

# Diskussionsbericht – Zu Vorfragen der Datenbereitstellung

Peer Sonnenberg\*

A. Einleitung	129
B. Gang der Diskussion	130
C. Fazit und Einordnung	137

## A. Einleitung

Die Tagung wurde beendet mit einer Schlussdiskussion. Es waren alle Tagungsteilnehmer aufgerufen, die gehörten Beiträge Revue passieren zu lassen und Fragen sowohl an einzelne Speaker zu ihren Vorträgen als auch an die offene Runde zu der allgemeinen Thematik zu stellen. Die Moderation übernahm *Tristan Barczak*<sup>1</sup>.

Im Laufe der Diskussion hat es im Wesentlichen drei thematische Schwerpunkte gegeben: Eine Datenbereitstellungspflicht, datenschutzrechtliche Kollisionen mit dem Datenrecht und die Regelungen zu Datenaltruismus und Datenvermittlungsdiensten gerade im Verhältnis zum Helferrecht. Dabei hatten alle drei Themen gemein, dass sie sich um die Bereitschaft und den rechtlichen Rahmen des Teilens von Daten (egal ob mit Privaten oder der öffentlichen Hand) drehten, sodass sie im Laufe der Diskussion zu einem einheitlichen Gespräch der Tagungsteilnehmer und Referenten verwoben werden konnten.

---

\* Peer Sonnenberg ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Öffentliches Recht, Medien- und Informationsrecht an der Universität Passau.

1 Prof. Dr. Tristan Barczak ist Inhaber des Lehrstuhls für Öffentliches Recht, Sicherheitsrecht und das Recht der neuen Technologien an der Universität Passau.

## B. Gang der Diskussion

Barczak, der sich eingangs bei den Referenten und insbesondere bei dem Organisator Kai von Lewinski<sup>2</sup> bedankte, gab sodann die Diskussion in die offene Runde frei. Der erste Beitrag kam von David Bomhard<sup>3</sup> gerichtet an Moritz Hennemann<sup>4</sup>: Bomhard habe da immer den Gesetzgeber im Blick, der die Vorstellung hätte, man könne einfach den „Datenhahn“ aufdrehen und dann könne der Gesetzgeber alles regeln mit den Daten. Hier rekurriert er auf die sehr bildliche Darstellung einer „Datenautobahn“ von Hennemann<sup>5</sup>: Sähe man Daten als das die Autos betreibende Öl an<sup>6</sup>, dann sei mit dem Vorhandensein dieses Öls noch nichts gewonnen. Vielmehr brauche man zusätzlich Fahrzeuge und Infrastruktur, was ggf. aus den Daten heraus entwickelt werden müsse. Folglich brauche man im Datenrecht doch erstmal die Zeit, ein passendes Ökosystem zu entwickeln, Datenpools aufzubauen und Experten entsprechend auszubilden, um die erhobenen Daten vernünftig auswerten zu können. Für Bomhard ist es damit zentral erforderlich, sich darauf zu konzentrieren, die Daten präventiv noch vor dem Ausnahmefall nutzbar zu machen. Dafür müsse schon jetzt ein entsprechendes Ökosystem aufgebaut werden und vor allem der „Sackgasse“ des Datenschutzrechts irgendwie begegnet werden.

Hennemann pflichtete ihm bei. Man dürfe nicht bei den Art. 14 ff. DA stehenbleiben, sondern müsse schon – ggf. auf nationaler Ebene – die vorgelagerte Frage einer Datenbereithaltungspflicht adressieren. Dabei verweist er maßgeblich auf den Beitrag von von Lewinski, wo diese Stoßrichtung erstmalig ausgeführt wird und die mit einer Strukturierungspflicht

---

2 Prof. Dr. Kai von Lewinski ist Inhaber des Lehrstuhls für Öffentliches Recht, Medien- und Informationsrecht an der Universität Passau. Er hat zuvor zum Thema „Informationelle Sozialpflichtigkeit“ vorgetragen.

3 Prof. Dr. David Bomhard ist Honorarprofessor für das Recht der Künstlichen Intelligenz sowie IT-, Software- und Datenrecht an der Universität Passau.

4 Prof. Dr. Moritz Hennemann ist Inhaber des Lehrstuhls für Zivilrecht mit Informationsrecht, Medienrecht, Internetrecht sowie Direktor des Instituts für Medien- und Informationsrecht an der Universität Freiburg. Er hat zuvor zum Thema „Blaulicht und Abschleppwagen auf der Datenautobahn“ vorgetragen.

5 Hennemann, in diesem Band, S. 63.

6 Hier wird eine altbekannte Metapher aufgegriffen, welche die zentrale wirtschaftliche Relevanz von Daten hervorheben soll, vgl. *The Economist*, The world's most valuable resource is no longer oil, but data (6. Mai 2017), abrufbar unter <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> (zuletzt abgerufen am 17.10.2025).

einhergeht<sup>7</sup>. Es sei zu erwägen, Unternehmen dazu zu verpflichten, bestimmte Datenbestände mit einer Vorstrukturierung vorzuhalten, so dass diese auch kurzfristig abrufbar sind. Eine solche Inpflichtnahme erfordere faktisch natürlich die Fachkompetenz auf staatlicher Seite, mit herausgegebenen Daten (technisch) umgehen zu können. *Hennemann* äußerte hier allerdings leise Zweifel, ob die (Notstandsverwaltungs-)Behörden derzeit schon hinreichend darauf vorbereitet sind, die verschiedensten Daten ggf. ganz unterschiedlicher Natur in allen Sachlagen auslesen und verwerten zu können. In der Tat, so *Hennemann*, seien hier Reallabore bzw. reale Übungsszenarien in einen beschränkten und geschützten Rahmen zu erwägen. Auf diese Weise könnte getestet werden, ob Behörden die übermittelten Daten tatsächlich benötigen und wie sie mit ihnen umgehen (können), oder ob Behörden nicht auf eine Dienstleistung des Dateneinhabers bei der Datenauswertung angewiesen sind bzw. sein sollten.

*Meinhard Schröder*<sup>8</sup> blieb mit seiner Ergänzung bei der Metapher der Datenautobahn und merkte an, es gehe beim Datenrecht im Ausnahmefall nicht nur um ein Infrastrukturvorhaben. Anders als in den Fällen, in denen aufgrund einer Bedarfsanalyse Infrastruktur errichtet werde, müsse hier zunächst der Bedarf generiert werden. Es sei letztendlich ein Henne-Ei-Problem, was zuerst da sein müsse: der Bedarf oder die Infrastruktur? Beim Data Act scheine es, so *Schröder*, wie beim Data Governance Act mehr in die vorbereitende Richtung zu gehen, dass also juristische Infrastruktur ohne konkreten Bedarf entstehen soll. Gleichzeitig weist er darauf hin, dass für einen Datenaltruismus, der praktisch bei einem Infrastrukturvorhaben weiterhelfen könnte, schlicht die Anreize fehlen würden. Dies zeige sich nicht zuletzt in der schwachen Erfolgsquote des Datenvermittlungsdienstes<sup>9</sup>.

Dass die Regelungen zu datenaltruistischen Diensten ohne echte Anreize ausgestaltet und deshalb äußerst unattraktiv seien, weiß *Hennemann* zu bestätigen. Insbesondere bezweifelt er, dass die Registerpublizität und die

---

7 v. *Lewinski*, in diesem Band, S. 37 (47), der auf entsprechende Tendenzen im Bevölkerungsschutz- und Anlagenrecht verweist.

8 Prof. Dr. *Meinhard Schröder* ist Inhaber des Lehrstuhls für Öffentliches Recht, Europarecht und Informationstechnologierecht an der Universität Passau. Er hat zuvor zum Thema „Rechtsschutz gegen Datenverlangen“ vorgetragen.

9 Zzt. der Diskussion existierten in Europa nur 10 Datenvermittlungsdienste. Zzt. der Veröffentlichung ist diese Zahl immerhin auf 24 gestiegen, vgl. *Europäische Kommission*, EU-Register der Datenvermittlungsdienste, abrufbar unter <https://digital-strategy.ec.europa.eu/de/policies/data-intermediary-services> (zuletzt abgerufen am 17.10.2025).

Erlaubnis, ein entsprechendes Logo tragen zu dürfen, die Menge an Pflichten, die auf datenaltruistische Unternehmen zukommen<sup>10</sup>, kompensieren können. Entsprechende anreizorientierten Regelungen wären in einem Umsetzungsgesetz zum Data Governance Act möglich (welches allerdings trotz abgelaufener Frist noch nicht final vorliegt<sup>11</sup>). Platz dafür wäre etwa im Vertrags- und AGB-Recht, im Vergaberecht oder im Steuerrecht (gerade neben allfälligen datenschutzrechtlichen Privilegierungen). Ebenso führe die Tätigkeit als Datenvermittlungsdienst zu einem sehr strengen Pflichtenkatalog (unter anderem eine Notifizierungspflicht<sup>12</sup>), der abschreckend wirke. Das Kalkül des Gesetzgebers, durch vergleichsweise strenge Regulierung besonders viel Vertrauen im Markt zu schaffen und dadurch die Nachfrage zu erhöhen, scheint *Hennemann* bisher nicht aufgegangen zu sein. *Hennemann* sieht auch Potenzial, soweit konkrete Anreize in Form von Privilegierungen gesetzt werden (etwa im Bereich des KI-Trainings oder in Bereichen, in denen keine sensiblen Daten verarbeitet werden).

Die genannten Schwächen des Datenaltruismus aufgreifend fragt *von Lewinski* sich und die Runde, ob der Datenaltruismus nicht vom Helferrecht im Bevölkerungsschutz – also gemeinnützige Organisationen wie dem DRK, den Johannitern oder dem THW – lernen könnte. Auf diesem Gebiet funktioniere im Notstandsfall altruistisches Handeln ja offenkundig. Was werde hier besser gemacht als beim EU-Gesetzgeber, fragt er *Hennemann*.

*Hennemann* zufolge sei es nur mehr als menschlich, anderen zu helfen – vor allem bei einem Unglücksfall. Das gebiete schon der Solidaritätsgedanke und die (hoffentlich nicht schwindende) zwischenmenschliche Nächstenliebe. So einfach sei es aber nicht beim Datenteilen. In der breiten Bevölkerung sei wohl das Bewusstsein noch nicht angekommen, welche Daten man habe, wie man sie teilen könne und welcher Gemeinwohlnutzen da-

---

10 Regelungen zum Datenaltruismus finden sich in den Art. 16 ff. DGA und umfassen etwa Registrierungs- und Transparenzpflichten, Unabhängigkeit von Organisationen zu Erwerbszwecken, Sicherheits- und Interoperabilitätsanforderungen und weitere Organisationspflichten.

11 Trotz Einleitung eines Vertragsverletzungsverfahrens vonseiten der Europäischen Kommission Ende Mai 2024 befand sich der Gesetzesentwurf eines deutschen Daten-Governance-Gesetz (DGG-E) zzt. der Diskussion noch im Beratungsverfahren im Digitalausschuss des Bundestages.

12 Die Pflichten eines Datenvermittlungsdienstes ergeben sich vornehmlich aus Art. 11 und 12 DGA. Nach Art. 11 Abs. 1 DGA muss ein Datenvermittlungsdienst seine Dienstleistung bei der zuständigen Aufsichtsbehörde – in Deutschland wohl die Bundesnetzagentur – anmelden. Diese Anmeldungen werden in einem Register der Europäischen Kommission geführt, Art. 11 Abs. 10 DGA.

raus erwüchse. Man denke hier nur an die Corona-Datenspende-App. Es gebe zwar bereits heute viele Möglichkeiten beispielsweise zu Forschungszwecken Daten zu spenden, daraus sei aber wohl noch keine allgemeine „Bewegung“ geworden. *Hennemann* habe etwa noch keine Verkehrs-Apps gesehen, die aktiv nachfragen, ob die erhobenen Daten an universitäre Institute zur Verkehrsforschung „gespendet“ werden – unbeschadet der Tatsache, ob die Daten überhaupt für die jeweiligen Forschungszwecke geeignet sind.

Zur Attraktivität von Datenspenden schlägt *Marie Wienroeder*<sup>13</sup> vor, man könne sich die Anreize digitaler Interaktion auf sozialen Netzwerken als Vorbild nehmen. Sie sieht den Vorteil des Helferrechts darin, dass physisches Anpacken gleichzeitig einem sozialen Zweck diene, indem man mit anderen interagiert und sozial aktiv wird – das gebe es bei der Datenspende im digitalen Raum so noch nicht.

Auch *Schröder* meint, dass die Helfertätigkeit beim DRK oder beim THW viel unmittelbarer einleuchte, während das Bedürfnis des Staates, Daten zu erlangen, vielleicht nicht so evident sei. Wenn man aber eine Datenbevorratungspflicht einführe, die durchaus zweckmäßig wäre, dann könne man gleichzeitig Anreize zur weiteren Bereitstellung erzeugen, da die Daten ohnehin schon entsprechend aufbereitet und bereitgehalten wären: Wer ohnehin zur teilungsfähigen Aufbereitung verpflichtet ist, für den sei es viel naheliegender, diese Aufbereitung weiter zu kommerzialisieren, indem entsprechende rechtliche Privilegien genutzt werden – eine Tätigkeit als Datenvermittlungsdienst könne damit durchaus an Attraktivität gewinnen.

Wenn das Stichwort Bevorratungspflicht fällt, dann muss man zugleich an die datenschutzrechtlich prominent diskutierte Frage der Vorratsdatenspeicherung denken. So wirft *Barczak* auch ein, dass eine solche Bevorratungspflicht wohl an den strengen Maßstäben der Rechtsprechung, insbesondere die des EuGHs<sup>14</sup>, scheitern würde (es fällt der Begriff der „Glasper-

---

13 *Marie Wienroeder* ist wissenschaftliche Mitarbeiterin am Lehrstuhl für Europäisches und Internationales Informations- und Datenrecht an der Universität Passau. Sie hat zuvor zum Thema „Außergewöhnliche Notwendigkeit“ vorgetragen.

14 Gemeint ist hier die beachtliche Kasuistik des EuGH zur Vorratsdatenspeicherung und Art. 7, 8 GRCh (vgl. EuGH, NJW 2014, 2169; ZD 2017, 124; NJW 2021, 531; NJW 2022, 3135; ZD 2022, 677; NJW 2024, 2099). Danach soll die Datenbevorratung v.a. auf das „absolut Notwendige“ beschränkt sein, was etwa bei einer flächendeckenden und anlasslosen Speicherung regelmäßig nicht der Fall ist. Eine pauschale notstandsrechtliche Datenbereithaltungspflicht, bei der der Notstand sich noch nicht konkret

lenspielerei“). In der Tat lassen sich in der Praxis schwer die Erhebung von personenbezogenen wie nicht-personenbezogenen Daten voneinander trennen, zumal – wie *Barczak* auch anmerkt – die begriffliche Abgrenzung der beiden Konzepte kaum möglich ist.

Nicht nur aus datenschutzrechtlicher Perspektive sei eine Datenbevorratungspflicht problematisch, merkt *Johannes Erny*<sup>15</sup> an. Man müsse sich auch bewusst sein, dass eine Datenbevorratung mit einer erheblichen Speicherkapazität einhergehe, die Kosten verursache. Das gelte nicht nur finanziell, sondern auch aus Umweltgesichtspunkten, zumal große Datenspeicher einen hohen Energieverbrauch haben.

Während *von Lewinski* Umweltbedenken der allgemeinen politischen Debatte zuordnet, hält er rechtlich die durch eine Bevorratungspflicht verursachten unternehmerischen Organisationskosten für maßgeblich. Datenbanken seien vielseitig ausgestaltbar. Und wenn das Datenrecht praktisch so ausgestaltet werden solle wie etwa das Anlagen- oder Umweltrecht, dann bedeute das, Unternehmen müssten eine riesige Datenmenge in allen erdenklichen Dimensionen dezentral bereithalten und eine definierte Schnittstelle vorweisen, wodurch dem Staat ein punktueller Zugriff bei Bedarf ermöglicht werde. Hinter diesem Vorhalteprozess verbergen sich weitere betriebliche und technische Prozesse, aus denen erhebliche Kosten erwachsen können. Gerade diese Einwirkung auf die betriebliche Organisation müsste man sich bei einer Datenbereitstellungspflicht ganz genau anschauen. Die genannten umwelttechnischen Bedenken würden die Gemengelage freilich gut illustrieren.

Als nächstes meldete sich *Harald Erkens*<sup>16</sup> zu Wort, der drei Beispiele aus der Praxis der (Notstands-)Verwaltung anbringt, aus denen sich konkrete Probleme des Datenrechts im Ausnahmefall ergäben. Die Beispiele zeigten, so *Erkens*, dass es in den entsprechenden Datenschutzgesetzen unbedingt der Schaffung von Sondertatbeständen für Notstandssituationen

---

angedeutet hat, dürfte demnach mit dieser Rechtsprechung kollidieren, soweit auch personenbezogene Daten erfasst sind.

15 *Johannes Erny* ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Öffentliches Recht mit Europäischen Verwaltungs-, Informations- und Umweltrecht an der Universität Freiburg.

16 *Harald Erkens* ist Referent im Bundesministerium der Verteidigung und hat zuvor zum Thema „Datenbereitstellung im Zivilschutz- und Verteidigungsfall“ vorgetragen.

bedürfe<sup>17</sup>. Als erstes nennt er den Winter 2018/2019, in dem in Bayern u.a. Krankenhäuser und Pflegeheime eingeschneit waren. Damals benötigten die Katastrophenschutzbehörden Daten, vor allem die Adressen der zahlreichen ambulant gepflegten Personen, darunter auch Heimbeatmungspatienten, Dialysepatienten usw. Dennoch hatten sich die Pflegekassen unter Verweis auf die DSGVO und aus Furcht vor entsprechenden Sanktionen zunächst geweigert, personenbezogene Daten und insbesondere Gesundheitsdaten der Betroffenen zur Verfügung zu stellen und so Auskunft etwa über den Pflegegrad oder über besondere Umstände wie das Erfordernis eines Liegendtransports zu geben. Letztendlich konnten die Bedenken der Pflegekassen, zumindest bezogen auf den konkreten Einzelfall, mit einem Verweis auf Art. 9 DSGVO zerstreut werden. Gleichwohl sind die in der Folge erhobenen Forderungen nach Schaffung eines gesetzlichen Erlaubnistatbestandes etwa im SGB X, der in Notstandssituationen insoweit für Rechtssicherheit sorgen könnte, bis heute ohne Ergebnis geblieben. *Erkens'* zweites Beispiel bezieht sich auf die Corona-Warn-App. Diese sei aufgrund datenschutzrechtlicher Bedenken nicht so leistungsfähig gewesen, wie sie hätte sein können. Solche Fälle würden das bedauerliche Signal an die Öffentlichkeit senden, dass eine effektive Pandemiebekämpfung am Datenschutz scheitere – ganz gleich, ob diese Aussage in ihrer Einfachheit zutreffe oder nicht. Zuletzt nennt er das in den letzten Jahren zunehmend relevante Beispiel der Spontanhelfer. Diesen werde nämlich seitens der zuständigen Behörden sowie der Hilfsorganisationen eine Registrierung schon allein im Hinblick auf Versicherungsschutz und Haftungsprivilegierung empfohlen. Es gebe aber in der Praxis mannigfaltige Gründe, warum sich ein Spontanhelfer gerade nicht registrieren lassen wolle. Deshalb sollte auch hier über die datenschutzrechtliche Steuerungsmöglichkeit eine gesetzliche Grundlage geschaffen werden, was letztendlich auch der Attraktivität der Spontanhilfe zugutekommen könnte.

*Barczak* findet, diese Beispiele zeigten sehr schön, in welchem Dilemma man sich in der deutschen Debatte bewege. Das Datenschutzrecht habe gerade hierzulande eine gesellschaftspolitisch gut verankerte Tradition. Zwar gewichten wir kollidierende sicherheitspolitische Belange heute höher als wir es früher getan hätten. *Barczak* erinnert sich jedoch an seine Zeit als wissenschaftlicher Mitarbeiter am BVerfG, genauer bei *Johannes Masing*,

---

17 Dass es auch in an sich notstandsfernen Gesetzen spezifische Regelungen zum Notstand gibt, hat *Erkens* bereits in seinem Vortrag nachgewiesen, *Erkens*, in diesem Band, S. 77 (88, 91).

der dort maßgeblich am Datenschutz mitgewirkt hat<sup>18</sup>. Das Datenschutzrecht habe in Karlsruhe unglaubliche Blüten getrieben. *Barczak* sieht es daher skeptisch, ob man an dieser Stelle maßgeblich deregulieren könne.

In der letzten Frage, gestellt von *Hennemann* an *Barczak*, geht es um dessen Perspektive zum Begriff des personenbezogenen Datums und den daran hängenden Implikationen für eine praktisch wirksame Datenregulierung. Könne man nicht den Begriff des personenbezogenen Datums, der derzeit eher weit ausgelegt werde<sup>19</sup>, unional einfachgesetzlich präzisieren, sodass zum Beispiel bei nicht sensiblen Daten oder anderen Kontexten, in denen es um große Datenmengen geht, modifizierende Regelungen getroffen werden können? Anderenfalls, so *Hennemann*, müsse man ohne eine Änderung der EuGH-Rechtsprechung auf längere Zeit mit der oben angesprochenen Sackgasse des Datenschutzrechts leben. Hierauf kann *Barczak* nur einen Blick in die Glaskugel werfen. Die DSGVO sei weiterhin – und hier schließe er den Kreis zum Eingangsreferat von *Louisa Specht-Riemenschneider*<sup>20</sup> – europäischer Goldstandard. Und dazu gehöre ja auch maßgeblich die Definition des personenbezogenen Datums. Vor diesem Hintergrund sieht *Barczak* – ohne sich auf unmittelbare Einblicke in den europapolitischen Betrieb zu berufen – keine Anzeichen von Änderungen oder internen Mehrheiten, geschweige denn von einer Änderung der EuGH-Rechtsprechung. Dass der EuGH von seiner strengen Lesart von Art. 4 Nr.1 DSGVO abrückt, würde in gewissem Maße auch *judicial*

---

18 Prof. Dr. *Johannes Masing* war von 2008 bis 2020 zuständiger Berichterstatter für u.a. das Persönlichkeitsrecht und den Datenschutz am BVerfG. Als solcher bereitete er zentrale datenschutzrechtliche Urteile wie zur Vorratsdatenspeicherung (BVerfGE 125, 160), zur Kfz-Kennzeichenkontrolle (BVerfGE 150, 244) oder zum Recht auf Vergessenwerden (BVerfGE 152, 152; 152, 216) vor.

19 Nach dem EuGH ist die Anwendung der DSGVO „sehr weit und die von [ihr] erfassten personenbezogenen Daten vielfältig“, vgl. nur *EuGH*, Urt. v. 7.5.2009, C-553/07, *EuZW* 2009, 546 Rn. 59 – *Rijkeboer*; *EuGH*, Urt. v. 20.12.2017, C-434/16, *NJW* 2018, 767 Rn. 33 – *Nowak*. Die Kontextspezifik und die beliebige Kombinierbarkeit können nahezu jedes Datum zu einem personenbezogenen machen. Vgl. zum Maßstab der indirekten Identifizierbarkeit etwa *EuGH*, Urt. v. 4.5.2022, T-384/20, *BeckRS* 2024, 3655 Rn. 45 ff. – OC.

20 Prof. Dr. *Louisa Specht-Riemenschneider* ist Inhaberin des Lehrstuhls für Bürgerliches Recht, Recht der Datenwirtschaft, des Datenschutzes, der Digitalisierung und der Künstlichen Intelligenz an der Rheinischen Friedrich-Wilhelms-Universität Bonn, sowie Bundesbeauftragte für den Datenschutz und die Informationssicherheit (BfDI). Sie hat zuvor zum Thema „Was kann das Datenrecht vom Datenschutzrecht lernen?“ vorgetragen.



*self-restraint* bedeuten, was *Barczak* letztendlich als nicht realistische Perspektive bewertet.

Damit hat sich ein gutes Schlusswort zur Tagung gefunden. *Von Lewinski* schließt damit die Diskussion und bedankt sich insbesondere noch einmal bei *Louisa Specht-Riemenschneider* und *Moritz Hennemann* – eine hatte die Forschungsstelle FREDI geschaffen und angeschoben, der andere hatte sie maßgeblich weitergeleitet.

### C. Fazit und Einordnung

Große Streitpunkte gab es also kaum. Einigkeit bestand vor allem darüber, dass eine vorgelagerte Datenbereithaltungspflicht, die insbesondere auf die Teilbarkeit und schnelle Abrufbarkeit der Daten abzielt, praktikabel und wünschenswert ist. Die rechtliche Umsetzbarkeit dieser Idee war hingegen unklar. Denn zumindest wenn es um personenbezogene Daten geht, legt der EuGH strenge Maßstäbe zur Vorratsdatenspeicherung an. Und selbst wenn Datenbereithaltungspflichten nur auf nicht-personenbezogene Daten abzielen, dann führt die weite Lesart des „personenbezogenen Datums“ des EuGH unweigerlich zu Abgrenzungsschwierigkeiten im Einzelfall und damit zu einer faktischen Sperrwirkung durch das Datenschutzrecht. Dass der EuGH von dieser Rechtsprechungslinie (und aber auch das BVerfG hinsichtlich seiner weitreichenden<sup>21</sup> Konzeption des Rechts auf informationelle Selbstbestimmung<sup>22</sup>) zukünftig zugunsten etwa einer effektiveren Notstandsverwaltung abweichen wird oder dass es zu entsprechenden

- 
- 21 So hat das BVerfG in seiner Volkszählung-Entscheidung konstatiert, es gebe keine belanglosen Daten mehr und es räumt dem Betroffenen eine Befugnis ein, *grundsätzlich* selbst über Preisgabe und Verwendung „seiner“ persönlichen Daten zu bestimmen, BVerfGE 1, 65 (43 f.) – Volkszählung.
- 22 Zu entsprechenden (dogmatischen wie rechtspolitischen) Kritiken und Diskussionen gerade hinsichtlich der Reichweite dieses Rechts, vgl. etwa *Albers*, Informationelles Selbstbestimmungsrecht, 2005, S. 238, 355, 601 ff.; *Bull*, Informationelle Selbstbestimmung – Vision oder Illusion?, 2. Aufl. 2011, S. 45 ff., 63 f., 136 f. *Behrendt*, Die Entlarvung des Rechts auf informationelle Selbstbestimmung, 2023, S. 393 ff. und *passim*; *Hoffmann-Riem*, Informationelle Selbstbestimmung in der Informationsgesellschaft, AöR 123 (1998) 513 (531 f.); *Britz*, Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: Brandt u.a. (Hrsg.), Offene Rechtswissenschaft, 2010, S. 561; *Poscher*, Die Zukunft der informationellen Selbstbestimmung als Recht auf Abwehr von Grundrechtsgefährdungen, in: Gander u.a. (Hrsg.), Resilienz in der offenen Gesellschaft, 2012, S. 167 (182 ff.).

Gesetzesänderungen kommen könnte, ist den Diskutanten indes nicht ersichtlich. Unabhängig davon muss man sich bei vergleichbaren Vorhaben immer vor Augen führen, dass Datenbereithaltungspflichten nicht nur eine immense Speicherkapazität erfordern, sondern auch dass die erforderlichen betrieblichen und technischen Umstrukturierungen zu finanziellen Belastungen der Unternehmen führen und letztendlich deren Berufsausübung (Art. 12 I GG; Art. 15 I GRCh) beschränken.

Das zweite Takeaway dieser Debatte adressiert die Rolle des Datenaltruismus insbesondere in Kombination mit Datenvermittlungsdiensten. Gerade in Notstandsfällen könnte beidem eine zentrale Rolle zukommen. Gleichzeitig ist das freiwillige Datenteilen recht unattraktiv ausgestaltet, sodass nicht zu erwarten ist, dass sich viele Dateninhaber bereitwillig als Datenvermittlungsdienst oder gar datenaltruistische Organisation anbieten werden. Dennoch ist ungeklärt, wie die Attraktivität von Datenaltruismus gesteigert werden könnte. Ideen wären etwa die AGB-rechtliche Einbettung von freiwilligen Datenspenden oder die steuerliche Absetzbarkeit. Dabei scheint man (noch) nicht vom Helferrecht lernen zu können, da Datenaltruismus als allgemeine Bewegung noch nicht in der Gesellschaft angekommen ist. Während man etwa beim THW mit anpackt, sozial aktiv wird und damit entsprechend zwischenmenschlicher Nächstenliebe handelt, verbindet man die Datenspende nicht mit diesen Attributen – sie kann jederzeit per Knopfdruck von der Couch aus getätigt werden, ohne dass man die unmittelbaren Auswirkungen seines altruistischen Handelns spüren kann.

Letztendlich zeigte die Diskussion, dass rechtliche Instrumente als Rechtsfiguren und -formen zwar existent sind, aber immer noch zahlreiche technische und auch rechtliche Vorfragen der Bereitstellungsinfrastruktur sowie Kollisionsfragen zum Datenschutzrecht nicht ausreichend geklärt sind.