verbraucherzentrale
Nordrhein-Westfalen

Jörg Pohle

DATENSCHUTZ: RECHTSSTAATSMODELL ODER NEOLIBERALE RESPONSIBILISIERUNG?

Warum Datentreuhänder kein Mittel zum Schutz der Grundrechte sind

Vortrag 5 der Reihe „Zu treuen Händen“ | Februar 2022

ZU TREUEN HÄNDEN?
Verbraucherdatenschutz und digitale Selbstbestimmung

Eine Online-Vortragsreihe der Verbraucherzentrale NRW e. V.

VERBRAUCHER INFORMATIK

mit Unterstützung durch das
Institut für Verbraucherinformatik der Hochschule Bonn-Rhein-Sieg

Impressum

Verbraucherzentrale Nordrhein-Westfalen e.V.
Kompetenzzentrum Verbraucherforschung NRW
Mintropstraße 27
40215 Düsseldorf
zutreuenhaenden@verbraucherzentrale.nrw

Gefördert durch

Ministerium für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz des Landes Nordrhein-Westfalen

ORIGINALBEITRAG

Verbraucherzentrale NRW, Düsseldorf 2022

AUTOR

Jörg Pohle, Dr. rer. nat., Postdoc und Leiter des Forschungsprogramms „Daten, Akteure, Infrastrukturen: Governance datengetriebener Innovation und Cybersicherheit“, Alexander von Humboldt Institut für Internet und Gesellschaft (HIIG), Berlin.

DOKUMENTATION „ZU TREUEN HÄNDEN?“
Alle Videos und Paper der Vortragsreihe finden Sie unter
https://www.verbraucherforschung.nrw/zu-treuen-haenden-tagungsreihe-datenintermediaere-datentreuhaender-60831

INHALT

I. ABSTRACT

Der Beitrag formuliert eine grundsätzliche Kritik an den derzeit diskutierten Vorstellungen zu Datentreuhändern. Er zeigt auf, dass Datentreuhänder, die einem individualistischen Datenkontrollparadigma folgen, nicht nur zur Fortschreibung einer neoliberalen Individualisierungs- und Responsibilisierungsstrategie im Datenschutzbereich dienen, sondern auch strukturell nicht in der Lage sind, den Schutz der Grundrechte bei der Informationsverarbeitung sicherzustellen.

II. ZUR EINFÜHRUNG

Datentreuhänder sind keine neue Erfindung. Als in den 1970er-Jahren die Idee der Datentreuhänder in die Datenschutzdiskussion eingeführt wurden, sollte ihre Funktion darin bestehen, den Graben zwischen der vom Datenschutzrecht geforderten Setzung eng umgrenzter Verarbeitungszwecke und dem für die datengetriebene wissenschaftliche Forschung notwendigen breiten Zweck, nämlich Forschung und Erkenntnisproduktion, zu überbrücken und dabei dennoch einen ausreichenden Schutz der Grundrechte der Betroffenen sicherzustellen. Inzwischen sind Datentreuhänder in der öffentlichen wie der Fachdebatte zu einem allgemeinen Lösungsmodell für den Datenschutzbereich avanciert. Zwei Gründe können als dafür ursächlich identifiziert werden: zum einen der verbreitete Glaube, dass Daten(-fluss-)kontrolle – vor allem durch die Betroffenen selbst vorgenommen – das eigentliche Problem sei, das der Datenschutz und das Datenschutzrecht zu lösen versuchten; zum anderen die zunehmende gesellschaftliche Durchsetzung von neoliberalen Responsibilisierungsstrategien, also der Übertragung von Verantwortung für die Lösung systemischer Probleme auf Individuen, einschließlich deren absehbarem Scheitern, das dann als Anknüpfungspunkt für Schuldvorwürfe dient.

Diesen individualistischen Verständnissen von Datenschutz und den an diese anschließenden Responsibilisierungspolitiken will der Beitrag ein Datenschutzverständnis entgegensetzen, das Datenschutz nicht als individuelle Befindlichkeit, private Neigung oder Schutz einer als privat verstandenen Sphäre und schon gar nicht als auf die Betroffenen abgewälzte Schutzverantwortung versteht, sondern als Mittel zur Feststellung und Durchsetzung der Bedingungen, unter denen moderne Informationsverarbeitung gesellschaftlich, also für alle Teile der Gesellschaft, akzeptabel sein kann (Podlech 1976, 24). Nicht nur war es diese gesellschaftspolitische Vorstellung von Datenschutz – und gerade nicht die heute in der Diskussion vorherrschenden individualistischen Privatheitsvorstellungen –, die die erste Phase der Datenschutzdiskussion in den 1970er-Jahren bestimmt hat (Pohle 2019), sie hat auch die Umsetzung des Datenschutzes im Recht wesentlich geprägt und prägt sie bis heute. Das lässt sich auch in der EU-Datenschutzgrundverordnung (EU-DSGVO) ablesen, selbst wenn diese die gesellschaftliche Akzeptabilität weniger breit definiert, als es die Debatte in den 1970er-Jahren gemacht hat, und sich vielmehr auf den Schutz der betroffenen Personen und ihrer Grundrechte und Grundfreiheiten (Art. 1 Abs. 1 und 2 DSGVO) beschränkt.

Vor diesem Hintergrund will der Beitrag eine grundsätzliche Kritik an Datentreuhändern, vor allem in ihrer heute vorwiegend diskutierten Form, formulieren. Er wird zeigen, wie Datentreuhänder nicht nur zur Fortschreibung einer neoliberalen Individualisierungs- und Responsibilisierungsstrategie im Datenschutzbereich dienen, sondern dass sie auch strukturell nicht in der Lage sein können, den Schutz der Grundrechte bei der Informationsverarbeitung sicherzustellen.

Auf dem Weg dahin will der Beitrag für einen schärferen analytischen Zugang zu der Debatte um den Datenschutz und das Datenschutzrecht, aber auch zu den einzelnen Lösungsvorschlägen, die in diesem Bereich vorgebracht werden, werben und sensibilisieren. Es geht darum, ein Verständnis dafür zu entwickeln, dass alle Lösungsvorschläge im Privacy- und Datenschutzbereich immer auf bestimmte Problemverständnisse zielen und dass sie, wenn überhaupt, immer nur die so verstandenen Probleme adressieren. Ohne eine Auseinandersetzung mit den jeweils zugrunde gelegten Problemverständnissen können die vorgeschlagenen Lösungen also gar nicht analysiert und bewertet werden.

Hier setzt der Beitrag an. Er gibt im Anschluss an die Einleitung einen Überblick über zwei sehr gegensätzliche Vorstellungen von Datenschutz, die zwar nicht die gesamte Debatte in diesem Bereich vollständig widerspiegeln, aber doch als zentrale Strömungen gelten können: das individualistische Datenkontrollparadigma einerseits und das „Rechtsstaatsmodell“ andererseits. Vor der Folie dieser beiden prototypischen Verständnisse wird dann die Datenschutzgrundverordnung auf die ihr zugrunde liegende Vorstellung befragt.

Im dritten Teil wird das neoliberale Regierungsmodell der Responsibilisierung eingeführt, unter dem Mechanismen von auf die Betroffenen abgewälzter Schutzverantwortung verstanden werden, die in der öffentlichen Debatte verbreitet als „Empowerment“ verkauft werden, im Falle des erwartbaren Scheiterns aber als Anknüpfungspunkt für Schuldvorwürfe dienen. Am konstruierten Beispiel eines responsibilisierten Lebensmittelrechts soll dieses Modell verdeutlicht werden.

Auf der Basis dieser Vorarbeiten wird sich der Hauptteil des Beitrags den Datentreuhändern widmen. In einem kurzen Überblick über die Geschichte der Debatte zu Datentreuhändern wird dargestellt, wie sich die Funktion, die Datentreuhändern zur Erfüllung zugeschrieben wurde und wird, seit ihrem Aufkommen in den 1970er-Jahren gewandelt hat. Wie die Beiträge in der neueren Literatur zu Datentreuhändern zeigen, liegt den derzeit diskutierten Vorschlägen für solche Treuhänder ein individualistisches und auf Daten(-fluss-)kontrolle zielendes Verständnis zugrunde, und es geht gerade nicht darum, dass diese Treuhänder den Schutz der Grundrechte und Grundfreiheiten der Betroffenen sicherstellen sollen. In Erweiterung der bestehenden, aber noch sehr leisen Kritik an Datentreuhändern wird anschließend gezeigt, dass diese Treuhänder auch strukturell nicht in der Lage sind, den Schutz der Grundrechte bei der Datenverarbeitung sicherzustellen.

Abschließend werden konkrete Handlungsempfehlungen an verbraucherpolitische Akteur:innen formuliert, die ihnen dabei helfen sollen, vermeintliche „Lösungen“ kritisch zu hinterfragen, vor allem wenn sie mit einem scheinbar positiven Framing wie „Selbstbestimmung“, „Empowerment“ oder „digitale Mündigkeit“ verbreitet werden. Das beginnt schon beim Framing des Problems und der Frage, ob die jeweilige Problembeschreibung für den konkreten Gegenstand angemessen und gesellschaftlich akzeptabel ist, aber auch, ob die Lösung für das beschriebene Problem wirksam ist. Aus Sicht eines auf Grundrechtsschutz zielenden Datenschutzes stellt sich konkret die Frage, ob die vorgeschlagene Lösung dazu beiträgt, Grundrechte zu schützen, oder ob es sich lediglich um eine Simulation von Grundrechtsschutz handelt. Und nicht zuletzt muss aus Sicht der Verbraucher:innen explizit gefragt werden, ob diesen Verantwortlichkeiten aufgebürdet werden sollen, die erstens nach dem Gesetz eigentlich die Datenverarbeiter verpflichten und zweitens von den Verbraucher:innen gar nicht erfüllt werden können, bei deren Scheitern sie dann allerdings mit Vorwürfen konfrontiert werden.

Vor einer inhaltlichen Auseinandersetzung mit dem Datenschutz und der Rolle, die Datentreuhänder in diesem Bereich übernehmen oder nicht übernehmen können, scheint es angeraten, zwei Prämissen explizit einzuführen, auf die sich die nachfolgenden Ausführungen stützen: erstens, dass Geeignetheit und Wirksamkeit einer vorgeschlagenen Lösung nicht vom Problembezeichner, sondern vom Problemverständnis abhängen, und zweitens, dass sowohl Privacy als auch Datenschutz wesensmäßig umstrittene Konzepte sind. Beide Prämissen sollen nun kurz eingeführt und dargestellt werden.

1. DIE EIGNUNG UND WIRKSAMKEIT EINER LÖSUNG HÄNGT WESENTLICH VOM PROBLEMVERSTÄNDNIS AB

Es ist eigentlich eine Binsenweisheit, dass Mittel nie universell gut oder schlecht, geeignet oder ungeeignet, wirksam oder unwirksam sind, sondern immer nur in Relation zu einem mehr oder weniger spezifischen Zweck. Und diese Ziel- oder Zweckvorstellungen sind gemeinhin auch Ausgangspunkt für die konkrete Gestaltung der Mittel, sie prägen damit diese Mittel und bestimmen ihre Charakteristika. Die Debatte in den beteiligten Wissenschaften spiegelt das nur ungenügend wider. So blenden etwa alle rechtsvergleichenden Arbeiten im Datenschutzrechtsbereich, etwa zwischen der DSGVO und dem California Consumer Privacy Act auf der einen oder dem chinesischen Datensicherheitsrecht auf der anderen Seite, die Zieldefinition der jeweiligen Gesetze genauso weitgehend aus wie informatische Arbeiten und fokussieren stattdessen ausschließlich auf die einzelnen Mittel, seien es die spezifischen gesetzlichen Regelungen, etwa zur Definition der unter das Gesetz fallenden Daten oder zu den Dokumentationspflichten, oder konkrete technische Maßnahmen wie Verfahren zur Verschlüsselung oder zum verteilten Rechnen. Die einzelnen rechtlichen oder technischen Mittel miteinander zu vergleichen, ohne dabei Bezug auf die Ziel- oder Zweckvorstellungen der Gesetze beziehungsweise der Technikgestaltung zu nehmen, ist aber nicht instruktiv. – Welcher Hammer besser ist, der Vorschlaghammer oder der Uhrmacherhammer, hängt vom Verwendungszweck ab.

Die Ziel- oder Zweckvorstellungen, für die konkrete Mittel entwickelt werden, sind wiederum abhängig von den jeweiligen Problemverständnissen. Auch dieser Aspekt wird in der Debatte oft unzulässig verkürzt, so etwa in dem in der informatischen Debatte einflussreichen Diktum Bruce Schneiers zur Situation im Bereich der IT-Sicherheit „The threats are what determines the policy, and the policy is what determines the design“ (Schneier 2000, 227) – es sind jedoch nicht die Bedrohungen, sondern die Bedrohungsvorstellungen, die die Schutzmaßnahmen anleiten. Und diese Problemverständnisse sind nicht notwendig korrekt, zeitlos oder unumstritten. Im Gegenteil stellen wir immer wieder fest, dass vermeintlich als gesichert geltende Erkenntnisse sich als falsch oder überholt herausstellen oder dass vermeintlich konsentierte Ansichten tatsächlich umstritten sind. Und gerade ein inhaltlicher Dissens „versteckt“ sich gerne hinter konsensual genutzten Bezeichnern, aus terminologischer Koinzidenz folgt aber keine Gleichheit der Konzepte. Um die Lösungen vergleichen und auf ihre Eignung und Wirksamkeit untersuchen zu können, ist daher nicht nur eine Auseinandersetzung mit Ziel- und Zweckvorstellungen, sondern auch mit den diesen zugrunde liegenden Problemverständnissen erforderlich. Das gilt umso mehr, weil Privacy und Datenschutz wesensmäßig umstrittene Konzepte sind.

2. PRIVACY UND DATENSCHUTZ SIND WESENSMÄßIG UMSTRITTENE KONZEPTE

Es hat in der Privacy-Debatte viele Jahrzehnte gedauert, bis sich die Erkenntnis durchgesetzt hat (vgl. Mulligan, Koopman und Doty 2016), dass es sich bei Privacy nicht um ein einheitliches oder auch nur durch eine Wittgensteinsche Familienähnlichkeit geprägtes Konzept handelt (so etwa prominent Solove 2002), sondern um ein „essentially contested concept“ (Gallie 1956), ein wesensmäßig umstrittenes Konzept. Gleiches gilt auch für Datenschutz, wobei dort der Nachweis allerdings allenfalls implizit erfolgt ist (vgl. Pohle 2018).

Als wesensmäßig umstrittene Konzepte werden mit Gallie Konzepte bezeichnet, die ihre Bedeutung im Wesentlichen durch die Perspektive derjenigen gewinnen, die sie betrachten. Das betrifft vor allem abstrakte Konzepte oder Ideen wie „Demokratie“ oder „Freiheit“, aber auch „Kunst“, die allenfalls einen konsentierten Kern haben, deren Bedeutung über diesen Kern hinaus aber perspektivabhängig konkretisiert wird. Die Perspektiven sind dabei abhängig von den unterschiedlichen Wertvorstellungen, die von den Betrachter:innen vertreten werden, und sie führen zu unterschiedlichen Ausfüllungen der Konzepte. Und diese über die Kernbedeutung hinausgehenden Bedeutungsinhalte sind dann notwendig umkämpft. Für „Demokratie“ führt dies etwa zum klassischen Antagonismus von repräsentativer und direkter Demokratie. Und dieser Gegensatz hat Implikationen, etwa für die Umsetzung im Recht oder in der Technik, trotz einer Einigung auf einen gemeinsamen Bezeichner – „democracy by design“ kann damit sowohl eine Umsetzung von repräsentativer wie von direkter Demokratie sein, aber nicht beides zugleich.

In der Diskussion um Privacy und Datenschutz zeigt sich das schon beim Bezeichner. Es gibt nicht einmal eine Einigung auf einen gemeinsamen Bezeichner, stattdessen konkurrieren viele verschiedene Bezeichner um die Aufmerksamkeit in der Diskussion über das Problemfeld: von (Computer, Information oder Data) Privacy, Privatheit, Privatsphäre, digitaler Intimsphäre oder informationeller Selbstbestimmung über Surveillance oder Dataveillance bis hin zu Datenschutz. Und bei der Frage, ob „Datenschutz“ und „Schutz von Daten“ synonym verwendet werden können, scheiden sich die Geister – in den Europäischen Verträgen, konkret in der EU-Grundrechtecharta, wird beides synonym genutzt und damit der juristische Sprachgebrauch geprägt, aber sowohl die Tatsache, dass wir über die tatsächliche Herkunft des Bezeichners nur wissen, dass sie unbekannt ist (Lewinski 2014, 3), wie auch der Vergleich mit Bezeichnern wie „Hochwasserschutz“, „Sonnenschutz“, „Katastrophenschutz“ oder „Prallschutz“ lassen doch starke Zweifel daran aufkommen, dass Datenschutz den Schutz der Daten meint.

Hinter den Konzepten stehen jedenfalls unterschiedliche Wertvorstellungen, ob zu Freiheit von oder Freiheit zu, Menschenwürde oder Persönlichkeit, Identität oder Agency. In den Konzepten werden auch unterschiedliche Schutzgüter identifiziert: von Geheimnissen oder einem zu schützenden privaten Bereich, über die kontextuelle Integrität oder die privaten oder persönlichen Daten, bis hin zu den Grundrechten oder den Freiheitsversprechen der bürgerlichen Gesellschaft. Und selbst einiges von dem, was in so manchen der verbreiteten Vorstellungen als Schutzmechanismen verstanden wird, die dem Schutz dieser Schutzgüter dienen sollen, etwa Geheimhaltung oder Vertraulichkeit von Daten oder Transparenz der Verarbeitung, Kontrolle der Daten, der Datenflüsse und ihrer Nutzungen, oder die angemessene Verfahrens- und Technikgestaltung, kann

in anderen Vorstellungen nicht das Mittel, sondern das Ziel sein, also das zu schützende Gut. Das gilt etwa für die Daten(-fluss-)kontrolle, vor allem wenn sie durch die betroffenen Personen selbst ausgeübt wird.

Nicht zuletzt deshalb soll die Daten(-fluss-)kontrolle als eines der zwei für diesen Beitrag als Bezugspunkte gewählten prototypischen Verständnisse dienen. Der andere und primäre Grund für ihre Auswahl ist ihre Verbreitung in der Diskussion um Datentreuhänder. Das zweite als Anknüpfungspunkt gewählte Verständnis ist das am Rechtsstaatsmodell orientierte und auf Grundrechtsschutz zielende Verständnis von Datenschutz, das nicht nur die erste Phase der Datenschutzdiskussion in den 1970er-Jahren bestimmt hat, sondern auch die Umsetzung des Datenschutzes im Recht wesentlich geprägt hat und bis heute prägt.

III. PRIVACY UND DATENSCHUTZ – ZWEI GEGENSÄTZLICHE VORSTELLUNGEN. UND WAS SAGT EIGENTLICH DIE DATENSCHUTZGRUNDVERORDNUNG?

Die beiden hier vorgestellten Zielvorstellungen von Privacy oder Privatheit beziehungsweise Datenschutz – das individualistische Datenkontrollparadigma einerseits und die am Rechtsstaatsmodell orientierte Vorstellung andererseits – spiegeln zwar nicht die gesamte Debatte in diesem Bereich vollständig wider, sie können gleichwohl als zwei der zentralen und wirkmächtigsten Strömungen gelten. Die explizite Einführung der beiden Vorstellungen soll die Grundlage schaffen, um einerseits die DSGVO daraufhin befragen zu können, welche Zielvorstellung ihr zugrunde liegt, und andererseits im dritten Kapitel eine fundierte Einordnung und Kritik der Vorschläge für Datentreuhänder leisten zu können.

1. DAS INDIVIDUALISTISCHE DATENKONTROLLPARADIGMA

Das Datenkontrollparadigma, in der englischsprachigen Literatur unter „privacy-as-control paradigm“ zu finden (vgl. Diaz und Gürses 2012), gehört zu den ältesten Zielvorstellungen, die in der modernen Debatte um die Folgen der computergestützten Informationsverarbeitung für Individuen und Gesellschaft entwickelt wurden. Bereits Alan Westin, dessen Buch „Privacy & Freedom“ die Debatte ganz wesentlich befeuert hat, versteht Privacy als Anspruch auf die Kontrolle des Informationsflusses: „The claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others“ (Westin 1967, 7). Dass Westin hier nicht nur Individuen, sondern auch Gruppen und Organisationen im Blick hatte, ist hingegen in der weiteren Debatte, von Ausnahmen abgesehen (Bloustein 1978), weitgehend ignoriert worden. Erst in den letzten Jahren sind zumindest Gruppen wieder in den Fokus der Aufmerksamkeit gerückt (Taylor, Floridi und Sloot 2017).

Auch das Bundesverfassungsgericht hat seiner Entscheidung im Volkszählungsurteil 1983 die Vorstellung einer individuellen Informations(-fluss-)kontrolle zugrunde gelegt, als es formulierte, dass das „informationelle Selbstbestimmungsrecht“, so der Name des neu entdeckten Grundrechts, „die Befugnis des Einzelnen, grundsätzlich selbst

über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“ gewährleiste.[1] Das Bundesverfassungsgericht erweckt dabei den Eindruck, als sei diese Befugnis eine notwendige Folge dessen, was es zwei Sätze zuvor als Zwischenfazit vorbringt, dass die freie Entfaltung der Persönlichkeit „unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus[setzt].“. Tatsächlich ist sie das nicht – der Schutz der Entfaltung der Persönlichkeit gegen unbegrenzte, also nicht unter Bedingungen gestellte Datenverarbeitung könnte natürlich auch ohne Rekurs auf eine solche individuelle Kontrollbefugnis sichergestellt werden, wie das in anderen vermachteten sozialen Beziehungen, etwa im Arbeitsrecht, im Mietrecht oder im Verbraucherrecht, auch geschieht. Vor allem aber verzichtet das Bundesverfassungsgericht auf Ausführungen dazu, ob die Ausübung dieser individuellen Kontrollbefugnis überhaupt eine Schutzwirkung entfalten kann und entfaltet – ein blinder Fleck, der bis heute die Debatte prägt.

Neben die „informationelle Selbstbestimmung“ sind inzwischen viele weitere Bezeichner für das individualistische Datenkontrollparadigma getreten. Dazu gehören etwa „Datensouveränität“ oder „Datenhoheit“. Für das Verständnis des zugrunde liegenden Problems, das gelöst werden soll, bringen sie ebenso wenig wie für die Frage, wie genau der Schutzmechanismus ausgestaltet werden soll. Ihre Funktion in der Debatte besteht stattdessen darin, als rhetorisches Mittel der Forderung Nachdruck zu verleihen, die in den bestehenden gesetzlichen Regelungen als unabdingbar gesetzten Prinzipien und Rechte, die als nicht abtretbar oder wegverhandelbar sind, in abdingbare Prinzipien und Rechte zu ändern.“ Die Pathetik des gewählten Bezeichners, besonders deutlich etwa bei „Hoheit“ oder „Souveränität“, korreliert dabei auffallend mit dem Umfang der für abtretbar erklärten Rechte der Betroffenen. Vergleichbares gilt für die Versprechungen, die gegenüber den Betroffenen abgegeben werden: Es diene ihrem „Empowerment“ und ermögliche es ihnen, dafür zu sorgen, dass die Datenverarbeitung entsprechend ihrer „individuellen Werte und Präferenzen“ ablaufe. Diesen Versprechungen zur Seite tritt eine Form des technischen „Solutionismus“ (Morozov 2013): „Selbstdatenschutz“ vor allem durch informationstechnische Systeme, die von den Betroffenen kontrolliert werden und es ihnen ermöglichen, für ihren eigenen Schutz zu sorgen.

Die prototypische Umsetzung des individualistischen Datenkontrollparadigmas im Recht ist eine Kombination aus „informierter Einwilligung“ und individuellen Betroffenenrechten, etwa den Rechten auf Auskunft, Berichtigung und Löschung.

2. DAS „RECHTSSTAATSMODELL“ DES DATENSCHUTZES

Das „Rechtsstaatsmodell“ des Datenschutzes ist nur unwesentlich jünger als das Datenkontrollparadigma und wurde seit Anfang der 1970er-Jahre vor allem in der Bundesrepublik ausgearbeitet (grundlegend Steinmüller et al. 1972, 60), unter maßgeblicher Beteiligung von zwei der späteren Kläger:innen im Volkszählungsverfahren vor dem Bundesverfassungsgericht, Adalbert Podlech und Wilhelm Steinmüller. In der englischsprachigen Literatur wird vergleichsweise selten auf das Rechtsstaatsmodell Bezug genommen, wenn auch in den letzten Jahren einige entsprechende Arbeiten erschienen sind (vgl. Citron 2008, Austin 2014).

1 BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983 – 1 BvR 209/83 –, Rn. 1–215, 147.

Das Problem, das der Datenschutz zu lösen sucht, wird dabei als technikvermitteltes gesellschaftliches Machtproblem verstanden, vergleichbar zum „Problem des Verfassungsstaates im politischen Bereich und […] der Kontrolle der Produktionsverhältnisse im wirtschaftlichen Bereich“ (Podlech 1976, 24). Es gehe um die „Feststellung und Durchsetzung der Bedingungen, unter denen das Informationsgebaren einer Gesellschaft für die Glieder der Gesellschaft akzeptabel sein kann“ (Podlech 1976, 24). Daher könne auch beim Lösungsansatz an die Erfahrungen angeknüpft werden, die mit der rechtsstaatlichen Einhegung des Staates gesammelt wurden: „Konzentrierung der diffusen gesellschaftlichen Macht auf den souveränen Staat, um die Machtfrage entscheidbar zu machen [unter Verweis auf Niklas Luhmann]; Entscheidung der Machtfrage durch die Restriktion auf konsensfähige Machtausübung [unter Verweis auf Wilhelm von Ockham]; Bewirkung der Restriktion durch Gewaltenteilung und Kompetenzbindung [unter Verweis auf Montesquieu]“ (Podlech 1976, 24 f.). Das heißt also, dass der Staat, der mit seinem Handeln ein Risiko für die Bürgerinnen und Bürger darstellt, eingehegt, an die Kette gelegt, gewaltenteilig organisiert wird, damit sich die einzelnen Gewalten gegenseitig kontrollieren und in ihrer Macht begrenzen. Der Staat wird direkt an die Grundrechte gebunden und muss sich selbst auch an die Regeln und Gesetze halten – und er muss die Einhaltung nachweisen, und wird dafür zur Verantwortung gezogen. Und in diesem Sinne lässt sich dann das Datenschutzrecht als die „folgerichtige Weiterentwicklung des rechtsstaatlichen Prinzips der Gesetzmäßigkeit der Verwaltung“ durch dessen Ausdehnung auf den privaten Bereich entsprechend gestalten (Steinmüller 1976, 14).

Dieses Verständnis bestimmt dann auch die konzeptionelle Umsetzung im Recht: Es ist erstens geprägt von Gewährleistungspflichten für Datenverarbeiter, die nach objektiven Kriterien und unabhängig vom Wissen und Wollen der Betroffenen umzusetzen sind. Die Gewährleistungspflichten umfassen zweitens Gestaltungsanforderungen an Informationsverarbeitungsprozesse und die dafür eingesetzten Mittel, einerseits die organisatorischen Strukturen und Verfahren und andererseits die informationstechnischen Systeme. Und das dritte Charakteristikum der Umsetzung im Recht besteht in der Institutionalisierung von externer Aufsicht und Kontrolle in einer Behörde, die über eigene Kontrollrechte verfügt und nicht nur solche, die aus den Rechten der Betroffenen abgeleitet sind.

Umsetzung und Durchsetzung werden demnach zwar über das Recht vermittelt, sind selbst aber immer als ein Ineinandergreifen von rechtlichen, organisatorischen und technischen Mechanismen gedacht, auch weil schon früh erkannt wurde, dass „soziale Freiheit [...] nunmehr nur noch möglich [ist], wenn sie von vornherein in die Konstruktion der Informationssysteme eingeplant, auch mit den Mitteln der modernen Daten- und Kommunikationstechnologien technisch und organisatorisch abgesichert und schließlich in ihrem sozialen Umfeld rechtlich verankert und gewährleistet wird“ (Steinmüller, Ermer und Schimmel 1978, 2).

3. WAS SAGT EIGENTLICH DIE DATENSCHUTZGRUNDVERORDNUNG?

Die EU-Datenschutzgrundverordnung dient, wie Artikel 1 explizit ausführt, dem Schutz von Menschen und ihren Grundrechten bei der Datenverarbeitung. Es sind also nicht, wie verbreitet kolportiert wird, Daten, die geschützt werden sollen, sondern „natürliche Personen bei der Verarbeitung personenbezogener Daten“ (Art. 1 Abs. 1 DSGVO). Und es sind auch nicht Privacy, Privatsphäre, Privatheit oder informationelle Selbstbestimmung, die geschützt werden sollen, sondern alle Grundrechte und Grundfreiheiten

(Art. 1 Abs. 2 DSGVO). Als europäisches Normenwerk adressiert sie dabei zuerst einmal die europäischen Grundrechte, wie sie in der EU-Grundrechtecharta verankert sind, aber das schließt nicht aus, dass auch die Grundrechte der Europäischen Menschenrechtskonvention und der Verfassungen der Mitgliedstaaten zur Auslegung herangezogen werden können.

Die DSGVO geht dabei von der Annahme aus, dass mit einer Informationsverarbeitung Risiken für die Grundrechte und Grundfreiheiten einhergehen können, und zielt dann darauf ab, dass diese Risiken unter Kontrolle gebracht werden. Das Datenschutzrecht kann somit, einem Vorschlag aus den 1970er-Jahren folgend, als die informationelle Dimension aller Grundrechte verstanden werden (vgl. Garstka 1977), da zu dem Zeitpunkt, als die Auswirkungen der Informationsverarbeitung als eigenständiges Problem, das es zu lösen gelte, begriffen wurden, die Grundrechte bereits weitgehend konkretisiert waren und ihnen deshalb eine explizite informationelle Dimension fehlte.

Die Datenschutzgrundverordnung ist geprägt von der Zuweisung von Verantwortung an den Datenverarbeiter. Er wird im Gesetz nicht nur als „Verantwortlicher“ bezeichnet, weil er „über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“ (Art. 4 Nr. 7 DSGVO), sondern auch, weil er verantwortlich gemacht wird, „sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt“ (Art. 24 Abs. 1 S. 1 DSGVO). Diese „Rechenschaftspflicht“ (Art. 5 Abs. 2 DSGVO) trifft den Verarbeiter unabhängig davon, was die „individuellen Werte und Präferenzen“ der Betroffenen sind oder sein mögen. Sie werden in der DSGVO – an manchen Stellen detaillierter als an anderen – umfassend ausbuchstabiert und bilden damit nicht nur Anknüpfungspunkte für konkrete Umsetzungsmaßnahmen, sondern auch für die Nachweisführung.

Neben umfangreichen Pflichten für Datenverarbeiter enthält die Datenschutzgrundverordnung auch individuelle Rechte der betroffenen Personen, darunter die Rechte auf Auskunft, Berichtigung und Löschung. So stark diese Rechte auch sein mögen und so sehr sie auch in der öffentlichen Debatte im Vordergrund stehen, stehen sie in der Verordnung doch im Schatten der Pflichten für die Verarbeiter. Bemerkenswerterweise sind nämlich allen Rechten mit Ausnahme des Rechts auf Datenübertragbarkeit nach Art. 20 DSGVO und des Widerspruchsrechts nach Art. 21 DSGVO gleichlautende objektive Pflichten der Verarbeiter vorgeschaltet: Vor dem Recht auf Auskunft nach Art. 15 DSGVO stehen die Informationspflichten nach Art. 13 und 14 DSGVO, vor dem Recht auf Berichtigung nach Art. 16 DSGVO steht die Pflicht zur Gewährleistung der Richtigkeit nach Art. 5 Abs. 1 lit. d) DSGVO, und vor dem Recht auf Löschung nach Art. 17 DSGVO steht die entsprechende Pflicht der Verarbeiter zur Löschung („Speicherbegrenzung“) nach Art. 5 Abs. 1 lit. e) DSGVO.

Die Datenschutzgrundverordnung lässt sich also beschreiben als eine Kombination aus einer an Rechtsstaatsgrundsätzen orientierten Regelungsarchitektur mit umfangreichen Pflichten für Verarbeiter einerseits – zum Vergleich sei hier auf Art. 1 Abs. 3 Grundgesetz verwiesen: „Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht.“ – mit starken individuellen Betroffenenrechten andererseits.

Diese Kombination ist weder konzeptionell noch historisch überraschend. Konzeptionell dienen die Betroffenenrechte als breitestmögliche Ausdehnung von Problemdetektoren, nach deren Anschlagen dann aufsichtsbehördliches Handeln ausgelöst werden kann. Historisch ist die DSGVO sehr weitgehend eine schlichte Weiterentwicklung der EG-

Datenschutzrichtlinie von 1995, die selbst wiederum zur Erzeugung politischer Kompromissfähigkeit Elemente aus allen Datenschutzrechtsregimen der damaligen EG-Mitgliedstaaten in recht eklektischer Weise zusammengeführt hat. Die Datenschutzgrundverordnung folgt demnach keinem sauberen Regulierungsdesign, sondern ist eher eine regulatorische Wundertüte.

Trotzdem ist der Schwerpunkt eindeutig: Die Regelungsarchitektur und der extrem starke Bezug auf Pflichten für Verarbeiter zeigen die Herkunft der EU-Datenschutzgrundverordnung aus dem Rechtsstaatsmodell.

IV. RESPONSIBILISIERUNG – EIN NEOLIBERALES REGIERUNGSMODELL

Hier soll nun das neoliberale Regierungsmodell der Responsibilisierung eingeführt werden, unter dem Mechanismen von auf die Betroffenen abgewälzter Schutzverantwortung verstanden werden, die in der öffentlichen Debatte verbreitet als „Empowerment“ verkauft werden, im Falle des erwartbaren Scheiterns aber als Anknüpfungspunkt für Schuldvorwürfe dient. Am konstruierten Beispiel eines responsibilisierten Lebensmittelrechts wird das Modell verdeutlicht.

1. RESPONSIBILISIERUNG – ZWISCHEN „EMPOWERMENT“ UND SCHULDVORWÜRFEN

Mit „Responsibilisierung“ wird in der Literatur zu Gouvernementalität der Prozess bezeichnet, durch den Akteure individuell für eine Aufgabe verantwortlich gemacht werden, die zuvor eine Verpflichtung eines anderen Akteurs war oder überhaupt nicht als Verantwortung anerkannt wurde (Shamir 2008; Soneryd und Uggla 2015). Die Akteure, denen die entsprechende Aufgabe – etwa die Bewältigung eines gesellschaftlichen Problems oder die Aufrechterhaltung eines öffentlichen Wertes – zuvor übertragen war, sind oft der Staat oder eine staatliche Behörde oder vom Staat durch das Recht in die Pflicht genommene private Organisationen, etwa die Hersteller von Produkten, die Anbieter von Dienstleistungen oder die Arbeitgeber. Im Zuge der Reponsibilisierung werden diese Aufgaben nun Individuen in Teilen übergeholfen. Damit einher geht die Umdefinition des Problems und seiner erwünschten Lösung beziehungsweise der zu erfüllenden Aufgabe: Sie werden nun in einer Form neu gefasst, in der die Lösung darin besteht, dass es bestimmter moralisch aufgeklärter Akteure bedarf – prototypisch: die verantwortungsbewusste Konsument:in – und diese mit ihren individuellen Wünschen, Bestrebungen und Entscheidungsmöglichkeiten einem unmoralischen Anderen gegenübergestellt wird: der unverantwortlichen oder verantwortungslosen Konsument:in (Giesler und Veresiu 2014, 841). Die ideologische Legitimierung erfolgt also über die Neubestimmung der Rollen und Identitäten von Individuen als Arbeitnehmer:innen, Sozialhilfeempfänger:innen, Manager:innen, Beamt:innen, Bürger:innen, Verbraucher:innen und so weiter, die als autonome, selbstbestimmte und selbsterhaltende Subjekte imaginiert werden, die als gleichberechtigte Partner:innen an einem marktlichen Austausch teilnehmen und von denen daher verlangt werden kann und muss, dass sie selbst Umsicht walten lassen und für sich selbst verantwortlich sein sollen und die Folgen auch selbst tragen müssen (Shamir 2008; Gray 2009; Pyysiäinen, Halpin und Guilfoyle 2017).

In diesem Responsibilisierungsprozess wird zwar die Verantwortung den Individuen in Teilen übergeholfen, sie erhalten allerdings damit nicht auch die Macht oder die Mittel,

dieser Verantwortung gerecht zu werden. Insoweit nun die Individuen aber zugleich stärker von den Folgen betroffen sind, verschiebt sich auch der Fokus der Aufmerksamkeit: „It is here that the creation of a new form of 'neo-liberal blaming the victim' begins to evolve." (Gray 2009, 330).

In der Informatik werden diese Responsibilisierungsprozesse inzwischen auch diskutiert, vor allem im Zusammenhang mit IT-Sicherheit (Renaud et al. 2018). Dabei werden systemische IT-Sicherheitsprobleme nicht auf der systemischen Ebene gelöst, sondern es wird ein „sicherheitsbewusstes" Verhalten von Nutzer:innen gefordert. Und wenn es zu Sicherheitsvorfällen kommt, dann wird den Nutzer:innen ihr Versagen und ihre individuelle Schuld vorgeworfen. Die Aufgaben, die Individuen in diesem Zusammenhang zugewiesen werden, sind jedenfalls nicht in der Lage, die systemischen Probleme zu lösen, denn diese liegen oft in der Systemgestaltung selbst, auf die die Nutzer:innen gar keinen Einfluss haben.

Bei der Responsibilisierung handelt es sich demnach um eine Verschiebung von Verantwortung von Institutionen auf Individuen. Das geschieht einerseits durch einen „Appell an die Freiheit", der an die positiven Erwartungen und subjektiven Hoffnungen und Wünsche der Einzelnen, aber auch die neoliberale Tradition der Vergötterung privater Entscheidungen auf Kosten des Gemeinwohls anknüpft. Andererseits gibt es aber auch eine „Responsibilisierung durch Bedrohung der persönlichen Kontrolle", die an den negativen Erwartungen, dem Gefühl der Unsicherheit, der Angst und der Bedrohung durch den Verlust der Kontrolle über die Ereignisse ansetzt (Pyysiäinen, Halpin und Guilfoyle 2017, 217). An dieser Stelle lässt sich eine enge, sich möglicherweise sogar gegenseitig verstärkende Verbindung zum verbreiteten individualistischen Datenkontrollparadigma beobachten, die bisher in der Forschung noch keine Aufmerksamkeit gefunden hat.

Prozesse der Responsibilisierung gehen in der öffentlichen Diskussion mit einem ausgesprochen positiven Framing einher. Nicht nur wird das Verhältnis zwischen Individuen und Organisationen als „equal partnership" verkauft (Gray 2009, 326), der Regulierungsansatz selbst wird als Abkehr von der legalistischen, bürokratischen, zentralisierten Top-down-Konfiguration von Autorität und als dezidiert anti-paternalistisch verstanden (Shamir 2008, 3 f.) und soll zu einem „Empowerment" der Individuen führen (vgl. den Gebrauch dieses Terms im Whitepaper der Open Knowledge Finland's MyData working group, Poikola, Kuikkaniemi und Honko 2015). In der Praxis sind die Ergebnisse der Responsibilisierung allerdings überwiegend negativ: Es findet erstens eine Individualisierung der „Lösung" systemischer Probleme statt, fehlende Kenntnisse, Macht und Mittel aufseiten der responsibilisierten Individuen führen zweitens zu ihrem wahrscheinlichen oder sogar sicheren Scheitern, das ihnen dann drittens individuelle Schuldvorwürfe einträgt („victim blaming") und viertens zu weiterer gesellschaftlicher Entsolidarisierung führt.

2. RESPONSIBILISIERUNG – EIN (KONSTRUIERTES) BEISPIEL

Am konstruierten Beispiel eines responsibilisierten Lebensmittelrechts, das dem geltenden Lebensmittelrecht gegenübergestellt wird, soll das Problem der Responsibilisierung verdeutlicht werden.

Nach geltendem Lebensmittelrecht dürfen Erzeugnisse in Deutschland nur dann als Lebensmittel in den Verkehr gebracht werden, wenn sie den rechtlichen Vorschriften entsprechen. Maßgebliche Rechtsvorschrift ist die Europäische Verordnung (EG) Nr.

178/2002 des Europäischen Parlaments und des Rates vom 28. Januar 2002 zur Festlegung der allgemeinen Grundsätze und Anforderungen des Lebensmittelrechts, zur Errichtung der Europäischen Behörde für Lebensmittelsicherheit und zur Festlegung von Verfahren zur Lebensmittelsicherheit. Zu den dort festgelegten allgemeinen Grundsätzen und Anforderungen gehört insbesondere die eigene Verantwortlichkeit der Lebensmittelunternehmer. Dieser ist sowohl verantwortlich für die korrekte Kennzeichnung als auch für die Unbedenklichkeit des Lebensmittels. Das Recht basiert in seiner Umsetzung auf vier aufeinander aufbauenden Mechanismen: Erstens sind bestimmte Inhaltsstoffe generell verboten, zweitens gibt es eine Zulassungspflicht für Zusatzstoffe und neuartige Lebensmittel, drittens treffen den Hersteller Umsetzungs- und Nachweispflichten und viertens gibt es Aufsichts- und Kontrollbehörden zur Kontrolle und Durchsetzung der rechtlichen Anforderungen.

In einem responsibilisierten Lebensmittelrecht würden die Strukturen anders aussehen und die Verantwortlichen anders verteilt sein: Verantwortlich für die korrekte Kennzeichnung dessen, was als Lebensmittel in den Verkehr gebracht wird, wären zwar immer noch die Lebensmittelunternehmer. Verantwortlich für die Unbedenklichkeit wären jetzt aber die Verbraucher:innen, denn sie sind die „moralischen Agenten“ (Giesler und Veresiu 2014, 841) als Träger:innen „selbstbestimmter Ernährung“ oder gar einer „Ernährungssouveränität“. Der Umsetzungsmechanismus würde dann wie folgt aussehen: Die Lebensmittelunternehmer träfe die Pflicht zur transparenten Darstellung der Inhaltsstoffe, wobei grundsätzlich alle Inhaltsstoffe zulässig sind, solange sie nur angegeben werden. Von Verbraucher:innen würde dann „Food Literacy“ erwartet, um anhand der angegebenen Inhaltsstoffe informiert über die Unbedenklichkeit der Lebensmittel entscheiden zu können. Da die meisten Verbraucher:innen eine solche „Food Literacy“ nicht mitbringen, würde sich der Diskurs auf Mechanismen zu ihrer Befähigung fokussieren und auf Akteure, die ihnen bei der Erlangung der als notwendig erachteten „Food Literacy“ zur Seite stehen. Die Pflicht zur eigenen Befähigung würde dabei einen Markt hervorbringen, auf dem „vertrauenswürdige Dritte“ Produkte und Dienstleistungen für „ethisches Selbstmanagement“ zur Verfügung stellen (Giesler und Veresiu 2014, 841).

Was hier als konstruiertes Beispiel für ein responsibilisiertes Lebensmittelrecht vielleicht als überzogen oder verzerrt erachtet wird, entspricht weitgehend dem, wie im Bereich der individualistischen Privacy- und Datenschutzvorstellungen sowohl argumentiert als auch operiert wird: Von den Verarbeitern wird in erster Linie Transparenz über die Verarbeitung verlangt. Den Rest müssen hingegen die Betroffenen mitbringen, und dazu gehört vor allem „Data Literacy“. Wenn sie diese Fähigkeit zur „digitalen Mündigkeit“ nicht besitzen, dann wird von ihnen verlangt, sie sich anzueignen – andernfalls sind sie eben „digital unmündig“ und müssen sich nicht wundern, wenn ihre Interessen und Rechte mit Füßen getreten werden, denn sie haben ja selbst nicht genug für deren Schutz getan. Zur Hilfe sollen ihnen aber zum einen „vertrauenswürdige Dritte“ eilen, eben solche Akteure wie die Datentreuhänder, für die dann noch positiv hervorgehoben wird, dass sie aus der Untauglichkeit des zweiten Mechanismus – der individuellen „Literacy“ – ein Geschäftsmodell machen können und sogar oft sollen. Zugleich werden damit zivilgesellschaftliche Akteure „abgeholt“ – auch sie werden im Grunde responsibilisiert – und damit pazifiert. Zum anderen bietet der Markt Produkte für den „Selbstdatenschutz“, die „digital self-defense“ oder die „digitale Selbstverteidigung“, die im Grunde mit dem gleichen Versprechen aufwarten wie der Zweite Zusatzartikel zur US-Verfassung: Wenn der Staat – bei der Datenverarbeitung natürlich auch Private – übergriffig wird, bewaffne und verteidige dich selbst.

V. DATENTREUHÄNDER – GESCHICHTE, FUNKTIONEN, KRITIK

Die Vorarbeiten ermöglichen nun eine sinnvolle Auseinandersetzung mit dem Konzept der Datentreuhänder. Die Funktion, die Datentreuhänder erfüllen sollen, hat sich, wie ein kurzer Blick in die Geschichte der Debatte zeigen wird, seit dem Aufkommen der Idee in den 1970er-Jahren stark gewandelt, (fast) nur der Name ist geblieben. Heute sollen Datentreuhänder in erster Linie der Unterstützung des individualistischen Datenkontrollparadigmas dienen, indem sie einige seiner offenkundigen fundamentalen Schwächen kompensieren. Die Sicherstellung des Schutzes der Grundrechte und Grundfreiheiten der Betroffenen ist hingegen nicht intendiert und kann von ihnen, wie in Erweiterung der bestehenden, aber noch sehr leisen Kritik an Datentreuhändern gezeigt wird, auch nicht geleistet werden.

1. DATENTREUHÄNDER – DIE GESCHICHTE UND KONSTRUKTION EINER „LÖSUNG“

Die ersten Vorschläge für Datentreuhänder wurden in den 1970er-Jahren unterbreitet. Während die US-amerikanische Debatte zwischen einer Orientierung an institutionellen Arrangements einerseits – etwa dem Vorschlag eines „link system“ von Astin und Boruch (1970) oder die „brokerage agencies“ und die „code linkage brokers“ von Boruch (1972) – und eher informatisch-technischen Aspekten andererseits – so die „insulated data banks“ von Boruch (1972) – oszilliert, ist die deutsche Debatte vor allem konzeptionell orientiert und besitzt einen starken juristischen Einschlag. Dazu gehört etwa der Vorschlag eines „Treuhand-Datenzentrums“ (Dammann 1975, 224), das zwischen den „Datenbesitzer“ – das ist, im Gegensatz zum heutigen Sprachgebrauch, die Stelle, bei der die Daten vorhanden sind – und die an der Auswertung interessierten Forscher:innen geschaltet wird und die technische Ausführung der wissenschaftlichen Datenverarbeitung übernimmt und dabei garantiert, „die damit verbundenen Risiken durch geeignete Vorkehrungen [zu] reduzieren und [zu] kontrollieren“ (Dammann 1975, 224). Zu den institutionellen Arrangements gehört auch die Einrichtung von „institutional review boards“ (Müller und Mochmann 1979, 724), die heute verbreitet als „use & access committees“ bezeichnet werden.

Im Verständnis der damaligen Debatte, vor allem der in Deutschland, sollten Datentreuhänder drei zentrale Funktionen erfüllen: erstens eine Abschottungsfunktion, zweitens eine Unterstützungsfunktion und drittens eine Ermöglichungsfunktion (umfassend Müller 1980). Dass organisatorische und funktionale Ausdifferenzierungen und gegenseitige Abschottungen Mittel zur Kontrolle und Beschränkung von Macht sind, war schon aus der Erfahrung mit Rechtsstaat und Gewaltenteilung bekannt und auf den Datenschutz übertragen worden (vgl. Steinmüller 1971). Seit dem Volkszählungsurteil wird diese Abschottung, für die Datentreuhänder eine Form der Institutionalisierung darstellen, als „informationelle Gewaltenteilung“[2] bezeichnet. Unterstützung sollten Datentreuhänder vor allem den Verarbeitern leisten, namentlich bei der Erfüllung ihrer gesetzlichen Pflichten, nicht wie in der heutigen Debatte den Betroffenen, indem sie „datenorientierte Schutzmaßnahmen“ (Müller 1980: 225) wie Anonymisierung anbieten und durchführen, die die Fähigkeiten des Verarbeiters übersteigen. Und ermöglichen sollten sie wissenschaftliche Forschung, darunter vor allem Sekundäranalysen sogenannter

2 BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983 – 1 BvR 209/83 –, Rn. 1–215, 206.

prozessproduzierter Daten, also etwa Daten, die beim Verwaltungshandeln anfallen (Bick und Müller 1977), oder die Verknüpfung von Daten aus verschiedenen Quellen oder zu verschiedenen Zeitpunkten für Langzeitstudien, wenn zwar die Form der Datenverarbeitung datenschutzriskant ist, aber sichergestellt werden kann, dass die Art der Verwendung keine Risiken für die Betroffenen darstellt (Müller 1980, 226).

Die Debatte um Datentreuhänder verebbte weitgehend, bis das Konzept Ende der 1990er-Jahre das erste Mal wiederentdeckt wurde (Bizer 1999), wenn es auch im Laufe der Zeit einzelne Projekte gab, in denen Datentreuhänderstrukturen praktisch umgesetzt wurden, etwa das von 1995 bis 2006 laufende Projekt „QuaSi-Niere: Qualitätssicherung in der Nierenersatztherapie“ (Metschke und Wellbrock 2002, 37 f.). Die zweite Wiederentdeckung, die sich für viele beteiligte Akteur:innen, ihren Schriften nach zu urteilen, eher als Neuentdeckung darstellt, lässt sich ungefähr Anfang bis Mitte der 2010er-Jahre verorten und hat zu einer inzwischen sehr breiten Debatte geführt. Die Debatte ist vor allem dadurch geprägt, dass Datentreuhänder sehr viel mehr Funktionen erfüllen sollen, als ihnen in der Vergangenheit zugeschrieben wurden, einschließlich gesamtgesellschaftlicher oder gesamtwirtschaftlicher Funktionen wie der „Stärkung europäischer Plattformen“ (Schwartmann und Weiß 2020, 19), und dass sie im Grunde als allgemeine Lösung verkauft werden, auch von Akteur:innen mit eigentlich konfligierenden Interessen. Der ausschlaggebende Grund für das Nichtaufbrechen der Interessenkonflikte liegt in der starken Fixierung auf den Akt des „Datenteilens“, der mit den Datentreuhändern „vereinfacht“ werden soll, unter Absehung der verfolgten Ziele, die es erlaubt, dass alle Beteiligten dann ihre je eigenen Zielvorstellungen darauf projizieren können. Diese Fixierung auf einzelne Mechanismen ohne Berücksichtigung des übergeordneten Ziels, etwa des der DSGVO, nämlich dem Schutz der Grundrechte, ist nicht nur charakteristisch für die vorliegenden Konzeptionen von Datentreuhändern, sondern auch für sogenannte „Personal-Information-Management-Systeme“ (PIMS) oder „Einwilligungsagenten“.

Zentrale Versprechen sind das „Empowerment“ von Betroffenen und deren „faire“ Beteiligung – gerne auch „Teilhabe“ genannt – an der ökonomischen Verwertung (vgl. die Übersicht über die in der gegenwärtigen Diskussion verbreiteten Zielvorstellungen bei Blankertz und Specht 2021, 9). Gemeinsam ist aber allen Befürworter:innen von Datentreuhändern auch das Hervorheben der Vorteile für Datenverarbeiter, die sogenannte „Datenwirtschaft“ und datengetriebene Geschäftsmodelle (so ganz offen die Bundesregierung in ihrer Datenstrategie 2021: 34–39, aber auch Lind und Suckfüll 2013 sowie Schwartmann und Weiß 2020, 19). Das wichtigste Ziel, das mit Datentreuhändern verfolgt werden soll, ist jedoch eindeutig das des „erleichterten Datenteilens“ – auch wenn nicht alle Akteur:innen es so apodiktisch formulieren wie die Bundesregierung, die als zentrales Kriterium für die Etablierung von Datentreuhändern formuliert, dass der „Datenaustausch nicht erschwert werden darf“ (Bundesregierung 2021, 34). Umstritten ist unter den Befürworter:innen allerdings, ob Datentreuhänder selbst ökonomische Interessen verfolgen können und sollen. Verbreitet wird dabei unterschieden zwischen ökonomischen Interessen an einer wirtschaftlichen Verwertung der Daten durch den Datentreuhänder, die eher abgelehnt wird (so etwa Lind und Suckfüll 2013, 16), und der Erbringung des Treuhanddienstes gegen Geld. Nur wenige fordern, auf eine Beschränkung ganz zu verzichten: „Wird Neutralität verstanden als ein Ausschluss eines Gewinnmotivs und einer vertikalen Integration, bleibt kein Spielraum für Ansätze, die stärker zur Datenauswertung beitragen und/oder sich aus den Daten bestehender Geschäftsbereiche erschließen lassen“ (Blankertz und Specht 2021, 21).

2. DATENTREUHÄNDER – KRITIK AN DER „EINWILLIGUNGSGENERIERUNGSMASCHINERIE“

Datentreuhänder werden in der Diskussion durchaus breit kritisiert. In den allermeisten Fällen beschränkt sich die Kritik allerdings auf bestimmte Teilaspekte, etwa die Gefahren einer fehlenden Neutralität oder die Rechtsunsicherheiten bei der Übertragung von Betroffenenrechten (die Übertragung aller Rechte sei möglich, so Kühling (2021, 784 f.); sie sei es nicht, hingegen Freiherr von Ulmenstein (2020, 532 f.)). Der größte Teil der Kritik verbleibt dabei im Framing des zu lösenden Problems als Datenkontrollproblem. In der Literatur gibt es nur zwei grundlegende Ausnahmen von der im Immanenten bleibenden Kritik an den Datentreuhändern. Auf der einen Seite ist das der Verbraucherzentrale Bundesverband (vzbv), auf der anderen Seite Malte Engeler, Richter am Schleswig-Holsteinischen Verwaltungsgericht.

Der vzbv gehört zu den wenigen Akteur:innen, die explizit problematisieren, dass die in der Diskussion befindlichen Datentreuhändermodelle nichts anderes als „Einwilligungsgenerierungsdienste“ (so Florian Glatzner vom vzbv auf dem „Datentag“ der Stiftung Datenschutz am 3. November 2021 in Berlin) sind und dass ihnen diese Funktion mit voller Absicht zugeschrieben wird. Die Anforderungen an Datentreuhänder, die der vzbv formuliert (vzbv 2020, 7 f.), sind sehr weitgehend, schließen explizit den Schutz der Grundrechte und Grundfreiheiten der Betroffenen mit ein und werden von keinem der derzeit diskutierten Treuhandmodelle auch nur ansatzweise erfüllt.

Malte Engeler sieht Datentreuhänder als Ausdruck und Verfestigung der Überbewertung der Einwilligung, die in der Praxis (fast) keine Schutzwirkung auf die Grundrechte hat (Engeler 2021: 4–6). In seinem Vortrag auf dem schon genannten „Datentag“ verglich er diesen Ansatz mit der Situation im Arbeitsrecht: Das bestehende Arbeitsrecht verbiete es einfach grundsätzlich, dass sich Arbeitnehmer:innen vertraglich binden können, sich mehr als acht Stunden pro Tag oder 48 Stunden pro Woche (bzw. wenn innerhalb von sechs Kalendermonaten oder innerhalb von 24 Wochen im Durchschnitt acht Stunden werktäglich nicht überschritten werden, mit Überstunden zehn Stunden pro Tag bzw. 60 Stunden pro Woche) ausbeuten zu lassen. Daher müsse also nicht die Frage nach einer Vereinfachung der individuellen Datenkontrolle gestellt werden, sondern die, „in welchem Umfang überhaupt derartige Verfahren zulässig sein sollen“ (Engeler 2021, 5). Die Fixierung auf die Einwilligung entziehe sich dem und – wie schon im Zusammenhang mit der Darstellung der Responsibilisierung als neoliberaler Regierungsstrategie aufgezeigt – wälzt ihre Beantwortung „auf eine als Selbstbestimmung getarnte Überforderung der Nutzenden ab“ (Engeler 2021, 6).

Daneben gibt es ein konzeptionelles Problem mit dem Anknüpfungspunkt, das alle derzeit diskutierten Datentreuhändermodelle teilen, das aber bisher nicht Gegenstand der Debatte ist: Die meisten Modelle gehen implizit davon aus, dass es einen expliziten Akt der Datenpreisgabe gibt, und es ist dann dieser explizite Akt, an den die Mechanismen, die aufseiten der Datentreuhänder vorgesehen sind, anknüpfen. Diesen Akt muss es allerdings gar nicht geben – es können im Gegenteil nämlich auch die Datenverarbeiter sein, die personenbezogene Daten überhaupt erst erzeugen. Das kann etwa durch nachträgliche Beobachtung des Verhaltens von Betroffenen geschehen, wie dies unter anderem beim Auswerten von Zugriffsdaten auf Servern oder Metadaten von Dokumenten möglich ist. Und noch weniger Beteiligte scheinen sich Gedanken darüber zu machen, wie Vorhersagen oder Einschätzungen in einem solchen Treuhandmodell abgebildet werden können oder müssen.

3. DATENTREUHÄNDER – KEINE LÖSUNG FÜR DEN GRUNDRECHTSSCHUTZ

Vor dem Hintergrund einer seit mehr als fünf Jahrzehnten währenden Datenschutzdiskussion und dem in der derzeitigen Debatte hegemonialen individualistischen Datenkontrollparadigma lassen sich (mindestens) fünf grundsätzliche Schwächen von Datentreuhändern, wie sie heute in der Debatte verstanden werden, identifizieren:

1) Verstärkung der Individualisierung und Subjektivierung eines immanent gesellschaftlichen Problems

Wenn Datenschutz nicht als individuelle Befindlichkeit, als private Neigung oder Präferenz, als Schutz einer als privat verstandenen Sphäre und schon gar nicht als auf die Betroffenen abgewälzte Schutzverantwortung verstanden werden soll, sondern als Mittel zur Feststellung und Durchsetzung der Bedingungen, unter denen moderne Informationsverarbeitung gesellschaftlich, also für alle Teile der Gesellschaft, akzeptabel sein kann (Podlech 1976, 24), dann muss sich das in der Wahl der Mittel und ihrer konkreten Ausgestaltung widerspiegeln – und bei den in der Debatte verbreiteten Datentreuhändermodellen ist das Gegenteil der Fall: Sie sollen explizit dem individualistischen Datenkontrollparadigma dienen, sie knüpfen dazu (fast ausschließlich) am Rechtsinstitut der individuellen Einwilligung an, sie operieren im Wesentlichen in Verlängerung der Betroffenenrechte, fungieren zugleich aber auch als Mittel zu deren Kommodifizierung, kurz: Sie zielen nicht auf eine gesellschaftliche Lösung eines gesellschaftlichen Problems, sondern auf eine individuelle Lösung für ein als individuell verstandenes Problem. Sie reproduzieren das Problem damit als individuelles, selbst im Scheitern – dann haben sich die Betroffenen eben schlicht den falschen Datentreuhänder ausgesucht, um ihre Interessen und Präferenzen zu vertreten. Wirksamer Grundrechtsschutz steht jedenfalls nicht auf der Agenda, die die Befürworter:innen für die Datentreuhänder schreiben.

2) Unbestimmtheit und Unbestimmbarkeit der Position zwischen Abstraktheit und Konkretheit

Die DSGVO ist sehr allgemein gehalten – oder juristisch: voller unbestimmter Rechtsbegriffe – und kann und muss erst in der Anwendung konkretisiert werden, denn die konkreten Grundrechtsgefährdungen ergeben sich aus den konkreten Verarbeitungstätigkeiten, aus den konkreten sozialen Beziehungen zwischen Verarbeitern und Betroffenen und aus den konkreten Interessen der Verarbeiter und den Zwecken, die sie verfolgen. Und nur auf der Basis dieser Konkretisierung, die von den Verantwortlichen selbst zu leisten ist (Art. 24 Abs. 1 DSGVO), können geeignete Maßnahmen gestaltet, ausgewählt und eingesetzt werden, die den konkreten Risiken wirksam begegnen. Für die Etablierung von Datentreuhändern gibt es jetzt zwei Möglichkeiten.

Erstens können sie auf der gleichen allgemeinen Ebene wie das Gesetz selbst operieren. Dann können sie Treuhänder für alle Arten von sozialen Beziehungen und alle Zwecke und Formen von Datenverarbeitung sein – sie können also die gleiche Anwendungsbreite wie das Gesetz abdecken. In der Folge können sie dann auch in großem Umfang operieren – und vor allem könnten sie den Datenverarbeitern als mächtige Akteure gegenübertreten. Dann sind sie allerdings mit dem gleichen Problem der Unkonkretheit konfrontiert, das auch die DSGVO auszeichnet – sie helfen also nicht bei der Konkretisierung und damit bei der Durchsetzung eines wirksamen Grundrechtsschutzes.

Oder sie operieren zweitens auf der konkreten Ebene, schneiden also ihre eigenen Tätigkeiten auf sehr spezifische Verarbeitungskontexte zu – und damit auf spezifische

Grundrechtsrisiken. Dann ist die sehr wahrscheinliche Folge allerdings, dass es eine große Anzahl unterschiedlicher Datentreuhänder geben wird, nämlich für die je unterschiedlichen Verarbeitungskontexte und Grundrechtsrisiken. Im Ergebnis tauschen wir also die derzeitige Situation, in der die Betroffenen vielen Verarbeitern gegenüberstehen, gegen eine Situation, in der sie vielen Datentreuhändern gegenüberstehen – gewonnen ist damit allerdings nichts.

3) Inhärente Verselbstständigungstendenz der Stellvertretungsposition

Jeder Stellvertretung wohnt die Tendenz zur Verselbstständigung inne (grundlegend Michels 1989, 370 f., umfassend Sofsky und Paris 1994, 178 ff.). Aus der Sicht der Befürworter:innen geht es bei der Etablierung von Datentreuhändern gerade darum, mit ihrer Hilfe einen „Datenschatz zu heben“. Das heißt aber, dass die Tendenz zur Verselbstständigung schon über die spezifische Incentivierung der Datentreuhänder eingebaut wird. Und auch wo sie nicht explizit eingebaut wird, kann sie, wie in anderen Fällen im Bereich des Datenschutzes, in der Praxis auftreten. Dies lässt sich etwa ganz gut an den Datenschutzaufsichtsbehörden sehen: Im Vordergrund stehen für sie inzwischen die Verwaltung des Datenschutzrechts, die eigene Selbstverwaltung und das Verfolgen ihrer eigenen (bürokratischen) Interessen, nicht mehr der Grundrechtsschutz der Betroffenen. Den Vorschlägen für Datentreuhänder, wie sie derzeit diskutiert werden, fehlen jedenfalls selbst grundlegende Hinweise auf Strukturen und Verfahren, mit denen eine Verselbstständigung unterbunden werden soll und die dies auch wirksam leisten könnten.

Darüber hinaus gibt es zwei unüberwindliche Asymmetrien, denen sich Datentreuhänder gegenübersehen:

4) Informationsasymmetrie gegenüber den Verarbeitern

5) Kontrollasymmetrie gegenüber den Verarbeitern

In ihrer derzeit konzipierten Form können Datentreuhänder grundsätzlich nur von den Betroffenen übertragene Rechte wahrnehmen, eigene Rechte haben sie hingegen nicht. Auch sind die Pflichten der Datenverarbeiter gegenüber den Betroffenen, die dann gegenüber den Datentreuhändern wahrgenommen werden könnten, nach der DSGVO beschränkt. Die Informationsrechte und -pflichten beziehen sich ausschließlich auf die Angabe der an der Verarbeitung beteiligten Akteur:innen, der verarbeiteten personenbezogenen Daten, der Zwecke, für die sie verarbeitet werden, und einiger weniger weiterer Aspekte der Verarbeitungstätigkeiten, etwa der Löschfristen. Nicht umfasst von den Informationsrechten und -pflichten sind Angaben dazu, welche Risiken im Zusammenhang mit der Verarbeitung entstehen oder entstehen können, welche Schutzmaßnahmen getroffen wurden, um diesen Risiken wirksam zu begegnen, und welche Restrisiken verbleiben. In der Folge operieren die Datentreuhänder im Zustand der gleichen Informationsasymmetrie gegenüber den Verantwortlichen wie die Betroffenen. Einzig die Datenschutzaufsichtsbehörden haben weitergehende Informationsrechte gegenüber den Verantwortlichen, aber solche oder ähnliche Rechte werden den Datentreuhändern gerade nicht übertragen – und das wäre wiederum auch nicht zielführend, denn die Datentreuhänder sind ja gerade selbst Verarbeiter und eben nicht Aufsichtsbehörde. Noch extremer sieht die Lage hinsichtlich der Kontrollasymmetrie aus – die Betroffenen haben nämlich keine Kontrollrechte gegenüber den Verarbeitern und können daher auch keine an die Treuhänder übertragen.

Im Ergebnis heißt das: Datentreuhänder, wie sie in der Diskussion mehrheitlich konzipiert werden, können vielleicht den Teil des Problems „lösen“, der im Zentrum der Aufmerksamkeit des individualistischen Datenkontrollparadigmas steht: das Matching von Datenverarbeitungswünschen der Verantwortlichen und individuellen Willenserklärungen der Betroffenen. Ganz sicher werden sie auch das Problem lösen, vor dem sich die „Datenwirtschaft“ sieht, nämlich Zugriff auf immer mehr (personenbezogene) Daten zu bekommen, um diese verwerten zu können. Was diese Datentreuhänder aber nicht lösen können, ist das Problem des Schutzes der Grundrechte der Betroffenen bei der Datenverarbeitung.

VI. ABSCHLUSS UND HANDLUNGSEMPFEHLUNGEN

Vor dem Hintergrund der Gegenüberstellung zweier gegensätzlicher Privatheits- beziehungsweise Datenschutzverständnisse – das als „Rechtsstaatsmodell“ bezeichnete Verständnis, das auch der Regelungsarchitektur der DSGVO zugrunde liegt, und das individualistische Datenkontrollparadigma, das den derzeitigen öffentlichen wie den Fachdiskurs bestimmt –, des neoliberalen Regierungsmodells der Responsibilisierung und der historischen und aktuellen Debatte um Datentreuhänder, ihre Funktionen und Eigenschaften, formuliert der Beitrag eine grundsätzliche Kritik an Datentreuhändern. Diese dienen nicht nur zur Fortschreibung einer neoliberalen Individualisierungs- und Responsibilisierungsstrategie im Datenschutzbereich, sondern sie sind auch strukturell nicht in der Lage, den Schutz der Grundrechte bei der Informationsverarbeitung sicherzustellen.

Daneben hat der Beitrag versucht, für einen schärfer analytischen Zugang zu der Debatte um den Datenschutz und das Datenschutzrecht, aber auch zu den einzelnen Lösungsvorschlägen, die in diesem Bereich vorgebracht werden, zu sensibilisieren. Weil alle Lösungsvorschläge im Privacy- und Datenschutzbereich immer auf bestimmte Problemverständnisse zielen und, wenn überhaupt, immer nur die so verstandenen Probleme adressieren, können die vorgeschlagenen Lösungen also gar nicht ohne eine Auseinandersetzung mit den jeweils zugrunde gelegten Problemverständnissen analysiert und bewertet werden.

Daraus lassen sich nun konkrete Handlungsempfehlungen an Akteur:innen ableiten, die sich dem Ziel einer guten Verbraucherpolitik verschrieben haben. Diese Akteur:innen sollen damit in die Lage versetzt werden, die (aus Sicht eines auf Grundrechtsschutz zielenden Datenschutzes) richtigen Fragen stellen zu können, wenn sie mit Lösungsvorschlägen im Datenschutzbereich – aber durchaus auch darüber hinaus – konfrontiert werden, gleich ob es sich dabei um Regulierungs- oder Umsetzungsvorschläge handelt.

1) Verbraucherpolitische Akteur:innen dürfen nicht nur auf die Lösung schauen, die ihnen verkauft wird, und sich vor allem nicht von schönen Bezeichnern wie „Datenhoheit“, „Datensouveränität“, „Selbstbestimmung“, „Empowerment“, „Mündigkeit“ oder „Vertrauen“ blenden lassen. Stattdessen müssen sie hinterfragen, wie das Problem genau verstanden und geframed wird, für das eine vorgeschlagene Lösung eine Lösung sein soll. Dazu gehört auch die Frage, ob die Problembeschreibung selbst überhaupt gesellschaftlich akzeptabel ist oder ob die Problembeschreibung schon eine Lösung in-

duziert, bei der gerade nicht die Vorteile, aber sehr wohl die Nachteile bei den Verbraucher:innen liegen. Und dann kann und sollte die Frage gestellt werden, ob die vorgeschlagene Lösung für das beschriebene Problem überhaupt wirksam ist.

2) Verbraucherpolitische Akteur:innen müssen insbesondere die Frage stellen, ob und inwieweit die vorgeschlagene Lösung dazu beiträgt, Grundrechte zu schützen – und es sich nicht nur um eine Simulation von Grundrechtsschutz handelt, die sich mit dem Verweis auf individuelle Wertvorstellungen oder Präferenzen von auf dem Markt agierenden Verbraucher:innen schmückt.

3) Verbraucherpolitische Akteur:innen müssen auch die Frage nach der Verantwortungsverteilung stellen, insbesondere die nach der Umverteilung von Verantwortung, die mit der Umsetzung des Lösungsvorschlags einhergehen würde. Zu fragen ist also insbesondere, ob den Verbraucher:innen Verantwortlichkeiten aufgebürdet werden, die erstens nach dem Gesetz eigentlich den Verarbeiter oder einen anderen Akteur verpflichten und zweitens von den Verbraucher:innen gar nicht erfüllt werden können, bei deren Scheitern sie dann allerdings mit Vorwürfen überzogen werden.

Auch effektive Verbraucherpolitik ist unter den Bedingungen der inzwischen nahezu vollständigen Durchdringung der Gesellschaft mit informationstechnischen Systemen nur noch möglich, wenn eine verbraucherpolitische Zielstellung „von vornherein in die Konstruktion der Informationssysteme eingeplant, auch mit den Mitteln der modernen Daten- und Kommunikationstechnologien technisch und organisatorisch abgesichert und schließlich in ihrem sozialen Umfeld rechtlich verankert und gewährleistet wird“ (Steinmüller, Ermer und Schimmel 1978, 2).

VII. LITERATURVERZEICHNIS

Astin, Alexander W. und Robert F. Boruch. 1970. A „link“ system for assuring confidentiality of research data in longitudinal studies. *American Educational Research Journal* 7, Nr. 4: 615–624.

Austin, Lisa M. 2014. Enough about me: Why privacy is about power, not consent (or harm). In: *A world without privacy: What law can and should do?*, hg. von Austin Sarat, 131–189. Cambridge: Cambridge University Press.

Bick, Wolfgang und Paul J. Müller. 1977. Die Buchführung der Verwaltungen als sozialwissenschaftliche Datenbasis. In: *Die Analyse prozeß-produzierter Daten*, hg. von Paul J. Müller, 42–88. Stuttgart: Klett-Cotta.

Bizer, Johann. 1999. Der Datentreuhänder – Lösungsmodell für den Datenzugang der Forschung. *Datenschutz und Datensicherheit* 23, Nr. 7: 392–395.

Blankertz, Aline und Louisa Specht. 2021. *Wie eine Regulierung für Datentreuhänder aussehen sollte*. Policy-Brief. Juli. Berlin: Stiftung Neue Verantwortung e.V. https://www.stiftung-nv.de/sites/default/files/regulierung_fuer_datentreuhaender.pdf (Zugriff: 11.02.2022).

Bloustein, Edward J. 1978. *Individual & group privacy*. New Brunswick: Transaction Publishers.

Boruch, Robert F. 1972. Strategies for eliciting and merging confidential social research data. *Policy Sciences* 3, Nr. 3: 275–297. https://doi.org/10.1007/BF01413684.

Bundesregierung. 2021. Datenstrategie der Bundesregierung. Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum. Kabinettfassung, 27. Januar. https://www.bundesregierung.de/resource/blob/992814/1845634/f073096a398e59573c7526feaadd43c4/datenstrategie-der-bundesregierung-download-bpa-data.pdf (Zugriff: 11.02.2022).

Citron, Danielle Keats. 2008. Technological due process. *Washington University Law Review* 85, Nr. 6: 1249–1313.

Diaz, Claudia, und Seda Gürses. 2012. Understanding the landscape of privacy technologies. *Proceedings of the Information Security Summit* 12: 58–63.

Engeler, Malte. 2021. Stellungnahme im Rahmen der Öffentlichen Anhörung im Ausschuss für Wirtschaft und Energie des Deutschen Bundestages am 21. April 2021 zum Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) (BT-Drucksache 19/27441). https://www.bundestag.de/resource/blob/836166/e95c01bdb37ed9f6c08ef027cd902e47/19-9-1056_Stellungnahme_SV_Dr-_Engeler_oeATTDSG_21-04-2021-data.pdf (Zugriff: 11.02.2022).

Freiherr von Ulmenstein, Ulrich. 2020. Datensouveränität durch repräsentative Rechtswahrnehmung – Begriffliche Prägung und normative Gestaltung sogenannter „Datentreuhänder“. *Datenschutz und Datensicherheit* 44, Nr. 8: 528–534. https://doi.org/10.1007/s11623-020-1319-8.

Gallie, Walter Bryce. 1956. Essentially contested concepts. *Proceedings of the Aristotelian Society* 56: 167–198.

Garstka, Hansjürgen. 1977. Auswirkungen innovativer Informationsstrukturen auf die Bedeutung und Reichweite verfassungsmäßiger Grundrechte. Arbeitspapier für das Werkstattgespräch „Gesellschaftliche Auswirkungen großer Informationssysteme“ der Gesellschaft für Informatik, 29./31.3.77, Hamburg. Arbeitspapier, Freie Universität Berlin.

Giesler, Markus und Ela Veresiu. 2014. Creating the responsible consumer: moralistic governance regimes and consumer subjectivity. *Journal of Consumer Research* 41, Nr. 3: 840–857. https://doi.org/10.1086/677842.

Gray, Garry C. 2009. The responsibilization strategy of health and safety: neo-liberalism and the reconfiguration of individual responsibility for risk. *The British Journal of Criminology* 49, Nr. 3: 326–342. https://doi.org/10.1093/bjc/azp004.

Kühling, Jürgen. 2021. Der datenschutzrechtliche Rahmen für Datentreuhänder – Was ist zu tun? *Datenschutz und Datensicherheit* 45, Nr. 12: 783–788. https://doi.org/10.1007/s11623-021-1537-8.

Lind, Hans-Günter und Hanns Suckfüll. 2013. Initiative zu einer Deutschen Daten-Treuhand (DEDATE) als Ultima Ratio der Persönlichen Digitalen Datenwirtschaft (PDD): Ansätze und Strukturen für eine gezielte Verwertung persönlicher digitaler Daten unter Berücksichtigung aller Interessengruppen – Dateneigentümer, Wirtschaft und Staat. Leipzig: Fraunhofer MOEZ. https://www.imw.fraunhofer.de/content/dam/moez/de/documents/Executive-Paper/DEDATE-gesamt.pdf (Zugriff 11.02.2022).

Metschke, Rainer und Rita Wellbrock. 2002. *Datenschutz in Wissenschaft und Forschung*. 3., überarbeitete Auflage. Schriftenreihe „Materialien zum Datenschutz“ 28, hg. von Berliner Beauftragter für Datenschutz und Informationsfreiheit und Hessischer Datenschutzbeauftragter. Berlin: Berliner Beauftragter für Datenschutz und Informationsfreiheit. https://www.forschungsdaten-bildung.de/files/metschkewellbrock2002.pdf (Zugriff 11.02.2022).

Michels, Robert. 1989. *Zur Soziologie des Parteiwesens in der modernen Demokratie. Untersuchungen über die oligarchischen Tendenzen des Gruppenlebens*. 4. Auflage. Stuttgart: Alfred Kröner Verlag.

Morozov, Evgeny. 2013. *To save everything, click here: The folly of technological solutionism*. New York: Public Affairs.

Müller, Paul J. 1980. Datentreuhänder – Ein Plädoyer für eine volle Ausschöpfung von Datenschutz-Maßnahmen. In: *Datenzugang und Datenschutz – Konsequenzen für die Forschung*, hg. von Max Kaase, Hans-Jürgen Krupp, Manfred Pflanz, Erwin K. Scheuch und Spiros Simitis, 225–229. Königstein: Athenäum Verlag.

Müller, Paul J. und Ekkehard Mochmann. 1979. Datenschutz und Sozialforschung – Bericht über eine internationale Konferenz. In: *Soziologische Analysen: Referate aus den Veranstaltungen der Sektionen der Deutschen Gesellschaft für Soziologie und der ad-hoc-Gruppen beim 19. Deutschen Soziologentag (Berlin, 17.-20. April 1979)*, hg. von Rainer Mackensen und Felizitas Sagebiel, 723–728. Berlin: Universitätsbibliothek der Technischen Universität Berlin.

Mulligan, Deirdre K., Colin Koopman und Nick Doty. 2016. Privacy is an essentially contested concept: A multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences 374(2083)*. https://doi.org/10.1098/rsta.2016.0118.

Podlech, Adalbert. 1976. Aufgaben und Problematik des Datenschutzes. *Datenverarbeitung im Recht* 5: 23–39.

Pohle, Jörg. 2018. Datenschutz und Technikgestaltung: Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung. Dissertation, Mathematisch-Naturwissenschaftliche Fakultät, Humboldt-Universität zu Berlin. https://doi.org/10.18452/19136.

Pohle, Jörg. 2019. Zu den gesellschaftlichen Auswirkungen zunehmender Verdatung und Automation – Erkenntnisse aus der Frühzeit und Hochphase der Datenschutzdebatte. In: *Komplexe Dynamiken globaler und lokaler Entwicklungen. Verhandlungen des 39. Kongresses der Deutschen Gesellschaft für Soziologie in Göttingen 2018*, hg. von Nicole Burzan. https://publikationen.soziologie.de/index.php/kongressband_2018/article/view/1157 (Zugriff: 11.02.2022).

Poikola, Antti, Kai Kuikkaniemi und Harri Honko. 2015. *MyData – A Nordic model for human-centered personal data management and processing*. Whitepaper. Helsinki: Open Knowledge Finland. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78439/MyData-nordic-model.pdf (Zugriff: 15.02.2022).

Pyysiäinen, Jarkko, Darren Halpin und Andrew Guilfoyle. 2017. Neoliberal governance and ‘responsibilization’ of agents: reassessing the mechanisms of responsibility-shift in neoliberal discursive environments. *Distinktion: Journal of Social Theory* 18, Nr. 2: 215–235, https://doi.org/10.1080/1600910X.2017.1331858.

Renaud, Karen, Stephen Flowerday, Merrill Warkentin, Paul Cockshott und Craig Orgeron. 2018. Is the responsibilization of the cyber security risk reasonable and judicious? *Computers & Security* 78: 198–211. https://doi.org/10.1016/j.cose.2018.06.006.

Renaud, Karen, Stephen Flowerday und Karl van der Schyff. 2021. Uncertainty in cyber de-responsibilisation. *Computer Fraud & Security* 2021, Nr. 8: 13–19. https://doi.org/10.1016/S1361-3723(21)00086-5.

Schneier, Bruce. 2000. Threat modeling and risk assessment. In: *E-Privacy: Datenschutz im Internet*, hg. von Helmut Bäumler, 214–229. Braunschweig: Vieweg Verlag.

Schwartmann, Rolf und Steffen Weiß, Hrsg. 2020. Datenmanagement- und Datentreuhandsysteme: Ein Arbeitspapier der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2020.

Shamir, Ronen. 2008. The age of responsibilization: on market-embedded morality. *Economy and Society* 37, Nr. 1: 1–19. https://doi.org/10.1080/03085140701760833.

Sofsky, Wolfgang und Rainer Paris. 1994. *Figurationen sozialer Macht: Autorität – Stellvertretung – Koalition*. Frankfurt am Main: Suhrkamp.

Solove, Daniel J. 2002. Conceptualizing privacy. *California Law Review* 90, Nr. 4: 1087–1155.

Soneryd, Linda und Ylva Uggla. 2015. Green governmentality and responsibilization: New forms of governance and responses to ‘consumer responsibility’. *Environmental Politics* 24, Nr. 6: 913–931. https://doi.org/10.1080/09644016.2015.1055885.

Steinmüller, Wilhelm. 1971. Allgemeine Grundsätze zur rechtlichen Regelung des Datenschutzes. In: *Datenschutz – Datensicherung*, hg. von Jochen Schneider, 13–17. Beiträge zur integrierten Datenverarbeitung in der öffentlichen Verwaltung 5. München: Siemens Aktiengesellschaft.

Steinmüller, Wilhelm. 1976. Informationsrecht und Informationspolitik. In: *Informationsrecht und Informationspolitik*, hg. von Wilhelm Steinmüller, 1–20. München: Oldenbourg Verlag.

Steinmüller, Wilhelm, Bernd Lutterbeck, Christoph Mallmann, Uwe Harbort, Gerhard Kolb und Jochen Schneider. 1972. Grundfragen des Datenschutzes. Gutachten im Auftrag des Bundesministeriums des Innern, BT-Drs. VI/3826, Anlage 1. https://dserver.bundestag.de/btd/06/038/0603826.pdf (Zugriff: 11.02.2022).

Steinmüller, Wilhelm, Leonhard Ermer und Wolfgang Schimmel. 1978. *Datenschutz bei riskanten Systemen: Eine Konzeption entwickelt am Beispiel eines medizinischen Informationssystems*. Berlin: Springer.

Taylor, Linnet, Luciano Floridi und Bart Van der Sloot, Hrsg. 2017. *Group privacy: New challenges of data technologies*. Cham: Springer.

Verbraucherzentrale Bundesverband e.V. 2020. Neue Datenintermediäre: Anforderungen des vzbv an „Personal Information Management Systems“ (PIMS) und Datentreuhänder. 15. September. Berlin. https://www.vzbv.de/sites/default/files/downloads/2020/09/17/20-09-15_vzbv-positionspapier_datenintermediaere.pdf (Zugriff: 11.02.2022).

Westin, Alan F. 1967. *Privacy and freedom*. New York: Atheneum.