Datenschutzrechtliche Gestaltungsmöglichkeiten jenseits der Ermächtigung des Individuums: Die Multi-Stakeholder-Datenschutz-Folgenabschätzung

Murat Karaboga

Zusammenfassung

Die fortschreitende Digitalisierung umfasst immer mehr Bereiche des Alltagslebens. Die damit verbundenen Gefahren waren ein wesentlicher Grund für die Entstehung der Datenschutz-Grundverordnung (DS-GVO), mit der die Ermächtigung des Individuums verfolgt wurde. Ähnlich wie schon in der Vergangenheit in anderen Bereichen (etwa im Verbraucher- oder Umweltschutz), ist angesichts der komplexen Digitalisierungsprozesse in den letzten Jahren jedoch in zunehmendem Maße die Frage in den Vordergrund gerückt, ob und inwiefern sich ein wirksamer Datenschutz auf Grundlage eines individualistischen Konzepts in Form der Ermächtigung des Individuums realisieren lässt. Vor dem Hintergrund dieser Debatten diskutiert der vorliegende Beitrag die Herausforderungen, denen sich individualistische Datenschutz-Konzeptionen ausgesetzt sehen und anschließend anhand ausgewählter Teilbereiche des Datenschutzrechts Lösungsansätze, die über die Fokussierung auf das Individuum hinausgehen und die als eine Art Mittelweg zwischen individualistischen und kollektivistischen Ansätzen verstanden werden können. Im Zentrum der Gestaltungsvorschläge steht die sog. Multi-Stakeholder-Datenschutz-Folgenabschätzung, die gemeinsam mit weiteren überindividuellen Maßnahmen geeignet wäre, die Gefahren moderner Datenverarbeitungen in angemessener Weise zu adressieren.

M. Karaboga (✉)
Fraunhofer-Institut für System- und Innovationsforschung ISI, Competence Center Neue Technologien, Karlsruhe, Deutschland
E-Mail: murat.karaboga@isi.fraunhofer.de

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_14

Schlüsselwörter

Datenschutz • Privatheit • Schutz personenbezogener Daten • Liberal-individualismus • Kollektivschutz • Soziale Privatheit

1 Einführung und Fragestellung

Die Frage, inwieweit der geltende Datenschutzrahmen überhaupt oder noch dafür geeignet ist, einen angemessenen Schutz vor den mannigfaltigen Gefahren moderner Datenverarbeitungen zu gewährleisten, ist in den vergangenen Jahren zunehmend in den Mittelpunkt der Privatheits- und Datenschutzdebatte gerückt. Kritisiert wird insbesondere, dass herrschende Datenschutzgesetze auf Grundlage einer als überholt angesehenen liberal-individualistischen Perspektive das Individuum fokussieren und damit gleich in mehrfacher Hinsicht Privatheit und Datenschutz nur unzureichend erfassen und schützen. Die Vielzahl an Texten zur Kritik an der liberal-individualistischen Aufladung von Privatheitskonzepten lässt sich grob in zwei Kategorien unterteilen. Der erste Literaturstrang befasst sich stärker mit dem Wert bzw. der Bedeutung, welcher Privatheit beigemessen wird. In diesem Literaturstrang wird insbesondere das individualistische anthropologische Grundverständnis kritisiert und etwa danach gefragt, ob Privatheit das Individuum schützt, wie Privatheit und Individualität zusammenhängen, worin der überindividuelle Wert von Privatheit liegt und ob Privatheit den selbstbestimmten Rückzug aus der Gesellschaft meint oder auch die selbstbestimmte Teilhabe meinen kann bzw. vielmehr meinen muss. Der zweite Literaturstrang befasst sich hingegen stärker mit den rechtlichen und praktischen Auswirkungen liberal-individualistisch aufgeladener Datenschutzgesetze. Hier wird einerseits gezeigt, dass die praktische Gestaltung von Datenschutzgesetzen die mit den erlassenen Gesetzen verfolgten Schutzziele konterkariert [1] und auf dieser Grundlage andererseits diskutiert, ob und inwiefern bestimmte datenschutzrechtliche Elemente den erwünschten Schutz besser gewährleisten könnten [2, 3]. Im vorliegenden Beitrag fokussiere ich auf den zweiten Literaturstrang und führe die bestehenden Arbeiten in Richtung der Konzeption konkreter Datenschutzrechte hin. Die forschungsleitende Frage dabei ist, wie Datenschutzrechte ausgestaltet werden könnten, die über die Ermächtigung des Individuums hinausgehen und mit denen die Adressierung der Folgen moderner Datenverarbeitungen besser gelingen könnte, denn die bestehende Literatur behandelt das Thema aktuell auf einer abstrakt-konzeptionellen Ebene [4, 5] oder beachtet auf isolierte Weise

nur einzelne datenschutzrechtliche Elemente [6, 7]. Um die genannte Frage zu beantworten führe ich zunächst anhand einer Diskussion von Teilbereichen der DS-GVO näher aus, worin sich der liberal-individualistische Fokus der Datenschutzgesetzgebung genau äußert. Im Anschluss zeige ich auf, in welcher Hinsicht die liberal-individualistischen Elemente der Datenschutzgesetzgebung kritisiert werden und weshalb die Idee der Ermächtigung des Individuums durch Datenschutzrechte regelmäßig in der Kritik steht. Schließlich diskutiere ich konkrete datenschutzrechtliche Gestaltungsmöglichkeiten, die über die Ermächtigung des Individuums hinausgehen. Hierbei fokussiere ich insbesondere auf das Element einer sog. Multi-Stakeholder-Datenschutz-Folgenabschätzung und zeige auf, wie sich deren Vorgaben mit anderen überindividuellen datenschutzrechtlichen Elementen zu einem soliden Schutzgerüst verbinden lassen könnten, das zur Adressierung der Gefahren moderner Datenverarbeitungen besser geeignet wäre, als das gegenwärtige Schutzregime.

2 Liberal-individualistische Elemente in der DS-GVO

Trotz der inzwischen vorhandenen Fülle an Kritik am liberal-individualistischen Datenschutz-Paradigma, bleibt in aller Regel unklar, welche datenschutzrechtlichen Elemente dem Paradigma der individuellen Kontrolle hinzugezählt werden. Mittels der folgenden Aufzählung bzw. Diskussion sollen anhand der einschlägigen Literatur [1–3, 8] nun daher zunächst die zentralen, dem liberal-individualistischen Datenschutz-Paradigma zuzuordnenden datenschutzrechtlichen Elemente der DS-GVO erörtert werden:

- Datenschutz-Grundsatz der Zweckbindung (Art. 5 (1) b)
- Datenschutz-Grundsatz der Datenminimierung (Art. 5 (1) c)
- Einwilligung (insb. Art. 4 (11), Art. 6 und 7)
- Informations- und Transparenzvorgaben bei der Verarbeitung personenbezogener Daten (Art. 12–14)
- Betroffenenrechte, das Auskunftsrecht (Art. 15), das Recht auf Berichtigung (Art. 16), auf Löschung (Art. 17), auf Einschränkung der Verarbeitung (Art. 18), das Recht auf Datenübertragbarkeit (Art. 20) sowie das Widerspruchsrecht (Art. 21)
- Einwilligung in automatisierte Einzelentscheidungen im Einzelfall einschließlich Profiling (Art. 22 (2) c)
- Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person (Art. 34)
- Rechtsbehelfe (Art. 77–79) und Haftung (Art. 82)

Die *Zweckbindung* stellt zusammen mit dem Recht auf Einwilligung ein zentrales Prinzip des EU-Datenschutzrechts dar. Ebenso wie die Einwilligung, ist auch sie eng verwandt mit dem Grundrecht auf informationelle Selbstbestimmung bzw. der ihr zugrunde liegenden Idee der persönlichen Kontrolle von Datenverarbeitungen [9]. Mit der Zweckbindung soll sichergestellt werden, dass ein Individuum Sicherheit darüber hat, dass eine Verarbeitung nur zu dem vom Individuum eingewilligten oder dem gesetzlich erlaubten Zweck dient [10]. Die Beschränkung der Datenverarbeitung auf das zur Erreichung des angegebenen Zwecks erforderliche Maß, wäre ohne die Angabe jenes Zwecks nicht möglich, sodass die Einwilligung wie auch die anderen Erlaubnistatbestände sowie die Datenschutz-Grundsätze nicht mehr wirksam wären [11]. Das datenschutzrechtliche Prinzip der *Datenminimierung* etwa, bindet die Verarbeitung personenbezogener Daten an den jeweiligen Zweck und verfolgt damit das Ziel, dass keine für die Erreichung eines zuvor bestimmten Zwecks nicht notwendigen personenbezogenen Daten verarbeitet werden: „Wenn etwa der Browser-Fingerprint des Kundenrechners, die zuvor besuchten Seiten sowie Alter und Geschlecht nicht für die Erfüllung eines E-Commerce-Vertrags erforderlich sind, ist die Erhebung dieser Daten zu unterlassen.“ [12] Damit ist das Zweckbindungsprinzip das zentrale Mittel zur „Erzeugung von Kontrollierbarkeit der Informationserhebung, -verarbeitung und -nutzung sowie der dabei verwendeten technischen wie nicht-technischen Mittel, indem es wohlgeordnete Organisationsstrukturen und Prozesse erzeugt, die zugleich transparent gemacht werden können – den Organisationen selbst, vor allem jedoch den Betroffenen und den Aufsichtsbehörden.“ [13]

Deren de lege lata enge Verzahnung mit und der übermäßige Fokus auf die individuelle Einwilligung bzw. individuelle informationelle Selbstbestimmung lassen sie zwar als liberal-individualistische Grundsätze erscheinen, doch sind sowohl das Zweckbindungs- als auch das Datenminimierungsprinzip darüber hinaus auch allgemeine Gestaltungskriterien informationstechnischer Systeme. Gerade die Zweckbindung „dient als konzeptionelle und operationale Klammer um den Prozess von Informationserhebung, -verarbeitung und Entscheidungsfindung, indem sie als Konstante in einem dynamischen Umfeld wirkt und damit einen festen Anker für die Prüfung sowohl der Handlungen wie der eingesetzten Mittel bietet.“ [13]

Der *Einwilligung* kommt im Datenschutzrecht zusammen mit dem Zweckbindungsprinzip eine zentrale Stellung zu: „Die Einwilligung ist der genuine Ausdruck des Rechts auf informationelle Selbstbestimmung.“ [10] Dem Recht auf Einwilligung ist es zu verdanken, dass das seit Mitte der 1970er-Jahre bestehende Problem ausufernder Spezialregelungen und Schutzlücken im Datenschutzrecht adressiert werden konnte [14, 15]. Ein wesentlicher Bestandteil dieses Rechts ist

die Vorstellung, dass die Einwilligung, etwa gemäß Art. 4 (11) DS-GVO, „in informierter Weise“ zu erfolgen hat.

Die detaillierte Bestimmung dessen, was unter „in informierter Weise“ zu verstehen ist, erfolgt in den Artikeln 12 bis 14 DS-GVO. Die informationelle Selbstbestimmung soll insbesondere dadurch erleichtert werden, dadurch dass alle Informationen, die dem Betroffenen dargestellt werden, *in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln* (Art. 12 (1)) sind. In den Folgeartikeln ist schließlich der lange Informationskatalog geregelt, der dem Betroffenen bereitzustellen ist, sofern die Daten beim Betroffenen (Art. 13) oder nicht beim Betroffenen (Art. 14) erhoben werden. Darunter fallen beispielsweise Namen und die Kontaktdaten des Verantwortlichen (Art. 13 (1) a und 14 (1) a), die Verarbeitungszwecke (Art. 13 (1) c und Art. 14 (1) c) oder die geplante Speicherdauer der Daten (Art. 13 (2) a bzw. Art. 14 (2) a).

Einen weiteren Eckpfeiler im liberal-individualistischen Datenschutzrechtsverständnis bildet der Komplex der *Betroffenenrechte.* Mit diesen soll gewährleistet werden, dass die von einer personenbezogenen Datenverarbeitung betroffenen Personen Mitwirkungsmöglichkeiten an der Datenverarbeitung erhalten und diese in ihrem Sinne beeinflussen können. Das Auskunftsrecht bildet dabei die Grundlage für die Wahrnehmung der weiteren, sog. Mitwirkungsrechte (d. h., die Rechte auf Berichtigung, Löschung, Sperrung und Widerspruch), indem sie es dem Betroffenen erlaubt, zu wissen, welche auf die eigene Person bezogenen Daten aus welcher Quelle stammen, zu welchen Zwecken sie verwendet und an wen sie ggf. transferiert werden. Der Idee nach soll sie als sog. *Instrument vorgelagerten Rechtsschutzes* die laufende Kontrolle der Verwendung der eigenen personenbezogenen Daten erlauben, sodass die Möglichkeit eines potenziellen negativen Eingriffs in die informationelle Selbstbestimmung bereits vorab sichtbar wird und der Betroffene entsprechende Maßnahmen ergreifen kann [10]. Ein Beispiel wäre, dass ein mögliches Fehl-Scoring einer Person durch die SCHUFA dadurch verhindert wird, dass jene Person zuvor Gebrauch von ihrem Auskunftsrecht macht, dadurch fehlerhafte Daten entdeckt und diese berichtigen, löschen oder die Verarbeitung einschränken lässt, sodass keine Fehlberechnung stattfindet und auch keine weiteren Schäden entstehen.

Trotz der zentralen Rolle der Einwilligung in der DS-GVO sind Verarbeitungen auch ohne diese zulässig. Dies betrifft insb. die Buchstaben b) bis f) des Artikels 6 der DS-GVO. Insbesondere für die Fälle von Art. 6 e) und f) sieht das *Widerspruchsrecht* die Möglichkeit des Opt-out vor, indem die betroffene Person ihre überwiegenden Interessen bekannt macht [10].

Mittels *Rechtsbehelfen* (Art. 77–79 DS-GVO) sollen die Betroffenen schließlich in die Lage versetzt werden, eine Verletzung ihrer Datenschutzrechte vor Gericht zu bringen und gegebenenfalls einen Schadensersatz (Art. 82 DS-GVO) einzuholen.

3 Kritik an liberal-individualistischen Datenschutzrechten

Konfrontiert ist der im liberal-individualistischen Datenschutzparadigma eingebettete Fokus auf die Ermächtigung des Individuums mit mehreren Problemkomplexen. Erstens findet bereits seit Jahrzehnten eine anhaltende *Überforderung der Individuen* statt, die angesichts omnipräsenter Datenverarbeitungen in einer in zunehmendem Maße digitalisierten Welt nur noch größere Ausmaße annehmen wird. Zweitens entstehen neue Gefahren im Zuge der Verbreitung von Big Data-Analysen, die personenbezogene Entscheidungen und Ergebnisse auch ohne die Nutzung personenbezogener Daten ermöglichen können, sodass die Gewährleistung *der informationellen Selbstbestimmung im Kontext moderner Datenanalyseverfahren unmöglich* wird.

3.1 Überforderung des Individuums

Das Problem der zunehmenden Überforderung des Individuums basiert auf vielen Ursachen und stellt eine auf absehbare Zeit unumkehrbare Entwicklung dar [16]. Immer mehr Bereiche des Lebens werden verdatet, indem eine Verknüpfung der digitalen und analogen Welt mittels Sensoren stattfindet. Im Ergebnis nimmt die Menge erhobener personenbezogener Daten enorm zu. Die auf diese Weise erzeugte Masse an Daten kann auf unbegrenzte Zeit gespeichert werden, da die Speicher-Kosten inzwischen sehr gering sind [17, 18]. Da zudem immer mehr Bereiche des Lebens digitalisiert werden, fällt es den Individuen zunehmend schwerer, sich der ständigen Erhebung personenbezogener Daten zu entziehen. Ein Anspruch oder gar Recht auf Offline-Alternativen ist politisch nicht in Sicht [19]. Lange Zeit erstreckte sich die Erhebung personenbezogener Daten auf Name, Wohnort, Telefonnummer usw. Durch den Einsatz moderner Sensortechnik und durch das Zusammenwachsen von digitaler und analoger Welt nimmt nicht nur die Datenmenge zu, sondern auch die Verschiedenheit und Aussagekraft der erhobenen Daten. Möglich werden so extrem detaillierte Einblicke in vielerlei individuelle Lebensbereiche und Alltagspraktiken [20].

Sehr tiefgehende Rückschlüsse über Individuen werden allerdings nicht nur mittels Sensorik und unmittelbarer Datenerhebung möglich, sondern auch durch fortschrittliche Verarbeitungsmethoden, deren genaue Funktionsweise das Verständnis der Betroffenen, aber zunehmend auch das Verständnis selbst der für eine Verarbeitung Verantwortlichen übersteigt [21]. Zudem werden personenbezogene Daten auf für Außenstehende, d. h. insbesondere für Betroffene, intransparente Weise, weltweit über Datenbroker gehandelt und aus verschiedensten Quellen zusammengeführt [22]. Sowohl moderne Verarbeitungsmöglichkeiten als auch die Nutzungspraktiken anderer Nutzerinnen und Nutzer digitaler Technologien und Dienste haben Auswirkungen auf die individuelle Privatheit, indem Informationen zum Teil entgegen dem Wunsch eines Individuums über soziale Kontexte hinweg zirkulieren [23]. Personenbezogene Daten legen dabei für den Einzelnen unüberschaubare Strecken zurück und passieren auch die Hoheitsgebiete von Staaten mit einem problematischen Datenschutzniveau, die unerlaubten Zugriff auf die Daten erhalten [24]. Im Ergebnis dieser Entwicklungen sind die Betroffenen damit konfrontiert, immer mehr datenschutzrelevante Entscheidungen in Bezug auf immer mehr und zunehmend wichtigere Bereiche ihres Lebens treffen zu müssen [25], die sie immer schlechter überblicken können [16, 25].

Damit die Betroffenen ihre Person betreffende Datenverarbeitungen überblicken und an diesen mitwirken können, sind Verarbeiter zu Transparenz gegenüber den Betroffenen verpflichtet, die in der Regel in Form von Datenschutzerklärungen erfolgt. Sobald datenverarbeitende Prozesse allerdings wirklich transparent, d. h. umfassend hinsichtlich der stattfindenden Verarbeitungen dargestellt werden, sind die Betroffenen meist überfordert. Der Wunsch der Betroffenen nach mehr Transparenz über immer komplexer werdende Verarbeitungsprozesse einerseits und nach einer einfach verständlichen, kurzen Darlegung dieser Komplexität andererseits, sind widerstreitende Ziele und verlangen nach einem Kompromiss. Beides gleichzeitig zu erreichen wird nicht möglich sein, weswegen Transparenzanforderungen unter Kritik stehen [26, 27]. Zuletzt hatten sich EU-Kommission und EU-Parlament während der Datenschutzreform die Verbesserung von Transparenz vorgenommen [28, 29]. Die bisherigen Erfahrungen mit der Anwendung der DS-GVO demonstrieren, dass wesentliche Verbesserungen weder im Hinblick auf die informierte Einwilligung [30, 31] festzustellen sind, noch im Hinblick auf die Wahrnehmung der Auskunftsrechte [32].

Dass ein Großteil der Betroffenen die Datenschutzerklärungen der von ihnen genutzten datenverarbeitenden Dienste vor einer Einwilligung nicht durchliest,

ist ein in diesem Zusammenhang lange bekanntes Problem. Datenschutzerklärungen gelten für die meisten Menschen als zu komplex und zu lang.[1] Aufgrund der vielen zu treffenden Nutzungs- bzw. Einwilligungsentscheidungen, die mittels individueller Aufmerksamkeits- und Zeitressourcen nicht zu bewältigen sind, entsteht schließlich das Problem der *Ermüdung* hinsichtlich der Zustimmung zu einer Verarbeitung *(consensual exhaustion).* Im Ergebnis willigen die meisten Nutzerinnen und Nutzer in die Nutzung eines Dienstes ein, ohne dass sie sich weitergehende Gedanken über die Konsequenzen machen. Entscheidend ist, ob sich mit der Nutzung eines Dienstes bestimmte kurzfristige Bedürfnisse befriedigen lassen und nicht, ob aufgrund von Privatheitsgefährdungen in der Zukunft möglicherweise ein individueller oder auch die Gesellschaft betreffender Nachteil erwachsen kann. Zudem manipulieren Verantwortliche mittels vielfältiger Design-Entscheidungen (sog. *nudging,* bzw. auf Deutsch: Anstupsen) das Nutzerverhalten in die von ihnen gewünschten Richtungen und bringen Betroffene so beispielsweise dazu, mehr personenbezogene Daten preiszugeben [25, 26, 34, 35].

Dass viele Datenschutzerklärungen gar nicht darauf eingehen, welche künftigen Verarbeitungen stattfinden werden, da sie dies zum Zeitpunkt der Erstellung der Datenschutzerklärung selbst gar nicht wissen können, stellt eine weitere Herausforderung dar. Folglich kann auch keine selbstbestimmte Einwilligung erfolgen, da die Betroffenen dies noch weniger wissen können [1].

Über das Thema Einwilligung hinaus gestaltet sich die Wahrnehmung von z. B. Auskunfts-, Korrektur- oder Löschungswünschen als umso schwieriger, je mehr Daten (teils gänzlich ohne das Wissen der Betroffenen) bei verschiedenen Verarbeitern lagern [24]. Zudem verpflichtet die bloße Existenz der Betroffenenrechte die Verantwortlichen zu keiner Aktion, die nicht vom Betroffenen initiiert wird. Damit hängt ihre Effektivität vom Interesse der Betroffenen an der tatsächlichen Ausübung ihrer Rechte ab – doch gerade dieses Interesse wurde bereits seit längerem angezweifelt [36]. So wurde zwar nach Inkrafttreten der DS-GVO ein Anstieg an Auskunftsersuchen festgestellt, die Zahlen pendelten sich seither allerdings auf einem sehr niedrigen Niveau ein [37, 38].

[1] Eine Studie aus dem Jahr 2008 rechnete aus, dass eine durchschnittliche US-amerikanische Person, die alle Datenschutzerklärungen aller von ihr genutzten datenverarbeitenden Produkte lesen möchte, jährlich 201 h (das sind mehr als acht volle Tage bzw. auf achtstündige Arbeitstage gerechnet 25 Arbeitstage) mit dieser Aufgabe verbringen würde [33].

3.2 Unmöglichkeit der informationellen Selbstbestimmung im Kontext moderne Datenanalyseverfahren (Big Data-Analysen)

Die zweite große Herausforderung, mit der das liberal-individualistische Datenschutz-Paradigma konfrontiert ist, stellen moderne Datenanalyseverfahren dar. Diese erschweren die informationelle Selbstbestimmung nicht nur, sondern machen sie bisweilen unmöglich.

Bei der Nutzung personenbezogener Daten für vielfältige Zwecke nehmen das Data-Mining und das Profiling eine zentrale Rolle ein. Während der Begriff des Data-Mining eher den Aspekt der systematischen Anwendung statistischer Auswertungsmethoden (heutzutage in der Regel und auch im Rahmen dieser Schrift etwas verkürzt als Big Data-Analysen bezeichnet) auf Datenbestände umfasst [39], wird mit Profiling die Anwendung der durch Data-Mining erzielten Ergebnisse in Form von Wahrscheinlichkeitswerten *(Scores)* auf personen- oder gruppenbezogene Entscheidungsprozesse bezeichnet [40, 41].[2] Ein sehr verbreiteter Einsatzzweck derartigen Scorings ist das Risikoprofiling bzw. die Risikobewertung z. B. im Rahmen der Vergabe von Krediten, wie sie in Deutschland seitens der Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA) [42] und vergleichbarer Organisationen (etwa im Bereich der Flugsicherung) praktiziert wird [43]. Werbetreibende können auf Basis derartiger Wahrscheinlichkeitswerte ihr Klientel zunehmend zielgerichteter adressieren. Je fortschrittlicher die während des Data-Mining angewendeten Analysealgorithmen sind und je mehr Daten Gegenstand der Analyse sind, umso präzisere Ergebnisse werden möglich (ebd.).

Die DS-GVO setzt in Art. 22 dem Scoring Grenzen, indem automatisierte Entscheidungen im Einzelfall, die der betroffenen Person gegenüber rechtliche Wirkung entfalten oder sie in ähnlicher Weise beeinträchtigen können, nur unter besonderen Umständen zulässig sind. D. h., dass das Datenschutzrecht erst greifen kann, sobald ein Profil auf eine *identifizierbare Person* bezogen wird, deren Identität dem Verantwortlichen bekannt ist, wie es etwa im Kredit-Scoring der SCHUFA der Fall ist [44]. Nicht betroffen von der Regelung ist dagegen die Erstellung von Profilen über Personen, deren Identität dem Verantwortlichen nicht

[2] Bei Profiling geht es vor allem darum, Gruppenattribute zu identifizieren (Menschen die X tun, tun auch Y, aber nicht Z). Derartige Ergebnisse können also Fahrer von blauen PKWs sein, die z. B. täglich um 14 Uhr die Kirche und im Anschluss das Altersheim besuchen. Entsprechend sind die Daten nicht zwingend auf einzelne identifizierbare Individuen bezogen, weshalb sie auch nicht als personenbezogene Daten gelten [3].

bekannt ist. Denn Datenverarbeitungsprozesse rücken zum Teil weg vom Individuum *(Vorkommnis)* hin zur Identifikation algorithmisch generierter Gruppen auf Grundlage gemeinsamer Eigenschaften *(Typen),* damit eine gruppenspezifische Behandlung (bspw. Kundenansprache) ermöglicht bzw. optimiert wird. Ob und warum ein Individuum Teil einer Gruppe ist, bleibt den Betroffenen verborgen. Zudem besteht die Gefahr, dass das Zustandekommen und die Diskriminierung einer Gruppe sogar den Datenanalysten selbst niemals bekannt werden wird, da die zugrunde liegenden Berechnungen oftmals intransparent oder zu komplex sind [21]. Dadurch, dass derartige (Gruppen-)Profile nicht dem Datenschutz unterliegen, nehmen die Betroffenen auch keine Notiz von der erfolgten Profilierung. In der Folge können die von einem derartigen nicht-personenbezogenem Gruppenprofiling Betroffenen auch keine Maßnahmen gegen möglicherweise verzerrende Darstellungen ihrer selbst ergreifen – die datenschutzrechtlichen *Betroffenenrechte* greifen in diesen Fällen schlicht nicht [3].

Das Recht auf *Einwilligung* beispielsweise baut darauf, dass diese in Kenntnis über die Verarbeitungszwecke erfolgt. Das Prinzip der *Zweckbindung* allerdings ist bereits seit längerem durch die Praxis datenverarbeitender Unternehmen herausgefordert, die die Zweckbindung missachten und jene für einen Zweck erhobenen Daten auch für viele weitere Zwecke verarbeiten, indem personenbezogene Daten anonymisiert oder pseudonymisiert und somit den Vorgaben des Datenschutzrechts entzogen werden (bspw. seitens Suchdiensten, Sozialen Online-Netzwerken oder Datenaggregatoren und -händlern). Neu hinzugekommen ist die Gefahr moderner Big Data-Analyseverfahren, deren Ziel darin besteht, dass sich mögliche Nutzungszwecke erst durch vielfache Analyseschleifen ergeben. Insofern stehen sich das Zweckbindungsprinzip und Big Data konträr gegenüber, weil eine Zweckbindung immer dann nicht erfolgen kann, wenn sich der Zweck erst im Laufe einer Analyse ergibt [11]. Mit der Erosion der Zweckbindung im Zuge von Big Data-Analysen schwindet zudem auch die Möglichkeit der Schaffung transparenter Organisationsstrukturen und Prozesse. Dieser Aspekt betrifft außerdem nicht mehr nur die Betroffenen und Aufsichtsbehörden, sondern, in dem Maße, in dem die Komplexität von Verarbeitungen zunimmt, auch die Verantwortlichen selbst, die zwar Ergebnisse erhalten, aber selbst zunehmend weniger begreifen, wie und auf Grundlage welcher Daten und Berechnungen diese im Detail zustande gekommen sind [45]. Erschwerend kommt hinzu, dass Big Data-Analysen gruppen- und personenbezogene Ergebnisse, die vom Datenschutzrecht nicht umfasst sind [3, 46] auch dann nach sich ziehen können, wenn die Analyse ausschließlich auf nicht personenbezogenen, anonymisierten oder pseudonymisierten Daten beruht. Eine auf diese Weise betroffene Person kann

in die Verarbeitung gar nicht einwilligen oder eine selbstbestimmte Informationskontrolle praktizieren, weil sie zu keinem Zeitpunkt selbst Daten über sich preisgibt und vielfach auch gar nicht wissen kann, dass sie betroffen ist [27].

Dies betrifft in besonderer Weise die Gewährleistung des Prinzips der *Datenminimierung*. Denn das Prinzip der Datenminimierung bezieht sich ausschließlich auf personenbezogene Daten bzw. darauf, dass auf zulässige Weise erhobene personenbezogene Daten so früh wie möglich gelöscht, anonymisiert oder pseudonymisiert werden. Das bedeutet, dass das Prinzip der Datenminimierung immer dann nicht greift, wenn der Zweck einer Verarbeitung nicht bekannt ist, aufgrund von Anonymisierung bzw. Pseudonymisierung kein Personenbezug vorhanden ist oder sich der Personenbezug eines Datums erst im Ergebnis einer Big Data-Analyse ergibt. Zwar könnte mithilfe des Datenminimierungsprinzips eine radikale Begrenzung von Big Data-Analyseverfahren erfolgen, doch würden damit nicht nur potenziell unerwünschte Auswirkungen von Big Data-Verfahren vermieden, sondern auch potentiell erwünschte Auswirkungen [41].

4 Datenschutzrechtliche Gestaltungsmöglichkeiten jenseits der Fokussierung auf die Ermächtigung des Individuums

Auf welche Weise könnte also informationelle Privatheit im Recht verbrieft werden, sodass die zentrale Rolle des Individuums zwar erhalten bleibt, aber zugleich auch die Grenzen der individuellen informationellen Selbstbestimmung berücksichtigt werden?

4.1 Konzeptionelle Vorüberlegungen

Zur Beantwortung dieser Frage konzentriere ich mich im Folgenden auf den in den letzten Jahren zunehmend prominenter gewordenen Ansatz, einen Teil der Verantwortung zur Gewährleistung des Datenschutzes weg von den Betroffenen hin zu anderen Entitäten – darunter insbesondere die Verantwortlichen, aber auch Vertreter von Betroffeneninteressen – zu übertragen [47–50]. Viele der Autorinnen und Autoren, die diesen Ansatz vertreten, gehen davon aus, dass das Rechtssystem zwar durchaus am Grundsatz festhalten sollte, dass das Individuum im Mittelpunkt des Rechts steht. Des Weiteren gehen sie aber auch davon aus, dass die absehbaren technischen und sozialen Veränderungen auf einem Meta-Level ansetzen, wo es weniger um das Individuum als solches, denn um Strukturen geht, die

sowohl ein einzelnes Individuum betreffen als auch darüber hinaus reichen und die Gesellschaft als Ganzes betreffen können. Deshalb wird vorgeschlagen, den Problemen nicht nur individuell, sondern vor allem kollektiv zu begegnen [49]. Entsprechend wird vom überwiegenden Teil dieser Autorinnen und Autoren auch nicht die vollständige Ersetzung der gegenwärtigen, am Individuum fokussierenden Datenschutzgesetze gefordert, sondern die Ergänzung bestehender Gesetze um nicht-individualistische Schutzmomente [49, 51, 52].[3]

Die Forderung nach der Übertragung eines größeren Teils der Verantwortung hin zu den Verarbeitern baut auf der Feststellung auf, dass sie es sind, die die Rahmenbedingungen festlegen, welche die Konstituierung des Subjekts je nach Technologie und Kontext in unterschiedlichem Maße beeinflussen. Allerdings gestaltet sich die Beantwortung der Frage, inwiefern nichtstaatliche Akteure stärker in die Verantwortung genommen werden können, nicht als trivial. Grundsätzlich gilt, dass aufgrund seiner besonderen Machtposition nur der Staat gegenüber den Bürgerinnen und Bürgern grundrechtsverpflichtet ist. Sofern Individuen Akteuren des Marktes gegenüberstehen, handelt es sich also im rechtlichen Sinne grundsätzlich um ein Verhältnis Gleicher unter Gleichen, da auch Marktakteure (also auch privatwirtschaftliche Unternehmen) ihrerseits Träger von Grundrechten sind. Während das oben skizzierte Verständnis nahelegt, im Falle eines Machtungleichgewichts zwischen Individuen einerseits und insbesondere marktbeherrschenden privatwirtschaftlichen Unternehmen andererseits, letzteren zusätzliche Pflichten aufzuerlegen, um einen Missbrauch ihrer Machtstellung zu verhindern, war die Umsetzbarkeit dieses Vorhabens aus juristischer Perspektive längere Zeit umstritten. Dies änderte sich im Laufe der letzten Jahre mit einigen neueren Urteilen[4] des Bundesverfassungsgerichts. Diese besagen im Grundsatz, dass anderen privaten Akteuren insbesondere dann zusätzliche grundrechtsschützende Pflichten auferlegt werden können, wenn diese durch die Organisation von Kommunikationsräumen in vergleichbare Pflichten und Garantenstellungen hineinwachsen, wie sie ansonsten nur der Staat wahrnimmt [31].

[3] Für weniger hilfreich halte ich hingegen den Vorschlag hinsichtlich der Einführung von Gruppenrechten in das Datenschutzrecht. Zwar kann diese Frage aus Platzgründen an dieser Stelle nicht erschöpfend erörtert werden, doch ist die Umsetzung von Gruppenrechten bereits bei klar identifizierbaren Gruppen mit zahlreichen Schwierigkeiten konfrontiert [53]. Im Falle von algorithmisch generierten Gruppen potenzieren sich diese noch weiter, sodass sie praktisch kaum infrage kommen dürften [45, 54].

[4] BVerfGE 128, 226 (Fraport); BVerfG, NJW 2015, 2485 (Bierdosen-Flashmob; BVerfGE 148, 267 (Stadion-Verbot); BVerfG, NJW 2019, 1935 (1936) (III. Weg).

Über die Verlagerung von Verantwortung hin zu den Verarbeitern hinaus, kann auch die Forderung nach einer verstärkten Kontrolle der Einhaltung der Regelungen seitens unabhängiger Aufsichtsbehörden sowie die kollektive Unterstützung der Individuen bei schwierigen Entscheidungen und Handlungen (beispielsweise durch Verbraucherschutzorganisationen, an denen bestimmte Betroffenenrechte in einem bestimmten Rahmen freiwillig abgetreten werden können) als Teil eines solchen überindividuellen Datenschutzes verstanden werden [49]. In ähnlicher Weise deuten Matzner und Richter auf ein demokratisch gesichertes *Standard*-Schutzniveau, das bereits im Normalzustand Raum für individuelle Privatheitspraktiken lässt, darüber hinaus aber auch kontextspezifische Spezialregelungen unterhalb und oberhalb des festgelegten Niveaus ermöglicht:

> „Die Idee [sic!] dass Individuen grundsätzlich das Recht haben, selbst über die Nutzung ihrer Daten zu bestimmen, bleibt wichtig und richtig. Notwendig ist aber ein Zusammenspiel aus Eigenverantwortung und kollektivem, demokratisch legitimiertem Schutz. Hier müssen mehrere Elemente ineinandergreifen: Ein interessengerechter Handlungsrahmen, der staatlich reguliert und durchgesetzt wird; in diesem Handlungsrahmen ein eigenverantwortlicher Selbstdatenschutz; und schließlich kollektive Prozesse der Aushandlung von Datenschutz unterhalb und oberhalb der staatlichen Ebene. Wenn Menschen selbst über den Umgang mit Informationen bestimmen, muss das nicht heißen [sic!] jede und jeder Einzelne bestimmt egozentrisch für sich. Auch Gruppen, Gemeinschaften, Gesellschaften, Angestellte einer Firma, Mitglieder eines Berufsverbandes, Bürger eines demokratischen Rechtsstaats und viele mehr können auf überindividueller Ebene für sich selbst bestimmen.“ [55]

Die Orientierung der gesetzlichen Regelungen an den für eine Verarbeitung Verantwortlichen ist kein Novum, sondern bildete den Ausgangspunkt der Datenschutzdiskurse der 1970er-Jahre. Der Fokus auf das Individuum kam erst im Laufe der Zeit hinzu und verdrängte nach und nach die vorherigen Schutzmomente. Davon zu sprechen, dass das EU-Datenschutzrecht einem liberal-individualistischen Datenschutz-Paradigma folgt, heißt aber auch nicht, dass keine nicht-individualistischen Elemente enthalten sind. Zu diesen können nach Sloot [2, 49] folgende Elemente der DS-GVO hinzugezählt werden:

- Die Datenschutzprinzipien bzw. -grundsätze („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“, „Zweckbindung“, „Datenminimierung“, „Richtigkeit“, „Speicherbegrenzung“ sowie „Integrität und Vertraulichkeit“) (Art. 5 DS-GVO)
- Sondervorschriften bei der Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DS-GVO)

- Informations- und Transparenzvorgaben bei der Verarbeitung personenbezogener Daten (Art. 12–14 DS-GVO)
- Vorgaben im Kontext automatisierter Einzelentscheidungen (Art. 22 DS-GVO)
- Vorgaben zur Datensicherheit zur Durchführung angemessener technischer und organisatorischer Maßnahmen (Art. 32 DS-GVO)
- Vorgaben zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO)
- Allgemeine Vorgaben zur Rechenschaftspflicht und der Verantwortung der für die Verarbeitung Verantwortlichen (Art. 24 DS-GVO)
- Führen eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DS-GVO)
- Vorgaben zur Zusammenarbeit mit den Datenschutzaufsichtsbehörden (Art. 31 DS-GVO)
- Meldung von Verletzungen des Schutzes personenbezogener Daten (Art. 33 und 34 DS-GVO)
- Datenschutz-Folgenabschätzung und vorherige Konsultation (Art. 35 und 36 DS-GVO)
- Beachtung der Regelungen bei der Übermittlung personenbezogener Daten in Drittländer (Art. 44–49 DS-GVO)
- Ziel von Sanktionen und Geldbußen bei Nichteinhaltung der Vorgaben (Art. 83–84 DS-GVO)

Zudem regeln die Art. 51–76 DS-GVO die Befugnisse der Datenschutzaufsichtsbehörden, denen die Rolle der Überwachung der Einhaltung der Verarbeiterpflichten zukommt. Diese Rechtselemente bilden eine gute Grundlage, von denen ausgehend ich im Folgenden erörtern möchte, wie weitere überindividuelle Datenschutz-Elemente Eingang in die Gesetzgebung finden könnten.

4.2 Die Multi-Stakeholder-Datenschutz-Folgenabschätzung (MS-DSFA)

Im Hinblick auf die Schwächen liberal-individualistischer Datenschutzrechte arbeitete ich im vorangegangenen Abschnitt zwei Herausforderungen heraus. Die erste große Herausforderung besteht in der Überforderung der Individuen, die mit der Masse der Individualrechte angesichts allgegenwärtiger Datenverarbeitungen und zahlreicher Entscheidungshürden schlicht überfordert sind. Die zweite große Herausforderung besteht in der Unmöglichkeit der informationellen Selbstbestimmung im Kontext moderner Datenanalyseverfahren. Die im Folgenden diskutierten Vorschläge adressieren in erster Linie die zweite Herausforderung.

Teilweise könnten sie aber durchaus auch zur Eindämmung der im Rahmen der ersten Herausforderung diskutierten Probleme herangezogen werden.

Aufgrund der vielfältigen negativen individuellen und gesellschaftlichen Auswirkungen moderner Datenverarbeitungen wurde immer wieder eine Einschränkung solcher Praktiken zwar begrüßt [56, 57], aber häufig blieb unklar, wie genau eine Einschränkung rechtlich verankert werden könnte. Ein meines Erachtens vielversprechender Diskussionsstrang widmet sich der Verschiebung des Fokus der Datenschutzgesetzgebung von der Regulierung personenbezogener Daten hin zur Regulierung personenbezogener Entscheidungen. Möglich würde dadurch, dass nicht nur die personenbezogenen, sondern alle für eine personenbezogene Entscheidung verwendeten Daten rechtlich adressierbar würden [3, 46]. Damit personenbezogene Entscheidungen wiederum rechtlich adressierbar werden können, ist jedoch zunächst die Herstellung von Transparenz über die Prozesse der Entscheidungsfindung notwendig [46, 58], die allerdings seitens datenverarbeitender Akteure regelmäßig unter Verweis auf die aus Sicht der Unternehmen dabei drohende Offenlegung von Geschäftsgeheimnissen zurückgewiesen wurde [59, 60].

Eine Möglichkeit der konkreten, rechtlichen Operationalisierung dieser Vorschläge, die das Risiko der Offenlegung von Geschäftsgeheimnissen auf ein Minimum reduziert, findet sich in jener Datenschutzliteratur, die von ähnlichen Lösungsvorschlägen aus den Bereichen des Verbraucher-, Arbeitnehmer- und Umweltschutzes inspiriert wurde [50, 61]. Kollektive Interessenvertretungen würden es in diesen Bereichen erlauben, dass die Interessen der Betroffenen trotz massiver Machtasymmetrien besser gewahrt bleiben, als wenn der Einzelne alleine gegenüber dem Arbeitgeber, Händler, Umweltsünder usw. auftritt [50].

Die auf diesen Feldern vorherrschende strukturelle Machtasymmetrie ist vergleichbar mit der Situation, der sich die Betroffenen bei modernen Datenverarbeitungskotexten gegenübersehen: Lock-In-Effekte, Unwissen über Datenverarbeitungen, Rechtsbehelfe usw. Allerdings gestaltet sich die Bestimmung des zu schützenden kollektiven Interesses im Falle moderner Datenanalyseverfahren als deutlich schwieriger als in traditionellen Kontexten, wie z. B. dem Arbeitnehmerschutz. Denn ArbeitnehmerInnen stellen eine klar umreißbare Gruppe dar, deren kollektives Interesse (bessere Löhne, mehr Freizeit, Gewährleistung der Arbeitssicherheit, usw.) sich aus ihrer Arbeitnehmerposition gegenüber dem Arbeitgeber unmittelbar ergibt. Das Verhältnis der von Big Data-Analysen Betroffenen zueinander ist dagegen schwer zu fassen. Die geteilten Attribute etwa, auf deren Grundlage algorithmisch generierte Gruppen konstituiert werden, sind den diesen Gruppen zugeordneten Betroffenen in der Regel nicht bekannt. Entsprechend kennt jemand, der auf diese Weise einem Profil zugeordnet wurde,

weder die Gründe für die eigene Profilierung noch die restlichen Mitglieder der Gruppe und besitzt daher kein oder nur sehr begrenztes Wissen über potenzielle kollektive Interessen, die geschützt werden könnten. Schließlich können sich die Parameter, auf deren Grundlage Gruppen konstituiert werden, aufgrund der Natur von Big Data-Analysen, Analyseschleifen vielfach zu wiederholen, ständig ändern. Zusätzlich kann abhängig vom Daten-Input auch die Gruppenzugehörigkeit einzelner Betroffener ständig variieren. Die beschriebenen Einschränkungen erschweren somit die Identifikation und Vertretung kollektiver Interessen (etwa durch die bewusste Wahl eines Repräsentanten) [50].

Die von derartigen Big Data-Analysen Betroffenen können eher mit Verbrauchern verglichen werden, die sich zwar untereinander ebenfalls nicht kennen, jedoch alle gleichsam unter ungesunden Lebensmitteln, unsicheren Produkten, unseriösen Geschäftspraktiken usw. leiden. Das kollektive Verbraucherinteresse besteht dabei etwa in der Bereitstellung gesunder Lebensmittel, sicherer Produkte und fairer Geschäftspraktiken. Im Bereich des Verbraucherschutzes stehen den Betroffenen in derartigen Fällen sowohl individuelle als auch kollektive rechtliche Schritte zur Verfügung. Darüber hinaus können sich Verbraucher an für den Verbraucherschutz zuständige Behörden und Verbraucherverbände wenden oder auch *Verbands- und/oder Sammelklagen* initiieren [50]. Der Einführung derartiger kollektiver Rechtsbehelfe kommt daher eine zentrale Rolle zu. Ihr Vorteil ist, dass sie sowohl dem Einzelnen weiterhin die Möglichkeit überlassen, eine individuelle Klage zu eröffnen, als auch all jenen Menschen, die mit einer individuellen Klage überfordert wären, die Möglichkeit bieten, sich an kollektiven Verfahren zu beteiligen [61]. Art. 80 DS-GVO greift hier eindeutig zu kurz, da er im ersten Absatz lediglich die Beauftragung klar regelt, die Klagemöglichkeit für Verbände etc. ohne eine explizite Beauftragung allerdings im zweiten Absatz der Entscheidungshoheit der Mitgliedstaaten überlässt.

Dass eine Privatheitsverletzung seitens einer kollektiven Interessenvertretung überhaupt angegangen werden kann, ist davon abhängig, ob Wissen über Datenschutzverletzungen besteht. Denkbar und praktisch umsetzbar wäre beispielsweise eine *Meldepflicht im Falle potentiell besonders riskanter Verarbeitungen* [62]. Die dabei als Maßstab heranzuziehende – im Rahmen der DS-GVO allerdings nicht-geregelte – Kritikalität bzw. das Risiko einer Verarbeitung könnte sich beispielsweise an den Vorschlägen der Datenethikkommission orientieren [63]. Damit zusammenhängend, besteht eine weitere Möglichkeit, den Herausforderungen gesellschaftlich unerwünschter Datenverarbeitungen zu begegnen, im Konzept der Risiko-Abschätzung, das in die DS-GVO Eingang in Form der *Datenschutz-Folgenabschätzung* (bzw. DSFA) in Art. 35 bzw. zur *Vorherigen Konsultation* in Art. 36 gefunden hat. Demnach sollen Verantwortliche hohe Risiken für

die Rechte und Freiheiten natürlicher Personen, die aus einer Datenverarbeitungsform hervorgehen können, identifizieren, analysieren und mittels geeigneter Maßnahmen eindämmen. Seit der Verabschiedung der DS-GVO ist eine EU-weite intensive Debatte rund um die Festlegung einer effektiven und effizienten DSFA-Methodik entstanden [64]. Es gibt zwar aktuell noch keine gesicherten Zahlen dazu, wie häufig DSFAs zur Anwendung kommen, doch zeichnet sich bereits seit längerem ab, dass das Instrument für Verantwortliche eher ein notwendiges Übel darzustellen scheint, als eine beliebte Methode zur Eindämmung von Grundrechtsrisiken [65, 66]. Diese Annahme deckt sich mit Erfahrungen aus der Vergangenheit: Selbstregulierungsinstrumente werden immer dann nicht ernst genommen, wenn der Zweck des Instruments darin liegt, eine Selbstbeschränkung von Organisationspraktiken zu erreichen [67, 68].

Abhilfe könnte ein Vorschlag schaffen, der das Moment der Interessenvertretung in der DSFA stärkt und die Risiko-Abschätzung stärker als *Multi-Stakeholder-Prozess* zu strukturieren vorschlägt, an dem, abhängig von der Art der Verarbeitung, neben dem Verarbeiter selbst, weitere Stakeholder aktiv partizipieren [50, 61]. Der Vorschlag würde somit zunächst insbesondere die Erweiterung des in Art. 35 Abs. 9 formulierten möglichen Einbezugs der von einer Verarbeitung Betroffenen oder ihrer Vertreter vorsehen. Denn ein weithin bekanntes Problem von Multi-Stakeholder-Prozessen ist die Unterrepräsentation zivilgesellschaftlicher Akteure und die Überrepräsentation (wirtschafts-)mächtiger Akteure. Die in Art. 35 (9) festgeschriebene Formulierung, wonach der Standpunkt von Betroffenen oder ihren Vertretern nur „gegebenenfalls“ einzuholen ist, öffnet Tür und Tor für die Durchführung einer DSFA als Checkbox-Tätigkeit, die von keiner anderen Instanz in relevantem Maße kontrolliert wird und letztlich nur als Vorwand zur Rechtfertigung einer umstrittenen Verarbeitung genutzt wird.

Ein solcher Multi-Stakeholder-DSFA-Prozess könnte folgendermaßen ablaufen (vgl. auch Abb. 1): Ein Unternehmen, das eine datenbasierte Verarbeitung plant, die aufgrund ihres Umfangs und/oder ihres Eingriffs in individuelle Rechte oder in gesellschaftliche Strukturen wahrscheinlich zu Privatheits-, Datenschutz- oder sonstigen gesellschaftlichen Risiken führen könnte, müsste verpflichtet sein, jene Verarbeitung einer Risikoanalyse zu unterziehen. Vor Durchführung der Risikoanalyse müsste sie die geplante Verarbeitung bei der zuständigen Datenschutzaufsichtsbehörde ankündigen bzw. melden. Je nachdem, welche gesellschaftlichen Bereiche betroffen sind, müssten weitere Akteure, die das Betroffeneninteresse vertreten, hinzugezogen werden, bspw. Verbraucherschutzorganisationen oder Anti-Diskriminierungsstellen. Die am Risikoabschätzungsprozess beteiligten Organisationen müssten, abhängig von der Art der jeweils geplanten Verarbeitung,

Abb. 1 Vorschlag für einen Multi-Stakeholder-DSFA-Prozess. (Eigene Darstellung, inspiriert von Mantelero 2016)

weitreichende Partizipationsrechte erhalten, damit das Ziel einer gesellschaftsverträglichen Datenverarbeitung erreicht werden kann. Je nach Verarbeitung und Risiko könnten die jeweiligen Vertreter z. B. von den Betroffenen Vollmachten einholen, um weitergehenden Zugriff auf personenbezogene Daten zu erhalten, Auskunftsersuchen zu stellen usw. Dies müsste in solchen Fällen, in denen die gesellschaftlichen Folgen einer Verarbeitung sehr weitreichend oder besonders unklar sind, auch die Einsicht in Staats- und Geschäftsgeheimnisse, etwa nähere Informationen zu den verwendeten Algorithmen aufseiten der Verantwortlichen umfassen. Um die nicht-legitime Veröffentlichung von Staats- oder Geschäftsgeheimnissen zu unterbinden, müssten derartige Einblicke allerdings hohen Verschwiegenheitsansprüchen genügen, solange kein sehr weitreichendes und gesellschaftlich relevantes Risiko von einer Verarbeitung ausgeht [50, 61].

Das überwiegende öffentliche Interesse sollte in solchen, besonders riskanten Fällen ausreichend sein, um den Eingriff in die unternehmerische Freiheit bzw. die Offenlegung von Staatsgeheimnissen zu begründen. Dadurch, dass entsprechende Geheimnisse, Algorithmen etc. nicht der allgemeinen Öffentlichkeit, sondern nur den konkret am Prozess mitwirkenden Personen aus den beteiligten Organisationen bekannt würden, könnte die missbräuchliche Weitergabe entsprechenden Wissens schließlich deutlich besser verhindert bzw. nachvollzogen werden.

Der abschließende Vorteil einer Multi-Stakeholder-DSFA gegenüber üblichen Risikoabschätzungsprozessen müsste schließlich in der Generierung von möglichst konkreten Ergebnissen liegen. Hier ist an eine weite Maßnahmenspanne zu denken, von der Definition von Zertifizierungskriterien über spezifizierte Datensicherheitsvorgaben bis hin zu risikoadäquater Regulierung (vgl. Abb. 2).

Zertifizierungen etwa hätten den Vorteil, dass sie ein stärkeres Anreizsystem für Unternehmen bzw. staatliche Stellen zur Durchführung von Multi-Stakeholder-DSFAs schaffen. Denkbar wäre, dass gewisse Verarbeitungen, weil die mit ihnen verbundenen Risiken ausreichend gesellschaftsverträglich vermindert wurden, auch ohne die Einwilligung der Betroffenen als rechtmäßig gelten. Dieser

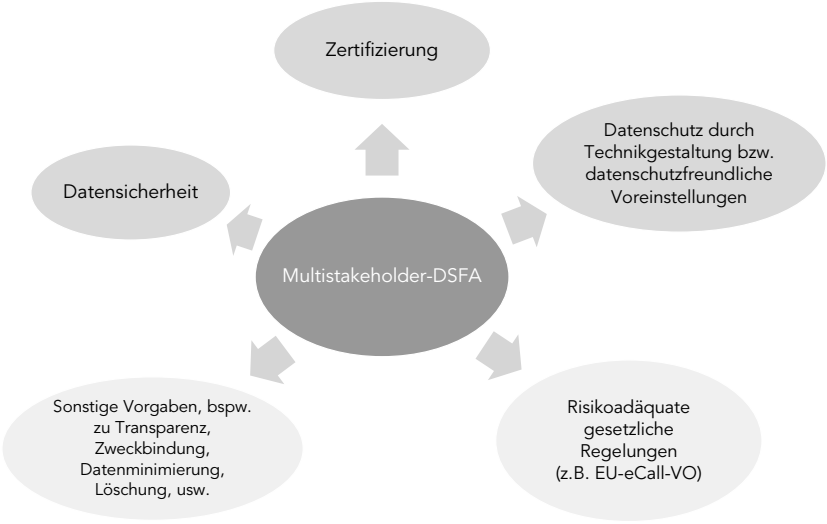

Abb. 2 Mögliche Ergebnisse eines Multi-Stakeholder-DSFA-Prozesses. (Eigene Darstellung)

Vorschlag wäre somit ein Kompromiss, der potenziell riskante Verarbeitungen unter Sicherheitsvorkehrungen erlauben würde und aufgrund der durch den Risikoabschätzungsprozess entstehenden bürokratischen Hürden zugleich der verantwortlichen Stelle durch anderweitige Zugeständnisse entgegenkommen würde. Die auf diese Weise begutachteten Verarbeitungen würden schließlich mittels Zertifizierung so gekennzeichnet werden können, dass ihre Gesellschaftsverträglichkeit deutlich wird und sie als Wettbewerbsvorteil fungieren kann. Neben Big Data-Analysen müssten Zertifizierungen auch für weniger umfangreiche Verarbeitungen möglich sein und unter staatlicher bzw. behördlicher Aufsicht ein hohes Schutzniveau signalisieren [50, 61]. Beim Zustandekommen der DS-GVO wurden aufgrund des Drucks aus der Wirtschaft keine qualitativen Zertifizierungskriterien festgelegt, sodass die in Art. 42 festgeschriebenen Vorgaben lediglich die Konformität einer Verarbeitung mit den Regeln der DS-GVO signalisieren, die Datenverarbeiter ohnehin befolgen müssen.

Die von einer derartigen Verarbeitung Betroffenen würden von dem Risikoabschätzungsverfahren deshalb profitieren, weil die am Verfahren partizipierenden Vertreter von Betroffeneninteressen aufgrund ihrer Verhandlungsposition und der größeren Sachkenntnis eine ansonsten nicht-regulierte Verarbeitung so mitgestalten würden, dass die Interessen der Betroffenen möglichst umfassend gewahrt bleiben. Freilich müsste jeder Betroffene, trotz der im o. g. Beispiel vorgeschlagenen Aushebelung der individuellen Einwilligung mittels kollektiver Einigungen, zu jedem Zeitpunkt die Möglichkeit haben, die zur Debatte stehende Verarbeitung mittels Opt-out zu widerrufen, sofern ein Personenbezug vorhanden ist. Je nach Verarbeitung und Risiko wäre auch die Einrichtung unterschiedlicher Opt-out-Möglichkeiten denkbar, um die Nachteile eines Alles-Oder-Nichts-Ansatzes zu vermeiden. So lange von einer Verarbeitung keine fundamentalen gesellschaftlichen Risiken ausgehen, die eine Übergehung des Individuums rechtfertigen, ist entscheidend, dass die Abtretung individueller Rechte an Interessenvertretungsorganisationen keine Verringerung der individuellen Entscheidungsmöglichkeiten gegenüber dem Falle der Nicht-Abtretung zur Folge hat. Dies schließt ein, dass die Abtretung der individuellen Einwilligungskompetenz vollständig beim jeweiligen Individuum liegen sollte [34, 69]. Im Zweifelsfall, wenn die Reichweite des gesellschaftlichen Interesses strittig ist, müsste die Entscheidungskompetenz stets weiterhin beim Individuum verbleiben. Ein grundlegendes Standard-Datenschutzniveau müsste allerdings auch in solchen Fällen absehbare Risiken minimieren. Wichtig wären in diesem Zusammenhang weitreichende *Datensicherheitsvorgaben,* aber auch Vorgaben zu *Privacy by Design und Default.* Das Ziel des Konzepts von Privacy by Default besteht in der technischen Umsetzung von Datenminimierungs-, Zweckbindungs- und Speicherfristvorgaben [70]. Das

Problem beim Erlassen derartiger Vorgaben resultiert daraus, dass die Festlegung von beispielsweise Standardeinstellungen, die Gültigkeit für alle Verarbeitungstypen beanspruchen müssen, sehr schwierig ist [71]. Eine Lösung dieses Problems könnte dadurch erreicht werden, dass die zu befolgenden Vorgaben im Ergebnis einer Multi-Stakeholder-DSFA oder eines partizipativen Privacy by Design, wie es bei Ochs und Lamla [6] diskutiert wird, erarbeitet werden. Derartige Vorgaben hätten den Vorteil, dass sie nur für bestimmte Verarbeitungen oder Verarbeitungsfelder anwendbar wären und die erwünschte Abstraktheit der gesetzlichen Regelungen somit unangetastet bliebe. Entscheidend für die Wirksamkeit von Privacy by Design- und Default-Vorgaben ist schließlich auch, dass sie sich sowohl an die für eine Datenverarbeitung Verantwortlichen als auch an die Hersteller datenverarbeitender Systeme richten [72].

Eine weitere Bedingung für das Gelingen des dargestellten Risikoabschätzungsprozesses, aber auch für die Gewährleistung der Einhaltung der weiteren in dem Abschnitt vorgeschlagenen, die verantwortliche Stelle betreffenden Vorgaben ist die *Ausstattung von Datenschutzaufsichtsbehörden mit ausreichender finanzieller und politischer Autonomie.* Das würde etwa bedeuten, dass die Behörden keinesfalls an ein Ministerium angegliedert und weisungsgebunden sein dürfen, sondern ausschließlich dem Parlament gegenüber rechenschaftspflichtig sind [50, 73].

Falls im Laufe von Risikoabschätzungsprozessen besonders riskante Verarbeitungssektoren oder -typen identifiziert werden, müssten zudem risikoadäquate gesetzliche Regelungen erlassen werden können. Beispielhaft für eine solche, risikoadäquate Regulierung ist die EU-eCall-Verordnung 2015/758 [74]. Darin wird auf detaillierte Weise geregelt, welche Vorkehrungen die Hersteller von eCall-Systemen treffen müssen, um Datenschutzgefährdungen zu vermeiden [75].

5 Schluss

Vor dem Hintergrund der Kritik am liberal-individualistischen Fokus des bestehenden Datenschutzrechts hat der vorliegende Beitrag datenschutzrechtliche Gestaltungsmöglichkeiten jenseits der Fokussierung auf das Individuum untersucht. Die diskutierten Vorschläge sehen keine bloße Ersetzung individuellen Datenschutzes durch kollektive Schutzmaßnahmen vor, sondern die Ergänzung individualistischer Schutzmomente. Der wesentliche Unterschied zwischen klassisch liberal-individualistischen Datenschutzrechten und den in im Rahmen dieses Papers vorgestellten Vorschlägen liegt einerseits in der (sanktionsbewährten) weiteren Übertragung von Verantwortung auf die für eine Verarbeitung

Verantwortlichen und andererseits im deutlichen Ausbau von kollektiven Vertretungsmöglichkeiten für Betroffene, auf die insbesondere dann zurückgegriffen wird, wenn eine Verarbeitung voraussichtlich zu individuellen und/oder gesellschaftlichen Risiken führt, denen die Individuen isoliert nicht begegnen könnten. Die Verlagerung von mehr Verantwortung an die Verarbeiter und die Ergänzung bestehender Datenschutzrechte durch kollektive Vertretungsmöglichkeiten berücksichtigt somit die gesellschaftlichen Effekte von Datenverarbeitungen, ohne dass die Selbstbestimmungsfähigkeit des Individuums negiert und ausschließlich in die Hände eines Kollektivs gelegt wird [50, 69].

Klar ist auch, dass kollektive Verfahren, wie das hier besprochene Multi-Stakeholder-DSFA-Modell, nicht für die Bearbeitung aller Datenschutz-Herausforderungen geeignet sein kann. Wie Bull [36] bereits vor mehr als zwei Jahrzehnten im Kontext der Nutzung von Gesundheitsdiensten zutreffend bemerkt hatte, stößt die Praxis der Zurateziehung kollektiver Akteure immer dann an ihre Grenzen, sobald es um gesamtgesellschaftlich heikle Themen geht. In anderen Worten: So lange kein gesellschaftlicher Konsens zu spezifischen Datenschutz-Fragen existiert, hilft auch die Delegation an Kollektivakteure nicht weiter.

Abschließend sei noch erwähnt, dass datenschutzrechtliche Lösungsansätze allein ohnehin nicht ausreichend sind: Um die negativen Folgen der im Beitrag beschriebenen modernen Datenverarbeitungen einzudämmen bräuchte es darüber hinaus weitere Strategien, beispielsweise aus dem Diskriminierungs- oder Wettbewerbsrecht, wie sie derzeit im Hinblick auf die Regulierung von Plattformen diskutiert werden [62, 76].

Danksagung Die diesem Beitrag zugrunde liegenden Arbeiten wurden mit Mitteln des Bundesministeriums für Bildung und Forschung (BMBF) unter den Förderkennzeichen 16KIS0741K gefördert.

Literatur

1. Helm, P., Seubert, S.: Normative Paradoxien der Privatheit in Zeiten von Big Data: Eine sozialkritische Perspektive auf eine digitale „Krise“ der Privatheit. In: Borucki, I., Schünemann, W.J. (Hrsg.) Internet und Staat (2019)
2. van der Sloot, B.: Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation. Int. Data Priv. Law **4**, 307 (2014)
3. Koops, B.-J.: The trouble with European data protection law. Int. Data Priv. Law **4**, 250–261 (2014)

4. Steeves, V.M.: Reclaiming the social value of privacy. In: Kerr, I., Steeves, V.M., Lucock, C. (Hrsg.) Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society, S. 191–208. Oxford University Press, Oxford (2009)
5. Cohen, J.E.: Configuring the Networked Self: Law, Code, and the Play of Everyday Practice. Yale University Press, New Haven [Conn.] (2012)
6. Ochs, C., Lamla, J.: Demokratische privacy by design. Kriterien soziotechnischer Gestaltung von Privatheit. Forschungsjournal Soziale Bewegungen. 30, 189–199 (2017). https://doi.org/10.1515/fjsb-2017-0040
7. Becker, C., Seubert, S.: Privatheit, kommunikative Freiheit und Demokratie. Datenschutz Datensich.-DuD **40**, 73–78 (2016)
8. Hagendorff, T.: Übersehene Probleme des Konzepts der Privacy Literacy. In: Roßnagel, A., Friedewald, M., Hansen, M. (Hrsg.) Die Fortentwicklung des Datenschutzes, S. 99–120. Springer Fachmedien Wiesbaden, Wiesbaden (2018). https://doi.org/10.1007/978-3-658-23727-1_6
9. BVerfG: Urteil vom 15.12.1983. (1983)
10. Roßnagel, A., Pfitzmann, A., Garstka, H.: Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern (2001)
11. Richter, P.: Datenschutz zwecklos? – Das Prinzip der Zweckbindung im Ratsentwurf der DSGVO. Datenschutz Datensich. **39**, 735–740 (2015). https://doi.org/10.1007/s11623-015-0510-9
12. Roßnagel, A., Friedewald, M., Geminn, C.L., Hagendorff, T., Heesen, J., Hess, T., Kreutzer, M., Neubaum, G., Ochs, C., Simo Fhom, H.: Policy Paper: Datensparsamkeit oder Datenreichtum? Zur neuen politischen Diskussion über den datenschutzrechtlichen Grundsatz der Datensparsamkeit. Fraunhofer Institut für System- und Innovationsforschung ISI, Karlsruhe (2017)
13. Pohle, J.: Zweckbindung Revisited. DANA – Datenschutz Nachrichten, S. 141–145 (2015)
14. Simitis, S.: Einleitung: Geschichte – Ziele – Prinzipien. In: Simitis, S. (Hrsg.) Bundesdatenschutzgesetz. Nomos, Baden-Baden (2011)
15. Kurz, C.: Spiros Simitis: „Man spielt nicht mehr mit dem Datenschutz!". https://netzpolitik.org/2015/spiros-simitis-man-spielt-nicht-mehr-mit-dem-datenschutz/. Zugegriffen: 7. Juli 2018
16. Hagendorff, T.: Das Ende der Informationskontrolle: digitale Mediennutzung jenseits von Privatheit und Datenschutz. Transcript, Bielefeld (2017)
17. Moor, J.H.: Towards a theory of privacy in the information age. ACM SIGCAS Comput. Soc. **27**, 27–32 (1997)
18. Seemann, M.: Das neue Spiel: Strategien für die Welt nach dem digitalen Kontrollverlust. Orange-Press, Freiburg im Breisgau (2014)
19. Karaboga, M., Matzner, T., Obersteller, H., Ochs, C.: Is there a right to offline alternatives in a digital world? In: Leenes, R., van Brakel, R., Gutwirth, S., De Hert, P. (Hrsg.) Data Protection and Privacy: (In)visibilities and Infrastructures, S. 31–57. Springer International Publishing, Cham (2017). https://doi.org/10.1007/978-3-319-50796-5_2
20. Karaboga, M., Matzner, T., Nebel, M., Ochs, C., Schütz, P., Simo Fhom, H., Morlok, T., Pittroff, F., von Pape, T., Pörschke, J.V.: White Paper Das versteckte Internet: Zu Hause – Im Auto – Am Körper. Fraunhofer-Institut für System- und Innovationsforschung, Karlsruhe (2015)

21. Taylor, L., Floridi, L., Sloot, B. van der (Hrsg.): Group Privacy: New Challenges of Data Technologies. Springer International Publishing, Cham (2017). https://doi.org/10.1007/978-3-319-46608-8
22. Bründl, S., Matt, C., Hess, T.: Wertschöpfung in Datenmärkten: Eine explorative Untersuchung am Beispiel des deutschen Marktes für persönliche Daten. Stober GmbH Druck und Verlag, Eggenstein (2015)
23. boyd, danah: Networked privacy. Surveill. Soc. **10**, 348–350 (2012). https://doi.org/10.24908/ss.v10i3/4.4529
24. Pearson, S.: Privacy, security and trust in cloud computing. In: Pearson, S., Yee, G. (Hrsg.) Privacy and Security for Cloud Computing, S. 3–42. Springer London, London (2013). https://doi.org/10.1007/978-1-4471-4189-1_1
25. Acquisti, A., Sleeper, M., Wang, Y., Wilson, S., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L.F., Komanduri, S., Leon, P.G., Sadeh, N., Schaub, F.: Nudges for privacy and security: understanding and assisting users' choices online. ACM Comput. Surv. **50**, 1–41 (2017). https://doi.org/10.1145/3054926
26. Solove, D.J.: Privacy Self-Management and the Consent Dilemma. Social Science Research Network, Rochester (2012)
27. Barocas, S., Nissenbaum, H.: Big data's end run around procedural privacy protections. Commun. ACM **57**, 31–33 (2014). https://doi.org/10.1145/2668897
28. Reding, V.: The European data protection framework for the twenty-first century. Int. Data Priv. Law **2**, 119–129 (2012)
29. Albrecht, J.P.: Hands Off Our Data. AktivDruck, Göttingen (2015)
30. Litman-Navarro, K.: Opinion|we read 150 privacy policies. They were an incomprehensible disaster. https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html, https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html (2019)
31. Roßnagel, A., Bile, T., Nebel, M., Geminn, C., Karaboga, M., Ebbers, F., Bremert, B., Stapf, I., Teebken, M., Thürmel, V., Ochs, C., Uhlmann, M., Krämer, N., Meier, Y., Kreutzer, M., Schreiber, L., Simo, H.: White Paper Einwilligung: Möglichkeiten und Fallstricke aus der Konsumentenperspektive. Fraunhofer Institut für System- und Innovationsforschung, Karlsruhe (2020)
32. Alizadeh, F., Jakobi, T., Boldt, J., Stevens, G.: GDPR-reality check on the right to access data: claiming and investigating personally identifiable data from companies. In: Proceedings of Mensch und Computer 2019 on – MuC'19, S. 811–814. ACM Press, Hamburg (2019). https://doi.org/10.1145/3340764.3344913
33. McDonald, A.M., Cranor, L.F.: The cost of reading privacy policies. J. Law Policy Inf. Soc. **4**, 543–568 (2008)
34. Bygrave, L.A., Schartum, D.W.: Consent, proportionality and collective power. In: Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., Nouwt, S. (Hrsg.) Reinventing Data Protection?, S. 157–173. Springer Netherlands, Dordrecht (2009). https://doi.org/10.1007/978-1-4020-9498-9_9
35. Utz, C., Degeling, M., Fahl, S., Schaub, F., Holz, T.: (Un)informed consent: studying GDPR consent notices in the field. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, S. 973–990. ACM, London (2019). https://doi.org/10.1145/3319535.3354212

36. Bull, H.-P.: Aus aktuellem Anlass: Bemerkungen über Stil und Technik der Datenschutzgesetzgebung. Recht der Datenverarbeitung, S. 148–153 (1999)
37. Norris, C.: The Unaccountable State of Surveillance: Exercising Access Rights in Europe. Springer, Berlin (2016)
38. Ausloos, J., Dewitte, P.: Shattering one-way mirrors–data subject access rights in practice. Int. Data Priv. Law **8**(1), 4–28, February 2018, (2018). https://doi.org/10.1093/idpl/ipy001
39. Calders, T., Custers, B.: What is data mining and how does it work? In: Custers, B., Calders, T., Schermer, B., Zarsky, T. (Hrsg.) Discrimination and Privacy in the Information Society, S. 27–42. Springer, Berlin (2013). https://doi.org/10.1007/978-3-642-30487-3_2
40. Hildebrandt, M.: Defining profiling: a new type of knowledge? In: Hildebrandt, M., Gutwirth, S. (Hrsg.) Profiling the European Citizen, S. 17–45. Springer Netherlands, Dordrecht (2008). https://doi.org/10.1007/978-1-4020-6914-7_2
41. Sloot, B. van der: From data minimization to data minimummization. In: Custers, B., Calders, T., Schermer, B., Zarsky, T. (Hrsg.) Discrimination and Privacy in the Information Society, S. 273–287. Springer, Berlin (2013). https://doi.org/10.1007/978-3-642-30487-3_15
42. Schaar, P.: Das Ende der Privatsphäre: der Weg in die Überwachungsgesellschaft. C. Bertelsmann, München (2007)
43. Degeling, M.: Profiling, Prediction und Privatheit: Über das Verhältnis eines liberalen Privatheitbegriffs zu neueren Techniken der Verhaltensvorhersage. In: Garnett, S., Halft, S., Herz, M., Mönig, J. M. (Hrsg.) Medien und Privatheit, S. 69–92. Medien, Texte, Semiotik 7. Passau: Verlag Karl Stutz (2014)
44. Hildebrandt, M.: Profiling: from data to knowledge: the challenges of a crucial technology. Datenschutz Datensich. – DuD **30**, 548–552 (2006). https://doi.org/10.1007/s11623-006-0140-3
45. Kammourieh, L., Baar, T., Berens, J., Letouzé, E., Manske, J., Palmer, J., Sangokoya, D., Vinck, P.: Group privacy in the age of big data. In: Taylor, L., Floridi, L., van der Sloot, B. (Hrsg.) Group Privacy: New Challenges of Data Technologies, S. 37–66. Springer International Publishing, Cham (2017). https://doi.org/10.1007/978-3-319-46608-8_3
46. Pohle, J.: Personal Data not found: Personenbezogene Entscheidungen als überfällige Neuausrichtung im Datenschutz. DANA – Datenschutz Nachrichten. 14–19 (2016)
47. Regan, P.M.: Legislating Privacy: Technology, Social Values and Public Policy. University of North Carolina Press, Chapel Hill (1995)
48. Marwick, A.E., boyd, danah: Networked privacy: how teenagers negotiate context in social media. New Media Soc. **16**, 1051–1067 (2014). https://doi.org/10.1177/1461444814543995
49. van der Sloot, B.: The individual in the big data era: moving towards an agent-based privacy paradigm. In: van der Sloot, B., Broeders, D., Schrijvers, E. (Hrsg.) Exploring the Boundaries of Big Data, S. 177–203. Amsterdam University Press, Amsterdam (2016)
50. Mantelero, A.: Personal data for decisional purposes in the age of analytics: from an individual to a collective dimension of data protection. Comput. Law Secur. Rev. **32**, 238–255 (2016). https://doi.org/10.1016/j.clsr.2016.01.014

51. Matzner, T., Ochs, C.: Chapter three: sorting things out ethically: privacy as a research issue beyond the individual. In: Zimmer, M., Kinder-Kurlanda, K. (Hrsg.) Internet Research Ethics for the Social Age: New Challenges, Cases, and Contexts, S. 39–73. Lang, New York (2017). https://doi.org/10.3726/b11077/16
52. Taylor, L., Sloot, B. van der, Floridi, L.: Conclusion: what do we know about group privacy? In: Taylor, L., Floridi, L., Sloot, B. van der (Hrsg.) Group Privacy, S. 225–237. Springer International Publishing, Cham (2017). https://doi.org/10.1007/978-3-319-46608-8
53. Jones, P.: Group rights. Stanford encyclopedia of philosophy (2016)
54. Mittelstadt, B.: From individual to group privacy in big data analytics. Philos. Technol. (2017). https://doi.org/10.1007/s13347-017-0253-7
55. Matzner, T., Richter, P.: Ausblick: Die Zukunft der informationellen Selbstbestimmung. In: Friedewald, M., Lamla, J., Roßnagel, A. (Hrsg.) Informationelle Selbstbestimmung im digitalen Wandel, S. 319–323. Springer Fachmedien Wiesbaden, Wiesbaden (2017). https://doi.org/10.1007/978-3-658-17662-4_18
56. Steeves, V.M.: Privacy, sociality and the failure of regulation: lessons learned from young Canadians' online experiences. In: Roessler, B., Mokrosinska, D. (Hrsg.) Social Dimensions of Privacy, S. 244–260. Cambridge University Press, Cambridge (2015). https://doi.org/10.1017/CBO9781107280557.013
57. Sevignani, S.: Privacy and capitalism in the age of social media. Routledge, New York (2016)
58. Koops, B.-J.: On decision transparency, or how to enhance data protection after the computational turn. In: Hildebrandt, M., de Vries, K. (Hrsg.) Privacy, Due Process and the Computational Turn, S. 196–220. Routledge, Abingdon (2013)
59. O'Neil, C.: Weapons of math destruction: how big data increases inequality and threatens democracy. Crown, New York (2016)
60. Krüger, J.: Wie der Mensch die Kontrolle über den Algorithmus behalten kann. https://netzpolitik.org/2018/algorithmen-regulierung-im-kontext-aktueller-gesetzgebung/. Zugegriffen: 11. Nov. 2018
61. Bygrave, L.A.: Data Protection Law : Approaching its Rationale, Logic and Limits. Kluwer Law International, London (2002)
62. Mantelero, A.: Social control, transparency, and participation in the big data world. J. Internet Law 23–29 (2014)
63. DEK: Gutachten der Datenethikkommission der Bundesregierung. Datenethikkommission der Bundesregierung, Berlin (2019)
64. Martin, N., Friedewald, M., Schiering, I., Mester, B.A., Hallinan, D., Jensen, M.: Die Datenschutz-Folgenabschätzung nach Art. 35 DSGVO: Ein Handbuch für die Praxis. Fraunhofer, Stuttgart (2020)
65. Martin, N., Mester, B.A., Schiering, I., Friedewald, M., Hallinan, D.: Datenschutz-Folgenabschätzung: Ein notwendiges „Übel" des Datenschutzes? Datenschutz Datensich. **44**, 149–153 (2020). https://doi.org/10.1007/s11623-020-1241-0
66. EDPS: EDPS Survey on Data Protection Impact Assessments under Article 39 of the Regulation. (2020)
67. Clarke, R.: Computer matching by government agencies: the failure of cost/benefit analysis as a control mechanism. Inf. Infrastruct. Policy **4**, 29–65 (1995)

68. Briegleb, V.: Selbstregulierung von Social Networks gescheitert. https://www.heise.de/newsticker/meldung/Selbstregulierung-von-Social-Networks-gescheitert-1857533.html. Zugegriffen: 12. Febr. 2018
69. Mantelero, A.: The future of consumer data protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics. Comput. Law Secur. Rev. **30**, 643–660 (2014). https://doi.org/10.1016/j.clsr.2014.09.004
70. Cavoukian, A.: Privacy by design: leadership, methods, and results. In: Gutwirth, S., Leenes, R., de Hert, P., Poullet, Y. (Hrsg.) European Data Protection: Coming of Age, S. 175–202. Springer Netherlands, Dordrecht (2013). https://doi.org/10.1007/978-94-007-5170-5_8
71. Hansen, M.: Data protection by design and by default à la European general data protection regulation. In: Privacy and Identity Management. Facing up to Next Steps, S. 27–38. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-55783-0_3
72. Husemann, C.: Datenschutz durch Systemgestaltung. In: Roßnagel, A. (Hrsg.) Das neue Datenschutzrecht: Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze, S. 163–171. Nomos, Baden-Baden (2018)
73. Schütz, P.: Zum Leben zu wenig, zum Sterben zu viel? Die finanzielle und personelle Ausstattung deutscher Datenschutzbehörden im Vergleich. In: Roßnagel, A., Friedewald, M., Hansen, M. (Hrsg.) Die Fortentwicklung des Datenschutzes, S. 251–268. Springer Fachmedien Wiesbaden, Wiesbaden (2018). https://doi.org/10.1007/978-3-658-23727-1_14
74. Europäische Union: Verordnung (EU) 2015/758 des Europäischen Parlaments und des Rates vom 29. April 2015 über Anforderungen für die Typgenehmigung zur Einführung des auf dem 112-Notruf basierenden bordeigenen eCall-Systems in Fahrzeugen und zur Änderung der Richtlinie 2007/46/EG. (2015)
75. Husemann, C., Pittroff, F.: Smarte Regulierung in Informationskollektiven – Bausteine einer Informationsregulierung im Internet der Dinge. In: Roßnagel, A., Friedewald, M., Hansen, M. (Hrsg.) Die Fortentwicklung des Datenschutzes, S. 337–359. Springer Fachmedien Wiesbaden, Wiesbaden (2018). https://doi.org/10.1007/978-3-658-23727-1_19
76. Nocun, K.: Datenschutz unter Druck: Fehlender Wettbewerb bei sozialen Netzwerken als Risiko für den Verbraucherschutz. In: Roßnagel, A., Friedewald, M., Hansen, M. (Hrsg.) Die Fortentwicklung des Datenschutzes, S. 39–58. Springer Fachmedien Wiesbaden, Wiesbaden (2018). https://doi.org/10.1007/978-3-658-23727-1_3