Zensus, Digitalisierung und Pfadänderungen im Datenschutz

Marion Albers

I. Volkszählung und pfadabhängiger Datenschutz

1. Die Volkszählung 1983 und die Geburt des Rechts auf informationelle Selbstbestimmung

a) Volkszählung und Massenprotest

Vor genau 30 Jahren ging eine Volkszählung in die Rechtsgeschichte ein. Nach zunächst im Wesentlichen aus Finanzierungsgründen gescheiterten Anläufen beschloss der Bundestag im Jahre 1982 einstimmig das Volkszählungsgesetz 1983[1]. Die darin vorgesehenen Volks-, Berufs-, Gebäude- und Arbeitsstättenzählungen sollten regional tiefgegliedert Grunddaten zur demografischen, wirtschaftlichen und sozialen Struktur der bundesrepublikanischen Gesellschaft erfassen, die aus Sicht der Gesetzgebung für die sachgerechte Erfüllung der zahlreichen Aufgaben des Staates, der Arbeitgeber und Gewerkschaften oder der Wissenschaft unentbehrlich waren. Die Volkszählung 1983 war methodisch als Totalerhebung angelegt. Sie wurde mit Hilfe von Fragebögen und Zählpersonen durchgeführt. Den zu befragenden Personen war eine sanktionsbewehrte Auskunftspflicht auferlegt. Nach § 2 VZG waren unter anderem Name und Anschrift, die rechtliche Zugehörigkeit zu einer Religionsgesellschaft, die Quelle des überwiegenden Lebensunterhalts, die Berufsausbildung, die Stellung im Beruf und im Anstaltsbereich die Eigenschaft als Insasse oder die Zugehörigkeit zum Personal zu erheben. § 5 VZG bestimmte, wer auskunftspflichtig war; §§ 6 und 7 VZG betrafen die Einsetzung ehrenamtlicher Zähler. § 9 VZG enthielt mehrere Ermächtigungen zur Weiterleitung gewonnener Daten, insbesondere auch einen Abgleich der erhobenen Daten mit dem Melderegister.

1 Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung v. 25.3.1982 (BGBl. I, 369). S. hierzu auch *S. Hartmann*, Der Zensus als Prüfstein des Datenschutzrechts, in diesem Band, S. 19 (21 f.).

Der Massenprotest, der sich daraufhin unter dem Stichwort „Volkszählungsboykott" mit Slogans wie „Meine Daten gehören mir" abspielte, war eine der größten Protestbewegungen in der Geschichte der Bundesrepublik. Dieses Phänomen wird nur verständlich mit Blick auf die gesamte damalige gesellschaftliche Situation. Vor dem Hintergrund der technischen Entwicklung automatisierter Datenverarbeitung, damals vor allem Großrechenanlagen, gab es umfassende gesellschaftliche Debatten über die Notwendigkeit des Datenschutzes. „Gläserner Bürger" war ein bekanntes Schlagwort, das nicht nur im Kontext der Volkszählung, sondern auch im Hinblick auf die Beobachtungs-, Auswertungs- und Übermittlungspraxis von Polizei und Verfassungsschutz oder auf den Umgang mit Daten durch private Akteure wie die SCHUFA oder mittels erster Personalinformationssysteme weit verbreitet war.[2] Die Verarbeitung personenbezogener Daten und Informationen war bis dahin ein weitgehend „rechtsfreier Raum", denn im überkommenen Regelungsregime wurden Entscheidungen, Handlungen oder Organisationsformen, nicht aber die Daten-, Informations- oder Wissensdimensionen als rechtsrelevant angesehen.[3] Es fehlten nicht nur strukturierende und begrenzende Vorgaben; der Umgang mit personenbezogenen Daten war auch oft völlig intransparent oder fehlerbehaftet und zugleich der näheren Kenntnis und Einflussnahme der Bürger und Bürgerinnen mangels einschlägiger Rechtspositionen entzogen. Die Volkszählung 1983 hat die in verschiedenen Feldern aufkommenden Datenschutzanliegen in einem Massenprotest kanalisiert. Das Volkszählungsgesetz 1983 war Gegenstand von mehr als tausend Verfassungsbeschwerden.

b) Das Volkszählungsurteil des BVerfG und seine Folgen

Das Volkszählungsurteil vom 15.12.1983 gehört zu den berühmtesten Urteilen des Bundesverfassungsgerichts (BVerfG). Das Gericht sah die im VZG 1983 vorgesehenen Regelungen der Datenerhebung als verfassungsmäßig an, sofern ergänzende verfahrensrechtliche Vorkehrungen für Durchführung und Organisation getroffen werden, während es die Übermittlungsregelungen, insbesondere auch den Melderegisterabgleich, für verfassungs-

2 Aus der damaligen Zeit etwa *N. F. Pötzl*, Total unter Kontrolle, Reinbek bei Hamburg, 1985.

3 Vgl. *M. Albers*, Information als neue Dimension im Recht, Rechtstheorie 2002, 61 (86 f.).

widrig hielt. Revolutionär und außerordentlich folgenreich ist das Urteil wegen der Geburt des Rechts auf informationelle Selbstbestimmung.

Erstmals hat das Gericht hier aus Art. 2 i. V. m. Art. 1 Abs. 1 GG die Befugnis des Einzelnen hergeleitet, „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen".[4] Diese Fassung des Schutzbereichs lässt sich mit Blick auf die vorangegangene Rechtsprechung, deren Kritik und Debatten in der rechtswissenschaftlichen Literatur gut erklären.[5] Zu den Vorläufern des Rechts auf informationelle Selbstbestimmung gehört das Recht auf Achtung der Privatsphäre, das sich ursprünglich auf einen räumlich und thematisch spezifizierten abgeschotteten Bereich bezog, der prinzipiell frei von unerwünschter staatlicher Einsicht bleiben sollte. Die Kritik an dieser Konzeption hob erstens hervor, die „Privatsphäre" könne nur relativ zu den Kenntnis erlangenden Personen oder Institutionen beschrieben werden[6], so dass nicht eine vorgegebene Sphäre, sondern die Fähigkeit des Individuums zu schützen sei, zu entscheiden, wem welche Angaben zugänglich werden.[7] Zweitens wies die Kritik darauf hin, dass es bei der Schutzbedürftigkeit weniger um die private Sphäre geht, in der bestimmte Daten entstehen, sondern darum, welche Informationen aus den Daten gewonnen und wie diese Informationen verwendet werden können.[8] Drittens fanden sich in der Literatur Ausarbeitungen, in denen in Weiterentwicklung des Schutzes einer Privatsphäre und mit Hilfe eines kybernetisch modellierten Zusammenspiels von Handeln und Information ein Selbstbestimmungsrecht des Einzelnen formuliert wurde, „welche

4 BVerfG, Urt. v. 15.12.1983 – 1 BvR 209 u.a./83 = BVerfGE 65, 1 (42 f.).

5 Ausf. Analyse bei *M. Albers*, Informationelle Selbstbestimmung, Baden-Baden, 2005, Open Access unter doi.org/10.5771/9783845258638, S. 151 ff. m. w. N.

6 *W. Steinmüller/B. Lutterbeck/C. Mallmann/U. Harbort/G. Kolb/J. Schneider*, Grundfragen des Datenschutzes. Gutachten im Auftrag des Bundesministeriums des Innern, 1971, BT-Dr. VI/3826, Anlage 1, 51. Ähnlich im Anschluss daran *C. Mallmann*, Datenschutz in Verwaltungs-Informationssystemen, München/Wien, 1976, S. 47 f., 78 f.; *O. Mallmann*, Zielfunktionen des Datenschutzes, Frankfurt a.M., 1976, S. 26; *B. Schlink*, Das Recht der informationellen Selbstbestimmung, Der Staat Bd. 25 (1986), 233 (242).

7 In der US-amerikanischen Debatte formulierte *A. F. Westin*, Privacy and Freedom, 6. Aufl., New York, 1970, S. 42, diesen Gedanken bereits früh. S. auch *Ch. Fried*, Privacy, 77 Yale Law Journal 1968, 475 (482): Privacy "is the *control* we have over information about ourselves" (Hervorh. i. Orig.).

8 *O. Mallmann*, S. 26. Vgl. auch *E. Benda*, Privatsphäre und „Persönlichkeitsprofil", in: Leibholz/Faller/Mikat/Reis (Hrsg.), Menschenwürde und freiheitliche Rechtsordnung: Festschrift für Willi Geiger, Tübingen, 1974, S. 23 (36 f.).

Individualinformationen er unter welchen Umständen an wen abgibt".[9] Es ist nicht schwer zu erkennen, dass das Bundesverfassungsgericht diese Stränge zusammenführt, indem es Bedingungszusammenhänge zwischen Verhaltensfreiheit und informationellem Schutz beschreibt, die individuelle Entscheidungsfähigkeit in den Mittelpunkt rückt und die Relevanz des Verwendungskontexts für die Bedeutung der Daten und die Schutzerfordernisse betont. Das dann im Volkszählungsurteil in bestimmtem Umfang eigenständig entwickelte Recht auf informationelle Selbstbestimmung war als neuartiges Recht geboren.[10]

Neuartig ist insbesondere, dass die auf Verhaltens- und Eigentumsfreiheiten zugeschnittenen Denkmuster und traditionelle Dogmatiken auf die Daten- und Informationsdimension erstreckt werden. Kernelement des Rechts auf informationelle Selbstbestimmung ist ein relativ abstraktes und damit weit reichendes individuelles Entscheidungsrecht, das von der Preisgabe von Daten über deren Verarbeitung bis hin zu deren Nutzung reicht. Den geschützten Personen werden „ihre" persönlichen Daten in normativ maßgeblicher Weise zugeordnet. Dem Gegenstand nach ist dieses im Kern abwehrrechtlich geschützte individuelle Entscheidungsrecht daten- und informationsorientiert, der Reichweite nach ist es prozess- und verarbeitungsorientiert.[11] Aus einem solchen Schutzbereich folgt, dass grundsätzlich jeder Schritt der Verarbeitung personenbezogener Daten als Eingriff in das Recht auf informationelle Selbstbestimmung anzusehen ist. Er bedarf entweder einer Einwilligung oder einer verfassungsmäßigen Rechtsgrundlage.

Mit Blick darauf, dass die rechtliche Bedeutung der Erhebung und Verarbeitung personenbezogener Daten vom Verwendungskontext abhängt,

9 *Steinmüller u.a.*, S. 86 ff., S: 88: Dementsprechend fließt „aus diesem Recht auf Selbstdarstellung das Recht, über die Abgabe von Individualinformationen selbst bestimmen zu können, und zwar hauptsächlich im Hinblick auf den Inhalt der abgegebenen Individualinformation und den Empfänger. Dieses Recht soll hier das informationelle Selbstbestimmungsrecht genannt werden." S. auch *C. Mallmann*, S. 47 ff.

10 Eigenständig gegenüber dem in der Literatur entwickelten informationellen Selbstbestimmungsrecht ist vor allem, dass sich das Entscheidungsrecht nicht nur auf die Ab- oder Preisgabe, sondern auch auf die Verwendung von Daten erstreckt. Insofern ist es – trotz der erläuterten Vorarbeiten – zutreffend, wenn *E. Benda*, Das Recht auf informationelle Selbstbestimmung und die Rechtsprechung des Bundesverfassungsgerichts zum Datenschutz, DuD 1984, 86 (87 f.), schreibt, das BVerfG habe den Schutzgehalt des RiS neu entwickelt.

11 Die Grundrechtsträger haben auch das Recht zu erfahren, von wem und zu welchen Zwecken sie betreffende personenbezogene Daten verarbeitet werden, aber dieses Recht ist im Rahmen des Konzepts grundsätzlich akzessorisch gestaltet.

unterscheidet das Gericht zwischen personenbezogenen Daten, die in individualisierter, nicht anonymisierter Form erhoben sowie in dieser Form genutzt werden, und Daten, die für statistische Zwecke bestimmt sind.[12] Für den ersten, im Volkszählungsurteil nicht entscheidungserheblichen Strang benennt es nur allgemeine Grundsätze: Ausschluss des Zugriffs auf Daten, an denen kein legitimes Interesse besteht, bereichsspezifische und präzise gesetzliche Regelung des Verwendungszwecks, Eignung und Erforderlichkeit der Daten für diesen Zweck, Verbot einer Sammlung personenbezogener Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken, Aufklärungs-, Auskunfts- und Löschungspflichten, Beteiligung von unabhängigen Datenschutzbeauftragten.[13] Für die Datenerhebung und -verarbeitung zu statistischen Zwecken als Hilfe zur Erfüllung öffentlicher Aufgaben werden die Phasen der Erhebung, Aufbereitung und Verarbeitung, in denen die Daten noch personenbezogen sind, und der Umgang mit statistisch aufbereiteten, nicht deanonymisierbaren Daten differenziert. Sofern und solange Daten personenbeziehbar sind, richten sich die Anforderungen des Rechts auf informationelle Selbstbestimmung auf eine möglichst frühzeitige Anonymisierung und effektive Anonymitätswahrung, auf eine möglichst baldige Löschung der Identifizierungsmerkmale, auf organisatorische Abschottungen und Geheimhaltungsverpflichtungen sowie auf eine Beteiligung und Kontrolle der Datenschutzbeauftragten. Statistikerarbeitung und (sonstiger) Verwaltungsvollzug sind im Grundsatz zu trennen.[14] Eine Weiterleitungsermächtigung ist jedenfalls dann verfassungswidrig, wenn der Zweck der Statistikerarbeitung und derjenige der Datenverarbeitung in dem neuen Kontext in dem Sinne miteinander unvereinbar sind, dass die Datenverarbeitung insgesamt widersprüchlichen Maßgaben unterliegt. Daran ist der Melderegisterabgleich gescheitert. Eine Datenverarbeitung für statistische Zwecke darf nicht so gestaltet werden, dass – etwa wegen der Gefahr falscher oder lückenhafter Angaben befragter Personen – die Erfüllung der Funktionen der Statistik gefährdet ist.

Das Volkszählungsurteil hat hiermit einige grundlegende rechtliche Vorgaben für Volkszählungen und Statistikerarbeitungen gesetzt. Noch weit darüber hinaus reichende Folgen kommen ihm aber wegen der Konstitutionalisierung des Umgangs mit personenbezogenen Informationen und Daten aufgrund des Rechts auf informationelle Selbstbestimmung zu. Dieses

12 BVerfGE 65, 1 (45 ff.).
13 BVerfGE 65, 1 (46).
14 BVerfGE 65, 1 (61).

Recht hat, wie erläutert, eine spezifische Schutzbereichsfassung erhalten, die die rechtlich relevanten Denk- und Beschreibungsmuster ebenso wie die Art und Reichweite der Vergesetzlichung entscheidend geprägt hat.

c) Modifikationen des Rechts auf informationelle Selbstbestimmung in der Folgerechtsprechung

Das Recht auf informationelle Selbstbestimmung hat breite Zustimmung, aber auch mehr oder weniger fundamentale Kritik erhalten.[15] In der verfassungsgerichtlichen Rechtsprechung war es lange Zeit in der im Volkszählungsurteil entwickelten Fassung recht fest etabliert. Mittlerweile ist es in bestimmtem Umfang im Fluss.

Zunächst haben sich die genetischen Grundlagen, die sich in der dem Volkszählungsurteil vorausgehenden Rechtsprechung finden, an zentralen Stellen verändert. Das Recht auf Achtung der Privatsphäre ist partiell umgestaltet worden: Nicht primär räumlich oder thematisch abgeschottete Sphären, sondern vor allem die erwartbaren beeinträchtigenden Folgen des Wissens anderer begründen den Schutz.[16] Das allgemeine Persönlichkeitsrecht umfasst, so hat das Gericht in einigen Entscheidungen ab dem Jahr 1998 klargestellt, keine pauschale Verfügungsbefugnis des Einzelnen über die Darstellung der eigenen Person. Vielmehr vermittelt es Schutzpositionen in sozialen Beziehungen, die mit Hilfe einer sozialen Perspektive und einer entsprechend komplexen Argumentation als inhaltlich begründete und begrenzte Positionen zu entwickeln sind.[17] Mit diesen Korrekturen sind tragende Grundlagen des Rechts auf informationelle Selbstbestimmung aufgegeben worden.

---

15 Zur Kritik etwa *Albers*, Selbstbestimmung, S. 156 ff., 280 ff.; *G. Britz*, Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: Hoffmann-Riem, Offene Rechtswissenschaft, Tübingen 2010, S. 561 (566 ff.); *M. Cornils*, Der grundrechtliche Rahmen für ein (trans-)nationales Datenschutzrecht im digitalen Zeitalter, in: Institut für Rundfunkrecht an der Universität zu Köln (Hrsg.), Datenschutz im digitalen Zeitalter – global, europäisch, national, München, 2015, S. 11 (32 ff.); *C. Franzius*, Das Recht auf informationelle Selbstbestimmung, ZJS 2015, 259 (263 ff.); *S. Behrendt*, Entzauberung des Rechts auf informationelle Selbstbestimmung, Tübingen, 2023, S. 49 ff.; *dies.*, Volkszählungen und informationeller Grundrechtsschutz, in diesem Band, S. 175 (184 ff.).

16 S. etwa BVerfG, Urt. v. 15.12.1999 – 1 BvR 653/96 = 101, 361 (382 ff.). Vgl. dazu *M. Albers,* Grundrechtsschutz der Privatheit, DVBl 2010, 1061 (1065 f.).

17 BVerfG, Beschl. v. 14.1.1998 – 1 BvR 1861/93 u. a. = BVerfGE 97, 125 (149); Beschl. v. 24.3.1998 – 1 BvR 131/96 = BVerfGE 97, 391 (403 ff.).

Einige weitere Entscheidungen haben dessen Schutzfunktionen und die Schutzreichweite dann in mehr oder weniger geglückter Weise modifiziert. Markant sind vor allem Entscheidungen, in denen das Gericht sich mit datengetriebenen Technologien und entsprechend umfassenden Datenverarbeitungen auseinandersetzen musste. So lässt es in der Entscheidung zur Rasterfahndung offen, ob das Recht auf informationelle Selbstbestimmung vor der Erhebung jedes einzelnen erfassten Datums schützt, also vollumfänglich auch die Personen, deren Daten lediglich für den automatischen (Massendaten-)Abgleich anhand von Suchbegriffen einbezogen und mangels Treffer gleich wieder automatisch gelöscht werden. Maßgeblich für den Schutz ist, so das Gericht, 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.[18] Andere Entscheidungen stellen heraus, die Gewährleistung informationeller Selbstbestimmung greife „insbesondere, wenn die Entfaltung der Persönlichkeit dadurch gefährdet wird, dass personenbezogene Informationen von staatlichen Behörden in einer Art und Weise genutzt und verknüpft werden, die Betroffene weder überschauen noch beherrschen können".[19]

In der Entscheidung „Recht auf Vergessen I" hat das Gericht das Recht auf informationelle Selbstbestimmung schließlich umgestaltet, soweit es um das Verhältnis zwischen Privaten geht.[20] Hier gewährleistet es kein allgemeines oder gar umfassendes Selbstbestimmungsrecht über die Nutzung der eigenen Daten, sondern „die Möglichkeit, in differenzierter Weise darauf Einfluss zu nehmen, in welchem Kontext und auf welche Weise die eigenen Daten anderen zugänglich sind und von ihnen genutzt werden, und so über der eigenen Person geltende Zuschreibungen selbst substantiell mitzuentscheiden".[21] Diese vor dem Hintergrund des entschiedenen Falles zu verstehende Formulierung bedarf allerdings erkennbar weiterer Ausarbeitung und Konkretisierung, und ebenso kann man kritisieren, dass die

18 BVerfG, Beschl. v. 4.4.2006 – 1 BvR 518/02 = BVerfGE 115, 320 (342 ff.). S: auch die Erörterungen in BVerfG, Beschl. v. 18.12.2018, 1 BvR 142/15– Automatisierte Kennzeichenkontrolle, Rn. 43 ff.

19 BVerfG, Beschl. v. 27. 5.2020 – 1 BvR 1873 u. 2618/13 – Bestandsdatenauskunft II, Rn. 92; Beschl. v. 10.11.2020 – 1 BvR 3214/15 – Antiterrordatei II, Rn. 71.

20 Auch unter Berücksichtigung der Dogmatik „mittelbarer Drittwirkung" hat ein individuelles Entscheidungsrecht über die Preisgabe und Verwendung persönlicher Daten hier immer inhaltliche und dogmatische Probleme bereitet.

21 BVerfG, Beschl. v. 6.11.2019, 1 BvR 16/13 – Recht auf Vergessen I, Leitsatz 3 und Rn. 83 ff.

nunmehr entstandene scharfe Differenz zur Fassung des Schutzbereichs im Bürger/Staat-Verhältnis nicht überzeugt. Denn es sind weniger Eigenheiten des Verhältnisses unter Privaten als vielmehr die Charakteristika des Schutzgegenstandes – Schutz im Hinblick auf den Umgang mit personenbezogenen Informationen und Daten –, die neue Ansätze notwendig machen.

2. Der Zensus 2022 und die Zukunft der Volkszählung

Bereits im Volkszählungsurteil hat sich das BVerfG damit auseinandergesetzt, ob die dort vorgesehene Totalerhebung nebst Fragenkatalog überhaupt geeignet und erforderlich ist, um dem Staat die für künftiges Planen und Handeln benötigten Informationen zu verschaffen. Im Ergebnis hat es weder eine Zusammenführung von Daten aus Registern noch anonymere Erhebungsformen für eine bessere Alternative gehalten. Allerdings hat es betont, dass die Gesetzgebung den Stand der Methodendiskussion in Statistik und Sozialforschung verfolgen muss und hier ebenso wie in anderen Feldern eine Beobachtungs- und Nachbesserungspflicht hat.[22]

Die einsetzbaren Methoden haben sich mittlerweile weiterentwickelt. Zudem hat sich das Umfeld der bereits in Registern oder Datenbasen erfassten und gespeicherten Daten deutlich verbreitert und verändert. Volkszählungen sind trotzdem nicht überflüssig, sondern immer noch eine notwendige komplementäre Absicherung und Ergänzung anderweitig verfügbarer Daten. Im Kontext der Überprüfung des Zensusgesetz 2011 hat das BVerfG mit Blick darauf, dass das GG teilweise unmittelbar an Einwohnerzahlen anknüpft, eine Verpflichtung des Bundes hergeleitet, für die Bereitstellung eines geeigneten und realitätsgerechten Zahlenmaterials zu sorgen.[23] Auch aus Sicht der EU werden umfassende und relativ abgesicherte Daten über die Bevölkerung und die Wohnungssituation für regional-, sozial- und umweltpolitische Maßnahmen benötigt, und dementsprechend sind alle Mitgliedstaaten im Wege der Verordnung über Volks- und Woh-

22 BVerfGE 65, 1 (54 ff.).

23 BVerfG, Urt. v. 19.9.2018 – 2 BvF 1 und 2/15, Rn. 164 ff. Als Ergebnis des Zensus 2011 wurden z. B. die Einwohnerzahlen von Hamburg und Berlin mit Folgen für die Zuweisungen aus dem Länderfinanzausgleich nach unten korrigiert. Für diese Zusammenhänge s. auch *L. Fischer/U. Hufeld*, Zensus und Steuern – Fiskalzensus: Informationsgewinnung und Datenverarbeitung im Finanz- und Steuerrecht, in diesem Band, S. 147 (162 ff., 166 ff.).

nungszählungen aus dem Jahr 2008 verpflichtet, alle zehn Jahre solche Daten bereitzustellen, wie sie im Anhang zur Verordnung noch detaillierter aufgelistet werden.[24] Daten- und Metadatenprogramm sowie die Methodik müssen dabei hinreichend vergleichbar sein, aber Details des Methodeneinsatzes (herkömmliche Zählungen, registergestützte Zählungen, Kombination aus herkömmlichen und/oder registergestützten Zählungen und/oder Stichprobenerhebungen, rollierender Zensus) sind den Mitgliedstaaten freigestellt.[25] Angesichts der Determination durch eine EU-Verordnung ergeben sich Datenschutzvorgaben auch aus unionalem Recht.[26] Nach Art. 4 Abs. 2 der Verordnung bleiben die Datenschutzbestimmungen der Mitgliedstaaten freilich unberührt, so dass sie zusätzlich greifen.

Getragen vom Zensusgesetz des Bundes, dem Zensusvorbereitungsgesetz und Ausführungsgesetzen der Bundesländer hat der Zensus 2022, wie schon der Zensus 2011, auf einen Methodenmix gesetzt.[27] In Teilen ist er registergestützt durchgeführt worden, indem einschlägige Daten unter anderem aus Melderegistern oder bestimmten anderweitigen Datensätzen oberster Bundesbehörden oder der Bundesagentur für Arbeit an das Statistische Bundesamt und die Statistischen Landesämter übermittelt und dort ausgewertet und aufbereitet werden (§§ 5, 7 und 8 ZensusG). Insbesondere das Melderegister ist eine zentrale Quelle, freilich nicht immer aktuell oder vollständig. Die registergestützte Erhebung wurde um primärstatistische Zählungen und Befragungen der Bevölkerung ergänzt. In diesem Rahmen fand neben prinzipiellen Online-Befragungen im Sinne des Online-First-Ansatzes eine Haushaltebefragung auf Stichprobenbasis statt (§§ 11 ff. Zen-

24 Verordnung (EG) Nr. 763/2008 der Europäischen Parlaments und des Rates v. 9.7.2008 über Volks- und Wohnungszählungen (ABl. EU L 218/14). S. zum Programm der Kommission zu übermittelnder statistischer Daten und Metadaten für Volks- und Wohnungszählungen weiter die Verordnung (EU) 2017/712 v. 20.4.2017 (ABl. EU L 105/1). Künftig soll eine EU-Verordnung über europäische Bevölkerungs- und Wohnungsstatistiken mit teilweise neuartigen Vorgaben greifen, s. dazu den Kommissionsvorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Bevölkerungs- und Wohnungsstatistiken v. 20.1.2023 (COM(2023) 31 final).

25 Art. 4 Abs. 1 der VO (EG) Nr. 763/2008.

26 Zur Datenschutzgrundverordnung und der dortigen Öffnungsklausel zu Gunsten der Statistik s. Art. 89 DSGVO.

27 Zur Verfassungsmäßigkeit der Vorschriften über den Zensus 2011 BVerfG, Urt. v. 19.9.2018 – 2 BvF 1 und 2/15, hier auch zur registergestützten Methodik. Zum Eilantrag und zur Verfassungsbeschwerde gegen die Regelung zur Pilotdatenübermittlung im Zensusvorbereitungsgesetz s. *Hartmann*, S. 32 ff. Näher zur Durchführung des Zensus *H. Poppenhäger*, Der Zensus 2022 in Thüringen, ThürVBl. 2022, 1 (4 f.).

susG). Solche ergänzenden Erhebungen sollten Daten beschaffen, wenn Register- oder Behördendaten nicht oder nicht in geeigneter Form vorhanden sind, sowie – neben anderen Maßnahmen zur Gewährleistung der Datenqualität (§§ 21 f. ZensusG) – der Absicherung und Richtigkeitsgewähr der anderweitig erarbeiteten Datenbasis dienen. Datenschutzrechtlich sollen die Differenzierung in einerseits Erhebungsmerkmale und andererseits Hilfsmerkmale, die einen unmittelbaren Personenbezug aufweisen oder herstellen, sowie deren möglichst frühzeitige Trennung und die Löschung der Hilfsmerkmale gewährleisten, dass im Ergebnis Aussagen rein statistischer Natur ohne Personenbezug generiert werden. Entsprechend den Ausführungen des Volkszählungsurteils zum Melderegisterabgleich gibt es ein „Rückspielverbot", d. h. ein Abgleich der erzeugten Daten mit den von den Meldebehörden übermittelten Daten und eine Rückmeldung an diese Behörden ist nach § 21 Abs. 4 ZensusG ausgeschlossen. Aufklärungs- und Unterrichtungspflichten gegenüber den Befragten ergeben sich aus § 17 BStatG. Die Datenverarbeitung wird überwacht von den dafür zuständigen Behörden, insbesondere vom Bundesbeauftragten für Datenschutz und Informationsfreiheit und vom Bundesamt für Sicherheit in der Informationstechnik. Im Ergebnis konnte der Zensus 2022 durchgeführt werden, ohne dass ein größerer Protest aus Datenschutzgründen zu vermerken war.

Für den 2031 anstehenden Zensus ist die vollständige Umstellung auf einen Registerzensus geplant: Alle geforderten Angaben sollen aus vorhandenen Registerdaten hergeleitet werden.[28] Im Hintergrund dieser markanten Weiterentwicklung stehen zum einen neue unionale Vorgaben zur Erarbeitung europäischer Bevölkerungs- und Wohnungsstatistiken, die einen regulatorischen Rahmen für die Zusammenführung demografischer Daten, Migrationsdaten und Volkszählungsdaten liefern und dabei sicherstellen sollen, dass Bevölkerungsstatistiken angesichts der demografischen, migrationsbedingten, sozialen und wirtschaftlichen Veränderungen in der Gesellschaft relevant, kohärent und vergleichbar bleiben.[29] Zum anderen stützt sich die Idee des Registerzensus auf die digitale Transformation

28 Ausf. *C. Grote*, Der Registerzensus – auf dem Weg zu einem zukunftsorientierten Zensus, Statistische Monatshefte Niedersachsen 2022, 690 (690 ff.). S. außerdem *Hartmann*, S. 38 ff.; *S. Dittrich/U. Halfpaap/S. Sattelberger/G. Thiel*, Entwicklung und Digitalisierung des Zensus aus Sicht des Statistischen Bundesamts, in diesem Band, S. 47 (62 ff.).

29 Kommissionsvorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Bevölkerungs- und Wohnungsstatistiken v. 20.1.2023 (COM(2023) 31 final). Zum Rechtssetzungsverfahren s. https://ec.europa.eu/info/

der Verwaltung[30] und einschlägige Gesetze, aus denen man die E-Government-Gesetze von Bund und Ländern[31], das Online-Zugangsgesetz[32] und das Registermodernisierungsgesetz[33] hervorheben kann. Leitideen sind hier das „One-Stop-Government", Online-Portale der Verwaltung und das „Once-only-Prinzip", nach dem die für Verwaltungsleistungen erforderlichen Daten nicht jedes Mal neu eingegeben, sondern aus gespeicherten Beständen abgerufen werden sollen. Aufbauend auf der bereits etablierten Steueridentifikationsnummer führt das Registermodernisierungsgesetz Regelungen zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung ein.[34] Diese soll im Verbund mit Anpassungen zahlreicher vorhandener Register (Anl. zu § 1 RegMoG), institutionellen Vorkehrungen und weiteren Vorgaben einen registerübergreifenden Zugriff auf eingebundene personenbezogene Daten ermöglichen. Für den damit auch konzipierbaren Registerzensus wird im Vorfeld ein Methodentest durchgeführt.[35] Zu den Bedingungen der Möglichkeit eines erfolgreichen Zensus auf einer solchen Basis zählen weitere Fortschritte der Digitalisierung und Modernisierung der Verwaltung, insbesondere auch im Hinblick auf die benötigten Register, deren Datenqualität, Zugänglichkeit und Interoperabilität. Datenumgang und Datenschutz mit passenden und auch innovativen Vorschriften abgesichert und flankiert werden müssen. Ein Novum ist zum Beispiel der „Datenschutzcockpit", der als eine IT-Komponente im Portalverbund eingerichtet werden soll und mittels dessen sich natürliche

law/better-regulation/have-your-say/initiatives/12958-Datenerfassung-Europaische-Bevolkerungsstatistik_de.

30 Dazu *G. Britz/M. Eifert*, Digitale Transformation der Verwaltung, in: Voßkuhle/Eifert/Möllers (Hrsg.), Grundlagen des Verwaltungsrechts Band I, 3. Aufl., München, 2022, § 26; sowie die Beiträge in *M. Seckelmann* (Hrsg.), Digitalisierte Verwaltung - Vernetztes E-Government, 3. Aufl., Berlin, 2024.

31 Auf Bundesebene Gesetz zur Förderung der elektronischen Verwaltung v. 25.7.2013 (BGBl. I, 2749), mit nachfolgenden Änderungen.

32 Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (OZG) v. 14.8.2017 (BGBl. I, 3122, 3138), mit nachfolgenden Änderungen.

33 Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz, RegMoG) v. 28.3.2021 (BGBl. I, 591), mit nachfolgenden Änderungen.

34 S. Art. 1 RegMoG: Identifikationsnummerngesetz (IDNrG). S. dazu auch *Fischer/Hufeld*, S. 145 ff.

35 Gesetz zur Erprobung von Verfahren eines Registerzensus (Registerzensuserprobungsgesetz) vom 9.6.2021 (BGBl. I, 1649). Die Durchführung von Erprobungsverfahren ist auch unionsrechtlich vorgegeben.

Personen Auskünfte zu Datenübermittlungen zwischen öffentlichen Stellen anzeigen lassen können (§ 10 OZG).

3. Relativ nachhaltige Pfadabhängigkeit der Ausgestaltung des Datenschutzes

Trotz der Modifikationen des Rechts auf informationelle Selbstbestimmung in der bundesverfassungsgerichtlichen Rechtsprechung, die für das Verhältnis unter Privaten bisher deutlicher ausfallen als im Hinblick auf den Staat, und trotz der Veränderungen durch die Europäisierung kann man der Ausgestaltung des Datenschutzes eine relativ nachhaltige Pfadabhängigkeit bescheinigen. „Pfadabhängigkeit" bedeutet, dass ein einmal gewähltes Konzept in der Folgezeit im Grundsatz aufrechterhalten und nur schrittweise und in begrenztem Umfang abgewandelt wird.[36] Im deutschen Recht gilt das im Staat/Bürger-Verhältnis für die eingriffsabwehrrechtliche Fassung des Schutzbereichs des Rechts auf informationelle Selbstbestimmung mit seinen Bezügen auf individuelle Entscheidungen, einzelne Daten und Verarbeitungsphasen ebenso wie für die erforderlichen gesetzlichen Grundlagen, die so gestaltet sein müssen, dass sie die in Gestalt eines Eingriffs in diesen Schutzbereich erfassten staatlichen Datenverarbeitungsmaßnahmen hinreichend bestimmt abdecken. Was Volkszählungen angeht, hat das BVerfG in seinem Urteil aus dem Jahr 2018 zum Zensus 2011 in den Passagen zum Recht auf informationelle Selbstbestimmung im Wesentlichen mit Textbausteinen aus dem Volkszählungsurteil 1983 gearbeitet.[37]

Der Zensus als Anlass der Entwicklung dieses Rechts hat sich dagegen hinsichtlich seiner Umsetzung und der eingesetzten Methoden in bestimmtem Umfang bereits verändert und soll mit der Umstellung auf einen Registerzensus noch weitaus stärker reformiert werden. Diese Innovationen betten sich ein in die digitale Transformation der Verwaltung sowie in den Wandel gesellschaftlichen Wissens und der Wissensgrundlagen, zu dem die Digitalisierung führt. Die übergreifenden Entwicklungen, auf die

36 Eine gewisse Pfadabhängigkeit des Datenschutzrechts kann man auch im Unionsrecht feststellen, dazu etwa *R.-D. Veit*, Einheit und Vielfalt im europäischen Datenschutzrecht, Tübingen, 2023, S. 103 ff.

37 BVerfG, Urt. v. 19.9.2018 – 2 BvF 1 und 2/15, Rn. 218 ff. Zur Relevanz von Textbausteinen in der Entscheidungspraxis, die Pfadabhängigkeiten erheblich fördert, s. auch *M. Albers*, Höchstrichterliche Rechtsfindung und Auslegung gerichtlicher Entscheidungen, VVDStRL Bd. 71 (2012), S. 257 (276).

das Stichwort „Digitalisierung" verweist, erfordern wiederum ganz neue Konzeptionen des grundrechtlichen Datenschutzes, die über die bisherigen Modifikationen des Rechts auf informationelle Selbstbestimmung in der verfassungsgerichtlichen Rechtsprechung weit hinausgehen.

II. Digitalisierung und Statistik

1. Digitalisierung und gesellschaftlicher Wandel

Nach den strategischen Zielen der Europäischen Kommission sollen die 2020er Jahre als „digitale Dekade" zu einem erfolgreichen digitalen Wandel Europas beitragen.[38] Was ist mit dem viele Debatten prägenden Schlagwort der „Digitalisierung" gemeint? Die ursprünglich primär informationstechnische Bedeutung bezeichnet die Umwandlung von Objekten analogen Formats in digitale und hier regelmäßig binäre Werte (vor allem 1 und 0 als Dualsystem). Die damit verbundene Technikentwicklung hat von der Datenverarbeitung durch Rechner über die Integration von rechnergestützter Datenverarbeitung (Computertechnik) und Datenübertragung (Nachrichtentechnik) bis hin zu Arrangements untereinander verknüpfter, nach bestimmten Standards und einheitlichen (Meta-)Protokollfamilien arbeitender Netze und Rechner geführt. Von besonderer Bedeutung ist das Internet als eine vielschichtige, im Grundsatz dezentral organisierte, aber differenziert vernetzte und (auch) durch minituarisierte und mobile Hardware gekennzeichnete Infrastruktur, die die Grundlage für zahlreiche Anwendungen und Kommunikationsformate bietet.[39] Aus sozialwissenschaftlicher Sicht hat man es dabei mit soziotechnischen Arrangements zu tun.[40] So hat das ab Anfang der 2000er Jahre beginnende Web 2.0 – das „Mitmach-Internet", das sich unter anderem durch „prosumer"generierte Inhalte aus-

38 S. dazu *Europäische Kommission*, Pressemitteilung v. 19. 2. 2020, Gestaltung der digitalen Zukunft Europas, https://ec.europa.eu/commission/presscorner/detail/de/ip_20_273; sowie Digitaler Kompass 2030: der europäische Weg in die digitale Dekade, und Erklärung zu den digitalen Rechten und Grundsätzen (COM(2021) 118 final), https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_de#relatedlinks.

39 Näher *M. Albers*, Recht & Netz: Entwicklungslinien und Problemkomplexe, in: Albers/Katsivelas (Hrsg.), Recht & Netz, Baden-Baden, 2018, S. 9 (10 ff.).

40 Vgl. *Ch. Fuchs*, Internet and Society. Social Theory in the Information Age, New York, 2008, S. 154 ff.

zeichnet – nicht nur die gesellschaftliche Kommunikation revolutioniert. Gefördert durch Mechanismen wie Lock-in-Effekte, hat es darüber hinaus zu neuen mächtigen Akteuren in Gestalt von Providern oder Betreibern von Suchmaschinen, Plattformen oder Sozialen Netzwerken geführt. Deren Rolle beschränkt sich keineswegs auf „gate-keeper"- Funktionen. Vielmehr beruhen ihre Geschäftsmodelle auf der massenhaften Auswertung und Weiternutzung von Daten, hier nicht allein, aber gerade auch von personenbezogenen Daten, und sie sind mit ihren weit reichenden kommerzialisierungsgetriebenen Aktivitäten Konstrukteure gesellschaftlichen und individuellen Wissens. Einen gleichermaßen deutlichen gesellschaftlichen Wandel bedingt das Web 4.0, das „Internet der Dinge"[41], das aus technischer Sicht die Vernetzung unterschiedlichster physischer Objekte mit dem Internet und darüber vermittelt auch untereinander beschreibt.[42] Die Datafizierung zahlreicher Vorgänge, die massenhafte Generierung von Daten, wachsende Speicher-, Verarbeitungs- und Auswertungsfunktionalitäten im Zusammenhang mit Cloud Computing, Big Data Analytics-Methoden oder Künstlicher Intelligenz steigern die Veränderungen, die die gesamte Gesellschaft betreffen. „Digitalisierung" ist vor diesem Hintergrund zu einem Bündelungsbegriff geworden, der weit über die ursprünglich informationstechnische Bedeutung hinaus auf den gesellschaftlichen, kulturellen oder ökonomischen Wandel zielt, der durch das binäre digitale Format, die dadurch erreichten Datenverarbeitungsmöglichkeiten, Konvergenzen und Zusammenspiele verschiedenster Techniken, umfassende Vernetzungen sowie die neue Rolle von Daten, Informationen, Wissen und veränderten Kommunikationsmustern entsteht.[43] Der beobachtbare Wandel hin zu einer

41 Der Begriff „Internet of Things" wird auf *K. Ashton* zurückgeführt, der damit die Vision eines gerade hinsichtlich der Datenverarbeitung relativ autonom operierenden Systems vernetzter Rechner und Dinge bezeichnete: That „Internet of Things" Thing, RFID Journal 1999, http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf.

42 Wearable Computing, Smart Houses, vernetzte Produktionsprozesse und automatisiert oder autonom fahrende Autos sind anschauliche Beispiele. Deren Funktionieren setzt mehr oder weniger weit reichende Datenverarbeitungen und -infrastrukturen voraus und generiert wiederum zahlreiche Daten, wobei Techniken und Verarbeitungsprozesse möglichst unauffällig im Hintergrund in Handlungsabläufe integriert sein sollen.

43 S. statt vieler die Beschreibungen bei *Ch. L. Geminn,* Deus ex machina? Grundrechte und Digitalisierung, Tübingen, 2023, S. 6 ff.

onl*i*fe"[44]-Welt ist disruptiv. Auch Staat und Verwaltung befinden sich, wie schon angeklungen, in digitalisierungsbedingten und -ermöglichten Transformationen.

2. Regulierungsstrategien vor dem Hintergrund der Digitalisierung

Vor dem Hintergrund dieses gesellschaftlichen Wandels hat die Europäische Kommission im Rahmen ihrer übergreifenden Strategien und Politiken seit Anfang dieses Jahrzehnts in einem umfassenden Paket zur „Gestaltung der digitalen Zukunft Europas" im Sinne einer „digitalen Souveränität"[45] zahlreiche Vorschläge für die Regulierung von Daten, Technologien und Infrastrukturen in Rechtssetzungsverfahren eingebracht.[46] Davon umfasst sind zunächst die inzwischen umgesetzten Verordnungen zu digitalen Märkten[47] und zu digitalen Diensten[48], die eine Regulierung von Torwächtern auch im Hinblick auf deren Umgang mit Daten oder Pflichten von Online-Plattformen etwa hinsichtlich nutzergenerierter illegaler Inhalte betreffen. Darüber hinaus geht es um den Aufbau eines gemeinsamen europäischen Datenraums bzw. sektoral abgegrenzter Datenräume, deren Ausgestaltung das Potenzial der Digitalisierung erschließen soll. Im Rahmen der Datenstrategie werden die datenschutzrechtlichen Vorschriften

44 Begriff bei *L. Floridi* (Hrsg.), The Onlife Manifesto, Cham, 2015; *M. Hildebrandt*, Smart Technologies and the End(s) of Law, Cheltenham 2016, S. 1 ff.

45 Übergreifender zum Begriff der „digitalen Souveränität" s. *P. Gehring*, Datensouveränität versus Digitale Souveränität: Wege aus dem konzeptionellen Durcheinander, in: Augsberg/Gehring (Hrsg.), Datensouveränität, Frankfurt/New York, 2022, S. 19 (19 ff.).

46 Zu den Grundlagen s. insbes. die Mitteilungen der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Aufbau eines gemeinsamen europäischen Datenraums" v. 25.4.2018 (COM(2018) 232 final), „Gestaltung der digitalen Zukunft Europas" v. 19.2.2020 (COM(2020) 67 final), „Eine europäische Datenstrategie" v. 19.2.2020 (COM(2020) 66 final), „Digitalstrategie der Europäischen Kommission. Digitale Kommission der nächsten Generation" v. 30.6.2022 (COM(2022) 4388 final), Weißbuch „Zur Künstlichen Intelligenz - ein europäisches Konzept für Exzellenz und Vertrauen, v. 19.2.2020 (COM(2020) 65 final).

47 VO 2022/1925/EU des Europäischen Parlaments und des Rates über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte) v. 14.9.2022 (ABl. L 265/1).

48 VO 2022/2065/EU des Europäischen Parlaments und des Rates über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste) v. 19.10.2022 (ABl. L 277/1).

– vor allem die Datenschutz-Grundverordnung (DSGVO)[49], die durch die Datenschutzrichtlinie für Polizei- und Strafjustiz[50], durch die e-privacy-Richtlinie[51] und durch weitere sektorspezifische Rechtsakte ergänzt wird – als eine erste grundlegende Säule eingeordnet, die einen „Rahmen für Vertrauen im digitalen Umfeld"[52] liefern soll. Freilich kommen inzwischen eine ganze Reihe weiterer Vorschriften oder Regulierungsvorschläge hinzu. Komplementär und in Abgrenzung zur DSGVO, aber durchaus in Einklang mit der dort in Art. 1 DSGVO festgehaltenen doppelten Finalität ist für nicht-personenbezogene Daten das Leitbild des freien Datenverkehrs festgehalten.[53] Open Data-Konzepte, wie sie zunehmend verankert werden, zielen darauf, dass bestimmte Datensätze und Dokumente des öffentlichen Sektors in offenen, maschinenlesbaren, zugänglichen, auffindbaren und weiterverwendbaren Formaten zur Verfügung gestellt werden und im privaten Sektor, gegebenenfalls gebunden an Bedingungen, weiterverwendet werden dürfen.[54] Dies soll innovative datenbasierte Geschäftsmodelle oder Forschungen, aber auch gemeinsame Government-to-Business-Datennut-

49 VO 2016/679/EU des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG v. 27.4.2016 (ABl. L 119/1).

50 RL 2016/680/EU des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119/89).

51 RL 2002/58/EG des Europäischen Parlaments und des Rates vom 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (ABl. L 201/37). Die Debatten zu einer e-privacy-Verordnung laufen noch.

52 Mitteilung der Kommission „Aufbau eines gemeinsamen europäischen Datenraums" v. 25.4.2018 (COM(2018) 232 final), S. 1.

53 S. dazu die VO 2018/1807/EU des Europäischen Parlaments und des Rates über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union vom 14.11.2018 (ABl. L 303/59), und die Leitlinien der Kommission vom 29.5.2019, die insbesondere die Abgrenzung zu den Regelungen über personenbezogene Daten in der DSGVO betreffen (COM(2019) 250 final). Zur Datenverkehrsfreiheit im Rahmen der doppelten Finalität der DSGVO und zur daraus resultierenden Schutzgutdebatte *J. Botta*, Die Datenverkehrsfreiheit – Ein Beitrag zur Schutzgutdebatte im Datenschutzrecht, in: Kuschel/Asmussen/Golla (Hrsg.), Intelligente Systeme – Intelligentes Recht, Baden-Baden, 2021, S. 251 (251 ff.).

54 RL 2019/1024/EU des Europäischen Parlaments und des Rates vom 20.6.2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (ABl. L 172/56); zur Abgrenzung im obigen Zusammenhang s. Art. 2 Abs. 1 lit h zu deren Anwendungsbereich.

zungen etwa in den Feldern des Umweltschutzes oder der Mobilität ermöglichen. Mit den Bestimmungen der Verordnung über europäische Daten-Governance[55] soll die Etablierung sektoraler Datenräume vorangetrieben werden, etwa der bereits konturierte europäische Raum für Gesundheitsdaten[56]. Unter anderem werden Rahmenbedingungen für den Datenaltruismus geschaffen, bei dem betroffene Personen Daten für benannte (Forschungs-)Zwecke mittels Einwilligung zur Verfügung stellen. In Ergänzung der Richtlinie über offene Daten wird unter bestimmten Bedingungen, zu denen z. B. technische Datenschutzkonzepte zählen, die Weiterverwendung besonders geschützter Daten erleichtert. Neue Institutionen wie Datenmittler, also Dienste für die gemeinsame Datennutzung, die auch im Sinne von „Datentreuhändern" operieren können, und datenaltruistische Organisationen erhalten eine Schlüsselrolle, unter anderem im Hinblick auf die Gewährleistung der Datenschutzrechte involvierter Personen. Ergänzend zur DSGVO und zur Daten-Governance-Verordnung dreht sich die europäische Datenverordnung darum, dass die im Rahmen des Internets der Dinge generierten personenbezogenen und nicht-personenbezogenen Daten durch verschiedene Akteure bereitgestellt, genutzt und kontrolliert werden können, damit das Wissens- und Wertschöpfungspotenzial dieser Daten möglichst gut ausgeschöpft wird.[57] Eine wichtige Rolle im Zusammenhang mit der Digitalisierung und ihrer Regulierung spielen außerdem Regelungen zur Künstlichen Intelligenz.[58]

Die Kommission geht im Grundsatz davon aus, dass sich die vorhandenen Datenschutzvorschriften als eine der Säulen ihrer Daten- und Digitalstrategie relativ nahtlos mit den hinzugekommenen Regulierungen vereinbaren lassen. Bei näherer Analyse gelangt man freilich an verschiedenen

55 VO 2022/868/EU des Europäischen Parlaments und des Rates über europäische Daten-Governance (Daten-Governance-Rechtsakt) v. 30.5.2022 (ABl. L 152/1).

56 Vorschlag der Europäischen Kommission für eine Verordnung des Europäischen Parlaments und des Rates über den europäischen Raum für Gesundheitsdaten v. 3.5.2022 (COM(2022) 197 final).

57 VO 2023/2854/EU des Europäischen Parlaments und des Rates über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datenverordnung) v. 13.12.2023 (ABl. L 1/71).

58 Mit dem Ausgangspunkt des Vorschlags der Europäischen Kommission für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) v. 21.4.2021 (COM (2021) 206 final), einigen Abänderungsvorschlägen im Trilogverfahren und der Einigung im Dezember 2023 werden hierzu in der ersten Hälfte des Jahres 2024 verbindliche europäische Vorgaben verabschiedet.

Stellen zu Bruchstellen, Inkompatibilitäten und Reformerfordernissen. Unabhängig davon wird klar, wie weitreichend das Recht des Umgangs mit personenbezogenen Informationen und Daten in übergreifende Zusammenhänge einzubetten sowie mit anderweitigen Regelungen zu koordinieren ist. Mit Blick auf die Rolle von Daten in der digitalisierten Gesellschaft und mit Blick auf neue normative Leitbilder wie Open Data, Wissens- und Wertschöpfungspotential von Daten oder gemeinsame Datenräume ist es seinerseits auf eine dynamische Novellierung angewiesen.

3. Statistik als Teil gesellschaftlicher Wissensgenerierung

Die Digitalisierung lässt die Statistik, die zentrale gesellschaftliche Wissensgrundlagen liefert und insofern als Teil einer informationellen Infrastruktur der Gesellschaft begriffen werden kann[59], nicht unberührt. Hervorheben kann man einerseits, dass sich die Datenbestände im öffentlichen und im privaten Bereich, auf die unter bestimmten Voraussetzungen im Rahmen der jeweiligen Regulierungen zugegriffen werden kann, mit „Open Data" und „Big Data" als Grundlagen ebenso vervielfachen wie verändern. Zudem stehen verbesserte Rechnerleistungen und Programme, auch solche mit Einsatz Künstlicher Intelligenz, zur Verfügung. Parallel dazu können ganz neue Erfassungs-, Auswertungs- und Erarbeitungsmethoden entwickelt werden.[60] Andererseits wachsen umgekehrt Bedarfe, die an die Statistik herangetragen werden. Zum Beispiel trägt sie selbst zur Weiterentwicklung der Künstlichen Intelligenz bei.[61] Und in der ausdifferenzierten und professionalisierten Verwaltung wird mittlerweile vielfach hochspezielles, möglichst präzises, abgesichertes und aktuelles Wissen benötigt, damit die Auf-

59 *K.-H. Ladeur*, Die Kommunikationsinfrastruktur der Verwaltung, in: Voßkuhle/Eifert/Möllers (Hrsg.), Grundlagen des Verwaltungsrechts, Band I, 3. Aufl., München, 2022, § 21 Rn. 83. Näher auch *P. Prenzel*, „Kann man das überhaupt messen?" – Der Bedarf an detaillierten räumlichen Bevölkerungsdaten in der Geographie am Beispiel kultureller Diversität, in diesem Band, S. 67 (68 ff.).

60 Dazu etwa *P. Struijs/ B. Braaksma/P. J. H. Daas*, Official statistics and Big Data, Big Data & Society 2014 1:1, https://doi.org/10.1177/2053951714538417; *J. Ridgway*, Implications of the Data Revolution for Statistics Education, International Statistical Review 2016, 528 (529 ff.). Außerdem *G. Schaal*, Big Data ergänzte Zensus-Daten: Ein Paradigma für republikanisch inspirierte Governance in der digitalen Konstellation, in diesem Band, S. 89 (93 ff.).

61 Dazu etwa die Stellungnahme der DAGStat, Die Rolle der Statistik in der Künstlichen Intelligenz, 2020.

gaben angemessen erfüllt werden können.[62] Gerade wegen der gesteigerten Breite und Komplexität der Datenbasis und wegen neuartiger Methoden ist die Statistik zunehmend auf passende infrastrukturelle und technische Rahmenbedingungen, auf Datenqualitätssicherungen und auf stete empirische Rückvergewisserungen angewiesen. All das wird von Diskussionen zur Ausgestaltung und partiell neuartigen Regulierung der Statistik begleitet. Es spiegelt sich auch in den Debatten um eine angemessene Erarbeitung und Gestaltung europäischer Bevölkerungsstatistiken und um den Zensus 2031 wider, hinsichtlich derer neue Regelungen neue Inhalte und neue Methoden einführen.[63]

III. Pfadänderungen im Datenschutz

Angesichts der „Digitalisierung" und ihrer Auswirkungen gerade auf Daten, Datenverarbeitungsprozesse und gesellschaftliches Wissen sind Datenschutzerfordernisse als solche aktueller denn je. Aber die Denkmuster und der Zugriff der 80er Jahre des letzten Jahrtausends wirken archaisch. Das zeigen die Herausforderungen und Probleme, mit denen man im Datenschutzrecht kämpft. Dazu zählen unter anderem die Entgrenzung und das Verschwimmen der Grundbegriffe oder die Abgrenzungs- und Koordinationserfordernisse. Das Recht auf informationelle Selbstbestimmung bedarf, auch mit vergleichendem und abstimmendem Blick auf die europäischen Menschen- und Grundrechte, einer Rekonzeptionalisierung, mittels derer sich dem Datenschutzrecht neue Pfade öffnen.

62 S. auch mit weitergehenden Überlegungen *I. Augsberg*, Verwaltung und Empirie, in: Kahl/Ludwigs (Hrsg.), Handbuch des Verwaltungsrechts, Bd. I: Grundstrukturen des deutschen Verwaltungsrechts, Heidelberg, 2021, S. 21 (Rn. 11 ff.). S. außerdem übergreifender zur Veränderung der Wissensgenerierung im Zusammenhang mit Verwaltungsaufgaben *K. Reiling*, Der Hybride. Administrative Wissensorganisation im privaten Bereich, Tübingen, 2016, S. 25 ff. Zum Verhältnis zwischen abgesichertem Wissen und rechtlichen Anforderungen an die Gesetzgebung s. – auch mit kritischen Überlegungen – *M. Seckelmann*, Wissen und Recht: Die Nutzung der Zensus-Daten in der Rechtswissenschaft, in diesem Band, S. 133 (133 ff.).

63 Oben Punkt I. 2. Ausf. dazu auch *B. Aragona/D. Zindato*, Counting people in the data revolution era: challenges and opportunities for population censuses, International Review of Sociology 26 (2016), 367 (367 ff.).

I. Herausforderungen und Probleme im Datenschutz

a) Entgrenzung und Verschwimmen der Grundbegriffe

Zentrale Grundbegriffe, die das Recht auf informationelle Selbstbestimmung ebenso wie das Datenschutzrecht insgesamt prägen, sind die Begriffe der „Daten" und der „personenbezogenen" Daten. Nach der Legaldefinition des Art. 4 Nr. 1 DSGVO sind „personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person") beziehen. Daraus ergibt sich für den Begriff der „Daten" nichts Näheres. Man kann lediglich rückschließen, dass Daten und Informationen als Synonyme eingeordnet werden. Dieses undifferenzierte Verständnis stammt aus den Anfangszeiten des Datenschutzes. Es trägt in durchaus erheblichem Umfang zu verfehlten Ausgestaltungen des Datenschutzrechts bei.[64] Dass man Daten und Informationen deutlich differenzieren muss, wird mit der Digitalisierung und hier nicht zuletzt mit dem damit einhergehenden Phänomen der „Datafizierung" offenkundig. In den neuen Rechtsakten der EU im Kontext der Daten- und Digitalstrategie finden sich dementsprechende Legaldefinitionen: Nach Art. 2 Nr. 1 des Daten-Governance-Rechtsakts sind „Daten" jede digitale Darstellung von Handlungen, Tatsachen oder Informationen sowie jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen auch in Form von Ton-, Bild- oder audiovisuellem Material.[65]

Diese sehr weite Legaldefinition erinnert an die etymologische Wurzel des Begriffs der Daten als etwas „Gegebenes", wonach mit „Daten" immer schon ein weites Spektrum erfasst worden ist: Unterscheidbarkeit von Gegebenheiten in der Wirklichkeit, nach Messeinheiten gemessene physikalische Werte, Zahlen, Buchstaben, Texte, Kommunikationselemente oder binäre digitale Einheiten. Vor diesem Hintergrund machen aus übergreifender Sicht hochabstrakte definitorische Ausgangspunkte Sinn: „[…] the general definition of a datum is: Dd) datum = def. x being distinct from y, where x and y are two uninterpreted variables and the relation of `being distinct', as well as the domain, are left open to further interpretation."[66] Mit welchen weiteren Faktoren diese Ausgangsdefinition aufgefüllt wird,

64 Ausführlich zum Erfordernis der Unterscheidung von Daten und Informationen *Albers*, Selbstbestimmung, S. 88 ff.

65 Ebenso Art. 2 Nr. 1 Datenverordnung.

66 *L. Floridi*, Information. A Very Short Introduction, Oxford, 2010, S. 23.

gestaltet sich je nach historischer Epoche und soziotechnischen Arrangements, je nach Perspektive und je nach Erkenntnisinteressen unterschiedlich; insofern ist der Begriff des Datums immer auch eine Konstruktion.[67] Daten sind nicht vergleichbar mit einem Ball, den man halten und weitergeben könnte; sie sind kein von Vornherein feststehendes physisches Objekt, das dem Recht vorgegeben wäre und dessen Handhabung es regulieren würde. Es ist umgekehrt: „Daten" werden mit Blick auf Regulierungs- und Schutzerfordernisse rechtsspezifisch und sogar rechtsgebietsspezifisch in bestimmtem Umfang erst konstituiert.

Das Datenschutzrecht greift bestimmte Beschreibungsmuster in rechtsspezifischer Weise auf und reformuliert sie aus dem rechtlich begründeten Regulierungs- und Schutzbedarf heraus. So verstanden, adressiert es mit dem Begriff der „Daten" Zeichen oder Zeichengebilde[68], die in einem bestimmten Format auf einem Datenträger gespeichert sind, in Verarbeitungsprozessen und -architekturen verarbeitet werden und in sozialen Kontexten informationelle Bedeutung gewinnen können. Dementsprechend dreht es sich nicht allein um Daten, sondern immer um ein Netzwerk miteinander zusammenhängender Elemente, zu dem Daten, Informationen, Wissen, Verarbeitungsprozesse und Verarbeitungskontexte gehören.[69] In solche Zusammenhänge bettet sich auch der Bezug auf gerade „personenbezogene" Daten ein.

Die „Personenbezogenheit" von Daten bedeutet nach der Legaldefinition in Art. 4 Nr. 1 DSGVO, dass Daten und Informationen mit ihren Aussagegehalten auf eine identifizierte oder identifizierbare natürliche Person verweisen.[70] Sie ist in den datenschutzrechtlichen Regelungen und, wie für die Daten- und Digitalstrategie der EU erläutert, in den Abgrenzungen zu

67 Zum Konstruktionscharakter auch *S. Leonelli*, The Philosophy of Data, in Floridi (Hrsg.), The Routledge Handbook of Philosophy of Information, Abingdon, 2016, S. 192 (192 ff.). Vgl. weiter *R. Kitchin*, The Data Revolution, Thousand Oaks, 2014, S. 2 ff.; *D. Rosenberg*, Data before the Fact, in: Gitelman (Hrsg.), "Raw data" is an oxymoron, Cambridge, Mass., 2013, S. 33 (36).

68 Daten und Zeichen sind dabei nicht deckungsgleich. Zu Relationalität und Verweisungsfunktion von Zeichen vgl. *Ch. W. Morris*, Foundations of the theory of signs, Chicago, 1938; *U. Eco*, Zeichen. Einführung in einen Begriff und seine Geschichte, Frankfurt a. M.,1977, S. 25 ff.

69 *M. Albers*, Informationelle Selbstbestimmung als vielschichtiges Bündel von Rechtsbindungen und Rechtspositionen, in: Friedewald/Lamla/Roßnagel (Hrsg.), Informationelle Selbstbestimmung im digitalen Wandel. Wiesbaden, 2016, https://doi.org/10.1007/978-3-658-17662-4_2, S. 11 (23 ff.).

70 S. weiter EG 26 zur DSGVO.

anderen Rechtsregimen ein ausschlaggebendes Kriterium. Die Idee, dass der Personenbezug ein hinreichendes und abschließendes Merkmal zur Begründung des Schutzbedarfs dieser Personen ist, stammt allerdings wiederum aus den Anfangszeiten des Datenschutzes. Das Volkszählungsurteil hatte mit einer überschaubaren, geradezu schlichten Konstellation zu tun: ein auszufüllender Fragebogen, Identifikatoren wie Name und Adresse sowie bestimmte und begrenzte Angaben über Wohnverhältnisse oder Beruf, die über den Fragebogen als Datenträger und den Zusammenhang der Fragen ohne weiteres den identifizierbaren Personen zuordbar waren. Heute ist demgegenüber klar, wie anforderungsreich der Begriff der Personenbezogenheit ist und wie entgrenzend er wirkt.

„Personenbezogenheit" ist weder eine intrinsische Eigenschaft von Daten noch haftet sie ihnen wie ein Etikett an. Sie ist Ergebnis einer sinngehaltszuschreibenden Leistung. Zum einen muss beantwortet werden, welche Identifikatoren eine Person spezifizieren. Zum anderen gibt es im Ansatz ein sehr breites Spektrum von sachlichen Angaben, die mit einer Person verknüpft werden können und dann etwas über sie aussagen. Vor- oder Zusatzwissen kann es ermöglichen, Daten, die für sich genommen nicht ohne Weiteres zuordbar sind, mit einer bestimmten Person in Verbindung zu bringen. Hinzu kommt, dass das Datenschutzrecht wegen seiner Schutz- und Steuerungsziele nicht erst und nur die Verarbeitungsschritte erfasst, bei denen eine unmittelbare Verknüpfung zwischen Daten und bestimmten Personen tatsächlich besteht. Solche Verknüpfungen, das dadurch entstehende Wissen über eine Person und dessen potenzielle Verwendung sollen gegebenenfalls gerade verhindert werden.[71] Möglichkeiten, dass im Laufe der Zeit mit zusätzlichen Verarbeitungsschritten oder in anderen Kontexten Verknüpfungen hergestellt werden, müssen daher in bestimmtem Umfang mitbedacht werden. Umgekehrt kann es nicht ausreichen, dass Daten von irgendwem irgendwann irgendwie mit einer Person verknüpft werden könnten, denn sonst wären sämtliche Daten als personenbezogen einzustufen; man landete bei einem „law of everything"[72]. Außerhalb reiner Identifizierungsdaten erfordert die Antwort auf die Frage, welche Daten sich auf eine Person beziehen, erstens (auch) eine Beschreibung der Qualität, die die Beziehung zwischen den Daten und der betroffenen Person

71 Vgl. auch *T. Herbst*, Was sind personenbezogene Daten?, NVwZ 2016, 902 (904).

72 *N. Purtova*, The law of everything. Broad concept of personal data and future of EU data protection law, Law, Innovation, and Technology 2018, DOI:10.1080/17579961.2018.1452176.

haben muss, und zweitens eine Beschreibung der Kontexte, in denen sich der Umgang mit Daten und Informationen vollzieht. In beiden Hinsichten kommen wertende Beurteilungen und Wahrscheinlichkeitsannahmen oder auch Prognosen ins Spiel. Insofern ist die Personenbezogenheit weder in isolierter Betrachtung eines einzelnen Datums noch mit Blick auf die einzelne Information, sondern im übergreifenden Kontext, unter Umständen je nach Beziehung und Akteur relativ sowie mit Hilfe wertender Entscheidungen vor dem Hintergrund der Schutzgüter und -erfordernisse zu bestimmen.[73] So lassen sich auch die Konstellationen erschließen, die mit dem Internet der Dinge häufiger auftreten: Daten verweisen in verschiedener Weise auf mehrere Personen, so dass Zuordnungen und Rechtspositionen ausführlicher begründet werden müssen.

Die Überlegungen zeigen, dass der Begriff der Personenbezogenheit den individuellen Schutzbedarf zum einen nicht erschöpfend beschreibt. Die häufig zitierte Ausführung des Bundesverfassungsgerichts im Volkszählungsurteil, es gebe „unter den Bedingungen der modernen Datenverarbeitung kein ‚belangloses Datum' mehr",[74] ist insofern richtig, als auch Daten, die für sich genommen belanglos erscheinen, in einem bestimmten Kontext oder in Verknüpfung mit anderen Daten einen Informationsgehalt erhalten können, mit Blick auf den eine Person schutzbedürftig ist. Das heißt aber nur, dass Daten nicht von Vornherein aus dem Schutz herausfallen dürfen. Relativ zu einem bestimmten Kontext ist eine Beschreibung personenbezogener Daten und Informationen oder von Verarbeitungsvorgängen als „trivial" oder „belanglos" ebenso möglich wie die Feststellung eines gesteigerten Schutzbedarfs. Allein die Tatsache, dass Daten oder Informationen auf eine Person verweisen, kann jedenfalls keine umfassendpauschale „Verfügungsbefugnis" dieser Person begründen; Schutzerfordernisse und Rechtspositionen brauchen ein komplexeres Fundament. Zum anderen wird auch deutlich, dass der Fokus personenbezogener Daten den individuellen Schutzbedarf nicht umfassend abdeckt. Etwa können

73 S. auch zur Weite des Begriffs „personenbezogene Daten" s. a. etwa *EuGH,* Urt. v. 19.10.2016, C-582/14, Rn. 32 ff. – dynamische IP-Adressen; Urt. v. 20.12.2017, C-434/16, Rn. 27 ff. – Prüfungsantworten und -anmerkungen; Urt. v. 22.6.2023, C-579/21, Rn, 41 ff. – Logdateien; Urt. v. 9.11.2023, C-319/22, Rn. 44 ff. – Fahrzeug-Identifizierungsnummern; alle abrufbar unter http://curia.europa.eu.

74 BVerfGE 65, 1 (45). S. auch zur Reformulierung in der jüngeren Rspr. des Gerichts BVerfG, Beschl. v. 18.12.2018, 1 BvR 142/15, Rn. 38: „Insofern gibt es unter den Bedingungen der elektronischen Datenverarbeitung kein schlechthin, also ungeachtet des Verwendungskontextes, belangloses personenbezogenes Datum mehr."

auch die statistische Bündelung von Daten oder Verfahren rechnergestützter Auswertung großer Massen statistischer Daten im Falle bestimmter Anwendungen der Ergebnisse mit nachteiligen oder diskriminierenden Effekten für Menschen(gruppen) problematisch sein und Regelungs- oder Schutzerfordernisse hervorrufen.[75] Unabhängig davon erscheinen die folgenreichen Unterschiede, die man hinsichtlich des Regelungsbedarfs bei personenbezogenen Daten einerseits und nicht-personenbezogenen Daten andererseits gemacht hat, wegen der Komplexität des „Personenbezugs" und angesichts der (Re-)Individualisierungsmöglichkeiten, die mit Blick auf die Verfügbarkeit und automatisierte Verknüpf- und Auswertbarkeit großer Datenmengen technisch mittlerweile entscheidend gesteigert werden[76], als ein zu rigider Ansatz. Stattdessen kommt es auf ein überzeugendes Zusammenspiel zwischen Datenschutzrecht und anderweitigen Rechtsregimen an. Das kann zugleich die Probleme abmildern, die man mit „personenbezogenen Daten" als ein rechtsgebietskonstituierendes Element des Datenschutzrechts hat.

b) Abgrenzungserfordernisse und Koordinationsbedarf

Mit dem Bezug auf personenbezogene Daten reicht das Datenschutzrecht weit. Internet und Digitalisierung haben deutlich gemacht und zudem weiter dazu geführt, dass sich viele Rechtsfragen unter dem Fokus des Umgangs mit personenbezogenen Daten als datenschutzrechtliche Rechtsfragen formulieren lassen. Dementsprechend hat die Rechtsprechung damit

75 *M. Schuler-Harms*, Die kommerzielle Nutzung statistischer Persönlichkeitsprofile als Herausforderung für den Datenschutz, in: Sokol (Hrsg.), Living by numbers: Leben zwischen Statistik und Wirklichkeit, Düsseldorf, 2005, S. 5 (10 ff.); *I. S. Rubinstein/R. D. Lee/P. M. Schwartz,* Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches, The University of Chicago Law Review, Bd. 75 (2008), 261 (262 ff., hier auch zur Verflochtenheit sach- und personenbezogener Suchmuster); *P. Richter*, Big Data, Statistik und Datenschutz-Grundverordnung, DuD 2016, 581 (582 ff.).

76 Zur übergreifenden Debatte, die sich vor allem auf Big Data- und Data-Mining-Verfahren in der Privatwirtschaft, u. a. bei den großen Online-Plattformen, Online-Suchmaschinen oder Data-Brokern, bezieht, s. *É. Gratton*, Understanding Personal Information: Managing Privacy Risks, LexisNexis, 2013, S. 21 ff.; *P. M. Schwartz/D. Solove,* The PII-Problem: Privacy and a New Concept of Personally Identifiable Information, New York University Law Review 86 (2011), 1814 (1815 ff.). Soweit es sich um Einzelangaben aus Bundesstatistiken handelt, ordnet § 21 BStatG als gesetzliche Regulierung ein Reidentifizierungsverbot an.

zu kämpfen, dass das Datenschutzrecht überkommene rechtsgebietsspezifische Regelungen mit neuen Mustern überlagert, ohne dass diese immer passend erscheinen oder dass es eine hinreichende Abstimmung verschiedener Muster gegeben hätte. Vor allem die Zivilrechtsprechung hat das Recht auf informationelle Selbstbestimmung in traditionellen Konstellationen etwa des Äußerungs- oder Informationsrechts zunächst häufig schlicht ausgeblendet, obwohl man es mit Blick auf Gewährleistungsbereich und Drittwirkung hätte thematisieren müssen. Inzwischen setzt sie sich, ebenso wie das BVerfG in der Recht auf Vergessen I-Entscheidung[77], damit auseinander, wie man den Anwendungsbereich des Datenschutzrechts und denjenigen des Äußerungsrechts gegeneinander abgegrenzt und wie man beide Rechtsregime miteinander koordinieren kann.[78] Solche Abgrenzungs- und Koordinationserfordernisse gibt es an vielen Stellen, zum Beispiel auch im Verhältnis von Datenschutzrecht und Allgemeinem Verwaltungsverfahrensrecht oder überkommenen statistikrechtlichen Vorgaben.

Die Entwicklung stimmiger Lösungen ist nicht abgeschlossen und bedarf ohnehin stets einer dynamischen Fortentwicklung. In ihrem Rahmen wird erstens deutlich, dass es immer schon unter bestimmten Aspekten verstreute und spezifisch zugeschnittene daten- und informationsrechtliche Vorgaben gegeben hat und dass das Datenschutzrecht in ein übergreifendes Informations- und Wissensrecht eingebettet werden muss, dessen Regelungen auch, aber keineswegs allein auf einen individualrechtlichen Schutz ausgerichtet sind. Zweitens müssen datenschutzrechtliche Konzeptionen im Zusammenspiel mit anderen Rechtsregimen, die bereits Schutzmechanismen bereitstellen, (weiter-)entwickelt werden. Überzeugende Abgrenzungen und eine überzeugende Koordination gelingen jedoch nur im Blick auf Schutzgüter und Schutzmechanismen der in Rede stehenden Rechtsregime.[79] Die insofern auftauchenden Herausforderungen verweisen somit

77 BVerfG, Beschl. v. 6.11.2019, 1 BvR 16/13 – Recht auf Vergessen I, Leitsätze 2 und 3 sowie Rn. 79 ff.

78 Grundlegend dazu *A. Schimke,* Das Medienprivileg als Koordinationsmechanismus. Zum Verhältnis von Datenschutz- und Äußerungsrecht im Internet, in: Albers/Katsivelas (Hrsg.), Recht & Netz, Baden-Baden, 2018, S. 155 (bes. 157 ff.); im Anschluss daran s. auch *S. Michel*, Bewertungsportale. Schnittstellen, Pfadabhängigkeiten und Konkurrenzprobleme des äußerungsrechtlichen und datenschutzrechtlichen Persönlichkeitsschutzes, Tübingen, 2022, S. 30 ff. Zum Blick auf andere Rechtsgebiete in Big Data-Zusammenhängen *M. Oostveen*, Protecting Individuals Against the Negative Impact of Big Data, Amsterdam, 2018, S. 180 ff.

79 Dazu die Überlegungen bei *Schimke,* S. 155, die die Einsatzbereiche des Äußerungs- und des Datenschutzrechts mit Blick auf Schutzinteressen, Schutzmechanismen und

zurück auf die Notwendigkeit einer Neukonzeption des Rechts auf informationelle Selbstbestimmung.

2. Wege zu Rekonzeptionalisierungen

Wege zu Rekonzeptionalisierungen können in diesem Rahmen nur noch angerissen werden. Wenn man danach sucht, liegt es nahe, den Blick auch auf die europäischen Vorgaben zu richten. Das empfiehlt sich zunächst wegen der mittlerweile weitreichenden Europäisierung, die, wie erläutert, auch den Bereich von Statistiken und Volkszählungen betrifft. Nicht selten bereitet die Antwort darauf, unter welchen Voraussetzungen und inwieweit welches Grundrechtsregime im Falle einer sekundärrechtlichen Determination nationalen Rechts greift, erhebliche Schwierigkeiten. Die dazu einschlägige Rechtsprechung von EuGH und BVerfG divergiert in bestimmten Punkten und wirft noch jeweils weitere Klärungserfordernisse auf[80]; zudem sind viele sekundärrechtliche Vorgaben hinsichtlich ihrer maßgeblichen Determinationsdichte interpretationsbedürftig. Eine gewisse Konkordanz der Gewährleistungsinhalte kann diese Schwierigkeiten zumindest abmildern. Mit ihr ist deshalb und auch aus anderen Gründen[81] zu rechnen. Unabhängig davon kann ein Rechtsvergleich dahingehend, ob europäische Grundrechtsgewährleistungen bessere Lösungen bieten, produktiv sein.

Als moderne Charta zeichnet sich die Charta der Grundrechte der Europäischen Union dadurch aus, dass sie dem Datenschutz ein eigenes Grundrecht widmet. Nach Art. 8 Abs. 1 GRCh hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Art. 8 Abs. 2 und 3 GRCh geben weitere teils maßgaben-, teils vorbehaltsetzende Vorgaben her: Personenbezogene Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder aufgrund einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und eine Berichtigung der Daten zu erwirken.

Eignung des jeweiligen Instrumentariums gegeneinander abzugrenzen und zu koordinieren sucht.

80 Näher dazu *Veit*, S. 244 ff. m. w. N. S. außerdem *H. Ruschemeier*, Grundrechtsdogmatische Fragen des Zensus im Mehrebenensystem, in diesem Band, S. 109 (125 ff.).

81 Insbesondere bezieht das BVerfG die Unionsgrundrechte in methodisch spezifizierter Weise als „Auslegungshilfe" in die Interpretation der Grundrechte des GG ein, vgl. BVerfG, Beschl. v. 6.11.2019, 1 BvR 16/13 – Recht auf Vergessen I, Rn. 60 ff.

Die Einhaltung dieser Vorschriften soll von einer unabhängigen Stelle überwacht werden.

Hinsichtlich des Schutzguts bleibt der Normtext des Art. 8 Abs. 1 GRCh vage. Trotzdem ergibt sich der Gewährleistungsgehalt weder lediglich mit Blick auf die Schutzgüter des Art. 7 GRCh[82] noch ist er umstandslos im Sinne eines Rechts auf informationelle Selbstbestimmung in der Fassung zu verstehen, die das BVerfG im Volkszählungsurteil entwickelt hat[83]. In seiner offenen Fassung liegt angesichts der Anforderungen, die der Gegenstand - Schutz im Hinblick auf den Umgang mit personenbezogenen Informationen und Daten - stellt, gerade seine Stärke. Die Formulierung „Recht auf Schutz" macht zunächst deutlich, dass es einer Ausgestaltung durch Recht bedarf. Das Grundrecht auf Datenschutz ist normgeprägt. Das bedeutet nicht, dass es gar keine grundrechtlichen Maßstäbe für die Rechtsetzung, -anwendung und -auslegung gäbe.[84] In bestimmtem Umfang lassen sich Maßstäbe aus Art. 8 Abs. 2 GRCh folgern.[85] Allerdings muss man berücksichtigen, dass sich dort eine eher unsystematische Zusammenstellung mehrerer Elemente unterschiedlicher Provenienz findet, die sich in der Datenschutzrichtlinie widerspiegelten, als Kernelemente eingeordnet und aufgegriffen wurden[86]. Schon da es nicht um eine Verfestigung bestimmter Figuren aus der damaligen Zeit gehen kann, ist es interpretatorisch sinnvoll, dass man die Funktionen, die die jeweiligen Elemente zur Gewährleistung eines Datenschutzes erfüllen, herausarbeitet und nähere Gewährleistungsinhalte funktional präzisiert und weiterentwickelt. Die Funktion der Maßgabe einer Verarbeitung personenbezogener Daten nach Treu und Glauben für festgelegte Zwecke und auf der Basis einer Einwilligung oder gesetzlich

82 So aber *R. Stentzel*, Das Grundrecht auf …?, PinG 2015, 185 (189 f.), vor dem Hintergrund der Vagheit des Art. 8 Abs. 1 GRCh.

83 Dem steht nicht nur der eigenständig gestaltete Normtext, sondern auch die Entstehungsgeschichte entgegen, im Rahmen derer eine an die bundesverfassungsgerichtliche Schutzbereichsbeschreibung angelehnte Fassung ausdrücklich verworfen wurde, s. *P. Hustinx*, EU-Datenschutzrecht: Die Überprüfung der Richtlinie 95/46/EG und die vorgeschlagene Datenschutz-Grundverordnung, https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_de, S. 20 f.

84 Verfassungsrechtliche Maßstäbe gibt es schließlich auch bei der vollständig rechtskonstituierten Eigentumsgewährleistung; sie zu entwickeln, ist lediglich anspruchsvoll.

85 S. auch *N. Marsch*, Das europäische Datenschutzgrundrecht, Tübingen, 2018, S. 130 f., 134 ff.

86 Vgl. zur Entstehungsgeschichte *Hustinx*, S. 20 f.

geregelten legitimen Grundlage besteht darin, einen Rechtsrahmen zu verlangen, über den die Verarbeitung personenbezogener Daten unter Berücksichtigung involvierter Interessen grundlegend begrenzt, problemorientiert und sachgerecht strukturiert sowie möglichst transparent gestaltet wird. Die Verankerung von Rechten auf Auskunft und Berichtigung stellt klar, dass Datenschutz nicht ohne schutzbedarfsgerechte Kenntnis-, Partizipations- und Einflussmöglichkeiten der betroffenen Personen zu gewährleisten ist. Das Erfordernis der Überwachung durch eine unabhängige Stelle verweist darauf, dass es wegen der gegenstandsbedingten Leistungsgrenzen individuell-subjektiver Rechte auch institutioneller Gewährleistungs- und Kontrollmechanismen bedarf.[87] Bei gegenstandsgerechter Konkretisierung des Art. 8 GRCh lässt sich im Ergebnis ein Bündel vielschichtiger und vielfältiger Anforderungen entwickeln, die ein komplexes und sich dynamisch weiterentwickelndes Gefüge unterschiedlicher Normen bedingen, welche untereinander und mit anderweitigen Regelungen verzahnt und abgestimmt sein müssen. Auf der Grundlage, die durch die Regulierung nach Maßgabe dieser Anforderungen entsteht, können andere Verbürgungen mit ihren Freiheits- und Schutzversprechen hinzutreten. Nicht nur aus Art. 7 GRCh, sondern auch aus anderen unter Umständen einschlägigen Gewährleistungen können spezifische inhaltliche Vorgaben für den Umgang mit personenbezogenen Informationen und Daten hergeleitet werden.

Damit sind zugleich Eckpunkte hin zu einer angemessenen Rekonzeptionalisierung des Rechts auf informationelle Selbstbestimmung umrissen. Die zu den Grundrechten des Grundgesetzes entwickelte Dogmatik ist so weit ausgebaut, dass grundrechtliche Bindungen und Rechtspositionen im Hinblick auf den Umgang mit personenbezogenen Informationen und Daten gegenstandsgerecht ausgearbeitet werden können.[88] In dem zunehmenden Zusammenspiel europäischer und nationaler Grundrechtsgewährleistungen kann so ein passendes Fundament entwickelt werden, das neue Regelungen im Zuge der Digitalisierung, die sich auch auf Volkszählungen erstrecken, angemessen zu steuern und zu tragen geeignet ist.

87 Dazu auch *A. Mantelero*, Beyond Data, The Hague, 2022, Open Access unter https://link.springer.com/book/10.1007/978-94-6265-531-7, S. 3 ff.

88 Ausf. mit Vorschlägen zu einer Neukonzeption des Rechts auf informationelle Selbstbestimmung *Albers*, Selbstbestimmung, S. 353 ff.

IV. Schluss

Das Volkszählungsurteil und das dort entwickelte Recht auf informationelle Selbstbestimmung waren zu ihrer Zeit revolutionär. Sie haben die Ausgestaltung des Datenschutzrechts nachhaltig geprägt. Im Rückblick ist freilich deutlich, dass die zu entscheidende Konstellation, die Volkszählung, viel zu simpel gestaltet war und nicht genügend Probleme ins Spiel brachte, als dass sie die Herausforderungen und die Regulierungs- und Schutzerfordernisse hinreichend hätte sichtbar machen können, die grundrechtliche Bindungen und Rechte im Hinblick auf den Umgang mit personenbezogenen Informationen und Daten mit sich bringen. Europäisierung und Digitalisierung machen es unausweichlich, bieten aber zugleich die Chance, das Recht auf informationelle Selbstbestimmung zu rekonzeptionalisieren. Damit könnten auf die Rechtsfragen, die sich mit Blick auf die anvisierte Reform des Zensus 2031 teilweise in neuer Weise stellen, passende Antworten gefunden werden. 40 Jahre Volkszählungsurteil markieren somit keine Entwicklung, die man heute als abgeschlossen feiern könnte. Im Gegenteil fängt eine umfassende Arbeit am Recht wieder an.