriff, siehe Jörg Pohle. „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, 2014, S. 45–58. URL: http://nbn-resolving.de/urn:nbn:de:kobv:11-100217316, S. 49 f.

4 Google ist eine „Weltvermessungsfirma“ (Martin Rost), ökonomisch allerdings in erster Linie eine Werbefirma mit angeschlossener Suchmaschine.

5 Das Management von Google trifft allerdings durchaus politisch relevante Entscheidungen, die dann als Technik, als Basis der Industrialisierung, auskristallisieren. Für diese saubere Trennung zwischen den unterschiedlichen Entscheidungsebenen, die sich auch in unterschiedlichen Folgen niederschlagen, danke ich Martin Rost.

6 Ulrich Dammann in Spiros Simitis, Hrsg. Bundesdatenschutzgesetz. 7. Aufl. Baden-Baden: Nomos Verlagsgesellschaft, 2011, § 3 Rn. 198.

7 Das gilt selbst für Konstrukte wie dezisionale Privatheit, siehe Beate Rössler. Der Wert des Privaten. Frankfurt am Main: Suhrkamp Verlag, 2001, S. 18, 25, 144 ff. wenn diese sich nicht schon auf jede von beliebigen Anderen beeinflusste Entscheidungsgrundlagen beziehen sollen, sondern sich – wie bei Rössler – auf intentionale Beeinflussung von Entscheidungen beschränken. Siehe dazu etwa die Verwendung des Begriffs „einmischen“, S. 148.

8 Siehe § 13 Abs. 6 TMG, siehe dazu auch die Diskussion zu dem von Marit Hansen angesprochenen Fall in Jörg Pohle und Andrea Knaut, Hrsg. Fundationes I: Geschichte und Theorie des Datenschutzes. Münster: Monsenstein und Vannerdat, 2014, S. 218, Rn. 35 und S. 225, Rn. 53 ff.

9 Einen ersten Schritt zur Überwindung dieser Beschränkung geht das Standard-Datenschutzmodell, siehe grundlegend Martin Rost. „Standardisierte Datenschutzmodellierung“. In: Datenschutz und Datensicherheit 36.6 (2012), S. 433–438, das personenbezogene Verfahren zugrunde legt. Damit soll bereits auf das Prozessieren von Daten, gleich welchen Ursprungs, auf Seiten von Organisationen verwiesen werden, wenn sie nur auf Personen bezogen werden. Siehe aber auch die eingeschränktere Definition im SDM-Handbuch, die immer noch auf dem Konzept der personenbezogenen Daten aufsetzt, Das Standard-Datenschutzmodell: Konzept zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, 2015. URL: https://www.datenschutz-mv.de/datenschutz/sdm/SDM-Handbuch_V09a.pdf, S. 7, 29, und zugleich die darüber hinausreichenden Beispiele, etwa S. 21 f.

10 Dieser Problembereich, also etwa die mögliche Diskriminierung auch anonymisierter Personen aufgrund statistischer Informationen, mag inzwischen durchaus diskutiert werden, siehe zuletzt Alexander Roßnagel und Maxi Nebel. „(Verlorene) Selbstbestimmung im Datenmeer: Privatheit im Zeitalter von Big Data“. In: Datenschutz und Datensicherheit (2015), S. 455–459, aber diese Diskussion führte bislang an keiner Stelle zu der Erkenntnis, dass das Problem in der arbiträren Anknüpfung an personenbezogene Informationen liegt.

11 Siehe Hans-Heinrich Maass. Information und Geheimnis im Zivilrecht. Stuttgart: Ferdinand Enke Verlag, 1970, S. 15.

12 Samuel D. Warren und Louis D. Brandeis. „The Right to Privacy“. In: Harvard Law Review (1890), S. 193– 220.

13 Josef Kohler. Das Autorrecht. Jena: Verlag Gustav Fischer, 1880.

14 James Whitmans Arbeit, in der es um das Verhältnis zwischen den europäischen und amerikanischen Ansätzen geht, kann nicht wirklich als wissenschaftlich durchgehen, und das nicht nur weil er aus unerfindlichen Gründen versucht, Warren und Brandeis Arbeit mit der Otto von Gierkes zu vergleichen, siehe James Q. Whitman. „The Two Western Cultures of Privacy: Dignity versus Liberty“. In: The Yale Law Journal 113.6 (2004), S. 1151–1221. Eine umfassende Untersuchung steht also noch immer aus.

15 Siehe Warren und Brandeis, „The Right to Privacy“, S. 197 f.

16 Kohler, Das Autorrecht, S. 137.

17 Warren und Brandeis, „The Right to Privacy“, S. 198.

18 Warren und Brandeis, „The Right to Privacy“, S. 195. Bei Kohler heißt es noch „das Heiligthum des geistigen Innenlebens“, siehe Kohler, Das Autorrecht, S. 142.

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

20 Siehe Ruebhausen und Brim, „Privacy and Behavioral Research“, S.1196 f. „first, the degree of individual consent that exists and, second, the degree of confidentiality that is maintained. The former concerns the conditions under which information is obtained from a person, the latter, the conditions under which the information is used.“

21 Dieser sehr pragmatische Grund für die Gewährleistung von privacy wird explizit angesprochen, siehe Ruebhausen und Brim, „Privacy and Behavioral Research“, S. 1198.

22 Zum Einfluss dieser Arbeit auf die historische Konstruktion des Zweckbindungsgrundsatzes, siehe Jörg Pohle. „Zweck-

bindung revisited“. In: Datenschutz Nachrichten 38.3 (2015), S. 141–145, S. 141.

23 Das nachfolgende gilt natürlich nur für Theorieansätze, die den Angreifer nicht in anderen Menschen verorten, sondern in Organisationen. Die meisten privacy-, Privatheits- und Privatsphäretheorien, aber auch einige der Theorien zum Datenschutz sind hinsichtlich der Angreifer personenfixiert.

24 Pohle, „Die immer noch aktuellen Grundfragen des Datenschutzes“, S. 49. Siehe dazu etwa die Darstellung der Organisationen bei Wilhelm Steinmüller u. a. Grundfragen des Datenschutzes. Gutachten im Auftrag des Bundesministeriums des Innern, BT-Drs. VI/3826, Anlage 1. 1971, S. 49, Ernst Benda. „Privatsphäre und „Persönlichkeitsprofil““. In: Menschenwürde und freiheitliche Rechtsordnung. Festschrift für Willi Geiger zum 65. Geburtstag. Hrsg. von Gerhard Leibholz u. a. Tübingen: J. C. B. Mohr (Paul Siebeck), 1974, S. 23–44, S. 27, Adalbert Podlech. „Aufgaben und Problematik des Datenschutzes“. In: Datenverarbeitung im Recht 5 (1976), S. 23–39, S. 25 oder James B. Rule u. a. The Politics of Privacy. New York: Elsevier, 1980, S. 25 ff.

25 Christoph Mallmann. Datenschutz in Verwaltungs-Informationssystemen. München, Wien: R. Oldenbourg Verlag, 1976, S. 32 mit Verweis auf Niklas Luhmann. „Zweck – Herrschaft – System. Grundbegriffe und Prämissen Max Webers“. In: Der Staat 3.2 (1964), S. 129–158 und Niklas Luhmann. Funktionen und Folgen formaler Organisation. Berlin: Duncker & Humblot, 1964. Hervorhebung im Original.

26 So explizit James B. Rule. Private Lives and Public Surveillance. London: Allen Lane, 1973, S. 29.

27 Siehe M. G. Stone und Malcolm Warner. „Politics, Privacy, and Computers“. In: The Political Quarterly 40.3 (1969), S. 256–267. S. 258.

28 Wilhelm Steinmüller. „Datenschutz als Teilaspekt gesellschaftlicher Informationskontrolle“. In: Datenschutz und Datensicherung. Hrsg. von Gerhard Löchner und Wilhelm Steinmüller. Karlsruhe: C. F. Müller Verlag, 1975, S. 35–95, S. 49.

29 Siehe etwa Paul J. Müller. „Informationsflüsse und Informationshaushalte“. In: Informationsrecht und Informationspolitik. Hrsg. von Wilhelm Steinmüller. München, Wien: Oldenbourg Verlag, 1976, S. 95–109, S. 96 f.

30 Dass es sich dabei nicht allein um eine auf die Bundesrepublik beschränkte Debatte handelte, zeigen die Ausführungen dazu bei Rule, Private Lives and Public Surveillance, S. 285.

31 Siehe etwa die Darstellung der Übertragung statistischer Informationen und deren Anwendung auf Individuen bei Eike Kühl. „Zeig uns dein Smartphone und wir leihen dir Geld“. In: Zeit Online (2015). URL: http://www.zeit.de/digital/internet/2015-12/kreditwuerdigkeit-scoring-smartphone-big-data.

32 Siehe dazu die thematische Kurzübersicht bei Steinmüller u. a., Grundfragen des Datenschutzes, S. 34.

33 Siehe etwa die Darstellung bei Klaus Lenk. „Datenschutz in der öffentlichen Verwaltung“. In: Datenschutz. Hrsg. von Wolfgang Kilian, Klaus Lenk und Wilhelm Steinmüller. Frankfurt am Main: Athenäum-Verlag, 1973, S. 15–50, S. 21 ff. Dabei ist jedoch durchaus zu beachten, dass der Begriff des Personenbezugs damals eher weit verstanden wurde, wie sich etwa an der Argumentation zur Relativität des Personenbezugs von Informationen bei Wilhelm Steinmüller. „Datenschutzrechtliche Anforderungen an die Organisation von Informationszentren“. In: Internationale Fachtagung: Informationszentren in Wirtschaft und Verwaltung. Hrsg. von P. Schmitz. Berlin, Heidelberg, New York: Springer, 1974, S. 187–205, S. 193 zeigt.

34 Siehe zu dieser Auseinandersetzung Jörg Pohle. „Die kategoriale Trennung zwischen »öffentlich« und »privat« ist durch die Digitalisierung aller Lebensbereiche überholt – Über einen bislang ignorierten Paradigmenwechsel in der Datenschutzdebatte“. In: »Worüber reden wir eigentlich?« Festgabe für Rosemarie Will. Hrsg. von Michael Plöse u. a. Humanistische Union. Berlin, i.E.

35 Thomas S. Kuhn. The Structure of Scientific Revolutions. 3. Aufl. Chicago, London: The University of Chicago Press, 1996, S. 37.

36 Siehe dazu Herbert Marcuse. One-Dimensional Man. Studies in the ideology of advanced industrial society. Reprint der 2. Auflage von 1991. London, New York: Routledge, 2002, S. 87 ff.

37 Bezeichnenderweise gibt es selbst in dem sehr umfassenden BDSG-Kommentar von Simitis an keiner Stelle eine Begründung für diese Entscheidung. Statt dessen wird einfach erklärt, Ziel sei „einzig und allein den Schutz vor den Folgen sicherzustellen, die eine Verarbeitung personenbezogener Angaben für die jeweils davon Betroffenen haben kann“, siehe Simitis, Bundesdatenschutzgesetz, Einleitung, Rn. 2.

38 Und sie sind zugleich sehr wirkmächtige Selbstbeschränkungen in der Gestaltung von Technik, siehe Jörg Pohle. „Das Scheitern von Datenschutz by Design: Eine kurze Geschichte des Versagens“. In: FIfF Kommunikation 32 (2015), S. 41–44, S. 43.

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

40 Wolfgang Zimmermann. „Privatsphäre. Aufruf zur Konstruktion einer realitätsbezogenen Bildwelt“. In: Fundationes I: Geschichte und Theorie des Datenschutzes. Hrsg. von Jörg Pohle und Andrea Knaut. Münster: Monsenstein und Vannerdat, 2014, S. 45–63, Rn. 35.

41 Siehe statt vieler zum Ziel des Datenschutzrechts als Normierung von „Datenmacht“ zur Sicherstellung ihrer Beschränkbarkeit und Kontrolle Kai von Lewinski. „Geschichte des Datenschutzrechts von 1600 bis 1977“. In: Freiheit – Sicherheit – Öffentlichkeit. Hrsg. von Felix Arndt. 48. Assistententagung Öffentliches Recht. Nomos Verlagsgesellschaft, 2009, S. 196–220, S. 200.

42 Siehe dazu Jörg Pohle. „Transparenz und Berechenbarkeit vs. Autonomie- und Kontrollverlust: Die Industrialisierung der gesellschaftlichen Informationsverarbeitung und ihre Folgen“. In: Mediale Kontrolle unter Beobachtung (i.E.). Dieser Fokus auf die Gesellschaft ist jedoch keineswegs neu. So werden schon Ende der 1970er Jahre „Verhinderung des Mißbrauchs personenbezogener Daten“ und „Gesamtheit der Maßnahmen zur Ermöglichung und Erhaltung sozialer Verhaltensräume für Individuen und Gruppen unter den Bedingungen moderner Informations- und Kommunikationssysteme“ als die beiden konzeptionellen Extrempunkte in der Datenschutzdebatte identifiziert, siehe Klaus Dette. „Einführung in das Kolloquium und Zusammenfassung der Ergebnisse“. In: Zweiweg-Kabelfernsehen und Datenschutz. Hrsg. von Klaus Dette, Rolf Kreibich und Wilhelm Steinmüller. Institut für Zukunftsforschung. München: Minerva Publikation, 1979, S. 3–13, S. 8.

43 Siehe schon Pohle, „Zweckbindung revisited“, S. 143.

44 Siehe schon Arthur Raphael Miller. „Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society“. In: Michigan Law Review 67.6 (1969), S. 1089–1246. S. 1221 i. V. m. S. 1119 f.

45 Ausführlich dazu Pohle, „Transparenz und Berechenbarkeit vs. Autonomie- und Kontrollverlust: Die Industrialisierung der gesellschaftlichen Informationsverarbeitung und ihre Folgen“.