Vertrauensinfrastrukturen der digitalen Gesellschaft

Vertrauen als Schlüsselkategorie zur Weiterentwicklung des Datenschutzes

Markus Uhlmann, Fabian Pittroff und Jörn Lamla

DOI 10.15501/978-3-86336-922-4_2

Abstract

Der Beitrag widmet sich Problemstellungen der Vertrauensbildung bei gegenwärtigen Herausforderungen des Datenschutzes. Wir argumentieren, dass Maßnahmen der Vertrauensbildung, die einseitig auf Verhaltensänderungen von Verbraucherinnen und Verbrauchern durch Aufklärung oder Entscheidungsarchitekturen setzen, den Herausforderungen des Datenschutzes nicht gerecht werden. Dazu stellen wir alternative Gestaltungsoptionen des Datenschutzes vor und plädieren für die Entwicklung neuer Professionen sowie für die Institutionalisierung von intermediären Organisationen.

Dieser Beitrag erscheint unter der Creative-Commons-Lizenz: Namensnennung – Weitergabe unter gleichen Bedingungen 3.0 Deutschland | CC BY-SA 3.0 DE Kurzform | http://creativecommons.org/licenses/by-sa/3.0/de/ Lizenztext| http://creativecommons.org/licenses/by-sa/3.0/de/legalcode

1 Einleitung

Anfang 2018 kam es zu einem Datenskandal beim Internetunternehmen Facebook; Daten aus rund 50 Millionen Nutzerprofilen gelangten illegitim an Dritte, die diese für Experimente zur Beeinflussung demokratischer Wahlen verwendeten (Cadwalladr und Graham-Harrison 2018). Mark Zuckerberg, Mitbegründer und bis heute CEO des Unternehmens, bezeichnete den Datenausfluss als „großen Vertrauensbruch" (Schuler 2018). Es sei Facebooks Aufgabe, „die Daten unserer Nutzer zu schützen. Wenn wir das nicht schaffen, haben wir es nicht verdient, den Menschen zu dienen" (Schuler 2018). Vertrauen wurde zum öffentlichen Problem – für das Datenunternehmen Facebook und für die Verbraucherinnen und Verbraucher, die dessen Dienste nutzen. Um die Vertrauenswürdigkeit von Internetdiensten entspinnen sich immer wieder solche Krisen und Kontroversen, die mit Fragen von Datenschutz und Privatheit zusammenhängen (Lagerspetz 2014, 140; Baumann und Lamla 2017).

Diese Krisen um Vertrauen und Privatheit haben indes nicht zu einer digitalen Abstinenz der Verbraucherinnen und Verbraucher geführt (Statistisches Bundesamt 2018), möglicherweise weil Praktiken der digitalen Vernetzung mittels Social Networking Sites (SNS) wie Facebook mittlerweile unerlässlich geworden sind, um am sozialen Leben teilzunehmen. Greifbar wird das Vertrauensproblem allerdings, wenn traditionelle Strategien des Datenschutzes teils vergeblich gegen digitale Vertrauens- und Privatheitsverstöße mobilisiert werden. Denn häufig bleibt unklar, welche Akteurinnen und Akteure diesen Datenschutz durchsetzen sollen und wie die Potenziale und Risiken von Technologien wie Big Data problemangemessen reguliert werden können (Ladeur 2015). Am eindrücklichsten zeigt sich die Vertrauenskrise aber daran, dass etablierte Instrumente des Datenschutzes vielfach an den Praktiken von Verbraucherinnen und Verbrauchern vorbeigehen und von Internetunternehmen zu ihren Zwecken umgedeutet werden (Mayer-Schönberger und Padova 2016). Beispielhaft sind hier allgemeine Geschäftsbedingungen, die für viele Verbraucherinnen und Verbraucher nicht nur weitgehend unverständlich bleiben, sondern auch umfassende kommerzielle Datennutzungspraktiken von Unternehmen legitimieren.

In der Praxis finden sich unterschiedliche Logiken der Vertrauensbildung, mit denen auf die Herausforderungen der Privatheit und des Datenschutzes

reagiert wird. Etabliert sind etwa Strategien, die auf die Aufklärung oder Beeinflussung von individuellen Verbraucherinnen und Verbrauchern setzen. Komplizierte Geschäftsbedingungen gelten hier als zentrale Hürde einer gelingenden Vertrauensbildung. Daran schließt üblicherweise die Frage an, wie so über Geschäftsbedingungen informiert werden kann, dass Verbraucherinnen und Verbraucher Privatheitsrisiken eigenständig beurteilen können. Vertrauen kann gemäß dieser Logik nur dann sichergestellt werden, wenn Verbraucherinnen und Verbraucher zu informierten Entscheidungen befähigt werden (Jandt 2008, 58). Im Gegensatz dazu deutet sich aus soziologischer Sicht an, dass die Konstitution von Vertrauen und die Erneuerung des Datenschutzes in der digitalen Welt kollektive Gestaltungsaufgaben sind, die grundlegend neue Konzepte der Regulierung erfordern, die über einseitige Maßnahmen der Aufklärung von Verbraucherinnen und Verbrauchern hinausgehen (Ladeur 2012). Dabei ist grundsätzlich davon auszugehen, dass nur ein austariertes Zusammenspiel verschiedener technischer, rechtlicher, professioneller, politisch-institutioneller und zivilgesellschaftlicher Ressourcen diesen Herausforderungen begegnen kann (Ochs und Lamla 2017; Husemann und Pittroff 2018).

Im Folgenden sollen unterschiedliche Optionen für die Neugestaltung von Datenschutz und Privatheit diskutiert werden. Ein vertrauenstheoretischer Zugang spielt dabei eine Schlüsselrolle: Erstens eröffnet die Vertrauenskategorie Möglichkeiten, um verschiedene Optionen der Datenschutzgestaltung hinsichtlich ihrer Problemangemessenheit zu beurteilen. Zweitens argumentieren wir im Anschluss an jüngere Überlegungen zur Fortentwicklung des Datenschutzes, dass die Vertrauenskategorie das Potenzial aufweist, alternative Ansätze der Datenschutzregulierung offenzulegen (Richards und Hartzog 2016). Dafür werden wir zunächst soziologische Grundlagen des Vertrauens erläutern und für ein Verständnis argumentieren, das die normativen und kollektiven Grundlagen des Vertrauens berücksichtigt (2.). Ausgehend von diesen Überlegungen werden wir gegenwärtige Herausforderungen des Datenschutzes vertrauenstheoretisch wenden und Überlegungen zur Vertrauensbildung in den Blick nehmen, die auf die Veränderung von Verbraucherpraktiken setzen (3.). Dabei argumentieren wir, dass Strategien der Vertrauensbildung, die vordergründig auf die Aufklärung oder Beeinflussung von Verbraucherinnen und Verbrauchern zielen, den gegenwärtigen Herausforderungen des Datenschutzes nicht ge-

recht werden. Auf der Grundlage dieser Überlegungen stellen wir Kriterien und alternative Optionen zur Datenschutzgestaltung vor (4.). In diesem Zusammenhang argumentieren wir, dass Ansätze der Datenschutzgestaltung auf die Frage antworten müssen, wie Internetdienste für die konkrete Verwendungsweise von Daten zur Verantwortung gezogen werden können. Da eine individuelle Kontrolle über Informationsflüsse nur bedingt realisierbar ist, müssen Verbraucherinnen und Verbraucher auf die Angemessenheit der Datennutzung durch Internetunternehmen vertrauen können. Dabei geht es um einen Datenschutz, der Privatheit unabhängig von individuellen Verbraucherentscheidungen gewährleistet (4.1). In diesem Zusammenhang werden wir die Aufmerksamkeit auf Problemstellungen der Schaffung neuer Institutionen richten, die sich der Realisierung eines solchen Datenschutzes annehmen (4.2). Exemplarisch werden wir Überlegungen zur Professionalisierung sowie zur Institutionalisierung intermediärer Organisationen diskutieren. Wir schließen mit einem Fazit, das die zentralen Überlegungen zusammenfasst.

2 Die normativen und kollektiven Grundlagen des Vertrauens

Wenngleich in soziologischen Debatten kein einheitliches Verständnis von Vertrauen herrscht, gibt es doch einige weitgehend unstrittige Kernaspekte. Ganz grundsätzlich bezieht sich Vertrauen auf Phänomene, bei denen sich Personen auf ein Entgegenkommen anderer verlassen, ohne dass dieses Entgegenkommen individuell kontrolliert und erzwungen werden könnte. Vertrauende Personen gehen vielmehr davon aus, dass andere Akteure bestimmten Erwartungen nachkommen, ohne die Gewissheit zu haben, dass diesen Erwartungen tatsächlich Rechnung getragen wird (Hartmann 2011, 271). Wenngleich diese Grundüberlegung vielen soziologischen Vertrauenstheorien zugrunde liegt, unterscheiden sich verschiedene theoretische Perspektiven deutlich hinsichtlich bestimmter Schwerpunktsetzungen.

So richten viele Ansätze einen Fokus auf die individuellen Handlungen der vertrauenden Akteurinnen und Akteure. Exemplarisch sind hier Überlegungen, die Vertrauen als individuelles Risikomanagement begreifen. Niklas Luhmann (2001, 149) zufolge könne nur dann sinnvoll von Vertrauen gesprochen werden, sofern Akteurinnen und Akteure über die Möglichkeit verfügen, die Risiken des Vertrauens zu reflektieren. Sofern Akteurinnen und Akteure lediglich positive Zukunftserwartungen pflegen, ohne dabei die Risiken von Entscheidungen beurteilen zu können, können sie nicht vertrauen, sondern nur zuversichtlich sein. Um sinnvollerweise von Vertrauenshandlungen sprechen zu können, müssen Akteurinnen und Akteure sich vielmehr für einen bestimmten Handlungskurs entscheiden und damit verbundene Risiken einschätzen können. Vertrauen bedeutet in diesem Zusammenhang, individuell wahrgenommene Risiken suspendieren zu können. Risiken werden bei Vertrauenshandlungen mit anderen Worten so behandelt, „als *ob* sie unproblematisch seien" (Möllering 2011, 291, kursiv im Original). Vertrauen ermöglicht gemäß dieser Überlegungen Handlungen in Situationen, in denen Akteure nur über begrenztes Wissen verfügen und mit Risiken konfrontiert werden. Vor diesem Hintergrund wird Vertrauen vielfach eine komplexitätsreduzierende und handlungsentlastende Bedeutung zugeschrieben (Luhmann 2000, 27 ff.).

Demgegenüber finden sich Theorien, die weniger individuelles Vertrauen als vielmehr die kollektiven und meist implizit bleibenden normativen Grundlagen des Vertrauens in den Vordergrund rücken. Dass Vertrauensphänomene eine normative Fundierung aufweisen, zeigt sich daran, dass enttäuschtes Vertrauen vielfach eine Reaktion der Empörung hervorruft (Hartmann 2011, 179). Ein wesentliches Merkmal für Vertrauen ist, dass auch nach einem Vertrauensbruch die enttäuschten Erwartungen nicht infrage gestellt werden. Vertrauenserwartungen sind vor diesem Hintergrund stets normative Erwartungen (Holton 1994, 4). Enttäuschtes Vertrauen ist dabei „mit der Annahme verbunden, dass der andere *uns* so nicht hätte behandeln dürfen" (Hartmann 2011, 179, kursiv im Original). Wenn Vertrauen gebrochen wurde, sind diejenigen, denen vertraut wurde, Verantwortlichkeiten nicht nachgekommen, die Vertrauende unterstellt hatten (Walker 2006, 80). Mit anderen Worten geht mit Vertrauen stets eine Delegation von Verantwortung an andere Akteurinnen und Akteure einher, die sich auf die Erfüllung normativer Erwartungen bezieht. Solche Erwartungen sind vertrauenden Personen meist weder bewusst noch reflexiv zugänglich, sondern liegen ihren Prak-

tiken implizit zugrunde. Der implizite Charakter von Vertrauenspraktiken wird insbesondere daran deutlich, dass normative Vertrauenserwartungen oftmals erst in der Folge eines Vertrauensbruchs offenkundig werden. Vertrauenserwartungen oder Vertrauenshandlungen sind damit gerade nicht auf individuelle Präferenzen oder bewusste Entscheidungen zu reduzieren (Endreß 2001, 176).

Der normative und implizite Charakter von Vertrauenserwartungen spielt schließlich auch eine zentrale Rolle, wenn es um Privatheit und Datenschutz geht. Auch wenn keine genaue Kenntnis über die involvierten Akteurinnen und Akteure besteht, die Daten von Verbraucherinnen und Verbrauchern erheben, verarbeiten und mit Dritten teilen, werden dennoch normative Erwartungen an die Datennutzung von Internetunternehmen herangetragen. Viele Verbraucherinnen und Verbraucher erwarten fast selbstverständlich, dass Informationen aus unterschiedlichen sozialen Kontexten nicht in illegitimer Weise miteinander verknüpft werden (Nissenbaum 2010). Sie gehen beispielsweise davon aus, dass auch in digitalen Umgebungen in angemessener Weise mit sensiblen Gesundheitsdaten umgegangen wird. Sofern etwa Gesundheitsdaten ohne Zustimmung in der Personalakte des Arbeitgebers landen, wird dies als grundlegende Vertrauens- und Privatheitsverletzung wahrgenommen (Martin 2016, 559). Privatheit setzt somit stets Vertrauen in kollektive Praktiken voraus, welche die Angemessenheit von Informationsflüssen garantieren. Verbraucherinnen und Verbraucher entscheiden sich nicht explizit für dieses Vertrauen, sondern legen es stillschweigend ihren Praktiken zugrunde (Becker und Seubert 2016, 77).

Im Folgenden diskutieren wir diese vertrauenstheoretischen Überlegungen im Licht möglicher Gestaltungsoptionen des Datenschutzes. Dabei wird deutlich, dass aus den vorgestellten Theorieperspektiven unterschiedliche Kriterien der Vertrauensbildung und der Gestaltung des Datenschutzes abgeleitet werden können. Dafür werden wir im nächsten Kapitel zunächst die Herausforderungen von Strategien zur Vertrauensbildung in den Blick nehmen, die Vertrauen als individuelles Risikomanagement begreifen. Nach einer kritischen Auseinandersetzung mit der Frage der Problemangemessenheit dieser Strategien folgt schließlich eine Diskussion von Ansätzen zur Datenschutzgestaltung, welche der Normativität und Kollektivität von Vertrauensphänomenen Rechnung tragen.

3 Vertrauen durch Aufklärung oder Entscheidungsarchitekturen

In diesem Kapitel werden wir zunächst klären, wie versucht wird, Vertrauen herzustellen, wenn dieses als individuelles Risikomanagement verstanden wird. Ein solches Vertrauensverständnis setzt voraus, dass Verbraucherinnen und Verbraucher über Risiken aufgeklärt werden können und auf dieser Grundlage informierte Entscheidungen treffen. Solche Ansätze der Vertrauensbildung müssen entsprechend versuchen, Verbraucherinnen und Verbraucher auch unter Bedingungen umfassender Datenverarbeitung, wie sie etwa in SNS oder im Internet der Dinge allgegenwärtig sind, informierte Entscheidungen zu ermöglichen. Exemplarisch sind hier Versuche, komplizierte Nutzungsvereinbarungen von Internetdiensten derart aufzubereiten, dass sie für Verbraucherinnen und Verbraucher verständlich sind und eine aufgeklärte Entscheidung nach sich ziehen. Verbraucherinnen und Verbraucher können in dieser Logik nur dann vertrauensbasierte Entscheidungen treffen, wenn sie über Privatheitsrisiken in Kenntnis gesetzt werden (Jandt 2008, 58; Pieters 2011, 57). Diese Strategie der Vertrauensbildung ist naheliegend, wenn Vertrauen als individuelles Risikomanagement verstanden wird. Allerdings fragt sich, inwiefern die dabei zugrundeliegende Vorstellung von rational kalkulierenden Akteurinnen und Akteuren den tatsächlichen Praktiken der Verbraucherinnen und Verbraucher entspricht. Versuche der Informierung und Aufklärung können auch zu einer Überforderung von Verbraucherinnen und Verbrauchern durch widersprüchliche Anforderungen führen. Einerseits werden informierte Entscheidungen und Kenntnisse über Datenschutzrisiken erwartet, andererseits setzen zeitgenössische Praktiken auf die vielfältige Verbreitung persönlicher Informationen. Etablierte Datenschutzprinzipien wie Datensparsamkeit oder individuelle Informationskontrolle werden dabei von den Praktiken der Verbraucherinnen und Verbraucher unterlaufen (Ladeur 2015).

Greifbar wird diese Problematik etwa an Praktiken des Fitness-Tracking, bei denen individuelle körperliche Aktivitäten durch vernetzte tragbare Geräte in Form von Mobiltelefonen oder Armbändern aufgezeichnet und ausgewertet

werden. Im Fitness-Tracking kreuzen sich unterschiedliche gesellschaftliche Dynamiken und damit verbundene Anforderungen (Husemann und Pittroff 2018). Die Attraktivität von Fitness-Tracking-Anwendungen für Verbraucherinnen und Verbraucher erklärt sich in diesem Licht durch zwei aktuelle Trends: Zum einen gelten biologische Parameter wie Gesundheitsdaten als gute Grundlage, um eine Verbesserung des Lebens insgesamt herbeizuführen und Fitness-Tracking hilft hier, die dafür nötigen Daten herzustellen (Gertenbach und Mönkeberg 2016). Zum anderen kann ein Trend zur Profilierung identifiziert werden, bei dem die Gestaltung und Ausstellung individueller Subjektivität durch die Veröffentlichung persönlicher Daten in Form von Profilen mittels SNS im Mittelpunkt steht (Reckwitz 2017). Hier helfen die Daten des Fitness-Trackings den Verbraucherinnen und Verbrauchern bei der Pflege und Optimierung einer profilförmigen Identität. Diese doppelte Einbettung der Praktiken des Fitness-Trackings macht deutlich, dass es nicht nur um ein Problem mangelhafter Aufklärung oder fehlender Durchsetzung normativer Prinzipien des Datenschutzes geht.

Auf diese Problemstellungen reagieren vermeintlich Strategien der Vertrauensbildung, welche ebenso auf die Veränderung von Verbraucherpraktiken setzen, dabei aber stärker die Kontextbedingungen individueller Verbraucherentscheidungen in den Vordergrund rücken. Exemplarisch sind hier verhaltensökonomische Ansätze, die auf Techniken des „Nudgings“ setzten, durch die individuelle Entscheidungen in bestimmte Richtungen geschoben („genudged“) werden sollen (Thaler und Sunstein 2009). Im Zentrum stehen hier sogenannte Entscheidungsarchitekturen, also die Gestaltung von Situationen, in denen bestimmte Entscheidungen erleichtert und andere erschwert werden sollen. So können Verbraucherinnen und Verbraucher beispielsweise durch die Gestaltung von Benutzeroberflächen oder Techniken der visuellen Repräsentation dazu bewegt werden, Entscheidungen zu treffen, die individuellen Privatheitspräferenzen Rechnung tragen (Acquisti 2009, 84). Wenngleich durch die Gestaltung von Entscheidungsarchitekturen die Kontextbedingungen von Verbraucherentscheidungen stärker in den Vordergrund rücken, setzen diese Strategien weiterhin vordergründig auf eine *Verhaltensveränderung der Verbraucherinnen und Verbraucher*. Dabei wird der Vorstellung eines rational kalkulierenden Entscheidungssubjekts zwar kritisch begegnet, individuelle Entscheidungen bleiben allerdings die normative Grundlage dieser Strategien. Rationale Entscheidungen werden nicht als empirische Gege-

benheit vorausgesetzt, sondern Verbraucherinnen und Verbraucher sollen zu rationalen Handlungen „genudged“ werden.

Indes verweisen soziologische Forschungen darauf, dass rational kalkulierende und entscheidende Akteurinnen und Akteure stets durch die Gestaltung von Situationen und Kontexten hervorgebracht werden. Dabei zeigen etwa Erkenntnisse aus den Science and Technology Studies, wie Akteurinnen und Akteure durch die Rahmung von Entscheidungssituationen erst zum reflexiven und rationalen Kalkulieren gebracht werden (Yeung 2017). Situationen der Entscheidung sind nicht einfach von sich aus gegeben, sondern entstehen durch Praktiken, die Technologien, Wissen und Interaktion organisieren (Mol 2008, 8). Dementsprechend können autonom entscheidende Akteurinnen und Akteure nicht ohne Weiteres vorausgesetzt werden. Darüber hinaus ist den kollektiven und normativen Grundlagen nachzuspüren, die der Gestaltung von Entscheidungsarchitekturen zugrunde liegen und so bestimmte Vorstellungen von Verbraucherinnen und Verbrauchern nahelegen. Schließlich bleibt oft ungeklärt, wer an der Gestaltung von Entscheidungsarchitekturen beteiligt ist. Sofern diese Gestaltung nicht von öffentlicher Diskussion und Kritik, professionsethischen Standards und transparenten rechtsstaatlichen Verfahren begleitet wird, ist die demokratische Legitimität von Entscheidungsarchitekturen fraglich (Yeung 2017, 119).

Abschließend stellt sich die Frage, ob Aufklärungsversuche oder Entscheidungsarchitekturen, die auf individuelle Verhaltensänderungen von Verbraucherinnen und Verbrauchern abstellen, Probleme adressieren können, die in Folge von Big-Data-Technologien aufkommen. Big Data bezeichnet Techniken der Erhebung und Auswertung von relativ vielen und relativ verschiedenen Daten (boyd und Crawford 2012). Damit ist die Hoffnung verbunden, mithilfe dieser neuen Methoden neue Erkenntnisse zu generieren. Sofern allerdings viele Risiken und Potenziale von Big-Data-Anwendungen erst durch zukünftige Verknüpfungen von Daten entstehen, auf die Verbraucherinnen und Verbraucher keinen unmittelbaren Einfluss haben, erscheinen Ansätze der Vertrauensbildung als unangemessen, die lediglich auf die Veränderung von Verbraucherentscheidungen setzen. Denn die soziotechnische Komplexität von Big Data bedingt, dass Verbraucherinnen und Verbraucher zukünftige Prozesse der Datennutzung nur schwerlich individuell kontrollieren können (Hirsch 2014, 390). Und selbst wenn Verbraucherinnen und Verbraucher zu informierten Entschei-

dungen in der Lage wären, könnte damit nicht den kollektiven Risiken begegnet werden, die durch korrelationsbasierte Big-Data-Analysen hervorgebracht werden (Albers 2014, 225). So erlauben Big-Data-Analysen auf der Grundlage von Nutzungspraktiken oft auch Rückschlüsse auf Personen, die bei keinem Online-Dienst registriert sind. Mit anderen Worten können auch sogenannte Nicht-Nutzerinnen und -Nutzer von Entscheidungen datenverarbeitender Organisationen betroffen sein, ohne dass sie einer Nutzungsvereinbarung zugestimmt haben (Matzner 2014).

Damit wird deutlich, dass Strategien zur Vertrauensbildung, die primär auf die Veränderung von Nutzungsverhalten setzen, insbesondere im Kontext der Herausforderungen von Big Data an Grenzen stoßen. In diesem Sinne wird die Frage nach alternativen Konzepten der Datenschutzgestaltung und Vertrauensbildung relevant, welche die hier besprochenen Problemstellungen ernst nehmen. Im Folgenden werden die damit einhergehenden Herausforderungen der Datenschutzgestaltung in den Blick genommen.

4 Vertrauen und alternative Ansätze Datenschutzregulierung

Im vorangegangenen Abschnitt wurde deutlich, dass Versuche der Modifizierung von Nutzungsverhalten durch Aufklärung oder Entscheidungsarchitekturen, die auf Techniken des Nudgings setzen, kaum problemangemessene Reaktionen auf gegenwärtige Datenschutzprobleme sind. Um in dieser Situation neue Gestaltungsspielräume zu gewinnen, bedarf es vielmehr Ansätze der Datenschutzgestaltung, die von vornherein auf einer kollektiven Ebene ansetzen. Im Folgenden werden wir argumentieren, dass ein Vertrauensverständnis, das die kollektiven und normativen Bedingungen des Vertrauens ernst nimmt, wesentliche Impulse für die Fortentwicklung des Datenschutzes bieten kann.

4.1 Vertrauensinfrastrukturen und die Krise der Privatheit

Um neue Lösungsansätze der Datenschutzgestaltung zu entwickeln, betonen aktuelle Diskussionen zur Fortentwicklung des Datenschutzes die Bedeutung der Vertrauenskategorie (Eichenhofer 2016, 49 f.; Richards und Hartzog 2016). Für die Einordnung dieser Überlegungen ist es unerlässlich, die in Kapitel 2 vorgestellten Überlegungen zu den normativen und kollektiven Dimensionen des Vertrauens in den Blick zu nehmen. Dabei argumentieren wir, dass Vertrauen stets eine Delegation von Verantwortung und Kontrolle impliziert, die auf der Grundlage normativer Erwartungen erfolgt. Dementsprechend fragt sich, an welche Akteurinnen und Akteure welche Verantwortungen delegiert werden können und welche normativen Erwartungen dabei relevant sind. Dabei setzt begründetes Vertrauen in Praktiken der Datennutzung ein problemangemessenes Zusammenspiel verschiedener Akteurinnen und Akteure, Institutionen und regulativer Techniken voraus. Nicht nur müssen Verbraucherinnen und Verbraucher darauf vertrauen können, dass Praktiken von Internetunternehmen bestimmten normativen Standards gerecht werden; ebenso ist gerechtfertigtes Vertrauen in Gesetzgebung und regulative Instrumente sicherzustellen, welche die Einhaltung von Datenschutzstandards kontrollieren und Verletzungen von normativen Erwartungen sanktionieren können (Will 2015). Dabei verweisen die Herausforderungen des Datenschutzes auf die Institutionalisierung von *Vertrauensinfrastrukturen*, die einen angemessenen Umgang mit Daten auch unabhängig von individuellen Verbraucherentscheidungen gewährleisten (Mayer-Schönberger und Padova 2016, 332). Damit rückt die Frage in den Vordergrund, wie rechtliche, technische, politisch-institutionelle und zivilgesellschaftliche Ressourcen mobilisiert werden können, welche die Kontrolle und Reproduktion normativer Erwartungen an Praktiken der Datennutzung sicherstellen. Diese Herausforderungen des Datenschutzes als Herausforderungen der Gestaltung von Vertrauensinfrastrukturen zu begreifen bedeutet schließlich, den Fokus auf die Analyse der Dynamiken zwischen verschiedenen Akteurinnen und Akteuren, Institutionen, sozialen Praktiken, Technologien etc. auszuweiten (Star 1999). Dabei geht es insbesondere um die Frage, wie eine Verteilung von Verantwortlichkeiten auf verschiedene Akteurinnen und Akteure wie etwa Anbieter, Datenschützer sowie Verbraucherinnen und Verbraucher sichergestellt werden kann. Von Vertrauensinfrastrukturen wird im Folgenden

gesprochen, wenn eine problemangemessene Verteilung von Verantwortlichkeiten unterstellt werden kann, die sich den Herausforderungen der Datenschutzgestaltung annimmt.

Wird Vertrauen in dieser Weise als Delegation von Verantwortung verstanden, dann rücken Praktiken datenverarbeitender Organisationen und nicht individuelle Verbraucherhandlungen in den Vordergrund der Datenschutzgestaltung (Balkin 2016). In diesem Sinne müssen Verbraucherinnen und Verbraucher darauf vertrauen können, dass die Datennutzungspraktiken von Organisationen den normativen Erwartungen an Informationsflüsse gerecht werden (Nissenbaum 2010).

Sobald Fragen nach der Angemessenheit von Informationsflüssen und damit nach der konkreten Verwendung von Daten in den Vordergrund rücken, kann sich Datenschutz nicht mehr auf die Regulierung von Datenerhebungen beschränken. Beispielhaft für eine solche Beschränkung ist das sogenannte Verbot mit Erlaubnisvorbehalt, das nach wie vor das Datenschutzrecht bestimmt. Dieses Prinzip sieht vor, dass nur solche Datenerhebungen zulässig sind, in die Verbraucherinnen und Verbraucher ausdrücklich zugestimmt haben. Während dieses Prinzip zu Anfangszeiten des Datenschutzes eine individuelle Informationskontrolle von Datenerhebungen ermöglichen sollte und damit zur Stärkung der Position von Verbraucherinnen und Verbrauchern gegenüber datenverarbeitenden Organisationen gedacht war, wird es in Zeiten umfassender Datenverarbeitung zunehmend dysfunktional. Denn sofern nur solche Daten erhoben werden dürfen, für die eine Einwilligung vorliegt, sind letztlich weitgehend pauschale und fiktive Einwilligungserklärungen die Regel (Ladeur 2015, 238; Schermer et al. 2014).

Eine solche Ausrichtung des Datenschutzes bringt nicht nur eine Reihe indirekter Nebenfolgen hervor. Eine Datenschutzgestaltung, die primär auf eine Begrenzung der *Datenerhebung* setzt, hat außerdem zur Folge, dass Herausforderungen der Vertrauenskonstitution vernachlässigt werden. So richten sich Vertrauenserwartungen nicht in erster Linie darauf, dass keine Daten erhoben werden dürfen oder Datenerhebungen einer individuellen Kontrolle zugeführt werden können. Vielmehr beziehen sich Vertrauenserwartungen darauf, dass konkrete Praktiken der *Datennutzung* kontextspezifischen informationellen Normen gerecht werden (Nissenbaum 2010, 231).

Indes bedeutet eine Ausrichtung des Datenschutzes, die auf explizite Einwilligungen für Datenerhebungen fokussiert, dass kontextspezifische informationelle Normen gerade nicht im Zentrum der Datenschutzregulierung stehen. Denn sofern darauf vertraut werden könnte, dass organisationale Praktiken der Datennutzung normativen Vertrauenserwartungen gerecht werden, müsste nicht für jede Datenerhebung eine explizite Einwilligung eingeholt werden (Schermer et al. 2014, 180; Sloan und Warner 2014). Die Fokussierung auf explizite Einwilligungen für Datenerhebungen ist mit anderen Worten symptomatisch für die Abwesenheit angemessener institutioneller Vertrauensgarantien und informationeller Normen, die für eine Regulierung der Verwendungsweise von Daten unerlässlich sind (Etzioni 2015, 25 f.). Da entsprechend keine verbindlichen sozialen Regeln und Normen der Datennutzung vorausgesetzt werden können, muss letztlich auf rechtliche Verbote der Datenerhebung gesetzt werden (Etzioni 2015, 25).

Eine Umstellung des datenschutzrechtlichen Fokus von der Regulierung der Datenerhebung auf die Verwendungsweise von Daten kann aber nicht nur vor dem Hintergrund einer vertrauenstheoretischen Perspektive begründet werden. Sie ist gegenwärtig umso dringlicher, insofern die Risiken und Potenziale von Big Data sich oftmals auf der Ebene der Datenverwendung zeigen. So kann durch eine Begrenzung der Datenerhebung nicht angemessen den Risiken von Big Data begegnet werden. Denn selbst wenn nur sehr wenige Daten erhoben werden, kann die zukünftige Zusammenführung verschiedener Daten erhebliche Privatheitsrisiken für Verbraucherinnen und Verbraucher mit sich bringen. Darüber hinaus wird der Blick für die Chancen von Big Data verschlossen, sofern Datenschutz in erster Linie auf die Begrenzung von Datenerhebungen setzt. Eine komplexitätsgerechte Big-Data-Regulierung, die den Blick für die Chancen und Potenziale von Big Data öffnet, muss entsprechend auf der Ebene der konkreten Datenverwendung ansetzen (Cate et al. 2014; Etzioni 2015, 19).

Wenngleich der Vorschlag einer Regulierung der konkreten Datennutzung eine sinnvolle Fortentwicklung des Datenschutzes verspricht, werden damit anspruchsvolle Bedingungen an die Datenschutzgestaltung herangetragen. Nicht nur ist weitgehend unklar, welche normativen Erwartungen und sozialen Regeln als kollektiv verbindlich unterstellt werden können, die etwa einer Regulierung der Datenverwendung im Kontext von Big Data zugrunde gelegt

werden können (Sloan und Warner 2014). Auch sind Fragen der kollektiven Verteilung von Verantwortung für Herausforderungen der Datenschutzgestaltung ungeklärt. Dass Verbraucherinnen und Verbraucher schließlich für Herausforderungen der Privatheit verantwortlich gemacht werden, die genau besehen kollektive Anstrengungen verlangen, ist entsprechend symptomatisch für die gegenwärtige Vertrauenskrise (Matzner et al. 2016). Auf diese Herausforderungen muss eine *Gestaltung* von Vertrauensinfrastrukturen antworten. Im nächsten Kapitel stellen wir deshalb Überlegungen zur Gestaltung von Vertrauensinfrastrukturen an, welche diese Herausforderungen des Datenschutzes in den Vordergrund rücken.

4.2 Ansatzpunkte der Gestaltung von Vertrauensinfrastrukturen

Im Folgenden werden wir im Sinne einer gleichzeitigen „Professionalisierung und Demokratisierung der Verbraucherpolitik" (Lamla 2013, 390, 394 f.) exemplarische Ansatzpunkte für Gestaltungsherausforderungen des Datenschutzes vorstellen. Wir werden einerseits für die Entwicklung neuer Professionen plädieren, die innerhalb von Organisationen normativ angemessene Praktiken der Datennutzung sicherstellen. Andererseits werden wir für eine Kontrolle von datenverarbeitenden Organisationen durch intermediäre Organisationen und eine breitere Öffentlichkeit argumentieren.

4.2.1 Professionalisierung

Zunächst fragt sich, wie innerhalb datenverarbeitender Organisationen normativ angemessene Praktiken der Datennutzung ermöglicht werden können. Wenn es um die Regulierung organisationaler Praktiken der Datennutzung geht, sind zunächst Überlegungen zur Institutionalisierung von Professionen unerlässlich. In diesem Zusammenhang ist insbesondere an Professionen zu denken, die als sogenannte *Informationstreuhänder* agieren (Balkin 2016). Informationstreuhänder sind klassischerweise in Medizin und Recht angesiedelt. Diesen Professionen wird nicht nur Vertrauen hinsichtlich ihrer Expertise entgegengebracht. Ebenso wird von ihnen erwartet, dass sie einen ehrlichen, diskreten und loyalen Umgang mit den sensiblen Informationen ihrer Klien-

tinnen und Klienten pflegen (Richards und Hartzog 2016, 457). Allerdings fragt sich, was es genau bedeutet, Professionen wie der Ärzteschaft zu vertrauen. In der Regel besteht keine persönliche Beziehung zwischen Professionen und ihren Klientinnen und Klienten und damit auch keine persönliche Vertrautheit, die Vertrauen rechtfertigen könnte. Eine Antwort auf diese Frage geben etwa die ethischen Standards, denen Ärztinnen und Ärzte unterstehen und deren Einhaltung von unabhängigen Organisationen wie Ärzteverbänden kontrolliert wird. Es ist dieses Bewusstsein über die normative Infrastruktur, in die Professionen eingebettet sind, die Vertrauen rechtfertigt (Hartmann 2011, 285).

Wie können diese Grundüberlegungen schließlich auf die Herausforderungen des Datenschutzes übertragen werden? Wenngleich die Praktiken der Datennutzung von Facebook grundlegende Unterschiede zu klassischen Informationstreuhändern aufweisen, wird in neueren Überlegungen auf die strukturellen Ähnlichkeiten zwischen klassischen Professionen und Internetunternehmen verwiesen (Balkin 2016, 1221). Zunächst zeichnet sich das Verhältnis von Professionen und ihren Klientinnen und Klienten ebenso wie das Verhältnis zwischen Verbraucherinnen und Verbrauchern und Internetunternehmen durch erhebliche Informationsasymmetrien aus. Weder die Praktiken von Professionen noch organisationale Datennutzungspraktiken von Internetunternehmen sind für Außenstehende leicht verständlich. Und selbst wenn hinreichend Informationen über diese Praktiken vorhanden wären, wäre es kaum möglich, sowohl die Datennutzungspraktiken von Internetdiensten als auch die Praktiken klassischer Professionen individuell zu kontrollieren. Und ebenso wie viele Verbraucherinnen und Verbraucher von den Leistungen klassischer Professionen abhängig sind, stellen auch Internetdienste zentrale Infrastrukturen für zeitgenössische Sozialität bereit. Dementsprechend sind Verbraucherinnen und Verbraucher in besonderer Weise auf ein normativ gerechtfertigtes Vertrauen in die Praktiken von Internetunternehmen angewiesen (Balkin 2016, 1183).

Die wesentliche Leistung von Professionen besteht nun einerseits darin, dass sie stellvertretend für Verbraucherinnen und Verbraucher und deren Interessen agieren. Dabei können Informationstreuhänder den Überforderungstendenzen entgegenwirken, die im Zusammenhang des Umgangs mit Datenschutzherausforderungen für Verbraucherinnen und Verbraucher bestehen. Andererseits erfüllen Professionen als Informationstreuhänder wesentliche Leistungen für die Reproduktion von normativ gehaltvollen Praktiken: Professionen tragen insbe-

sondere dazu bei, dass abstrakte Datenschutzprinzipien an konkrete Praktiken angebunden werden (Vedder und Naudts 2017, 14). Mit Blick auf die Praktiken von Professionen erscheint es deshalb als unangemessen, die Vertrauensbeziehungen zu Informationstreuhändern vertragstheoretisch aufzulösen oder auf die Einhaltung rechtlicher Grundsätze zu reduzieren (Balkin 2016, 1201). Vielmehr wird mit dem Verweis auf Professionalisierungsprozesse anerkannt, dass eine Regulierung unzureichend ist, die auf die Durchsetzung von abstrakten Datenschutzprinzipien setzt und dabei den Bezug zu organisationsinternen Praktiken der Datennutzung verliert.

Wenngleich damit deutlich wird, dass eine Professionalisierung von Informationstreuhändern auf Probleme der Regulierung organisationaler Praktiken antworten kann, bleiben eine Reihe offener Fragen. So ist gegenwärtig ungeklärt, welche Organisationen die ethischen Standards kontrollieren, denen die Praktiken von Informationstreuhändern unterliegen. Unklar ist außerdem, aus welchen Akteurinnen und Akteuren sich Informationstreuhänder zusammensetzen sollen. Geht es um die Entwicklung einer grundlegend neuen Profession, die gleichermaßen ethische, rechtliche und informatische Expertise miteinander vereint oder kommen vielmehr verschiedene Professionen infrage, die sich den Herausforderungen der organisationalen Regulierung der Datennutzung annehmen (Vedder und Naudts 2017, 14)? Darüber hinaus können professionelle Praktiken innerhalb datenverarbeitender Organisationen nicht allen Herausforderungen der Vertrauensbildung begegnen. So kann begründetes Vertrauen und die Vertrauenswürdigkeit organisationaler Praktiken nur dann gewährleistet werden, wenn disruptive Praktiken der Datennutzung überhaupt transparent werden und wirksame Sanktionen für Datenschutzverstöße mobilisiert werden können. Und schließlich bleiben die normativen Erwartungen und Verantwortlichkeiten unklar, die an Informationstreuhänder adressiert werden, sofern keine kollektiv und normativ verbindlichen sozialen Regeln der Datennutzung unterstellt werden können, die etwa zur Regulierung von Big Data herangezogen werden könnten. Vor diesem Hintergrund stellt sich die Frage nach institutionellen Strukturen und regulativen Techniken, die normative Prinzipien des Datenschutzes kontrollieren, Vertrauensbrüche sanktionieren und die Entwicklung neuer sozialer Regeln der Datennutzung ermöglichen. Im nächsten Abschnitt argumentieren wir, dass für diese Problemstellungen der Datenschutzgestaltung intermediäre Organisationen unerlässlich sind.

4.2.2 Intermediäre Organisationen

Wenn wir im Folgenden von intermediären Organisationen sprechen, ist mithin an Organisationen wie „Stiftung Warentest", NGOs oder Aufsichtsbehörden im Feld der Finanzmarkt- oder Umweltregulierung zu denken. Intermediäre Organisationen kontrollieren die Einhaltung regulativer Standards, machen Verstöße gegen Normen transparent und geben damit schließlich öffentlich Auskunft über die Vertrauenswürdigkeit der regulierten Organisationen. Grundsätzlich kommt solchen Intermediären die Aufgabe zu, die Verwirklichung regulativer Zielsetzungen zu unterstützen. Dabei befinden sich intermediäre Organisationen genau zwischen regulierenden Instanzen und Regelungsadressaten (Abbott et al. 2017, 7).

Werden intermediäre Organisationen im Zusammenhang der Herausforderungen des Datenschutzes zum Thema gemacht, wird häufig für unabhängige Aufsichtsbehörden argumentiert, die für die Kontrolle organisationaler Praktiken der Datennutzung zuständig sind (Mantelero 2016, 252; Mittelstadt et al. 2016, 13; Tutt 2017). Aufsichtsbehörden würden prüfen, inwiefern datenverarbeitende Organisationen Maßnahmen zur Verringerung, Vermeidung und Identifizierung von Datenschutzrisiken ergreifen. Eine solche Rechenschaftspflicht datenverarbeitender Organisationen gegenüber Aufsichtsbehörden hat zum Ziel, dass Internetunternehmen nicht erst dann für ihre Praktiken haften, nachdem Datenschutzrisiken zu tatsächlichen Problemen geführt haben. Vielmehr geht es darum, die Betreiber von Internettechnologien zu einer proaktiven Verantwortungsübernahme für den Umgang mit Risiken der Datennutzung zu veranlassen. In diesem Sinne wären datenverarbeitende Organisationen dazu angehalten, gegenüber Aufsichtsbehörden nachzuweisen, dass ihre Praktiken normativen Kriterien der Datennutzung gerecht werden (Costa 2012). Darüber hinaus ist es unerlässlich, dass die Ergebnisse unabhängiger Kontrollen veröffentlicht werden. Dabei könnte die verbindliche Vergabe von Zertifikaten durch unabhängige Vertrauensintermediäre darüber Auskunft geben, inwiefern datenverarbeitende Organisationen Vorsorgemaßnahmen für die Nutzung von Risikotechnologien übernehmen (Will 2015, 12). Kriterien der Zertifizierung sollten dabei flexibel und anpassungsfähig sein, um auf neue Datenschutzrisiken und Technologieentwicklungen rechtzeitig reagieren zu können (Bile et al. 2018, 97). Sofern eine Institutionalisierung verbindlicher Zertifizierungsmaßnahmen erfolgt, wird das Problem der Vertrauensbildung nicht mehr im

Sinne einer Ermöglichung individueller Vertrauenshandlungen begriffen, die etwa durch Verbraucheraufklärung zuwege gebracht wird. Vielmehr besteht die Herausforderung der Vertrauenskonstitution in der Schaffung von Institutionen, die Praktiken von datenverarbeitenden Organisationen kontrollieren und Auskunft über die Vertrauenswürdigkeit von datenverarbeitenden Organisationen geben (Bile et al. 2018, 98; Meijboom et al. 2006, 432).

Bei diesen Überlegungen zur Zertifizierung und Kontrolle handelt es sich keineswegs um grundlegend neue Konzepte der Datenschutzgestaltung. Die Notwendigkeit von unabhängigen Kontrollen durch Datenschutz-Audits und Zertifizierung wird seit geraumer Zeit diskutiert (Roßnagel 1997). Allerdings werden diese Instrumente bislang kaum umgesetzt und auch die Datenschutzgrundverordnung sieht keine Pflicht zur Zertifizierung vor. Die Teilnahme an Zertifizierungsmaßnahmen ist für datenverarbeitende Organisationen freiwillig und die Kontrollen durch Aufsichtsbehörden orientieren sich vielfach nur an der Einhaltung bestehender Datenschutzgrundsätze. Anreize für Internetunternehmen zur kontinuierlichen Verbesserung von Datenschutzmaßnahmen werden damit kaum geschaffen, was vor dem Hintergrund rasanter Technologieentwicklungen mit Skepsis zu beurteilen ist (Bile et al. 2018, 95).

Schließlich kann begründetes Vertrauen in Internetunternehmen nur dann gewährleistet werden, wenn Vertrauensbrüche durch disruptive Praktiken der Datennutzung wirksam sanktioniert werden können. Hier wäre beispielsweise denkbar, dass auf Datenschutzverstöße durch einen Entzug von Zertifikaten reagiert wird, was einen Verlust von Reputation und Vertrauenswürdigkeit nach sich ziehen würde. Ebenso könnten Sanktionen auf der Grundlage von Bußgeldern erfolgen. Sanktionspotenziale sollen dabei dazu beitragen, dass Organisationen ihre Praktiken an regulativen Normen orientieren. Sofern regulative Maßnahmen keine wirksamen Sanktionen vorsehen oder diese gar nicht erst erfolgen, weil Datenschutzverstöße nur selten aufgedeckt werden, ist fraglich, ob datenverarbeitende Organisationen sich an regulativen Standards ausrichten (Will 2015, 12).

Zudem hängt die Legitimität und Glaubwürdigkeit regulativer Maßnahmen davon ab, inwiefern Verstöße gegen Standards transparent gemacht werden können (Will 2015, 12). Dieser Bedarf an Transparenz besteht besonders für Fragen des Datenschutzes. Denn Privatheits- und Vertrauensverletzungen

spielen sich vielfach jenseits alltäglicher Erfahrbarkeit ab. Im Gegensatz zu gesellschaftlichen Kontexten, in denen die Verwirklichung von Risiken überaus offensichtlich zu Tage tritt – etwa im Fall von Atomkraft oder industrieller Lebensmittel – generieren Big-Data-Technologien kollektive Risiken, die im Verborgenen bleiben können (Mantelero 2016). Vor diesem Hintergrund ist über Transparenzmaßnahmen nachzudenken, welche die Öffentlichkeit über schädliche Datennutzungstechniken informieren. Allerdings sind Transparenzmaßnahmen, die Datenschutzverstöße der Öffentlichkeit zugänglich machen, mit grundsätzlichen Herausforderungen konfrontiert. Wie etwa Frank Pasquale (2015) ausführlich herausgearbeitet hat, wird die Intransparenz privatökonomischer Praktiken von Dienstanbietern rechtlich durch Geschäftsgeheimnisse abgesichert. In diesem Zusammenhang stellt sich die Frage nach regulativen Techniken, die einerseits das Aufdecken von Datenschutzverstößen erlauben und andererseits keine Geschäftsgeheimnisse verletzen. So zeigt etwa Cohen (2012, 237), dass in anderen gesellschaftlichen Bereichen regulative Techniken entwickelt wurden, die einerseits eine öffentliche Informierung über Verstöße gegen regulative Normen ermöglichen und zugleich die Wahrung von Geschäftsgeheimnissen gewährleisten. Zu denken wäre hier exemplarisch an Finanzaufsichtsbehörden, die dafür zuständig sind, Normverstöße transparent zu machen, dabei aber in der Pflicht stehen, Geschäftsgeheimnisse zu wahren (Black 2003, 20). Dass Datenschutzverstöße und Vertrauensbrüche öffentlich gemacht werden können, trägt nicht nur dazu bei, dass begründetes Vertrauen in die Zuverlässigkeit regulativer Techniken sichergestellt wird. Auch unterscheidet sich die öffentliche Informierung von Verbraucherinnen und Verbrauchern über Vertrauensbrüche ganz grundsätzlich von Maßnahmen der Vertrauensbildung, die auf der Grundlage individueller Aufklärung von Verbraucherinnen und Verbrauchern über Risiken der Datennutzung informieren. Denn das Aufdecken von Vertrauensbrüchen, das durch unabhängige Vertrauensintermediäre initiiert wird, zielt nicht vordergründig auf individuelle Informierung von Verbraucherinnen und Verbrauchern, sondern auf die Herstellung einer kritischen Öffentlichkeit. Dementsprechend muss die Gestaltung von Vertrauensinfrastrukturen immer auch auf die Frage abstellen, wie kommunikative und lernfähige Vertrauensbeziehungen ermöglicht werden können. Vertrauensbeziehungen sind damit, politisch betrachtet, stets demokratische Beziehungen. Die demokratische Legitimität von regulativen Maßnahmen des Datenschutzes entscheidet sich

mit anderen Worten daran, ob Konflikte einer öffentlichen Kontrolle zugeführt werden können (Kohring 2011, 281; Ochs und Lamla 2017).

Zusammenfassend lässt sich festhalten, dass intermediäre Organisationen eine wesentliche Rolle für die Institutionalisierung einer problemangemessenen Vertrauensinfrastruktur übernehmen. Vertrauenswürdigkeit durch die Vergabe von Zertifikaten, unabhängige Kontrollen, Sanktionspotenziale und die Informierung der Öffentlichkeit sind die zentralen Herausforderungen, auf welche eine Institutionalisierung von Vertrauensintermediären reagieren muss. Aber auch hier bleibt offen, wie eine konkrete Institutionalisierung von intermediären Organisationen verwirklicht werden kann und welche Akteurinnen und Akteure dafür infrage kommen. Zu fragen wäre etwa, wie verschiedene Interessengruppen wie etwa Verbraucherinnen und Verbraucher, Regierungen, Internetunternehmen, Wissenschaft, NGOs etc. durch unabhängige Vertrauensintermediäre repräsentiert werden können. Einen Ansatzpunkt bieten hier sogenannte Multi-Stakeholder-Dialoge, die verschiedene Interessengruppen zusammenbringen und von intermediären Organisationen begleitet werden (Will 2015, 13).

5 Fazit

Die vorangegangenen Überlegungen haben deutlich gemacht, dass Vertrauensbildung in der digitalen Welt ein Zusammenspiel verschiedener regulativer Techniken, Institutionen und Akteure erfordert. Dabei haben wir argumentiert, dass ein normativ fundiertes Vertrauensverständnis neue Problemsichten für den Umgang mit Herausforderungen der Datenschutzgestaltung eröffnet. Die zentrale Herausforderung der Vertrauens- und Datenschutzgestaltung besteht darin, dass Verbraucherinnen und Verbraucher auch unabhängig von individuellen Entscheidungen darauf vertrauen können, dass datenverarbeitende Organisationen normativen Erwartungen an Praktiken der Datennutzung entsprechen. Hierbei geht es auch um die Frage, wie solche normativen Erwartungen reproduziert, deren Einhaltung kontrolliert sowie

Vertrauensbrüche sanktioniert werden können. In diesem Zusammenhang wurde deutlich, dass Ansätze zur Vertrauensbildung, die auf die Veränderung von Nutzungspraktiken durch Aufklärung oder Entscheidungsarchitekturen setzen, diesen Herausforderungen kaum gerecht werden. Alternativ plädieren wir für Gestaltungsoptionen, die darauf abzielen, dass datenverarbeitende Organisationen Verantwortung für die Verwendung riskanter Technologien wie Big Data übernehmen. Die zentrale Herausforderung gegenwärtiger Datenschutzgestaltung besteht dabei in der Schaffung neuer Institutionen, welche die Reproduktion, Kontrolle und das Lernen normativ angemessener Praktiken der Datennutzung gewährleisten. In diesem Zusammenhang haben wir exemplarisch die Institutionalisierung professioneller Praktiken und intermediärer Organisationen diskutiert. Insgesamt ist festzuhalten, dass die gegenwärtigen Herausforderungen der Datenschutzgestaltung eine problemangemessene Vertrauensinfrastruktur voraussetzen, die Rahmenbindungen für eine kollektive Verteilung von Verantwortlichkeiten schafft.

Literatur

Abbott, Kenneth, David Levi-Faur und Duncan Snidal. 2017. Introducing regulatory intermediaries. The *ANNALS of the American Academy of Political and Social Science* 670, Nr. 1: 6-13.

Acquisti, Alessandro. 2009. Nudging privacy. The behavioral economics of personal information. *IEEE Security & Privacy* 7, Nr. 6: 82-85.

Albers, Marion. 2014. Realizing the complexity of data protection. In: *Reloading data protection: Multidisciplinary insights and contemporary challenges*, hg. von Serge Gutwith, Ronald Leenes und Paul de Hert, 213-235. Dordrecht: Springer.

Balkin, Jack M. 2016. Information fiduciaries and the first amendment. *UC Davis Law Review* 49, Nr. 4: 1183-1234.

Baumann, Joel und Jörn Lamla, Hrsg. 2017. *Privacy Arena: Kontroversen um Privatheit im digitalen Zeitalter*. Kassel: Kassel University Press.

Becker, Carlos und Sandra Seubert. 2016. Privatheit, kommunikative Freiheit und Demokratie. *Datenschutz und Datensicherheit* 40, Nr. 2: 73-78.

Bile, Tamer, Christian Geminn, Olga Grigorjew, Charlotte Husemann, Maxi Nebel und Alexander Roßnagel. 2018. Fördern und Fordern: Regelungs-

formen zur Anreizgestaltung für einen wirksameren Schutz von Privatheit und informationeller Selbstbestimmung. In: *Privatheit und selbstbestimmtes Leben in der digitalen Welt: Interdisziplinäre Perspektiven auf aktuelle Herausforderungen des Datenschutzes*, hg. von Michael Friedewald, 83-126. Wiesbaden: Springer.

Black, Julia. 2003. *Mapping the contours of contemporary financial services regulation*. London: Centre for Analysis of Risk and Regulation.

boyd, danah und Kate Crawford. 2012. Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society* 15, Nr. 5: 662-679.

Cadwalladr, Carole und Graham-Harrison. 2018. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. 17. März. <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> (Zugriff: 3. April 2018).

Cate, Fred H., Peter Cullen und Viktor Mayer-Schönberger. 2014. Data protection principles for the 21st century: Revising the 1980 OECD Guidelines. Oxford Internet Institute. <https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf>

Cohen, Julie E. 2012. *Configuring the networked self: Law, code, and the play of everyday practice*. London: Yale University Press.

Costa, Luiz. 2012. Privacy and the precautionary principle. *Computer Law & Security Review* 28, Nr. 1: 14-24.

Eichenhofer, Johannes. 2016. Privatheit im Internet als Vertrauensschutz. Eine Neukonstruktion der Europäischen Grundrechte auf Privatleben und Datenschutz. *Der Staat* 55, Nr. 1: 41-67.

Endreß, Martin. 2001. Vertrauen und Vertrautheit. In: *Vertrauen: Die Grundlage des sozialen Zusammenhalts*, hg. von Martin Hartmann und Claus Offe, 161-203. Frankfurt am Main: Campus.

Etzioni, Amitai. 2015. *Privacy in a cyber age: Policy and practice*. New York: Palgrave and Macmillan.

Gertenbach, Lars und Sarah Mönkeberg. 2016. Lifelogging und vitaler Normalismus: Kultursoziologische Betrachtungen zur Neukonfiguration von Körper und Selbst. In: *Lifelogging: Digitale Selbstvermessung und Lebensprotokollierung zwischen disruptiver Technologie und kulturellem Wandel,* hg. von Stefan Selke, 25-43. Wiesbaden: Springer.

Hartmann, Martin. 2011. *Die Praxis des Vertrauens*. Suhrkamp-Taschenbuch Wissenschaft 1994. Berlin: Suhrkamp.

Hirsch, Dennis. 2014. The glass house effect: Big data, the new oil, and the power of analogy. *Maine Law Review* 66, Nr. 2: 374-395.

Holton, Richard. 1994. Deciding to trust, coming to believe. *Australian Journal of Philosophy* 72, Nr. 1: 63-76.

Husemann, Charlotte und Fabian Pittroff. 2018. Smarte Regulierung in Informationskollektiven: Bausteine einer Informationsregulierung im Internet der Dinge. In: *Die Zukunft des Datenschutzes*, hg. von Alexander Roßnagel, Michael Friedewald und Marit Hansen, DuD-Fachbeiträge. Wiesbaden: Springer Vieweg.

Jandt, Silke. 2008. *Vertrauen im Mobile Commerce: Vorschläge für die rechtsverträgliche Gestaltung von Location Based Services*. Baden-Baden: Nomos.

Kohring, Matthias. 2011. Zuversicht statt Vertrauen? Probleme der Vertrauenskonstitution in modernen Gesellschaften. *Erwägen – Wissen – Ethik* 22, Nr. 2: 279-282.

Ladeur, Karl-Heinz. 2012. Neue Institutionen für den Daten- und Persönlichkeitsschutz im Internet: „Cyber-Courts" für die Blogosphere. Datenschutz in Netzwerken gegenüber dem Staat und Providern (insbesondere „social media" wie Facebook). *Datenschutz und Datensicherheit* 36, Nr. 10: 711-715.

—. 2015. Die Gesellschaft der Netzwerke und ihre Wissensordnung: Big Data, Datenschutz und die relationale Persönlichkeit. In: *Die Gesellschaft der Daten*, hg. von Florian Süssenguth, 225-261. Bielefeld: transcript.

Lagerspetz, Olli. 2014. The worry about trust. In: *Trust, computing, and society*, hg. von Richard Harper, 120-143. Cambridge: Cambridge University Press.

Lamla, Jörn. 2013. *Verbraucherdemokratie: Politische Soziologie der Konsumgesellschaft*. Berlin: Suhrkamp.

Luhmann, Niklas. 2000. *Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität*. Stuttgart: Lucius & Lucius.

—. 2001. Vertrautheit, Vertrauen und Zuversicht: Probleme und Alternativen. In: *Vertrauen: Die Grundlage des sozialen Zusammenhalts*, hg. von Martin Hartmann und Claus Offe, 143-160. Frankfurt am Main: Campus.

Mantelero, Alessandro. 2016. Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. *Computer Law & Security Review* 32, Nr. 2: 238-255.

Martin, Kirsten. 2016. Understanding privacy online: Development of a social contract approach to privacy. *Journal of Business Ethics* 137, Nr. 3: 551-569.

Matzner, Tobias. 2014. Why privacy is not enough in the context of „ubiquitous computing" and „big data". *Journal of Information, Communication and Ethics in Society* 12, Nr. 2: 93-106.

Matzner, Tobias, Philipp K. Masur, Carsten Ochs und Thilo von Pape. 2016. Do-it-yourself data protection – Empowerment or burden? In: *Data protection on the move: Current Developments in ICT and Privacy/Data Protection*, hg. von Serge Gutwirth, Ronald Leenes und Paul De Hert, 277-305. Dordrecht: Springer.

Mayer-Schönberger, Viktor und Yann Padova. 2016. Regime change? Enabling Big Data through Europe's new data protection regulation. *The Columbia Science & Technology Law Review*, Nr. 17: 315-335.

Meijboom, Franck, Tatjana Visak und Frans Brom. 2006. From trust to trustworthiness: Why information is not enough in the food sector. *Journal of Agricultural and Environmental Ethics* 19, Nr. 5: 427-442.

Mittelstadt, Brent, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter und Luciano Floridi. 2016. The ethics of algorithms: Mapping the debate. *Big Data & Society* 3, Nr. 2: 1-21.

Mol, Annemarie. 2008. *The logic of care: Health and the problem of patient choice*. London: Routledge.

Möllering, Guido. 2011. Vertrauen als Lösung durch Aufheben. *Erwägen – Wissen – Ethik* 22, Nr. 2: 291-293.

Nissenbaum, Helen. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press.

Ochs, Carsten und Jörn Lamla. 2017. Demokratische Privacy by Design. Kriterien soziotechnischer Gestaltung von Privatheit. *Forschungsjournal Soziale Bewegungen* 30, Nr. 2: 189-199.

Pasquale, Frank. 2015. *The black box society: The secret algorithms that control money and information*. Cambridge: Harvard University Press.

Pieters, Wolter. 2011. Explanation and trust: What to tell the user in security and AI. *Ethics and Information Technology* 13, Nr. 1: 53-64.

Reckwitz, Andreas. 2017. *Die Gesellschaft der Singularitäten*. Berlin: Suhrkamp.

Richards, Neil und Woodrow Hartzog. 2016. Taking trust seriously in privacy law. *Stanford Technology Law Review* 19, 431-472.

Roßnagel, Alexander. 1997. Datenschutz-Audit. *Datenschutz und Datensicherheit* 21, Nr. 9: 505-515.

Schermer, Bart W., Bart Custers und Simone Hof. 2014. The crisis of consent: How stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology* 16, Nr. 2: 171-182.

Schuler, Marcus. 2018. Das war ein großer Vertrauensbruch. *tagesschau*. 22. März. <http://www.tagesschau.de/ausland/zuckerberg-cnn-101.html> (Zugriff: 3. April 2018).

Sloan, Robert H. und Richard Warner. 2014. Beyond notice and choice: Privacy, norms, and consent. *Journal of High Technology Law* 14, Nr. 2: 370-414.

Star, Susan Leigh. 1999. The ethnography of infrastructure. *American Behavioral Scientist* 43, Nr. 3: 377-391.

Statistisches Bundesamt. 2018. IT-Nutzung: Private Nutzung von Informations- und Kommunikationstechnologien. <https://www.destatis.de/DE/ZahlenFakten/GesellschaftStaat/EinkommenKonsumLebensbedingungen/ITNutzung/Tabellen/ZeitvergleichComputernutzung_IKT.html> (Zugriff: 3. April 2018).

Thaler, Richard H. und Cass R. Sunstein. 2009. *Nudge: Improving decisions about health, wealth and happiness*. London: Penguin Books.

Tutt, Andrew. 2017. An FDA for algorithms. *Administrative Law Review* 69, 83-123.

Yeung, Karen. 2017. ‚Hypernudge': Big Data as a mode of regulation by design. *Information, Communication & Society* 20, Nr. 1: 118-136.

Vedder, Anton und Laurens Naudts. 2017. Accountability for the use of algorithms in a big data environment. *International Review of Law, Computers & Technology* 31, Nr. 2: 206-224.

Walker, Margaret Urban. 2006. *Moral repair: Reconstructing moral relations after wrongdoing*. Cambridge: Cambridge University Press.

Will, Matthias Georg. 2015. Privacy and Big Data: The need for a multi-Stakeholder approach for developing appropriate privacy regulation in the age of Big Data. Discussion Paper No. 2015-03 of the Chair in Economic Ethics, Martin-Luther-University Halle-Wittenberg.

Über die Autoren

Markus Uhlmann, M.A. ist wissenschaftlicher Mitarbeiter am DFG-GRK „Privatheit und Vertrauen für mobile Nutzer“ im Fachgebiet Soziologische Theorie an der Universität Kassel. Webseite: https://www.uni-kassel.de/fb05/fachgruppen/soziologie/soziologische-theorie/team/markus-uhlmann-ma.html.

Fabian Pittroff, Dipl. Pol./M.A. ist wissenschaftlicher Mitarbeiter im Graduiertenprogramm „Ökologien des sozialen Zusammenhalts“ und assoziierter Doktorand des DFG-Graduiertenkollegs „Privatheit und Vertrauen für mobile Nutzer“ im Fachgebiet Soziologische Theorie an der Universität Kassel. Webseite: https://www.uni-kassel.de/fb05/fachgruppen/soziologie/soziologische-theorie/team/fabian-pittroff-dipl-pol-ma.html.

Prof. Dr. Jörn Lamla ist Professor für Soziologische Theorie an der Universität Kassel. Webseite: https://www.uni-kassel.de/fb05/fachgruppen/soziologie/soziologische-theorie/team/prof-dr-joern-lamla.html.