DuD-Fachbeiträge

Michael Friedewald · Jörn Lamla
Alexander Roßnagel *Hrsg.*

RESEARCH

Informationelle Selbstbestimmung im digitalen Wandel

DuD
Datenschutz und Datensicherheit

Springer Vieweg

Michael Friedewald · Jörn Lamla
Alexander Roßnagel
(Hrsg.)

Informationelle Selbstbestimmung im digitalen Wandel

Springer Vieweg

Herausgeber
Dr. Michael Friedewald
Fraunhofer Institut für System- und Innovationsforschung
Karlsruhe, Deutschland

Prof. Dr. Alexander Roßnagel
Universität Kassel
Deutschland

Prof. Dr. Jörn Lamla
Universität Kassel
Deutschland

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

DuD-Fachbeiträge
ISBN 978-3-658-17661-7 ISBN 978-3-658-17662-4 (eBook)
DOI 10.1007/978-3-658-17662-4

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Vieweg
© Springer Fachmedien Wiesbaden GmbH 2017
Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.
Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.
Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Vieweg ist Teil von Springer Nature
Die eingetragene Gesellschaft ist Springer Fachmedien Wiesbaden GmbH
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Inhaltsverzeichnis

Informationelle Selbstbestimmung als vielschichtiges Bündel von Rechtsbindungen und Rechtspositionen

Marion Albers

1. Einleitung

Das Recht auf informationelle Selbstbestimmung gehört in Deutschland zu den zentralen Leitgedanken des Datenschutzes. Im Anschluss an das Volkszählungsurteil des Bundesverfassungsgerichts (BVerfG) ist es in gesellschaftlichen Diskussionen ebenso wie in verschiedenen Wissenschaftsdisziplinen populär geworden. Mittlerweile wird es zudem in einigen transnationalen Debatten erwähnt.[1]

In den Diskussionen ist allerdings oft nicht klar, was »informationelle Selbstbestimmung« genau bedeutet. Meist wird sie mit eher diffusen Vorstellungen verknüpft, dass jeder eine gewisse »Kontrolle« über »seine« Daten haben müsse. Ihre breite Popularität erklärt sich nicht zuletzt damit, dass sie vage und implikationsreich zugleich ist. Dieser Beitrag beschäftigt sich aus rechtlicher Sicht mit ihren Grundlagen und ihrer Konzeption, den Folgen und den Herausforderungen. Die Bedeutung und die Funktionen, die (das Recht auf) informationelle Selbstbestimmung aus dieser Perspektive hat, erschließen sich nur im Blick auf übergreifendere rechtliche Zusammenhänge.

Meine Überlegungen münden in mehrere Ergebnisse. Für die Entwicklung des Schutzes einzelner Personen im Hinblick auf den Umgang mit sie betreffenden Daten und Informationen hat das in seinen Grundzügen im Volkszählungsurteil entwickelte Recht auf informationelle Selbstbestimmung (2.1) entscheidende Fortschritte gebracht. Das gilt unter anderem, weil es sich durch einen unmittelbaren Bezug auf die Daten- und Informationsebene auszeichnet, dabei einen relativ hohen Abstraktionsgrad aufweist und so die »Privatsphäre« als das bis dahin zentrale Schutzgut abgelöst hat (2.2). »Privatsphäre« oder auch »Privatheit« sind mit he-

* Prof. Dr. Marion Albers | Universität Hamburg | marion.albers@uni-hamburg.de

1 Z. B. Schwartz, »The Computer in German and American Constitutional Law«, S. 677ff., 701; siehe ebenfalls Raab und Goold, *Protecting Information Privacy*, S. 17; mit differenzierenden Überlegungen: Rouvroy und Poullet, »The Right to Informational Self-Determination and the Value of Self-Development«, S. 45, 52ff.; zum Überblick über die einschlägigen Grundrechte in europäischen Ländern: Leenes, Koops und De Hert, *Constitutional Rights and New Technologies*.

© Springer Fachmedien Wiesbaden GmbH 2017
M. Friedewald et al. (Hrsg.), *Informationelle Selbstbestimmung im digitalen Wandel*, DuD-Fachbeiträge, DOI 10.1007/978-3-658-17662-4_2

terogenen traditionellen Bedeutungsgehalten belastet und in ihren Implikationen viel zu eng, als dass sie als Leitbeschreibungen des Datenschutzes taugten.[2] So positiv bestimmte Leistungen des Rechts auf informationelle Selbstbestimmung sind, so sehr ist dessen inhaltliche und rechtsdogmatische Ausgestaltung defizitär (2.3). Differenzierungen und Weiterentwicklungen in der verfassungsgerichtlichen Rechtsprechung nach dem Volkszählungsurteil haben eher zu einigen kontraproduktiven Stabilisierungen, zu Unklarheiten und zu Bruchstellen als zu konzeptionellen Änderungen geführt (2.4). Unter anderem arbeitet das BVerfG die »informationelle Selbstbestimmung« bis heute mit Hilfe gewohnter dogmatischer Denkmuster ab. Daten und Informationen sind jedoch eigenständige Kategorien, die sich strukturell von den sonst im Grundrechtsdenken prägenden Kategorien, vor allem »Entscheidung« oder »Handlung«, unterscheiden. Überzeugende grundrechtliche Bindungen und Schutzpositionen setzen deswegen eine gegenstandsgerechte Dogmatik und an vielen Stellen spezifisch zugeschnittene Konstruktionen voraus. Nicht zuletzt vor dem Hintergrund der Europäisierung des Datenschutzes ist es Zeit für neue Konzeptionen (3). Die aus grundrechtlicher Sicht wichtigsten Aspekte werden in drei Abschnitten illustriert. Erstens hat man im Datenschutz nicht allein mit Daten, sondern mit einem komplexen Netzwerk mehrerer Grundelemente zu tun: Daten und Informationen, Wissen und Verarbeitungsprozesse, Entscheidungen und Entscheidungsfolgen (4). Zweitens lässt sich der Datenschutz nicht auf ein einheitliches Schutzgut reduzieren. Aus heutiger Sicht ist es eine geradezu absurde Idee zu meinen, man könne ein so vielfältiges Feld in nur einem grundrechtlichen Schutzgut auffangen. Stattdessen verweist der Datenschutz auf ein komplexes Bündel von Rechtsbindungen und Rechtspositionen, die auf unterschiedlichen Ebenen anzusiedeln sind und das Individuum in der Sozialität schützen (5). Drittens bedarf es vielfältiger Regulierungskonzepte, die das Datenschutzrecht angemessen mit den sachbezogenen Vorschriften im öffentlich- oder im privatrechtlichen Bereich verzahnen, Muster des Risiko- oder des Technikrechts aufgreifen, bereits bei der System- und Technikgestaltung ansetzen, individuelle Kenntnis- und Einflussrechte gewährleisten oder überindividuelle Implementations- und Kontrollmechanismen institutionalisieren (6). Datenschutzrecht ist alles andere als bürokratisch. Es erweist sich als modern, als spannend und als ein vielschichtiges, interdisziplinär ausarbeitungsbedürftiges Feld (7).

[2] Ausführungen zur Privatheit als Konzept und zu den verschiedenen Relationen zwischen Privatheit und Recht: Albers, »Privatheitsschutz als Grundrechtsproblem«, S. 15ff.

2. Konzeption des Rechts auf informationelle Selbstbestimmung

2.1. Das Volkszählungsurteil des Bundesverfassungsgerichts

Das Recht auf informationelle Selbstbestimmung ist im Jahre 1983 vom BVerfG im Volkszählungsurteil aus Art. 2 i. V. m. Art. 1 GG[3] hergeleitet worden.[4] Verfahren und Urteil standen im Fokus öffentlicher Aufmerksamkeit, denn die beabsichtigte Volkszählung hatte, ähnlich wie heute die Vorratsdatenspeicherung, eine gesellschaftsweite Protestbewegung ausgelöst. Ein damals innovatives Grundsatzurteil war das Ergebnis: Jede Person hat, so die vom BVerfG gewählte Beschreibung des Schutzbereichs, das Recht, »grundsätzlich selbst über die Preisgabe und Verwendung ihrer persönlichen Daten zu bestimmen«.[5]

Genese und Ausgestaltung des Rechts auf informationelle Selbstbestimmung lassen sich gut erklären. Das Gericht hat zum einen an seine Rechtsprechung zum Grundrecht auf Achtung der Privatsphäre und zum verfassungsrechtlichen Persönlichkeitsrecht angeknüpft und zugleich auf die Kritik an eben dieser Rechtsprechung reagiert.[6] Darüber hinaus verarbeitet es Vorarbeiten zum Datenschutzrecht, die auf der Basis eines relativ schlichten kybernetischen Modells bereits ein informationelles Selbstbestimmungsrecht entworfen hatten.[7] Zum anderen hebt es Wechselwirkungen zwischen der Selbstbestimmung und der Entscheidungs- und Verhaltensfreiheit einerseits und dem Schutz persönlicher Daten andererseits hervor.[8] Die Ausdehnung des Grundrechtsschutzes auf den Umgang mit personenbezogenen Daten und Informationen gestaltet es dann ganz in Anlehnung an die Entscheidungs- und Verhaltensfreiheit. Ebenso wie jede Person ihre Handlungen wählen kann, hat sie das Recht, über die Verarbeitung »ihrer« personenbezogenen Daten selbst zu bestimmen.

Kernelement des Rechts auf informationelle Selbstbestimmung ist danach ein relativ abstraktes und dadurch weit reichendes individuelles Entscheidungsrecht, das sich von der Preisgabe bis zur Verwendung personenbezogener Daten erstreckt.

---

3 Art. 2 Abs. 1 GG lautet: »Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit [...]«. Art. 1 Abs. 1 GG hält fest: »Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.«

4 BVerfGE 65, 1 (42ff.).

5 BVerfGE 65, 1 (43). Zur Analyse der Entscheidung und ihrer Hintergründe: Albers, *Informationelle Selbstbestimmung*, S. 149ff.

6 Dazu sogleich in Abschnitt 2.2 dieses Beitrags

7 Siehe dazu Steinmüller u. a., *Grundfragen des Datenschutzes*, Anl. 1; literarische Quellen des Volkszählungsurteils werden offengelegt bei Heußner (Berichterstatter im entscheidenden Senat), »Das informationelle Selbstbestimmungsrecht in der Rechtsprechung des Bundesverfassungsgerichts«, S. 280f.

8 BVerfGE 65, 1 (42f.).

Im Hintergrund steht das überkommene dogmatische Modell, dass Grundrechte primär dem Schutz von Individuen gegen Eingriffe des Staates dienen, die im Ergebnis nicht unzulässig, aber nur dann verfassungsmäßig sind, wenn sie eine Reihe verfassungsrechtlicher Anforderungen erfüllen. Das hergeleitete Entscheidungsrecht ist insofern, passend zum Sachverhalt des Volkszählungsurteils, als ein individuelles Abwehrrecht gegen staatliche Eingriffe geschützt. Aus der Fassung des Schutzbereichs folgt, dass grundsätzlich jeder Schritt der Verarbeitung personenbezogener Daten als Eingriff in das Recht auf informationelle Selbstbestimmung einzustufen ist. Entsprechend den verfassungsrechtlichen Anforderungen an Eingriffe bedürfen sämtliche Datenverarbeitungsschritte einer Rechtsgrundlage, die unter anderem die Grundsätze der Zweckfestlegung und der Zweckbindung, das Bestimmtheitsgebot und den Verhältnismäßigkeitsgrundsatz beachtet.[9] Auskunftsrechte der Grundrechtsträger kommen hinzu, sind aber konzeptionell akzessorisch.

2.2. Leistungen des Rechts auf informationelle Selbstbestimmung

Leistungs- und Funktionsbeschreibungen hängen vom Bezugskontext und von gewählten Perspektiven ab. Einige zentrale Leistungen des Rechts auf informationelle Selbstbestimmung sollen hervorgehoben werden. Aus gesellschaftspolitischer Sicht hat es dem Datenschutz breite Aufmerksamkeit verschafft. Aus grundrechtsdogmatischer Perspektive ist der Schutz von Personen hinsichtlich des Umgangs anderer mit personenbezogenen Informationen und Daten seither als selbstständiges Grundrechtsthema anerkannt. Ein gewisser Schutz ist zwar bereits vorher aus dem Recht auf Achtung der Privatsphäre und aus dem allgemeinen Persönlichkeitsrecht hergeleitet worden. In beiden Fällen handelte es sich aber um ein anderweitig abgestütztes Schutzgut, das sich über einen Schutz bestimmter Verhaltensweisen hinaus auf die Daten- und Informationsebene erstreckte. Datenschutz blieb insofern an ein anderweitiges Schutzgut gekoppelt und dadurch beschränkt. Beispielsweise wurde die zu achtende »Privatsphäre« in der ursprünglichen Rechtsprechung mit Hilfe einer verräumlichenden Metaphorik als abgeschotteter Bereich verstanden, in dem man allein oder in Ruhe gelassen werden will.[10] Soweit diese Sphäre reichte, schützte sie in ihr stattfindende Verhaltensweisen oder Kommunikationen und schloss ein, dass Vorgänge oder Dokumente, die in ihr entstanden oder sich in ihr befanden, dem staatlichen Einblick grundsätzlich entzogen blieben. Man musste konkretisieren, was eigentlich zur »Privatsphäre« zählte, und der Datenschutz setzte das Vorliegen einer solchen Sphäre voraus. Kritik an diesem Konzept stellte sich schnell ein.

---

[9] BVerfGE 65, 1, 44ff.

[10] So konzipiert auch in dem einflussreichen Aufsatz von Warren und Brandeis, »The Right to Privacy«, S. 193ff.

Hinweise auf die »Relativität der Privatsphäre«[11] hoben die Pluralisierung und Individualisierung des Privatheitsverständnisses hervor. Grundrechtsdogmatisch lässt sich diese Kritik aber auffangen, indem man das Selbstverständnis der geschützten Personen bei der Konkretisierung des Schutzbereichs so weit wie möglich berücksichtigt und im Übrigen, wie es im Recht immer erforderlich ist, typisiert. Entscheidend war und ist ein anderer Kritikpunkt: Für Datenschutzerfordernisse komme es weniger auf die private Sphäre als Entstehungskontext bestimmter Daten als vielmehr darauf an, welche Informationen aus erlangten Daten gewonnen und wie sie verwendet würden.[12] Dieses Argument lenkt den Blick von Daten auf die Gewinnung und Verwendung von Informationen und auf deren Folgen für die betroffene Person. Es trifft die zentrale Schwäche des Privatsphärenkonzepts. In der Rechtsprechung des BVerfG hat es schnell Fälle gegeben, in denen man Informationen mit Blick auf ihren Aussagegehalt als »privat« einstufen konnte, ohne dass sie einer privaten Sphäre entstammten. Beispiel ist ein in der Regenbogenpresse abgedrucktes »Interview« mit Prinzessin Soraya über Privatangelegenheiten, das die Presse frei erfunden hatte.[13] Im Volkszählungsurteil greift das BVerfG ausdrücklich das Argument auf, dass dem Verwendungszusammenhang für die rechtliche Beurteilung von Daten(verarbeitungen) zentrale Bedeutung zukommen muss. Damit rückt es den Umgang mit personenbezogenen Daten und Informationen als solchen in den Mittelpunkt. Der darauf gerichtete Grundrechtsschutz wird flexibilisiert und für vielfältige Schutzerfordernisse geöffnet. Die damals wie heute relevante Überwachung von politischen Aktivitäten oder von Demonstrationen beispielsweise lässt sich nicht unter die »Privatsphäre« und bestenfalls mit Mühe unter eine erweitert verstandene Privatheit quälen. Privatheit mag, angemessen konzipiert, Teilfacetten des Datenschutzes erfassen; Datenschutz ist aber weitaus mehr als Privatheitsschutz. Der unmittelbar auf personenbezogene Daten und Informationen gerichtete Schutz und die Öffnung für vielfältige, gegebenenfalls künftig erst entstehende Schutzerfordernisse sind ein wichtiger Fortschritt, den das Recht auf informationelle Selbstbestimmung gebracht hat.

2.3. Defizite des Rechts auf informationelle Selbstbestimmung

Defizite des Rechts auf informationelle Selbstbestimmung lassen sich vor allem damit erklären, dass das BVerfG den neuartigen Schutzgegenstand unter den konventionellen grundrechtsdogmatischen Zugriff gepresst und vollständig in Denkmustern der traditionellen Eingriffsabwehr einzufangen versucht hat. Die traditionelle Ein-

[11] So z. B. Schlink, »Das Recht der informationellen Selbstbestimmung«, S. 242; siehe auch Solove, *The Digital Person*, S. 212f.

[12] Frühzeitig Simitis, »Chancen und Gefahren der elektronischen Datenverarbeitung«, S. 680.

[13] BVerfGE 34, 269.

griffsabwehr arbeitet aus dogmatischen Gründen mit individualistisch konzipierten Schutzgütern, die als nicht aus sich heraus strukturell begrenzt gedacht werden können: individuelle Handlungen, die man nach Maßgabe des eigenen Willens realisiert, oder individuelles Eigentum an Sachen, über deren Gebrauch man selbst entscheidet. Ganz im Sinne dieser Denkweise wird der Schutzgehalt des Rechts auf informationelle Selbstbestimmung mit einem eigentumsanalogen, allein das Individuum fokussierenden Ansatz beschrieben[14], nämlich als Verfügungsbefugnis über die Preisgabe und dann von anderen vorgenommene Verarbeitung personenbezogener Daten.[15]

Ein solcher Zugriff wird der eigenständigen Kategorialität und den Charakteristika von Daten, Informationen und Wissen aber nicht gerecht. Er bringt ontische Vorstellungen mit sich, als seien Informationen eine Art Abbild der Realität oder Daten eine Art Ball, den man zurückhalten, weitergeben oder verwenden könnte und der sich bei all dem nicht verändert. Daten und Informationen werden zudem behandelt, als seien sie Synonyme. Es geht unter, dass an der Verarbeitung personenbezogener Daten und vor allem an der Gewinnung oder Verwendung der aus den Daten entwickelten Informationen andere, seien es staatliche Stellen, seien es andere Private, strukturell mit eigenen (Interpretations- und Verarbeitungs-) Leistungen beteiligt sind. Vor diesem Hintergrund ist es kein Zufall, dass sich der Schutzbereich »informationeller« Selbstbestimmung auf Daten, nicht etwa auf Informationen bezieht. Ein grundsätzlich bestehendes Recht einer Person, darüber zu entscheiden, welche Informationen andere über sie gewinnen und wie sie sie verwenden, wirkte eigenartig. Es griffe, soweit es sich um Private handelt, tief in deren eigene Freiheiten ein, und zwar selbst dann, wenn man diese Freiheiten nicht als prinzipiell unbegrenzte Freiheiten zur beliebigen Informationsgewinnung und -verwendung konstruiert. Da sich personenbezogene Informationen im Rahmen sozialer Zusammenhänge als etwas »zwischen« Menschen einstufen und außerdem nicht ontisch verstehen lassen, geht ein auf individualistische Attributionen

[14] Zwar hat das BVerfG auch die oft zitierten Ausführungen festgehalten: »Der Einzelne hat nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über ›seine‹ Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Information, auch soweit sie personenbezogen ist, stellt ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann.«, BVerfGE 65, 1 (46). Diese Ausführungen stehen aber im Zusammenhang mit den Einschränkungsvorbehalten und ändern nichts am Zuschnitt des Schutzbereichs.

[15] Die Beschreibung deckt sich mit einigen amerikanischen Konzeptionen von privacy Ende der 1960er/Anfang der 1970er Jahre, vgl. vor allem Westin, *Privacy and Freedom*, S. 42; Fried, »Privacy (A Moral Analysis)«, S. 428f., bei dem es heißt: »Privacy is the *control* we have over information about ourselves (. . .), is control over knowledge about oneself«. Umfassend zu den überkommenen und einflussreichen amerikanischen Konzeptionen Solove, »Conceptualizing Privacy«, S. 1099ff. Übergreifender mit Blick auch auf internationale und europäische Entwicklungen Gratton, *Understanding Personal Information*, S. 1ff.

beschränktes Denken fehl. Informationen, aber auch Daten können einer Person selbst dann, wenn sie in ihrem Aussagegehalt auf diese Person verweisen, nicht grundsätzlich[16] eigentumsähnlich zugeordnet werden.[17] Ein solcher Ansatz passt nicht und er zieht eine Vielzahl weiterer Defizite nach sich.

Der Schutzbereich des Rechts auf informationelle Selbstbestimmung bezieht sich auf Daten, näher auf das einzelne personenbezogene Datum, und im Weiteren auf dessen Verarbeitung in einer Abfolge bestimmter Schritte – Erhebung, Speicherung, Veränderung, Nutzung, Übermittlung. Damit gelangt man zu einem isolierend auf einzelne Daten und Verarbeitungsschritte ausgerichteten Blick statt, wie es gegenstandsgerecht wäre, zu einem kontext- und prozessbezogenen Ausgangspunkt, in dessen Rahmen sich problembezogen bestimmte Verarbeitungsschritte fokussieren ließen. Wegen der Fassung des Schutzgehalts und des daraus resultierenden Erfordernisses einer gesetzlichen Regelung für jeden Schritt der Verarbeitung personenbezogener Daten ist im Laufe der Zeit eine Fülle gesetzlicher Vorschriften entstanden, die jedoch zum Teil wenig substantiellen Steuerungsgehalt aufweisen und mit den sachbezogenen Vorschriften des jeweiligen Regelungsfeldes unzureichend abgestimmt sind. »Verrechtlichungsfalle« lautet hierzu das Schlagwort. Des weiteren kommt nicht hinreichend zum Ausdruck, welch elementare Rolle Kenntnis-, Einfluss- und Partizipationsrechte der betroffenen Personen im Datenschutzrecht spielen müssen. Sowohl unter inhaltlichen als auch unter grundrechtsdogmatischen Aspekten greifen die Lösungen des Gerichts zu kurz.

2.4. Weitere Entwicklungen des Rechts auf informationelle Selbstbestimmung

Nach dem Volkszählungsurteil hat sich das Recht auf informationelle Selbstbestimmung in der Rechtsprechung des BVerfG einerseits in den Grundzügen stabilisiert,

---

[16] Formen der Kommerzialisierung sind unabhängig davon, ob man sie in Teilbereichen für sinnvoll hält oder nicht – vgl. dazu Weichert, »Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung«, S. 1464ff.; »Wem gehören die privaten Daten?«, bes. S. 283ff. – immer (nur) eine unterverfassungsrechtliche Frage der gesetzgeberischen Gestaltung von Eigentumsrechten. Vgl. auch den allenfalls in begrenzten Feldern überzeugenden Ansatz bei Buchner, *Informationelle Selbstbestimmung im Privatrecht*, S. 201ff. Siehe außerdem Buchner, »Die Einwilligung im Datenschutzrecht«, S. 39ff. Ebenfalls zur Diskussion, wenn auch nicht immer überzeugend, Unseld, *Die Kommerzialisierung personenbezogener Daten*.

[17] Die Kritik daran ist im juristischen Kontext zunehmend verbreitet, vgl. etwa Albers, »Zur Neukonzeption des grundrechtlichen ›Daten‹schutzes«, S. 113, 119, 123; Trute, »Verfassungsrechtliche Grundlagen«, Kap. 2.5, Rn. 19, 21, 22; Ladeur, »Das Recht auf informationelle Selbstbestimmung«, S. 48ff.; Britz, »Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts«, S. 566ff. Vgl. auch Allen, »Privacy As Data Control«, S. 865ff.

andererseits in bestimmtem Umfang weiterentwickelt. Zugleich werden in der Rechtsprechung zahlreiche Bruchstellen und Unklarheiten erkennbar.[18]

Bis heute bleibt der Grundansatz des Gerichts der im Volkszählungsurteil gewählten Beschreibung des Schutzbereichs ebenso verhaftet wie den traditionellen dogmatischen Denkmustern. Informationelle Selbstbestimmung schützt, so hält das Gericht regelmäßig fest, »die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen«.[19] In manchen Entscheidungen finden sich freilich Relativierungen: In der Entscheidung zur Rasterfahndung hat das Gericht offen gelassen, ob das Recht auf informationelle Selbstbestimmung vor der Erhebung jedes einzelnen erfassten Datums schützt. Als maßgeblich hat es angesehen, dass die Datenerhebung und -verarbeitung auf die Gewinnung von Erkenntnissen über Verdachtsmomente und gefahrenverstärkende Eigenschaften von Personen zielt und Personen »in das Visier staatlicher Überwachungstätigkeit« gelangen können.[20] Hier klingt eine Differenzierung von Daten und Informationen an. Sie scheint auch in anderen Fällen auf[21], dies in der Regel freilich erst zur Bestimmung der Eingriffsintensität und im Rahmen der Abwägung.[22] In weiteren Entscheidungen beschreibt das Gericht informationelle Selbstbestimmung als einen »den grundrechtlichen Schutz von Verhaltensfreiheit und Privatheit« flankierenden und erweiternden Schutz, der schon auf der Stufe der Persönlichkeitsgefährdung beginne.[23] Teilweise sieht es in der Erhebung von Daten aus öffentlich zugänglichen Quellen keinen Eingriff, soweit sich nicht aus deren systematischer Erfassung, Sammlung und Verarbeitung die für das Recht auf

---

[18] Vgl. hierzu bereits ausführlich Albers, »Umgang mit personenbezogenen Informationen und Daten«, § 22 Rn. 62ff.

[19] Vgl. zuletzt aus der ständigen Rechtsprechung BVerfG, Urteil vom 19.04.2016, 1 BvR 3309/13, Rn. 56, abrufbar unter http://www.bverfg.de.

[20] BVerfGE 115, 320 (342ff.). Die Auseinandersetzung mit dem Schutzgehalt des Rechts auf informationelle Selbstbestimmung liegt bei der Rasterfahndung nahe: Einerseits bedingt diese Methode der rechnergestützten Massendatenverarbeitung die Erhebung und Verarbeitung einer Vielzahl einzelner, dabei auch für sich genommen belangloser personenbezogener Daten, deren Verarbeitung unter bestimmten Umständen praktisch folgenlos bleiben kann; andererseits steht dies im Kontext sicherheitsbehördlicher Ermittlungen mit deren potenziellen Folgen für davon Betroffene.

[21] Vgl. auch die Reformulierung in BVerfGE 118, 168 (185); 120, 378 (399); 130, 151 (183f.), es gebe unter den Bedingungen der elektronischen Datenverarbeitung bzw. angesichts der Verarbeitungs- und Verknüpfungsmöglichkeiten kein *schlechthin, also ungeachtet des Verwendungskontextes*, belangloses personenbezogenes Datum (Hervorhebung von M. A.).

[22] Vgl. etwa BVerfGE 133, 277 (350ff.).

[23] BVerfGE 118, 168 (184f.); 120, 274 (312); 120, 351 (360); 120, 378 (397ff.). Vgl. auch BVerfG (Kammer), Beschl. vom 24.07.2015, 1 BvR 2501/13, http://www.bverfg.de, Rn. 11: »Das Recht auf informationelle Selbstbestimmung trägt Gefährdungen und Verletzungen der Persönlichkeit Rechnung, die sich für den Einzelnen aus informationsbezogenen Maßnahmen ergeben«.

informationelle Selbstbestimmung spezifische Gefährdungslage ergibt.[24] Dass mit einer solchen Schutzbegrenzung ein Rückfall in eine viel zu schlichte Differenz zwischen geschützter Privatheit und nicht geschützter Öffentlichkeit droht, belegt die Entscheidung zum Cybercrime-Convention-Gesetz.[25] All dies zeigt, dass das BVerfG den Reformbedarf bei der Beschreibung des Schutzguts zwar sieht;[26] es geht jedoch nicht den Weg hin zu einer grundlegenden und umfassenden konzeptionellen Veränderung, sondern bleibt bei punktuell-eklektizistischen, unterkomplexen und teilweise verfehlten Modifikationen stehen.

Dogmatisch sind die Denkmuster der traditionellen Eingriffsabwehr weiterhin prägend für den Zugriff des Gerichts: Den Schutzbereich bestimmt ein individualistisch gestaltetes Schutzgut. Eingriffe in den Schutzbereich sind dann, aber auch nur dann verfassungsmäßig, wenn sie auf einer gesetzlichen Grundlage beruhen und das Bestimmtheitsgebot, das Übermaßverbot sowie alle weiteren einschlägigen verfassungsrechtlichen Anforderungen einhalten. Dieser Zugriff bewirkt unter anderem, dass das Übermaßverbot als wesentliche Grundlage datenschutzrechtlicher Anforderungen herhalten muss. Damit wird diese Figur überfordert. Immerhin wird in einigen Entscheidungen die Gewährleistung der Kenntnismöglichkeiten der geschützten Grundrechtsträger von einer zunächst lediglich akzessorischen Schutzvorkehrung[27] zu einer eigenständigen Komponente in Gestalt leistungsrechtlicher Schutzpositionen aufgewertet, welche gegenstands- und problembezogen gesetzlich ausgestaltet werden müssen.[28] Für die rechtlichen Bindungen im Verhältnis unter Privaten greift das Gericht auf Schutzpflichten und/oder auf die Dogmatik der

[24] BVerfGE 120, 274 (344f.); 120, 351 (361f.). Die Ausführungen betreffen das bloße behördliche Surfen im Internet oder Angaben aus Telefonbüchern oder Handelsregistern. Vgl. auch die Ausführungen in BVerfGE 120, 378 (399). In der Entscheidung zur Online-Überwachung verneint das Gericht einen Eingriff grundsätzlich selbst dann, wenn eine staatliche Stelle unter Verschleierung ihrer Identität im Rahmen internetvermittelter Kommunikationsbeziehungen zu Grundrechtsträgern Daten über diese sammelt, weil es hier von vornherein am Vertrauen hinsichtlich der Identität der Kommunikationspartner fehle, BVerfGE 120, 274 (345). Diese Ausführung ist in ihrer Pauschalität nicht tragfähig und von einer überholten Dichotomie von »realer« und »virtueller« Welt geprägt.

[25] BVerfG, Beschl. vom 21.06.2016, 2 BvR 637/09, mit Sondervotum *Huber*, abrufbar unter http:\\www.bverfg.de.

[26] Das liegt auch deshalb nahe, weil sich die genetischen Grundlagen des Rechts auf informationelle Selbstbestimmung inzwischen ihrerseits an zentralen Stellen geändert haben, vgl. näher Albers, »Umgang mit personenbezogenen Informationen und Daten«, Rn. 64, mit Hinweisen auf die relevanten Entscheidungen.

[27] Im Volkszählungsurteil hat dies wegen der Fallkonstellation ausgereicht.

[28] Vgl. BVerfGE 120, 351 (362ff.); BVerfG (Kammer), DVBl 2001, S. 275. Die BKA-Entscheidung, BVerfG, Beschl. v. 20.04.2016, 1 BvR 966/09 u. a., http:\\www.bverfg.de, Rn. 134ff., ordnet Kenntnismöglichkeiten demgegenüber wiederum dem Übermaßverbot bei eingriffsabwehrrechtlichem Ausgangspunkt zu.

»mittelbaren Drittwirkung« zurück.[29] Die Probleme der Grundkonzeption werden dadurch in dieses Verhältnis übertragen und teilweise verschärft.

Die näheren verfassungsrechtlichen Anforderungen an Gesetze oder an behördliche Maßnahmen und gerichtliche Entscheidungen sind im Laufe der Zeit differenziert und verfeinert worden. Das gilt umso mehr, als der »grundrechtliche Datenschutz« nicht nur im Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, sondern auch in anderen Freiheitsgewährleistungen verankert wird. Zu den relevanten Gewährleistungen gehört insbesondere die Verbürgung des Telekommunikationsgeheimnisses. Das Gericht bezeichnet Art. 10 Abs. 1 GG als eine gegenüber dem Recht auf informationelle Selbstbestimmung »spezielle Garantie«. Die aus den beiden Grundrechten folgenden Anforderungen werden partiell parallelisiert.[30] Sie reichen von Einschreit- und Verarbeitungsschwellen, dies teilweise auch in Form eines gestuften Datenzugangs verschiedener Stellen, über die Zweckfestlegung und prinzipielle Zweckbindung nebst Kennzeichnungspflichten zur Sicherstellung der Zweckbindung bis hin zur Gewährleistung eines besonders hohen Standards der Datensicherheit durch Verpflichtungen Privater im Falle der »vorsorglich anlasslosen« Datenspeicherung.[31] Als Grundlage der entwickelten Anforderungen dienen regelmäßig das Übermaßverbot oder die Figur der organisations- und verfahrensrechtlichen Schutzvorkehrungen.[32]

Funktionsbeschreibung und Ausgestaltung wichtiger Bausteine können allein auf der Folie des Übermaßverbots oder der Schutzvorkehrungen aber nicht gelingen. Das zeigt sich etwa mit Blick auf die Bausteine der Zweckfestlegung, Zweckbindung und Zweckänderung.[33] Darüber hinaus verweisen sowohl das Übermaßverbot als auch die Figur der »Schutzvorkehrungen« in bestimmtem Umfang auf die inhaltlichen Aussagen des Schutzbereichs zurück. Diese müssen somit überzeugend

---

29 BVerfGE 84, 192 (194ff.); BVerfG (Kammer), Beschluss vom 17.07.2013, 1 BvR 3167/08, , Rn. 19, http:\\www.bverfg.de.

30 Vgl. exemplarisch BVerfGE 100, 313 (358); 109, 279 (325f.); 110, 33 (53); 125, 260 (310).

31 Zu den näheren Maßgaben etwa BVerfGE 100, 313 (360f.); 109, 279 (379f.); 115, 320 (359ff.); 118, 168 (186ff.); 120, 351 (366ff.); 120, 378 (407ff.); 125, 260 (325ff.); 130, 151 (187ff.); 133, 277 (320ff.); in Form einer übegreifenden Zusammenfassung s. auch BVerfG, Beschl. v. 20.04.2016, 1 BvR 966/09 u. a., Rn. 93ff., http://www.bverfg.de.

32 Vgl. zuletzt BVerfGE 130, 151 (187ff.); 133, 277 (320ff.); BVerfG, Beschl. v. 20.04.2016, 1 BvR 966/09 u. a., http:\\www.bverfg.de, Rn. 93ff., bes. 103ff.

33 Nicht treffend hierzu etwa BVerfG, Beschl. v. 20.04.2016, 1 BvR 966/09 u. a., http://www.bverfg.de, Rn. 278ff.: Hier geht das BVerfG davon aus, der Gesetzgeber und die jeweilige Eingriffsgrundlage bestimmten den Zweck und die Zweckbindung bestimme sich nach der Reichweite der Erhebungszwecke in der für die jeweilige Datenerhebung maßgeblichen Ermächtigungsgrundlage, anstatt als Ausgangspunkt zugrundezulegen, dass Gesetzgeber und Gesetz einen begrenzenden und strukturierenden Rahmen setzen, innerhalb dessen die Akteure, hier die Sicherheitsbehörden, Verwendungszwecke konstellations- oder fallorientiert weiter spezifizieren müssen. Vgl. zu diesen Bausteinen näher: Albers, *Informationelle Selbstbestimmung*, S. 497ff.

ausgearbeitet sein, damit die Präzisierung und Relationierung der jeweils involvierten Interessen oder die funktionalen Erwägungen, mit Hilfe derer die nötigen Schutzvorkehrungen bestimmt werden, normativ abgesichert sind. Anderenfalls entsteht die Gefahr, dass Anforderungen hervorgezaubert werden, die im zu entscheidenden Fall durchaus passen mögen, aber normativ nicht stringent hergeleitet und deswegen nicht hinreichend stabilisierbar sind.

Bislang hat sich das BVerfG noch nicht konsequent genug auf die Charakteristika und Anforderungen eines gerade informations- und datenorientierten Schutzes ein- und umgestellt. Insgesamt wird im individualistisch-eingriffsabwehrrechtlichen Zuschnitt des Rechts auf informationelle Selbstbestimmung nicht deutlich, wie sehr der Datenschutz auf eine schutzzielgerechte, sich auf mehreren Ebenen bewegende, vielfältige Bausteine umfassende und miteinander koordinierende Ausgestaltung im Wege verschiedener Ebenen und Formen des Rechts angewiesen ist.

3. Zeit für eine Neukonzeption

Seit einiger Zeit ist nicht nur das Datenschutzrecht, sondern auch dessen grundrechtliche Basis, das Recht auf informationelle Selbstbestimmung, Gegenstand von Reformdiskussionen. Hinweise auf veränderte gesellschaftliche und technische Rahmenbedingungen greifen dabei zu kurz. Vielmehr müssen die grundlegenden Denkmuster, mit denen man arbeitet, kritisch reflektiert und gegenstandsgerecht angelegt werden. Zukunftsorientierte Lösungen liegen nicht in einer Rückkehr zur Privatsphäre oder in einer Hinwendung zur Privatheit als Leitidee. Sobald deutlich ist, um welch fundamentale und eigenständige Kategorien es sich bei Daten und Informationen handelt, wird erkennbar, dass der grundrechtliche Datenschutz als ein vielschichtiges Bündel von Rechtsbindungen und Rechtspositionen ausgearbeitet werden muss.

Für eine Neukonzeption ist es auch deswegen an der Zeit, weil das Datenschutzrecht vor einer weit reichenden Europäisierung steht. Ab dem Jahr 2018 werden sowohl die neue Datenschutz-Grundverordnung als auch die neue Datenschutz-Richtlinie in den Bereichen der Straftatenverhütung, -untersuchung, -aufdeckung und -verfolgung oder der Strafvollstreckung greifen. Damit wird sich der Grundrechtsschutz in Teilen von den nationalen Gewährleistungen auf die Grundrechte der Charta der Europäischen Union (GrC) verlagern. Wie weit diese Verlagerung reichen wird, hängt von mehreren, partiell klärungsbedürftigen Faktoren ab, etwa von der Gestaltung des Vorrangs der Verordnung gegenüber nationalem Recht oder vom Aussagegehalt der Öffnungsklauseln zu Gunsten der Mitgliedstaaten. Unabhängig von den insoweit voraussehbaren Streitfragen werden die unionalen Grundrechte erheblich an Relevanz gewinnen. Ein »Recht auf informationelle Selbstbestim-

mung«, wie das BVerfG es hergeleitet hat, enthält die GrC aber nicht, und bereits aus rechtsmethodischen Gründen darf man deutsche Konzeptionen nicht einfach in die unionale Charta hineinlesen. Art. 8 Abs. 1 GrC sieht vor: »Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.« Art. 8 Abs. 2 und 3 GrC halten das Erfordernis einer Zweckfestlegung, einen Einwilligungs- oder Gesetzesvorbehalt, Kenntnis- und Berichtigungsrechte sowie die Datenschutzkontrolle durch eine unabhängige Stelle fest. Art 7 GrC schützt in weit gehendem Gleichklang mit Art. 8 Abs. 1 der Europäischen Menschenrechtskonvention (EMRK) das Recht jeder Person auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation. Eine gefestigte Dogmatik, wie die jeweiligen Inhalte und die Beziehungen zwischen diesen Rechten zu interpretieren sind, muss sich erst noch herausbilden.[34] In der Entscheidung des EuGH zur Vorratsdatenspeicherung klingt an, dass Art. 8 GrC in einer nicht auf das Privatleben beschränkten Weise die Verarbeitung personenbezogener Daten in den Blick nimmt und daran eigenständige Anforderungen stellt, während Art. 7 GrC in inhaltlicher Akzentuierung dem Schutz des Privatlebens dient.[35] Die Grundrechte-Charta enthält noch eine Reihe anderer inhaltlicher Freiheiten, etwa die Meinungsäußerungs- oder die Berufsausübungsfreiheit. Auf unionaler Ebene gibt es somit kein Verfügungsrecht, sondern ein »Recht auf Schutz« personenbezogener Daten, ergänzt um bestimmte inhaltliche Maßstäbe.

In den nächsten Jahren ist mit wechselseitigen Einflüssen der Aussagegehalte unionaler und nationaler Gewährleistungen aufeinander zu rechnen. Denn das Recht auf Schutz personenbezogener Daten ist konkretisierungsbedürftig[36] und die Rechtsprechung des EuGH noch nicht ausgefeilt, so dass dieser Art. 8 GrC künftig mit konkreteren Vorgaben auffüllen, sich hier von passenden nationalen Schutzkonzeptionen anregen lassen und diese dann europäisch zuschneiden wird. Umgekehrt kann man bei der Suche nach einem neuen Konzept für das deutsche Recht auf informationelle Selbstbestimmung aufgreifen, dass die unionale Fassung als ein »Recht auf Schutz« akzentuiert ist, das ganz abstrakt formuliert und mit sinnvollen normativen Maßgaben anzureichern ist. Damit man nicht immer wieder mit entscheidungsrelevanten Abgrenzungsschwierigkeiten der Anwendbarkeit entweder unionaler oder nationaler Grundrechte zu kämpfen hat, ist eine gewisse Konvergenz der Schutzkonzeptionen bei Eigenständigkeiten im Detail angezeigt. Für eine gegenstandsgerechte Konzeption ist wichtig, wie der Gegenstand zu erfassen ist, mit dem man zu tun hat, wie die grundrechtlich geschützten Interessen zu begreifen und

[34] Näher Albers, »Umgang mit personenbezogenen Informationen und Daten«, Rn. 43ff.

[35] EuGH, Urt. v. 8.4.2014, C-293/12 u. C-594/12, Rn. 29f.

[36] Vgl. hierzu auch Stentzel, »Das Grundrecht auf…?«, S. 188ff., hier mit der These, dass (nur) das »Privatleben« des Art. 7 GrC schutzgutrelevante Maßstäbe liefere.

zu konkretisieren sind und wie sich vor diesem Hintergrund Regulierungskonzepte gestalten müssen.

4. Der Gegenstand des Datenschutzes als Netzwerk mehrerer Elemente

Datenschutz zielt nicht auf den Schutz von Daten, sondern auf den Schutz der Personen, auf die sich Daten beziehen. Gegenstand des Schutzes sind dann aber auch gar nicht personenbezogene Daten als solche.[37] Man muss diese isolierte Betrachtung um mehrere Elemente erweitern: auf basaler Ebene um das Element der Information, in der Strukturdimension um Wissen, in der Zeitdimension um Verarbeitungsprozesse und im weiteren Kontext um Entscheidungen und Entscheidungsfolgen. Daten, Informationen, Wissen oder Entscheidungen sind grundlegende Kategorien, die viele Disziplinen benutzen und die disziplinenspezifisch in Abhängigkeit von Rahmung und Erkenntnisinteressen definiert werden.[38] Im hier fokussierten rechtlichen Zusammenhang kommt es darauf an, sie vor dem Hintergrund normativer Schutz- und Ausgestaltungserfordernisse angemessen zu erfassen.

Daten lassen sich als Zeichen beschreiben, die auf einem Datenträger festgehalten und so vergegenständlicht sind.[39] Sie sind immer selektiv und weniger als einzelnes Datum von Bedeutung, sondern im Rahmen von wissensrelevanten Speicher- und Verknüpfungsformen in der Strukturdimension und Datenverarbeitungsprozessen in der Zeitdimension. Daten, Speicherformen und Verarbeitungsprozesse werden durch die verschiedenen Medien, Techniken und Netze geprägt. Aus rechtlicher Sicht ist entscheidend, dass Daten aufgrund ihrer Vergegenständlichung einen fassbaren Anknüpfungspunkt für eine rechtliche Steuerung bieten. Relevanz gewinnen sie jedoch erst als potentielle Informationen. Ihr Informationsgehalt ist freilich keine intrinsische Eigenschaft, die den Daten anhaftet.[40]

Informationen sind Sinnelemente mit einer zweigliedrigen Struktur: Auf der einen Seite knüpfen sie an etwas in der Außenwelt Beobachtetes, an Mitteilungsinhalte oder an Daten an. Auf der anderen Seite werden sie durch Interpretationsleis-

[37] Damit relativiert sich in sinnvoller Weise die rechtliche Bedeutung der »Personenbezogenheit«. Diese kann schwer festzustellen sein und ergibt sich nicht selten erst im Kontext oder Ablauf der Verarbeitungsnetze und -schritte. Dazu Gratton, *Understanding Personal Information*, S. 21ff., 93ff. Zudem lässt sich der Datenschutz so besser mit Rechtsbindungen und Schutzpositionen abstimmen, die man – etwa als Diskriminierungsschutz – in den Feldern entwickeln muss, in denen es nicht um personenbezogene Informationen und Daten geht.

[38] Vgl. Floridi, *Information: A Very Short Introduction*, S. 19ff. Zur Diskussion darum, ob es ein einheitliches begriffliches »Ur-Konzept« geben kann Floridi, »Information«, S. 40ff.

[39] Ausführlich zu Konzepten Kitchin, *The Data Revolution*, S. 2ff.

[40] Siehe mit Bezug auf Kommunikation Ashby, *An introduction to Cybernetics*, S. 124: »The information conveyed is not an intrinsic property of the individual message.«

tungen vollendet, mittels derer die beobachteten Phänomene, die Mitteilungsinhalte oder die Daten sinnhaft verstanden werden.[41] Informationen bezeichnen also Sinnelemente, die als Inhalt einer Beobachtung, einer Mitteilung oder eines Datums mit Hilfe einer Interpretationsleistung erzeugt werden. Vor diesem Hintergrund sind Daten und Informationen keine Synonyme, sondern im Gegenteil strikt zu unterscheiden. Informationen sind auf elementare Weise kontextabhängig. Indem sie eine Interpretationsleistung voraussetzen, die im jeweiligen Wissens- und Deutungskontext und in Abhängigkeit von den je situativen Interpretationsbedingungen erfolgt, verweisen sie auf die Strukturen und Prozesse, in deren Rahmen sie überhaupt erst gebildet werden können.

In der Strukturdimension ist Wissen an der Erzeugung von Informationen beteiligt.[42] Es ermöglicht die Interpretationsleistungen und begrenzt die Interpretationsmöglichkeiten. Wissen stützt sich auf Wissensgrundlagen, zu denen Texte, Akten, Datenbanken, aber auch institutionelle Arrangements gehören. Es ist nicht etwa als »Vorrat« von Erkenntnissen im Hintergrund stets präsent. Vielmehr kann es immer nur selektiv im jeweiligen sozialen Kontext nach Maßgabe der darin bestehenden Erkenntnisinteressen, Handlungsmuster oder Rahmenbedingungen aufgebaut werden. Daher ist es Faktor und Produkt des Kontexts, in dem sich der Umgang mit Informationen und Daten vollzieht.[43] Wissen ist nicht unbedingt etwas gemeinsam Geteiltes. In komplexeren Zusammenhängen hat man im Gegenteil mit pluralisierten Wissensregimen zu tun.[44] Wissen verweist weiter auf Ungewissheit und auf Nichtwissen als Komplementär- oder Gegenbegriffe, die Interpretationsleistungen und Informationsproduktion mitbeeinflussen.

In der Zeitdimension kommt der Prozesscharakter der Datenverarbeitung und der Informationsflüsse hinzu. Bei organisiertem und linearem Verlauf sind die Erhebung, die Speicherung und die Veränderung an der vorgesehenen, mehr oder weniger bestimmten Nutzung der Daten als Informationen orientiert. Umgekehrt baut die Nutzung auf der Datenbasis auf, die durch die Erhebung, Speicherung und Veränderung begründet wird. Datenverarbeitungsprozesse verlaufen allerdings regelmäßig nicht linear: Daten können gespeichert, abgerufen und mit verändertem Gehalt erneut gespeichert werden; die einzelnen Phasen können faktisch weitgehend voneinander entkoppelt werden; Daten können in mehrere Verarbeitungszusammenhänge einfließen. Die rechtliche Bedeutung eines Datenverarbeitungsschritts

41 Siehe ausführlich: Albers, »Information als neue Dimension im Recht«, S. 67ff.

42 Zum Wissen als im Datenschutz relevanter Ebene siehe auch Hildebrandt, »Who is Profiling Who?«, S. 240ff.

43 Siehe näher Albers, »Umgang mit personenbezogenen Informationen und Daten«, § 22, Rn. 14ff. Vgl. auch Trute, »Wissen – Einleitende Bemerkungen«, S. 15f. Als stets Kontextualisiertes wird Wissen von eben den Kontexten geprägt, in denen es aktualisiert wird und zu denen es beiträgt.

44 Ausführlich dazu Wehling, »Wissensregime«, S. 704ff.

erschließt sich nicht in isolierender Betrachtung, sondern erst im Mitdenken der jeweils zu bestimmenden Verarbeitungszusammenhänge, die die Gewinnung und Verwendung von Informationen einschließen. Diese verleihen dem Umgang mit Daten seine spezifische soziale Relevanz. Die übliche Konzentration auf die Datenverarbeitungsprozesse ist deshalb eine verkürzte Perspektive. Man muss die komplexen Abläufe und Netze in den Blick nehmen, in denen Informationen, Daten und die verschiedenen Verarbeitungsschritte verwoben sind.

Nicht zuletzt spielen auch die Verknüpfungen zwischen Informationen oder Wissen einerseits und (potentiellen) Handlungen oder Entscheidungen der datenverarbeitenden staatlichen oder privaten Stellen andererseits eine Rolle. Informationen und Wissen sind prägende Faktoren in Entscheidungs- und Handlungszusammenhängen; auch dienen sie als Grundlage bestimmter Entscheidungen und Handlungen. Daran knüpfen sich eine Reihe von Folgen an, die sich unter bestimmten Umständen als Nachteil für die Person beschreiben lassen, auf die sich Daten und Informationen beziehen. Je nach gewählter Abstraktionsebene und gewähltem Bezugskontext können dies unterschiedliche Nachteile sein, sei es, dass sich Rahmenbedingungen negativ verändern, sei es, dass (potentielle) Entscheidungen nachteilige Folgen nach sich zögen, sei es, dass die betroffene Person ein ihr eigentlich zustehendes Verhalten anpasst, damit sie keine Nachteile erfährt. Sofern so vermittelte Nachteile normativ unerwünscht sind[45], ist der Schutz davor – oder bereits vor den Risiken, dass solche Nachteile entstehen – einer der Gründe für Datenschutz.[46] Es gibt weitere Gründe, die man bei der Bestimmung geschützter Interessen ausarbeiten kann, die sich eben deshalb als Bündel von Schutzpositionen darstellen. An dieser Stelle soll nur deutlich werden, dass das Verständnis des Datenschutzes voraussetzt, dass man relevante Entscheidungs- und Handlungszusammenhänge mitdenkt. Umfang und Form hängen davon ab, wie relativ lose oder verdichtet die Beziehung zwischen Daten und Wissen, Handlungen und Entscheidungen in dem fokussierten Kontext ist.

Schon diese grobe Beschreibung zeigt, dass sich Datenschutz um einen hochkomplexen Gegenstand dreht. Er erfordert ein Denken in sozialen Relationen, in Prozessen und in Kontexten. Man muss mit der Unterscheidung von Daten und Informationen operieren und das Wissen und die Verarbeitungsprozesse im Kontext ebenso mitberücksichtigen wie Handlungs- und Entscheidungszusammenhänge

[45] Das ist keineswegs bei allen Nachteilen der Fall.

[46] Schon da die hier gemeinten Nachteile vielfältig sein und sich in vielfältigen Formen vermitteln und realisieren können, bedeutet dies nicht, dass Datenschutz rein instrumentell-akzessorisch dem Verhaltensschutz in dem Sinne diente, dass er das »eigentlich« geschützte freie Verhalten bereits im Vorfeld vor Gefährdungen bewahren soll. Siehe jedoch in diese Richtung, im Einzelnen allerdings differenziert Britz, »Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts«, S. 569ff.; Poscher, »Die Zukunft der informationellen Selbstbestimmung als Recht auf Abwehr von Grundrechtsgefährdungen«, S. 178ff.

und damit verbundene Folgen. Angesichts einer zunehmenden Lösung von Datenverarbeitungen aus konkreten Handlungszusammenhängen können Handlungs- und Entscheidungszusammenhänge (oder: »Verwendungskontexte«) zwar abstrahiert, typisiert oder als Zukunftsszenarien formuliert, aber nicht vollkommen ausgeblendet werden. Daten dürfen somit nicht isoliert betrachtet, sie müssen vielmehr in einem Netzwerk mehrerer Grundbegriffe begriffen werden. In diesem Netzwerk sind sie ein zentraler Anknüpfungspunkt der rechtlichen Regulierung, freilich nicht der einzige Anknüpfungspunkt.[47] Datenschutz zielt auf die Regulierung der Datenverarbeitung, aber eben auch auf die Regulierung der Informations- und Wissenserzeugung in Handlungs- und Entscheidungszusammenhängen und damit verbundener nachteiliger Folgen für die betroffenen Personen.

5. Geschützte Interessen betroffener Personen

Das leitet über zum nächsten Punkt: Wie kann man die geschützten Interessen der betroffenen Personen beschreiben? Die bisherigen Ausführungen erhellen bereits, dass die Idee individueller Verfügungsbefugnisse über Daten nicht die zentrale Leitidee des Datenschutzes sein kann. Vielschichtige, inhaltlich vielfältige und mehrdimensionale Gewährleistungen drängen sich auf.

Im Ausgangspunkt muss man sich vergegenwärtigen, dass sich ein grundrechtlicher Schutz im Hinblick auf den Umgang anderer mit personenbezogenen Informationen und Daten von den Schutzgütern des traditionellen Grundrechtsverständnisses unterscheidet. Es gibt zwar den zu schützenden Grundrechtsträger. Schutzgegenstand ist aber nicht etwa *seine* Verhaltensfreiheit. Er soll vielmehr im Hinblick auf die ihn betreffenden Informationen und Daten geschützt werden, die in Wissens- und Deutungskontexten erzeugt und prozediert werden und an denen staatliche Stellen oder andere Private schon wegen der notwendigen Interpretations- und Verarbeitungsleistungen beteiligt sind. Darauf gerichtete Schutzpositionen sind nicht individualistisch, sondern nur als Positionen im Hinblick auf die Sozialität des Individuums zu begreifen, denn Schutzpositionen im Hinblick auf Informationen oder das (potenzielle) Wissen anderer über einen selbst setzen das Mitdenken der anderen bereits in der Grundstruktur des Schutzgegenstandes voraus. Warum und inwieweit die betroffene Person zu schützen ist, muss deswegen aus überindividueller Perspektive mit typisierendem Blick auf den Kontext und auf erwartbare nachteilige Folgen begründet werden. Im Übrigen reicht ein Schutz nicht aus, der allein auf die Abwehr und das Unterlassen einer Verarbeitung personenbezogener Daten oder

[47] Die rechtliche Regulierung muss an mehrere Punkte anknüpfen; daher wäre es beispielsweise verfehlt, statt auf Daten einfach auf Informationen abzustellen und den einen Begriff durch den anderen zu substituieren.

einer Gewinnung und Verwendung personenbezogener Informationen gerichtet ist. Da sich diese Prozesse auf Seiten der anderen, also losgelöst von der zu schützenden Person, vollziehen, ist es genauso wichtig, dass diese von den sie betreffenden Daten- und Informationsverarbeitungen erfährt und Einfluss darauf nehmen kann. Sie benötigt also nicht nur Abwehr-, sondern weitere Rechte, namentlich Wissens-, Partizipations- oder Einflussrechte und zudem Rechte, die aus Rechtsbindungen folgen, die eine institutionalisierte Gewährleistung von Datenschutzanforderungen vorgeben.

Geht man den Gefahren und Schutzerfordernissen, auf die Datenschutz reagieren soll, näher nach, erkennt man, dass sie auf unterschiedlichen Ebenen angesiedelt sind. Auf einer grundlegenden Ebene geht es um die Problematik eines potenziell allumfassenden, unbegrenzten und intransparenten Umgangs des Staates oder anderer Privater mit personenbezogenen Informationen und Daten. Schon in den 1970er Jahren war das Schlagwort hierzu: »gläserner Bürger«, und mit dem Internet haben sich die Gefahren gesteigert. Das Erfordernis eines Schutzes vor derartigen Gefahren ist durch – wenn auch in verschiedenen Zeiten und Zusammenhängen wurzelnde – literarische Metaphern und Narrative kulturell verankert und popularisiert worden, vor allem durch Orwells »Big Brother«,[48] aber auch durch Benthams »Panopticon«[49] oder durch Kafkas »Der Prozess«.[50] In Ergänzung dieser staatszentrierten Werke mag man mit Blick auf soziale Netzwerke jüngere treffsichere Romane hinzunehmen, zum Beispiel Dave Eggers' »The Circle«.[51] Daniel Solove hat aufgezeigt, dass die bekannte Big Brother-Metapher bestimmte Datenschutzprobleme effektiv einfängt,[52] dass es aber die Kafka-Metapher ist, die das Problem mangelnden Wissens und mangelnden Einflusses im Hinblick auf das Wissen anderer über einen selbst illustriert.[53] Gleich der Beginn des Werkes lässt spüren, wie bedrohlich dies sein kann: »Jemand musste Josef K. verleumdet haben, denn ohne dass er etwas Böses getan hätte, wurde er eines Morgens verhaftet.« Warum denn, fragt er die Wächter, und erhält die lapidare Antwort: »Wir sind nicht dazu bestellt, Ihnen das zu sagen.«

Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG kann auf dieser grundlegenden Ebene passende grundrechtliche Bindungen und Schutzpositionen hergeben. Denn diese Normenkombination lässt sich dahin auslegen, dass sie »*essentielle, existentiale*

48 Orwell, *1984*.
49 Bentham, *The Panopticon Writings*, S. 29ff.
50 Kafka, *Der Prozess*.
51 Eggers, *The Circle*.
52 Solove, »Privacy and Power«, S. 1399.
53 Ebd., S. 1426.

Voraussetzungen für die Ausübung jeglicher Freiheit« schützt.[54] Rechtsbindungen und Rechtspositionen richten sich zunächst darauf, dass der Umgang mit personenbezogenen Informationen und Daten nicht weitgehend ungebunden, unbegrenzt und undurchschaubar verläuft. Die Entwicklung und die freie Entfaltung der Persönlichkeit erfordern eine relative Erwartungs- und Orientierungssicherheit der Individuen im Hinblick auf ihre soziale Umwelt, die die Möglichkeit eines Vertrauens beispielsweise darauf umfasst, dass gewisse Sichtbarkeitsschranken zwischen verschiedenen Kontexten und Rollen bestehen, dass nicht überall fehlerhafte Datensätze und entsprechend verzerrte Bilder zur eigenen Person kursieren oder dass man nicht in jeder Situation ohne eine Chance des Vergessens mit einer längst überholten Vergangenheit belastet wird. Ein solches Vertrauen und sein Schutz bedeuten nicht, dass man nicht von unerwartetem Wissen überrascht werden könnte; die Fähigkeit, enttäuschte Erwartungen zu verarbeiten, und die Fähigkeit zur Selbstbehauptung gehören zur Persönlichkeitsentwicklung und -entfaltung. Könnte man jedoch gar kein prinzipielles Vertrauen auf »kontextuale Integrität«[55] aufbauen, wären Verunsicherungen, Befangenheiten im Umgang mit anderen und Mechanismen der erwartungsvermittelten Anpassung des Verhaltens in einem Umfang zu befürchten, der mit der geschützten Freiheit der Persönlichkeitsentfaltung unvereinbar wäre.[56] Die auf eine begrenzende, strukturierende und transparenzsichernde Grundregulierung gerichteten Grundrechtsgarantien werden im Weiteren durch Garantien ergänzt, aufgrund derer den geschützten Personen grundsätzliche Möglichkeiten zu eröffnen sind, Kenntnis über die sie betreffenden Datenbestände und Wissensbausteine staatlicher Stellen oder, in relativiertem Umfang, anderer Privater zu erlangen. Diese Wissenskomponente des Persönlichkeitsschutzes hat Bedeutung für die Persönlichkeits- und Identitätsbildung, für das Selbstwertgefühl und die Selbst-Behauptung, für die orientierunggebende Einschätzung des Bildes, das die soziale Umwelt sich bildet, oder für die Realisierung von Verhaltensoptionen. Die Prozesse der Verarbeitung personenbezogener Informationen und Daten dürfen außerdem nicht vollständig an den geschützten Personen vorbei verlaufen. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG verlangt angemessene Einflusschancen. Je nach Wissenskontext braucht man zum Beispiel Möglichkeiten zur Beeinflussung der Datenbestände, zur Berichtigung oder Löschung bestimmter Angaben oder zur ei-

---

54 Saladin, »Persönliche Freiheit als soziales Grundrecht?«, S. 100 (Hervorhebung im Original; für die schweizerische Bundesverfassung); zum Ansatz für das GG Albers, *Informationelle Selbstbestimmung*, besonders S. 455f.

55 Nissenbaum, »Privacy as Contextual Integrity«, S. 119ff.; *Privacy in Context*, S. 129ff.

56 An dieser Stelle (und an anderen Stellen) fließen Folgenerwägungen ein, die empirische Anker benötigen, allerdings keine rein empirisch zu beurteilende Fragen sind. Das gilt schon deshalb, weil man im Recht und bei den normativen Überlegungen die theoretischen und methodischen Grenzen einer empirischen Verifizierung von Annahmen über Folgen – zumal auf der Grundlagenebene der Gesellschaft, auf der sich die Folgenerwägungen hier bewegen – mitreflektieren muss.

genen Stellungnahme oder Gegendarstellung. Darüber hinaus sind unterschiedliche Bausteine einer Gewährleistung des Datenschutzes durch Institutionen notwendig. Denn den geschützten Individuen erschließen sich viele der Komponenten und vernetzten Prozesse moderner Datenverarbeitungen angesichts derer Komplexität in unaufhebbarer Weise nur begrenzt; ein rein auf die Zuerkennung von Individualrechten konzentrierter Ansatz erreicht die Schutzziele nicht. Sämtliche dieser auf der grundlegenden Ebene herleitbaren Rechtsbindungen und Rechtspositionen sind nicht schlicht auf Staatsabwehr angelegt. Grundrechtsdogmatisch greift ein Zugriff über das Konzept der Eingriffsabwehr viel zu kurz. Vielmehr geht es um komplexe Regulierungsaufträge, denen im Wege der Rechtsetzung und -umsetzung nachzukommen ist.[57]

Sofern und sobald diese Grundrechtsvorgaben umgesetzt sind und deswegen in rechtlich verlässlicher Weise gewährleistet ist, dass Informations- und Datenverarbeitungen in angemessen begrenzter, strukturierter und transparenter Form verlaufen, kann man bestimmte Verarbeitungskontexte abgrenzen und den Umgang mit personenbezogenen Informationen und Daten sowie dessen Folgen kontext- und akteursbezogen noch näher beschreiben. Erst auf der Basis einer Grundregulierung wird also auf einer zweiten Ebene eine spezifischere Beschreibung möglich, in welchen Kontexten welche Informationen erzeugt und wie sie genutzt werden und welche nachteiligen Folgen die betroffene Person in konkreten Konstellationen überhaupt zu erwarten hat.[58] Auf dieser zweiten Ebene können dann einzelne, bestimmte Themen und Felder ansprechende Freiheitsgewährleistungen weitere Rechtsbindungen und Rechtspositionen an genau der Stelle hergeben, an der ein Schutzbedarf begründbar ist. Vor der Überwachung der Teilnehmer/innen einer Versammlung durch den Verfassungsschutz mit ihren nachteiligen Folgen für die Versammlungsfreiheit beispielsweise gewährt Art. 8 GG, das Grundrecht auf Versammlungsfreiheit, einen substanzhaltigen Schutz. Dieses Grundrecht gibt einen viel anreicherungsfähigeren und stärkeren Schutz her als ein blasses Verfügungsrecht über persönliche Daten. Mit Blick auf die inhaltlich differenzierten, vielfältigen Freiheitsgewährleistungen, seien es diejenigen des GG, seien es die der EU-Charta, kann man auf der zweiten Ebene ein Panorama an Rechtsbindungen und Schutzpositionen entwickeln, die kontext- und gefährdungsspezifisch zugeschnitten werden können.

---

[57] Ausführlich und mit tiefer gehenden Begründungen zu diesen Überlegungen Albers, *Informationelle Selbstbestimmung*, S. 454ff.

[58] Hier geht es um einen Zugriff aus verfassungsrechtlicher Perspektive mit dem Erkenntnisinteresse, eine inhaltlich und dogmatisch angemessene Schutzkonzeption zu entwickeln. Selbstverständlich könnte man aus soziologischer Perspektive und insbesondere ex post soziale Grenzen einer Verarbeitung oder Weiterleitung personenbezogener Daten beschreiben. Aus rechtlicher Perspektive geht es aber darum, inwieweit es verlässliche rechtliche Grenzen im Rahmen einer aus ex ante-Perspektive zu entwerfenden Schutzkonzeption gibt.

Datenschutz umfasst also ein komplexes Bündel von Rechtsbindungen und Rechtspositionen, die sich im Rahmen einer Zwei-Ebenen-Konzeption entfalten lassen.[59] Dieses Bündel ist entwicklungsoffen, d. h. es kann immer wieder an neu entstehende oder erkannte Gefährdungen angepasst werden.[60]

6. Regulierung im Datenschutz

Nur noch kurz soll aufgezeigt werden, dass man auf der Basis eines Bündels grundrechtlicher Rechtsbindungen und Rechtspositionen im Rahmen einer Zwei-Ebenen-Konzeption zu einer sinnvollen Regulierung im Feld des Datenschutzes gelangen kann. Ebenso wie man die Gewährleistungsinhalte in Gestalt mehrdimensionaler und vielschichtiger Bindungen und Schutzpositionen entfalten kann, erlauben die Grundrechtsnormen ein multidimensionales Verständnis der Gesetzesvorbehalte. Rechtsnormen erscheinen dann in vielfältigen Funktionen und vielfältiger Gestalt: Sie können Freiheiten beschränken, aber auch erst herstellen, konkretisieren und ausgestalten. Damit lassen sich angemessene Regulierungskonzepte an die entwickelbaren Gewährleistungsinhalte anknüpfen.

Solche Konzepte erfordern statt einer bloßen Steuerung der Verarbeitungsschritte eine Vielzahl ineinander greifender, nicht zuletzt mit Figuren des Risiko- und des Technikrechts operierende Bausteine. Dazu zählen zum Beispiel Elemente der Systemgestaltung, Anreize oder Vorgaben zur Technikentwicklung und Technikgestaltung, neue Formen der Kenntnis- und Einflussrechte Betroffener, institutionelle Qualitäts- und Kontrollgewährleistungen oder auch institutionalisierte Verfahren, in denen konkrete Schutzstandards für konkrete Komplexe erst noch ausgearbeitet und auf die sich darin ergebenden Schutzerfordernisse zugeschnitten werden.[61] Hier sind in den letzten Jahrzehnten bereits diverse Komponenten entwickelt worden. Den erarbeiteten Bausteinen fehlt jedoch als Gesamtkonzept eine stimmige verfassungsrechtliche Rückbindung und sie stehen bislang oft eher nebeneinander statt passend miteinander verzahnt zu sein. Wie die Bausteine näher auszugestal-

[59] Zur Zwei-Ebenen-Konzeption als gegenstandsbedingter und angemessene Schutzkonzeptionen erst ermöglichender Zugriff, Albers, *Informationelle Selbstbestimmung*, S. 353ff. Die zwei Ebenen ergeben sich mit Blick auf die Charakteristika des Gegenstandsfeldes als Grundmodell. Beim Entwurf näherer Regulierungskonzepte muss man in Abhängigkeit vom Kontext weitere Ebenendifferenzierungen vornehmen.

[60] Zum Erfordernis der präzisen Beschreibung von Gefährdungen siehe ebenfalls, wenn auch mit unterschiedlichen Ansätzen, Gratton, *Understanding Personal Information*, S. 219ff.; Drackert, *Die Risiken der Verarbeitung personenbezogener Daten*.

[61] Gesetzesrecht fungiert somit nicht nur als Instrument, mittels dessen feststehende Schutzpositionen gewährleistet oder auch eingeschränkt werden. Es kann und muss hier u. a. auch dazu dienen, institutionelle Arrangements oder Verfahren zu etablieren, in denen konkrete Schutzerfordernisse in bestimmten Kontexten mit Hilfe angemessener Verfahrensweisen erst noch spezifiziert werden.

ten, zu kombinieren und zu koordinieren sind, hängt nicht zuletzt von dem in den Blick genommenen Regelungsbereich ab. Denn als fundamentale Querschnittsdimension und wegen des engen Zusammenhanges zwischen Daten, Informationen, Wissen, Handlungen und Entscheidungen muss das Datenschutzrecht nicht nur in sich, sondern auch mit den schon vorhandenen sachlichen Rechtsvorschriften abgestimmt werden. Dies weist auf die Differenzierungserfordernisse innerhalb des Datenschutzrechts hin. Etwa muss man gründlich darüber nachdenken, in welchen Hinsichten ein einheitliches Datenschutzrecht für staatliche und private Bereiche sinnvoll ist. Auch unterhalb dieser groben Unterscheidung gibt es eine Vielzahl von Feldern – video- oder zunehmend drohnenüberwachte öffentliche und private Räume, Ärztinnen/Patienten-Beziehungen in Gesundheitssektoren, Arbeitsverhältnisse, soziale Netzwerke, e-commerce, Wearables oder Fitness Tracker –, in denen bestimmte Techniken mit bestimmten Folgen eingesetzt und spezifische Risiken hinsichtlich des Umgangs mit personenbezogenen Daten und Informationen ausgelöst werden. Das heißt nicht, dass man jedes Feld für sich detailliert regeln müsste. Die Lösung der Frage, wann und inwieweit allgemeine Regelungen passen oder wann und inwieweit man sektor- oder technikspezifische Regelungen benötigt, gehört jedoch zu den anspruchsvollsten Herausforderungen, vor denen man im Datenschutzrecht steht.

Abschließend kann ein Bogen zurück zur populären Idee der »Kontrolle« über die »eigenen« Daten geschlagen werden. Man braucht diese Idee nicht für vollkommen obsolet zu halten. Man muss sie aber richtig einordnen. »Kontrolle« beschreibt keine Schutzposition, sondern eher in vereinfachender Form eines der Instrumente, mit denen die anderweitig zu begründenden vielschichtigen Schutzpositionen der Betroffenen im Hinblick auf den Umgang mit personenbezogenen Informationen und Daten in Feldern realisiert werden können, in denen die Idee einer individuellen Kontrolle über Daten in bestimmtem Umfang passt. Im Verhältnis beispielweise zu einem Sozialleistungsträger, bei dem jemand Leistungen beantragt, überzeugt diese Idee nicht, denn Sozialleistungen hängen von der Mitteilung bestimmter Angaben ab und Grenzen der Mitteilungspflichten oder der Weiterleitungsbefugnisse lassen sich besser auf andere Argumente stützen. Im Bereich sozialer Netzwerke, im e-commerce oder bei Wearables und Fitness Trackern kann die Idee aber partiell geeignet sein und sich etwa in gesetzlich verankerten individuellen Gestaltungs-, Unterlassungs-, Löschungs- oder Informationsansprüchen widerspiegeln. Freilich können Nutzer und Nutzerinnen trotzdem komplexe Techniken und Verarbeitungsabläufe, in die Diensteanbieter involviert sind, weder vollständig überschauen noch vollkommen kontrollieren. Die Kontrollidee kann somit selbst hier nicht als erschöpfend begriffen werden. Datenschutz ist weitaus vielschichtiger und inhaltsreicher auszuarbeiten.

7. Schluss

Im Ergebnis ist die »informationelle Selbstbestimmung« dann, aber auch nur dann zukunftsfähig, wenn man sie grundlegend neu konzipiert. Bei Daten, Informationen oder Wissen hat man es mit einem Netzwerk fundamentaler Kategorien zu tun. Informationelle Selbstbestimmung muss als Bündel grundrechtlicher Bindungen und Rechtspositionen begriffen werden, das sich sowohl inhaltlich als auch dogmatisch vielschichtig gestaltet. Dies mündet in vielfältige Regulierungskonzepte, die auch mit einem neuartigen, weniger gesetzeszentrierten Rechtsverständnis kompatibel wären. So verstanden ist das Paradigma der informationellen Selbstbestimmung leistungsfähiger als beispielsweise dasjenige der Privatheit. »Informationelle Selbstbestimmung« würde nicht nur international anschlussfähig, sondern könnte internationale Debatten, die oft ihrerseits in überkommenen Mustern verharren, sogar positiv vorantreiben. Passende rechtliche Ausarbeitungen sind auf die Erkenntnisse anderer Disziplinen angewiesen, etwa auf Erkenntnisse aus der Sozialwissenschaft, der Technikwissenschaft oder der Informationswissenschaft. All das macht die Beschäftigung mit informationeller Selbstbestimmung und mit dem Datenschutzrecht so spannend.

Literatur

Albers, Marion. »Information als neue Dimension im Recht«. In: *Rechtstheorie* 33.1 (2002), S. 61–89.

– *Informationelle Selbstbestimmung*. Bd. 6. Studien zu Staat, Recht und Verwaltung. Baden-Baden: Nomos, 2005.

– »Privatheitsschutz als Grundrechtsproblem«. In: *Privatheit. Strategien und Transformationen*. Hrsg. von Stefan Halft und Hans Krah. Passau: Stutz, 2013, S. 15–44.

– »Umgang mit personenbezogenen Informationen und Daten«. In: *Grundlagen des Verwaltungsrechts. Band II: Informationsordnung, Verwaltungsverfahren, Handlungsformen*. Hrsg. von Wolfgang Hoffman-Riem, Eberhard Schmidt-Aßmann und Andreas Voßkuhle. 2. München: C. H. Beck, 2012, S. 107–234.

– »Zur Neukonzeption des grundrechtlichen ›Daten‹schutzes«. In: *Herausforderungen an das Recht der Informationsgesellschaft: 26. Tagung der wissenschaftlichen Mitarbeiterinnen und Mitarbeiter der Fachrichtung Öffentliches Recht*. Hrsg. von Andreas Haratsch, Dieter Kugelmann und Ulrich Repkewitz. Stuttgart u. a.: Richard Boorberg Verlag, 1996, S. 113–139.

Allen, Anita L. »Privacy As Data Control: Conceptual, Practical, and Moral Limits of the Paradigm«. In: *Connecticut Law Review* 32 (2000), S. 861–875.

Ashby, W. Ross. *An introduction to Cybernetics*. 5. Aufl. London: Chapman & Hall, 1963.

Bentham, Jeremy. *The Panopticon Writings*. Hrsg. von Miran Božovič. London: Verso, 1995.

Britz, Gabriele. »Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts«. In: *Offene Rechtswissenschaft*. Hrsg. von Wolfgang Hoffmann-Riem. Tübingen: Mohr, 2010, S. 561–596.

Buchner, Benedikt. »Die Einwilligung im Datenschutzrecht – vom Rechtfertigungsgrund zum Kommerzialisierungsinstrument«. In: *Datenschutz und Datensicherheit (DuD)* 34.1 (2010), S. 39–43.

– *Informationelle Selbstbestimmung im Privatrecht*. Tübingen: Mohr, 2006.

Drackert, Stefan. *Die Risiken der Verarbeitung personenbezogener Daten: Eine Untersuchung zu den Grundlagen des Datenschutzrechts*. Berlin: Duncker & Humblot, 2015.

Eggers, Dave. *The Circle: A novel*. New York: Knopf, 2013.

Floridi, Luciano. »Information«. In: *The Blackwell Guide to the Philosophy of Computing and Information*. Hrsg. von Luciano Floridi. Malden, Mass.: Wiley-Blackwell, 2004, S. 40–62.

– *Information: A Very Short Introduction*. Oxford und New York: Oxford University Press, 2010.

Fried, Charles. »Privacy (A Moral Analysis)«. In: *Yale Law Journal* 77.1 (1968), S. 475–493.

Gratton, Éloise. *Understanding Personal Information: Managing Privacy Risks*. LexisNexis, 2013.

Heußner, Hermann. »Das informationelle Selbstbestimmungsrecht in der Rechtsprechung des Bundesverfassungsgerichts«. In: *Die Sozialgerichtsbarkeit (SGb)* 7 (1984), S. 279–285.

Hildebrandt, Mireille. »Who is Profiling Who? Invisible Visibility«. In: *Reinventing Data Protection?* Hrsg. von Serge Gutwirth u. a. Dordrecht: Springer, 2008, S. 239–252.

Kafka, Franz. *Der Prozess*. Hrsg. von Max Brod. Berlin: Die Schmiede, 1925.

Kitchin, Rob. *The Data Revolution: Big data, Open Data, Data Infrastructures & their Consequences*. Los Angeles: Sage, 2014.

Ladeur, Karl-Heinz. »Das Recht auf informationelle Selbstbestimmung: Eine juristische Fehlkonstruktion?« In: *Die öffentliche Verwaltung (DöV)* 62.2 (2009), S. 45–55.

Leenes, Ronald E., Bert-Jaap Koops und Paul De Hert, Hrsg. *Constitutional Rights and New Technologies: A Comparative Study*. Bd. 15. Information Technology and Law Series. Den Haag: T. M. C. Asser Press, 2008.

Nissenbaum, Helen. »Privacy as Contextual Integrity«. In: *Washington Law Review* 79.1 (2004), S. 101–139.
– *Privacy in Context*. Stanford: Stanford University Press, 2010.
Orwell, George. *1984: Ein utopischer Roman*. Rastatt und Zürich: Diana Verlag, 1950.
Poscher, Ralf. »Die Zukunft der informationellen Selbstbestimmung als Recht auf Abwehr von Grundrechtsgefährdungen«. In: *Resilienz in der offenen Gesellschaft*. Hrsg. von Hans-Helmuth Gander u. a. Bd. 1. Sicherheit und Gesellschaft. Freiburger Studien des Centre for Security and Society. Baden-Baden: Nomos, 2012, S. 167–191.
Raab, Charles D. und Benjamin J. Goold. *Protecting Information Privacy*. Research Report 69. Equality und Human Rights Commission, 11. Juli 2011. URL: https://www.equalityhumanrights.com/sites/default/files/research-report-69-protecting-information-privacy.pdf (besucht am 14. 10. 2016).
Rouvroy, Antoinette und Yves Poullet. »The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy«. In: *Reinventing Data Protection?* Hrsg. von Serge Gutwirth u. a. Dordrecht: Springer, 2009, S. 45–76.
Saladin, Peter. »Persönliche Freiheit als soziales Grundrecht?« In: *Le droit social à l'aube du XXIe siècle*. Hrsg. von Alexandre Berenstein. Lausanne: Payot, 1989.
Schlink, Bernhard. »Das Recht der informationellen Selbstbestimmung«. In: *Der Staat* 25 (1986), S. 233–250.
Schwartz, Paul. »The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination«. In: *American Journal of Comparative Law* 37 (1989), S. 675–701.
Simitis, Spiros. »Chancen und Gefahren der elektronischen Datenverarbeitung«. In: *Neue Juristische Wochenschrift (NJW)* 24.16 (1971), S. 673–682.
Solove, Daniel J. »Conceptualizing Privacy«. In: *California Law Review* 90.4 (2002), S. 1087–1155.
– »Privacy and Power: Computer Databases and Metaphors for Information Privacy«. In: *Stanford Law Review* 53.6 (2001), S. 1393.
– *The Digital Person*. New York: New York University Press, 2004.
Steinmüller, Wilhelm u. a. *Grundfragen des Datenschutzes - Gutachten im Auftrag des Bundesinnenministeriums*. Bundestagsdrucksache VI/2826. 1971.
Stentzel, Rainer. »Das Grundrecht auf…? Auf der Suche nach dem Schutzgut des Datenschutzes in der Europäischen Union«. In: *PinG - Privacy in Germany* 3.5 (2015), S. 185–190. URL: https://www.pingdigital.de/PinG.05.2015.185 (besucht am 14. 10. 2016).

Trute, Hans-Heinrich. »Verfassungsrechtliche Grundlagen«. In: *Handbuch des Datenschutzrechts*. Hrsg. von Alexander Roßnagel. München: C. H. Beck, 2003, S. 157–187.

– »Wissen – Einleitende Bemerkungen«. In: *Wissen – Zur kognitiven Dimension des Rechts*. Hrsg. von Hans Christian Röhl. Berlin: Duncker & Humblot, 2010, S. 11–38.

Unseld, Florian. *Die Kommerzialisierung personenbezogener Daten*. München: Herbert Utz Verlag, 2010.

Warren, Samuel D. und Louis D. Brandeis. »The Right to Privacy«. In: *Harvard Law Review* 4.5 (1890), S. 193–220.

Wehling, Peter. »Wissensregime«. In: *Handbuch Wissensoziologie und Wissensforschung*. Hrsg. von Rainer Schützeichel. Konstanz: UVK Verlagsgesellschaft, 2007, S. 704–712.

Weichert, Thilo. »Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung«. In: *Neue Juristische Wochenschrift (NJW)* 54.20 (2001), S. 1463–1469.

– »Wem gehören die privaten Daten?« In: *Informatik – Wirtschaft – Recht – Regulierung in der Wissensgesellschaft*. Hrsg. von Jürgen Taeger und Andreas Wiebe. Baden-Baden: Nomos, 2004, S. 281–298.

Westin, Alan F. *Privacy and Freedom*. 6. Aufl. New York: Atheneum, 1970.