

Bibliothek zur Zeitschrift für Schweizerisches Recht
Beiheft 63

Informationelle Selbstbestimmung: Intuition, Illusion, Implosion

Florent Thouvenin



Zeitschrift für Schweizerisches Recht
Revue de droit suisse
Rivista di diritto svizzero
Revista de dretg svizzer

Gegründet 1852

Neue Folge seit 1882

ISSN 0254-945X

Band I: 5 Hefte pro Jahr

Band II: Referate und Mitteilungen des Schweizerischen Juristenvereins (SJV)

Davon profitieren Sie mit einem Abo der «ZSR»:

- Aktuelle Aufsätze zu zentralen Entwicklungen in der Gesetzgebung, der Gerichtspraxis und der Rechtslehre, verfasst von ausgewiesenen Expertinnen und Experten aus Wissenschaft und Praxis
- Schwerpunktheft zu Revisionen und neuen Gesetzen
- Jeweils die neuesten Referate und Mitteilungen des Schweizerischen Juristenvereins

Informationelle Selbstbestimmung: Intuition, Illusion, Implosion

Florent Thouvenin

Florent Thouvenin

Informationelle Selbstbestimmung

Intuition, Illusion, Implosion

Informationelle Selbstbestimmung

Bibliographische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der
Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind
im Internet unter <http://dnb.dnb.de> abrufbar.

Alle Rechte vorbehalten. Dieses Werk ist weltweit urheberrechtlich geschützt.
Insbesondere das Recht, das Werk mittels irgendeines Mediums (grafisch, technisch,
elektronisch und/oder digital, einschliesslich Fotokopie und downloading) teilweise
oder ganz zu vervielfältigen, vorzutragen, zu verbreiten, zu bearbeiten, zu übersetzen,
zu übertragen oder zu speichern, liegt ausschliesslich beim Verlag. Jede Verwertung
in den genannten oder in anderen als den gesetzlich zugelassenen Fällen bedarf
deshalb der vorherigen schriftlichen Einwilligung des Verlags.

ISBN 978-3-7190-4553-1

© 2023 Helbing Lichtenhahn Verlag, Basel
www.helbing.ch



Inhaltsverzeichnis

A. Einleitung	1
B. Historische Entwicklung: Intuition	5
1. Ausgangspunkt	5
2. Aufnahme	7
3. Wendepunkt	12
4. Zwischenerkenntnis	14
C. Tatsächliche Umsetzung: Illusion	15
1. Grundsätze der Datenbearbeitung	15
2. Rechtmässigkeit der Datenbearbeitung	16
2.1 Bearbeitung durch Bundesorgane	17
2.2 Bearbeitung durch Private	19
3. Rechte und Pflichten	22
4. Durchsetzung des Datenschutzrechts	24
5. Zwischenerkenntnis	26
D. Normative Analyse: Implosion	29
1. Bearbeitung durch Bundesorgane	29
2. Bearbeitung durch Private	32
2.1 Menschliche Interaktion	32
2.2 Bedarf und Aufwand, Kosten und Nutzen	34
2.3 Daten als öffentliche Güter	37
3. Zwischenerkenntnis	40
E. Erkenntnisse und Alternativen	43

A. Einleitung*

Das schweizerische Datenschutzrecht beruht auf der Idee der informationellen Selbstbestimmung. Das Bundesgericht hält seit Jahren in konstanter Rechtsprechung fest, dass die Bundesverfassung jeder Person ein Grundrecht auf informationelle Selbstbestimmung vermittelt¹. Dies entspricht auch der Auffassung des Bundesrates, welcher in der Botschaft zur Totalrevision des Datenschutzgesetzes (DSG) zum Zweck des Gesetzes ausgeführt hat: «Das DSG konkretisiert auf Gesetzesebene das in Art. 13 Abs. 2 BV festgehaltene Recht auf informationelle Selbstbestimmung im Zusammenhang mit Personendaten, d. h. das Recht der betroffenen Person, grundsätzlich selbst zu bestimmen, ob und zu welchen Zwecken Daten über sie bearbeitet werden dürfen»². Dieses Verständnis ist in der Lehre zwar nicht unwidersprochen geblieben³, bildet aber die herrschende Auffassung⁴. Der Begriff der informationellen Selbstbestim-

* Der Autor dankt Prof. Dr. Peter Hettich für wertvolle Hinweise und MLaw Samuel Mätzler, Rechtsanwalt, für die Unterstützung bei den Recherchen und bei der Ausarbeitung des Fussnotenapparates.

¹ BGE 148 II 349, 356; BGE 147 I 103, 128; BGE 145 IV 42, 46; BGE 144 I 281, 301; BGE 144 I 126, 131; BGE 140 I 2, 22; BGE 138 II 346, 359 f.; BGE 133 I 77, 85; BGE 129 I 232, 245; BGE 128 II 259, 268.

² Botschaft Totalrevision DSG, BBl 2017, 6941 ff., 7010. Die Botschaft stellt zugleich klar, dass damit keine Neuerung verbunden sei, sondern der Zweck des neuen DSG dem Zweck des alten DSG entspreche (a.a.O.) und es bestätigt durch den Verweis auf BGE 140 I 2, 22 die Übereinstimmung mit der Rechtsprechung des Bundesgerichts.

³ Siehe dazu namentlich: THOMAS GÄCHTER/PHILIPP EGLI, Informationsaustausch im Umfeld der Sozialhilfe, Jusletter vom 6. September 2010, Rz. 28 und 36 ff.; EVA MARIA BELSER, in: Eva Maria Belser/Astrid Epiney/Bernhard Waldmann, Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011, § 6 Rz. 118 und 168; EVA MARIA BELSER, Zur rechtlichen Tragweite des Grundrechts auf Datenschutz: Missbrauchsschutz oder Schutz der informationellen Selbstbestimmung?, in: Astrid Epiney/Tobias Fasnacht/Gaëtan Blaser (Hrsg.), Instrumente zur Umsetzung des Rechts auf informationelle Selbstbestimmung/Instruments de mise en oeuvre du droit à l'autodétermination informationnelle, Zürich/Basel/Genf 2013, 27 und ausführlich 33 ff.; ebenfalls kritisch REGINA E. AEBI-MÜLLER, Personenbezogene Informationen im System des zivilrechtlichen Persönlichkeitsschutzes, unter besonderer Berücksichtigung der Rechtslage in der Schweiz und in Deutschland, Bern 2005, Rz. 597 ff.

⁴ DAVID ROSENTHAL/YVONNE JÖHRI, Handkommentar zum Datenschutzgesetz, Zürich/Basel/Genf 2008, DSG I N 4; URS MAURER-LAMBROU/SIMON KUNZ, in: Urs Maurer-Lambrou/Gabor P. Blechta (Hrsg.), Basler Kommentar zum Datenschutzgesetz, Basel 2014, DSG I N 19; PHILIPPE MEIER, Protection des données: fondements, principes généraux et droit privé, Bern 2011, § 1 Rz. 17; grundlegend JÖRG PAUL MÜLLER/MARKUS SCHEFER, Grundrechte in der Schweiz, 4. Aufl., Bern 2008, 164 ff.; RAINER J. SCHWEIZER/LEA S. STRIEGEL, in: Bernhard Ehrenzeller/Patricia Egli/Peter Hettich/Peter Hongler/Benjamin Schindler/Stefan G. Schmid/Rainer J. Schweizer (Hrsg.), St. Galler Kommentar, Die Schweizerische Bundesverfassung, Zürich/St. Gallen 2023, BV 13 N 79; ALEXANDRE FLÜCKIGER, L'autodétermination en matière de données personnelles: un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété?, AJP 2013, 837 ff., 846 f.; ebenso, wenn auch eine andere Auffassung vertretend, BELSER, in: Belser/Epiney/Waldmann (Fn. 3), § 6 Rz. 60 f.; MAYA HERTIG RANDALL/JULIEN MARQUIS, in: Vincent Martenet/Jacques Dubey (Hrsg.), Constitution fédérale, Commentaire romand, Basel 2021, BV 13 N 62.

mung ist längst auch zum politischen Schlagwort geworden. Er findet sich in parlamentarischen Initiativen⁵, Motionen⁶, Postulaten⁷ und Interpellationen⁸ und wurde auch in der Debatte zur Totalrevision des DSG in den Räten immer wieder ins Feld geführt⁹.

Die Idee der «informationellen Selbstbestimmung» ist intuitiv überzeugend. Die Selbstbestimmung ist ein zentrales Konzept westlicher Gesellschaften, das rechtlich in vielerlei Hinsicht abgesichert ist. In der Informationsgesellschaft liegt es nahe, die Selbstbestimmung auch auf Informationen auszudehnen und der einzelnen Person nicht nur die Bestimmung über sich selbst, sondern auch über die sie betreffenden Informationen zuzugestehen. Es erstaunt deshalb wenig, dass die informationelle Selbstbestimmung auch bei juristischen Laien zu einem allgemein bekannten und anerkannten Konzept geworden ist, auf das in persönlichen Diskussionen und in den Medien regelmässig verwiesen wird¹⁰. Der Gehalt der Idee wird dabei allerdings kaum je konkretisiert. Vielmehr begnügt man sich meist damit, den Begriff anzuführen und dem Gegenüber zu überlassen, was er oder sie darunter verstehen mag. In der Verbindung von intuitiver Überzeugungskraft und inhaltlicher Offenheit liegt denn auch die Stärke des Begriffs, dessen Einfluss wirkungsgeschichtlich kaum hoch genug eingeschätzt werden kann: Es kommt gar nicht darauf an, was der Gehalt eines Rechts auf informationelle Selbstbestimmung ist und sein kann – vielmehr reicht es, den Begriff in den Raum zu stellen und daraus Schlüsse zu ziehen oder Forderungen abzuleiten. Die informationelle Selbstbestimmung ist damit in der Schweiz (und darüber hinaus) zu einem Axiom der Informationsgesellschaft geworden, das nicht mehr zu hinterfragen ist.

Ebendies tut dieser Beitrag aus drei Perspektiven: einer historischen, einer rechtstatsächlichen und einer normativen. Dabei wird sich zeigen, dass die Idee

5 Parlamentarische Initiative Schelbert 06.460 «Datenschutz. Vom Schutz vor Missbrauch zum Recht auf Selbstbestimmung»; Parlamentarische Initiative Vischer 14.413 «Grundrecht auf informationelle Selbstbestimmung».

6 Motion Reimann 11.3990 «Freiheit stärken. Recht an den eigenen Daten sichern»; Motion von Felten 96.3103 «Rufnummernanzeige im ISDN. Wahrung der Grundrechte».

7 Postulat Heim 17.3435 «Digitale Gesundheitsagenda. Chancen und Risiken»; Postulat Béglé 16.3386 «Kontrolle über persönliche Daten. Informationelle Selbstbestimmung fördern».

8 Interpellation Glättli 21.3580 «Regulierung der Gesichtserkennung im öffentlichen Raum»; Interpellation Hollenstein 05.3067 «Bedroht die Anwendung von Radio Frequency Identification (RFID) den Datenschutz?».

9 Votum BR Sommaruga AB 2018 S 618; Votum Glättli AB 2019 N 1778; Votum BR Keller-Sutter AB 2019 N 1815.

10 Beispielhaft: <<https://www.srf.ch/kultur/gesellschaft-religion/naiver-umgang-mit-big-data-der-zwang-zur-digitalisierung-schraenkt-unsere-autonomie-ein>>; <<https://www.srf.ch/kultur/netzwelt/das-digitale-ich/big-data-und-was-sie-uns-antun-eine-uebersicht>>; <<https://www.nzz.ch/digital/schluss-mit-dem-gejammer-ld.711908>>; <<https://www.republik.ch/2020/07/27/das-kranke-dossier>> (zuletzt besucht am 20. Juni 2023).

eines Rechts auf informationelle Selbstbestimmung einer näheren Überprüfung nicht standhält. Die Betrachtung der historischen Entwicklung (B.) wird erkennen lassen, dass Bundesrat und Bundesgericht den Begriff Ende der 80er bzw. Anfang der 90er Jahre aus dem sog. Volkszählungsurteil des deutschen Bundesverfassungsgerichts vom 15. Dezember 1983¹¹ übernommen, aber nie eine eigene Begründung für die Anerkennung eines Grundrechts auf informationelle Selbstbestimmung vorgelegt haben. Das Bundesgericht scheint sich stattdessen auf die intuitive Überzeugungskraft des Begriffs zu verlassen. Das kann nicht genügen. Als besonders problematisch erweist sich das Fehlen eigener Reflexion, weil das Bundesgericht die Idee der informationellen Selbstbestimmung im Verlauf der Zeit zunehmend absoluter verstanden hat, während das Bundesverfassungsgericht seine Rechtsauffassung vor einigen Jahren stark relativiert hat. Die Analyse der tatsächlichen Umsetzung (C.) wird deutlich machen, dass nur wenige Bestimmungen im schweizerischen DSG als Ausdruck der informationellen Selbstbestimmung verstanden werden können. Die Idee kann damit allenfalls die konzeptionelle Grundlage einzelner Normen, aber nicht des ganzen Gesetzes bilden. Das gilt ganz besonders für die Bestimmungen über die Bearbeitung von Personendaten durch Bundesorgane, die sich nicht auf ein Grundrecht auf informationelle Selbstbestimmung stützen lassen. In der Umsetzung in Gesetzesnormen und erst recht bei deren Anwendung auf die Vielfalt der Datenbearbeitungen erweist sich die informationelle Selbstbestimmung damit weitgehend als Illusion. Die normative Analyse (D.) wird schliesslich zeigen, dass sich diese Idee nicht nur kaum umsetzen lässt, sondern auch überzeugende Gründe bestehen, weshalb sie nicht umgesetzt werden sollte. Vor diesem Hintergrund fällt die Idee der informationellen Selbstbestimmung weitgehend in sich zusammen – sie implodiert.

11 BVerfGE 65, 1.

B. Historische Entwicklung: Intuition

1. Ausgangspunkt

Die Idee eines Rechts auf informationelle Selbstbestimmung lässt sich auf das Buch von ALAN WESTIN zu Privacy and Freedom von 1967 zurückführen. Er spricht sich darin für ein Recht des Einzelnen aus, «to decide what information about himself should be communicated to others and under what circumstances»¹². WESTIN hat zwar den Begriff der informationellen Selbstbestimmung nicht verwendet, mit seinem Beitrag aber die Grundlage dafür gelegt, dass die Idee seither eine der zentralen Theorien in der US-amerikanischen Debatte zum «Right to Privacy» ist¹³. Für das Schweizer Recht ist diese Debatte allerdings weitgehend irrelevant, weil der Begriff der «Privacy» im US-amerikanischen Recht ungleich weiter gefasst wird als derjenige der Privatsphäre und des Datenschutzes im Schweizer Recht.

Wirkungsgeschichtlich zentral ist für die Schweiz das sog. Volkszählungsurteil des deutschen Bundesverfassungsgerichts von 1983¹⁴. Das Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung vom 25. März 1982 (Volkszählungsgesetz 1983) sah für Frühjahr 1983 eine Volkszählung in Form einer Totalerhebung vor. Gegen dieses Gesetz wurden mehrere Verfassungsbeschwerden eingereicht. Mit Urteil vom 15. Dezember 1983 stellte das Bundesverfassungsgericht fest, dass zahlreiche Vorschriften des Volkszählungsgesetzes erheblich und ohne Rechtfertigung in Grundrechte des Einzelnen eingriffen. Diese Vorschriften erklärte es für nichtig und das gesamte Bundesgesetz für verfassungswidrig. In den zentralen Passagen der Urteilsbegründung hob das Bundesverfassungsgericht die Bedeutung der Selbstbestimmung als «elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens»¹⁵ hervor und hielt fest, dass «Wert und Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt»¹⁶ «im

¹² ALAN F. WESTIN, Privacy and Freedom, New York 1967, 7.

¹³ CHARLES FRIED, Privacy, The Yale Law Journal 1968, 475–493, 482; RANDALL P. BEZANSON, The Right to Privacy Revisited: Privacy, News, and Social Change, 1890–1990, California Law Review 1992, 1133–1175, 1150 ff.; ADAM MOORE, Defining Privacy, Journal of Social Philosophy 2008, 411–428, 414 ff.; kritisch dazu: RUTH GAVISON, Privacy and the Limits of Law, The Yale Law Journal 1980, 421–471, 427 ff; siehe auch DANIEL J. SOLOVE, Understanding Privacy, Cambridge (MA)/London 2008, 24 ff.

¹⁴ BVerfGE 65, 1.

¹⁵ BVerfGE 65, 1, 43.

¹⁶ BVerfGE 65, 1, 41.

Mittelpunkt der grundgesetzlichen Ordnung»¹⁷ stehen. Dem Schutz der Person diene das im Grundgesetz gewährleistete allgemeine Persönlichkeitsrecht, das «auch die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen [umfasst], grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden»¹⁸. Denn «wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiss»¹⁹. Daraus folgert das Bundesverfassungsgericht: «Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus»²⁰. Dieser Schutz sei deshalb vom Grundrecht auf Schutz der Persönlichkeit umfasst. Dieses gewährleiste insoweit «die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen»²¹.

Direkt im Anschluss an diese Umschreibung des Grundrechts auf informationelle Selbstbestimmung weist das Bundesverfassungsgericht allerdings mit aller Deutlichkeit auf die Grenzen eines solchen Rechts hin: «Dieses Recht auf 'informationelle Selbstbestimmung' ist nicht schrankenlos gewährleistet. Der Einzelne hat nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über 'seine' Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Information, auch soweit sie personenbezogen ist, stellt ein Abbild sozialer Realität dar, das nicht ausschliesslich dem Betroffenen allein zugeordnet werden kann. Das Grundgesetz hat, wie in der Rechtsprechung des Bundesverfassungsgerichts mehrfach hervorgehoben ist, die Spannung Individuum – Gemeinschaft im Sinne der Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person entschieden [Nachweise]. Grundsätzlich muss daher der Einzelne Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen»²².

2. Aufnahme

Das Volkszählungsurteil des Bundesverfassungsgerichts wurde in der Schweiz recht bald und sehr direkt aufgegriffen. In der *Botschaft für das erste Datenschutzgesetz* hat der Bundesrat unter Verweis auf das Urteil unter dem Titel «Allgemeine Ziele eines Datenschutzgesetzes» ausgeführt: «Jedermann soll, soweit die Rechtsordnung nichts anderes vorsieht, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen und frei über die Aufnahme und Gestaltung seiner Informations- und Kommunikationsbeziehungen entscheiden können»²³. Eine Begründung für das Bestehen einer solchen Berechtigung, die über den blossen Verweis auf das Volkszählungsurteil hinausgeht, führte der Bundesrat nicht an. Von einem Grundrecht auf informationelle Selbstbestimmung ist an dieser Stelle allerdings nicht die Rede. Und auch der Begriff der informationellen Selbstbestimmung wird bei den Ausführungen zu den allgemeinen Zielen des DSG nicht verwendet. Dieser findet sich erst bei den Erläuterungen der einzelnen Bestimmungen und auch dort nur im Bereich des Privatrechts, und zwar beim Widerspruchsrecht der betroffenen Personen (Art. 12 Abs. 2 lit. b aDSG; Art. 9 Abs. 2 lit. b DSG) und bei den Ausführungen zur arbeitsrechtlichen Regelung (Art. 328b OR)²⁴. Mit dem Widerspruchsrecht sollte dabei «als eigentliche Neuerung das Selbstbestimmungsrecht der betroffenen Personen über ihre Daten garantiert und geschützt werden»²⁵.

Bei den Ausführungen zu den allgemeinen Zielen des DSG stellt die Botschaft klar, dass es sich beim Recht, selbst «über die Preisgabe und Verwendung seiner persönlichen Daten [zu] bestimmen», um einen Grundsatz handelt und die Rechtsordnung etwas anderes vorsehen kann, insb. wenn ein überwiegendes Interesse an einer Informationsbeschaffung besteht²⁶. Diese Einschränkung ist zwar ungleich weniger deutlich als im Volkszählungsurteil des Bundesverfassungsgerichts, erscheint an dieser Stelle aber doch hinreichend klar. Anderes gilt für die Ausführungen zum Privatrecht und damit für die einzigen beiden Stellen in der Botschaft, an welchen der Begriff der informationellen Selbstbestimmung verwendet wird²⁷. Hier fehlt jeder Hinweis auf Einschränkungen, was den Eindruck zu erwecken vermag, dass das Recht auf informationelle Selbstbestimmung unter Privaten einschränkungslos gelten soll.

17 Ebenda.

18 BVerfGE 65, 1, 42.

19 BVerfGE 65, 1, 43.

20 Ebenda.

21 Ebenda.

22 BVerfGE 65, 1, 43 f.

23 Botschaft DSG, BBl 1988 II 413, 418.

24 Botschaft DSG, BBl 1988 II 413, 459 und 488.

25 Botschaft DSG, BBl 1988 II 413, 459.

26 Botschaft DSG, BBl 1988 II 413, 418.

27 Botschaft DSG, BBl 1988 II 413, 459 und 488.

Das *Bundesgericht* hat den Begriff der informationellen Selbstbestimmung erstmals 1994 in seiner amtlich publizierten Rechtsprechung verwendet²⁸. In einem Urteil, in dem es über das Recht eines Arbeitnehmers auf Einsicht in seine Personalakte zu entscheiden hatte, führte es aus, dieses «Einsichtsrecht [sei] als Teil des informationellen Selbstbestimmungsrechts zu verstehen [Nachweise], das auch der Datenschutzgesetzgebung des Bundes zugrunde lieg[e]»²⁹. Dabei verwies das Gericht zwar auf die Ausführungen in der Botschaft zu den allgemeinen Zielen des DSG, wies aber (anders als die Botschaft) in keiner Weise auf die Einschränkungen der informationellen Selbstbestimmung hin. Ein solcher Hinweis fehlte auch im nächsten Entscheid des Bundesgerichts, der 2001 erging. Zu beurteilen war auch hier eine privatrechtliche Konstellation, nämlich die Veröffentlichung der Fotografie einer bekannten Persönlichkeit in einer Zeitschrift. Das Bundesgericht qualifizierte die gegen den Willen der Persönlichkeit erfolgende Publikation als Verletzung des Rechts am eigenen Bild und des «privatrechtlichen, im DSG konkretisierten Rechts auf informationelle Selbstbestimmung»³⁰.

Ein Grundrecht auf informationelle Selbstbestimmung anerkannte das Bundesgericht erst nach dem Inkrafttreten der totalrevidierten Bundesverfassung am 1. Januar 2000. In einem Entscheid von 2002, in dem es um das Erstellen eines DNA-Profiles in einem Strafverfahren ging, hielt das Bundesgericht fest, dass «Art. 13 Abs. 2 BV den Einzelnen vor Beeinträchtigungen [schützt], die durch die staatliche Bearbeitung seiner persönlichen Daten entstehen (Recht auf informationelle Selbstbestimmung)»³¹. Gleich im Anschluss führte es aus, «der verfassungsrechtliche Datenschutz [sei] Teil des Rechts auf eine Privat- und persönliche Geheimsphäre»³². Erstaunlicherweise legte das Bundesgericht keinerlei Begründung für das neu geschaffene Grundrecht vor und äusserte sich auch nicht zu dessen Gehalt. Letzteres holte es allerdings schon ein Jahr später in einem nächsten Entscheid nach, in dem es eine Volksinitiative für ungültig erklärte, mit der Einbürgerungsgesuche der Urnenabstimmung unterstellt werden sollten. Das Bundesgericht führte hier die Umschreibung des Grundrechts auf informationelle Selbstbestimmung ein, die im Wesentlichen bis heute Bestand hat. Es hielt fest: «Art. 13 BV gewährleistet das Recht auf eine

Privat- und eine persönliche Geheimsphäre. Abs. 2 schützt den Einzelnen vor Beeinträchtigungen, die durch die staatliche Bearbeitung seiner persönlichen Daten entstehen (Recht auf informationelle Selbstbestimmung; [Nachweise]). Die einzelne Person soll selbst bestimmen können, ob und zu welchem Zwecke Informationen über sie bearbeitet werden»³³. Der letzte Satz, der den Gehalt des neuen Grundrechts umschreibt, wird dabei nur durch einen Verweis auf die Kommentierung von Art. 13 Abs. 2 BV durch RAINER J. SCHWEIZER im St. Galler Kommentar zur Bundesverfassung gestützt. Das Bundesgericht führt auch hier keine Begründung an, weder für das Bestehen eines Grundrechts noch für die Umschreibung seines Gehalts. Das kann nicht genügen.

Das Vorgehen des Bundesgerichts ist umso problematischer, als die Kommentierung von SCHWEIZER diesen Mangel nicht zu beheben vermag, im Gegenteil. Er führte aus: «So wie Abs. 2 in der neuen BV formuliert worden ist, ist er missglückt. Im Rahmen des verfassungsrechtlichen Persönlichkeitsschutzes bedeutet Datenschutz nicht nur Schutz vor Missbrauch persönlicher Daten, sondern etwas viel Grundsätzlicheres. Das BGer hat unter der aBV schon 1987 (im Anschluss an ausländische höchstgerichtliche Rechtsprechung) anerkannt, dass es ein ungeschriebenes Grundrecht auf informationelle Selbstbestimmung gibt (vgl. BGE 113 Ia 1; 113 Ia 257; ausdrücklich auch BGE 120 II 118; 122 I 153; 127 III 481; vgl. auch BVerfGE 65, S. 1 ff., 41 ff.; 80, S. 367 ff., 373 ff.). Der grundrechtliche Kerngehalt ist demnach, dass die einzelne Person gegenüber fremden, staatlichen oder privaten Bearbeitungen von sie betreffenden Informationen letztlich bestimmen können muss, ob und zu welchem Zwecke diese Informationen über sie bearbeitet werden»³⁴. SCHWEIZER begründet sein Postulat im Wesentlichen damit, dass sich der Einzelne nur bei Bestehen eines solchen Grundrechts gegen staatliche und private Informationstätigkeit, insb. gegen ein «störendes Beobachten, Ausschnüffeln, Kontrollieren, Steuern oder vor Dritten Blossstellen und Disqualifizieren» wehren könne³⁵. Die Begründung fällt damit nicht nur knapp aus, sondern ist auch höchst einseitig, weil sie allein die betroffene Person in den Blick nimmt und die Notwendigkeit der Bearbeitung von Daten durch Staat und Private ausblendet. Schwerer wiegt, dass SCHWEIZER seine Ausführungen auf die Behauptung stützt, das Bundesgericht habe schon 1987 ein Grundrecht auf informationelle Selbstbestimmung anerkannt. In den von ihm als Belege angeführten BGE 113 Ia 1 und BGE 113 Ia 257 wird aber weder der Begriff der informationellen Selbstbestimmung erwähnt noch ist von einem Grundrecht die Rede. Die ebenfalls angeführten

28 Der erste Verweis auf das Volkszählungsurteil findet sich zwar schon sieben Jahre früher in BGE 113 Ia 1, 6. Das Bundesgericht geht hier aber nicht auf das Grundrecht auf informationelle Selbstbestimmung ein, sondern nimmt nur Bezug auf den Gedanken des Bundesverfassungsgerichts, wonach der Eintrag in einer Datenbank die betroffene Person davon abhalten könne, sich völlig frei zu bewegen; siehe dazu ausführlich STEFANIE-DANIELA WALDMEIER, Informationelle Selbstbestimmung – ein Grundrecht im Wandel?, Diss. Zürich 2015, 8 f.

29 BGE 120 II 118, 121; ebenso: BGE 122 I 153, 162.

30 BGE 127 III 481, 494.

31 BGE 128 II 259, 268.

32 Ebenda.

33 BGE 129 I 232, 245.

34 RAINER J. SCHWEIZER, in: Bernhard Ehrenzeller/Philippe Mastronardi/Rainer J. Schweizer/Klaus A. Vallender (Hrsg.), Die schweizerische Bundesverfassung, Kommentar, Zürich/Basel/Genf 2002, BV 13 N 38.

35 Ebenda.

BGE 120 II 118, 122 I 153 und BGE 127 III 481 betreffen privatrechtliche Konstellationen; hier wird zwar der Begriff der informationellen Selbstbestimmung verwendet, aber in keiner Weise ein entsprechendes Grundrecht erwähnt. Die Behauptung, das Bundesgericht habe schon längst ein Grundrecht auf informationelle Selbstbestimmung anerkannt, ist damit falsch. Zwar hat das Bundesgericht im Jahr des Erscheinens der Kommentierung von SCHWEIZER (2002) tatsächlich ein solches Grundrecht geschaffen³⁶. Dieser Entscheid lag dem Autor beim Verfassen der Kommentierung aber offenbar nicht vor, zumal er ihn sonst sicherlich zitiert hätte. Mit der Behauptung des Autors, das Bundesgericht habe längst ein Grundrecht auf informationelle Selbstbestimmung anerkannt, entbindet er sich selbst von der Notwendigkeit, eine hinreichende Begründung für das Bestehen des von ihm postulierten Grundrechts anzuführen.

Damit zeigt sich, dass das Bundesgericht weder selbst noch über den Verweis auf die Kommentierung von RAINER J. SCHWEIZER eine Begründung für das Bestehen eines Grundrechts auf informationelle Selbstbestimmung vorgelegt hat. Das gilt auch für den Gehalt des Grundrechts, der darin gesehen wird, dass jede Person «selbst bestimmen können [soll], ob und zu welchem Zwecke Informationen über sie bearbeitet werden»³⁷. Hierfür verweist das Bundesgericht auf SCHWEIZER, der den Gehalt mit der Wendung «demnach» allein aus dem Begriff der informationellen Selbstbestimmung ableitet. Wie in der Rechtsprechung des Bundesgerichts fehlt auch bei SCHWEIZER jeder Hinweis auf die Schranken eines Grundrechts auf informationelle Selbstbestimmung, auf welche das deutsche Bundesverfassungsgericht bei dessen Schaffung mit aller Deutlichkeit hingewiesen hatte³⁸.

Ein nächster Entscheid des Bundesgerichts ging nicht über das Bisherige hinaus und verwies lediglich auf das Bestehen des Grundrechts auf informationelle Selbstbestimmung³⁹. In der Folge ist das Bundesgericht aber in mehreren Entscheiden einen Schritt weiter gegangen, indem es ein eigentliches *Herrschaftsrecht an Personendaten* anerkannt hat. Im Entscheid Google Street View von 2012 führte es aus: «Im Bereich des Datenschutzes garantiert das verfassungsmässig geschützte Recht auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV und Art. 8 Ziff. 1 der Konvention vom 4. November 1950 zum Schutze der Menschenrechte und Grundfreiheiten [EMRK; SR 0.101]), dass grundsätzlich ohne Rücksicht darauf, wie sensibel die fraglichen Informationen tatsächlich sind, dem Einzelnen die Herrschaft über seine personenbezogenen Daten

zusteht [Nachweise]»⁴⁰. In einem Entscheid zum Genfer Polizeigesetz führte es 2014 aus: «Dans le domaine de la protection des données, le droit à l'auto-détermination en matière d'informations personnelles, consacré par la Constitution (art. 13 al. 2 Cst. et art. 8 CEDH), garantit que l'individu demeure en principe maître des données le concernant, indépendamment du degré de sensibilité effectif des informations en cause [Verweis auf Entscheid Google Street View]». Eine Begründung für das Bestehen eines solchen Herrschaftsrechts führte das Gericht in beiden Entscheiden nicht an.

Das Bundesgericht hat dieses äusserst weitgehende Verständnis der informationellen Selbstbestimmung allerdings wieder aufgegeben. Die aktuelle Umschreibung, die sich in mehr oder minder identischer Form in den meisten jüngeren Entscheiden findet⁴¹, lautet: «Der Schutz der Privatsphäre umfasst den Anspruch jeder Person auf Schutz vor Missbräuchen ihrer persönlichen Daten (so ausdrücklich Art. 13 Abs. 2 BV). Im Bereich des Datenschutzes garantiert das verfassungsmässige Recht auf informationelle Selbstbestimmung, dass grundsätzlich ohne Rücksicht darauf, wie sensibel die fraglichen Informationen tatsächlich sind, jede Person gegenüber fremder, staatlicher oder privater Bearbeitung von sie betreffenden Informationen bestimmen können muss, ob und zu welchem Zweck diese Informationen über sie bearbeitet werden»⁴². Dieses Verständnis entspricht auch der Auffassung des Bundesrates in der Botschaft zum totalrevidierten DSG und der herrschenden Lehre⁴³.

Wie die kurze Analyse zeigt, steht die Entstehung des Grundrechts auf informationelle Selbstbestimmung in der Schweiz auf äusserst tönernen Füßen. Materiell tragfähig ist einzig der Verweis auf das Volkszählungsurteil des Bundesverfassungsgerichts in der Botschaft zum DSG und in der Rechtsprechung des Bundesgerichts⁴⁴. Allein auf dessen Erwägungen lässt sich die Anerkennung

40 BGE 138 II 346, 360; ebenso: BGE 145 IV 42, 46: «Das in Art. 13 Abs. 2 BV verankerte Recht auf informationelle Selbstbestimmung ist als Unterfall des Rechts auf Privatsphäre konzipiert [Nachweise]. Dieses garantiert dem Einzelnen die Herrschaft über seine personenbezogenen Daten, ohne Rücksicht darauf, wie sensibel die fraglichen Informationen sind.»

41 Eine Ausnahme ist BGE 145 IV 42, 46, in welchem das Bundesgericht wieder eine «Herrschaft» über die personenbezogenen Daten postuliert.

42 BGE 144 I 126, 131; im Wortlaut praktisch identisch auch BGE 148 I 233, 235 f., in welchem das Recht auf informationelle Selbstbestimmung mit dem Schutz der «informationellen Integrität» gleichgestellt wird; BGE 147 I 346, 349; mit Verweis auf den in Fn. 41 erwähnten Entscheid, aber ohne Annahme der Herrschaft BGE 147 I 103, 128 und BGE 146 I 11, 13. Ein etwas verkürzter Textbaustein, noch ohne Hinweis darauf, dass die Sensibilität der Informationen unerheblich ist, findet sich in den etwas älteren Entscheiden, etwa BGE 144 II 91, 105; BGE 144 II 77, 84; BGE 142 II 340, 346 f.; BGE 140 I 2, 22; BGE 129 I 232, 245.

43 Siehe dazu vorn, A.

44 BGE 120 II 118, mit Verweis auf die Botschaft, die ihrerseits auf das Urteil des Bundesverfassungsgerichts verweist; BGE 122 I 153; BGE 127 III 481, allerdings für privatrechtliche Konstellationen und nur mit Verweis auf die Botschaft; BGE 113 Ia 1, allerdings ohne Ausführungen zu einem Grundrecht auf informationelle Selbstbestimmung.

36 Siehe dazu gerade vorstehend, B.2.

37 BGE 129 I 232, 245.

38 Siehe dazu vorn, B.1.

39 BGE 133 I 77, 85.

eines solchen Grundrechts stützen. Das ist deshalb von Bedeutung, weil sich die Rechtsprechung in Deutschland und in der Schweiz in der Folge auseinanderentwickelt haben. Während die Schweiz das Grundrecht auf informationelle Selbstbestimmung zunehmend absoluter verstand und zwischenzeitlich gar von einem Herrschaftsrecht an den eigenen Daten ausging, hat das Bundesverfassungsgericht sein Verständnis von einem Recht auf informationelle Selbstbestimmung in einem jüngeren Urteil stark relativiert.

3. Wendepunkt

Im sog. «Recht auf Vergessen I»-Entscheid vom 6. November 2019 hatte das Bundesverfassungsgericht über eine Verfassungsbeschwerde gegen eine zivilrechtliche Entscheidung des Bundesgerichtshofs zu entscheiden. Dieser hatte die Klage eines Mannes gegen das Zugänglichmachen von mehr als 30 Jahre alten Presseberichten in einem Online-Archiv abgewiesen, in denen unter Nennung seines Namens über ihn berichtet wurde. Der Mann war 1982 rechtskräftig wegen Mordes verurteilt worden, nachdem er im Jahr davor auf einer Yacht bei einer Atlantiküberquerung zwei Menschen erschossen und einen dritten schwer verletzt hatte. 2002 war der Mann nach verbüßter Strafe aus der Haft entlassen worden. Mit Verfassungsbeschwerde rügte er eine Verletzung seines als Grundrecht geschützten allgemeinen Persönlichkeitsrechts. Das Bundesverfassungsgericht hat sich im Entscheid unter anderem zum Recht auf informationelle Selbstbestimmung geäußert, das eine eigene Ausprägung des allgemeinen Persönlichkeitsrechts und im Sinn einer mittelbaren Drittwirkung auch für das Verhältnis unter Privaten relevant sei⁴⁵. Es hat dabei die Bedeutung des Rechts auf informationelle Selbstbestimmung stark relativiert.

Mit Verweis auf das Volkszählungsurteil hielt das Bundesverfassungsgericht fest, das «Recht auf informationelle Selbstbestimmung [sei] von der Rechtsprechung zunächst als Schutz gegenüber der Datenerhebung und -verarbeitung des Staates und seiner Behörden entwickelt» worden, es gebe aber keinen Grund, diesen Grundrechtsschutz nicht auch auf das Verhältnis unter Privaten zu erstrecken⁴⁶. Unter Privaten stehe dem Recht auf informationelle Selbstbestimmung allerdings die Freiheit anderer gegenüber «selbst Informationen aufzugreifen, zu verarbeiten und nach eigenen, auch wechselnden Zwecken zu nutzen»⁴⁷. Daraus folgert das Gericht an der entscheidenden Stelle: «Ebenso wenig wie das Recht der Darstellung der eigenen Person enthält das Recht

auf informationelle Selbstbestimmung ein allgemeines oder gar umfassendes Selbstbestimmungsrecht über die Nutzung der eigenen Daten. Das Recht auf informationelle Selbstbestimmung gewährleistet den Einzelnen aber die Möglichkeit, in differenzierter Weise darauf Einfluss zu nehmen, in welchem Kontext und auf welche Weise die eigenen Daten anderen zugänglich und von ihnen genutzt werden. Es enthält damit die Gewährleistung, über der eigenen Person geltende Zuschreibungen selbst substantiell mitzuentcheiden»⁴⁸. «Ausgehend von dem Ziel des Rechts auf informationelle Selbstbestimmung, Schutz vor Gefahren angesichts neuartiger Möglichkeiten der Datenverarbeitung zu gewähren [Nachweise], [ist] es primär als Gewährleistung zu verstehen, die – neben der ungewollten Preisgabe von Daten auch im Rahmen privater Rechtsbeziehungen [Nachweise] – insbesondere vor deren intransparenter Verarbeitung und Nutzung durch Private schützt»⁴⁹.

Vom im Volkszählungsurteil vertretenen und in der Schweiz rezipierten Konzept, wonach das Recht auf informationelle Selbstbestimmung «die Befugnis des Einzelnen [ist], grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen»⁵⁰, ist damit nicht viel übrig geblieben. Während eine ungewollte Preisgabe und eine intransparente Nutzung von Daten im Rahmen privater Rechtsbeziehungen nach wie vor erfasst werden, vermittelt das Grundrecht nach dem heutigen Verständnis des Bundesverfassungsgerichts namentlich kein «allgemeines oder gar umfassendes Selbstbestimmungsrecht über die Nutzung der eigenen Daten»⁵¹, sondern nur das Recht, «in differenzierter Weise darauf Einfluss zu nehmen, in welchem Kontext und auf welche Weise die eigenen Daten anderen zugänglich und von ihnen genutzt werden»⁵² und über «der eigenen Person geltende Zuschreibungen selbst substantiell mitzuentcheiden»⁵³. Das Grundrecht soll dabei insb. vor «intransparenter Verarbeitung und Nutzung durch Private»⁵⁴ schützen.

Das Bundesverfassungsgericht hat das Grundrecht auf informationelle Selbstbestimmung mit diesem Entscheid zwar nicht aufgegeben, in der Substanz aber derart relativiert, dass der Begriff den Gehalt nicht mehr spiegelt. Man darf wohl davon ausgehen, dass das Bundesverfassungsgericht das mit dem Volkszählungsurteil geschaffene Grundrecht nicht als «informationelle Selbstbestimmung» bezeichnet hätte, wenn es dessen Gehalt schon damals so eng verstanden hätte, wie heute.

48 BVerfGE – 1 BvR 16/13, 87.

49 BVerfGE – 1 BvR 16/13, 90.

50 BVerfGE 65, 1, 43.

51 BVerfGE – 1 BvR 16/13, 87.

52 Ebenda.

53 Ebenda.

54 BVerfGE – 1 BvR 16/13, 90.

45 BVerfGE – 1 BvR 16/13, 83.

46 BVerfGE – 1 BvR 16/13, 85.

47 BVerfGE – 1 BvR 16/13, 87.

4. Zwischenerkenntnis

Die Analyse der historischen Entwicklung des Grundrechts auf informationelle Selbstbestimmung zeigt, dass weder das Bundesgericht noch der Bundesrat je eine Begründung für dessen Bestehen vorgelegt haben. Die materielle Grundlage für das schweizerische Grundrecht bildet vielmehr allein das Volkszählungsurteil des deutschen Bundesverfassungsgerichts. Nachdem dieses den Gehalt des Grundrechts vor einigen Jahren stark eingeschränkt hat, fehlt dem inhaltlichen Verständnis des Bundesgerichts heute jede Grundlage. Spätestens jetzt müsste es eingehend begründen, weshalb es ein Grundrecht auf informationelle Selbstbestimmung, verstanden als «Recht der betroffenen Person, grundsätzlich selbst zu bestimmen, ob und zu welchen Zwecken Daten über sie bearbeitet werden dürfen»⁵⁵, geben soll. Ohne eine solche Begründung beruht die Rechtsprechung des Bundesgerichts nur noch auf der intuitiven Überzeugungskraft des Begriffs der informationellen Selbstbestimmung. Das kann nicht genügen.

C. Tatsächliche Umsetzung: Illusion

Neben der Frage, ob das Bestehen eines Grundrechts auf informationelle Selbstbestimmung von Bundesrat oder Bundesgericht je hinreichend begründet wurde, stellt sich die nicht weniger grundlegende Frage, ob die Idee der informationellen Selbstbestimmung im DSG tatsächlich umgesetzt worden ist. Sollte dies zutreffen, liesse sich mit guten Gründen vertreten, dass der Gesetzgeber das Bestehen eines Rechts auf informationelle Selbstbestimmung mit Erlass des DSG implizit anerkannt und das Bundesgericht dieses Recht lediglich als Grundrecht qualifiziert hat.

Eine direkte Antwort auf diese Frage lässt sich dem DSG nicht entnehmen. Der Zweckartikel verweist jedenfalls nicht auf den Schutz des Grundrechts auf informationelle Selbstbestimmung, sondern – inhaltlich äusserst weit – auf den Schutz der Persönlichkeit und der (nicht näher spezifizierten) Grundrechte der betroffenen Personen (Art. 1 DSG). Die Frage muss damit indirekt, durch eine Analyse der Kernbestimmungen des DSG beantwortet werden. Im Vordergrund stehen dabei die Grundsätze der Datenbearbeitung, die Bestimmungen zur Rechtmässigkeit der Datenbearbeitung durch Private und Bundesorgane und diejenigen über die Pflichten der Verantwortlichen und Auftragsbearbeiter sowie die Rechte der betroffenen Personen. Zu beachten sind aber auch die Bestimmungen über die Durchsetzung des Datenschutzrechts, insb. die Rechtsansprüche der betroffenen Personen gegenüber privaten Datenbearbeitern, die Vorschriften über die Aufgaben und Befugnisse des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) und die Strafbestimmungen.

1. Grundsätze der Datenbearbeitung

Die Grundsätze der Datenbearbeitung bilden den normativen Kern des schweizerischen Datenschutzrechts. Sie lassen sich allerdings kaum mit der Idee der informationellen Selbstbestimmung erklären.

Die Grundsätze der Erkennbarkeit und der Zweckbindung (Art. 4 Abs. 3 f. aDSG; Art. 6 Abs. 3 DSG) sind zwar wesentliche Voraussetzungen für die informationelle Selbstbestimmung, weil die Ausübung dieses Rechts erfordert, dass die betroffenen Personen über die Verarbeitung der sie betreffenden Daten informiert sind und die Daten nicht zu Zwecken bearbeitet werden, die für sie nicht erkennbar sind. Die beiden Grundsätze vermitteln den betroffenen Personen aber keine Möglichkeit, darüber zu bestimmen, ob und zu welchem Zweck Daten über sie bearbeitet werden. Dasselbe gilt für den Grundsatz der Datensicherheit (Art. 7 aDSG; Art. 8 DSG). Dessen Einhaltung ist zwar eine

⁵⁵ Siehe dazu vorn, A. und B.2.

unabdingbare Voraussetzung für informationelle Selbstbestimmung, weil bei fehlender Datensicherheit weder der Verantwortliche noch die betroffenen Personen die Bearbeitung der Daten durch unbefugte Dritte kontrollieren oder verhindern können. Auch dieser Grundsatz vermittelt den Betroffenen aber keine Möglichkeit zur Bestimmung über die Bearbeitung der sie betreffenden Daten.

Auch die weiteren Grundsätze der Datenbearbeitung, der Grundsatz der Rechtmässigkeit (Art. 4 Abs. 1 aDSG; Art. 6 Abs. 1 DSG), der Grundsatz der Bearbeitung nach Treu und Glauben (Art. 4 Abs. 2 aDSG; Art. 6 Abs. 2 DSG), der Grundsatz der Verhältnismässigkeit (Art. 4 Abs. 2 aDSG; Art. 6 Abs. 2 DSG), der Grundsatz der Richtigkeit (Art. 5 aDSG; Art. 6 Abs. 5 DSG) und der Grundsatz der Speicherbegrenzung (Art. 6 Abs. 5 DSG⁵⁶) zielen nicht darauf ab, den betroffenen Personen Kontrolle über die Bearbeitung der sie betreffenden Daten zu vermitteln. Die Grundsätze der Datenbearbeitung setzen vielmehr allgemeine Leitplanken, die bei der Bearbeitung von Personendaten von Privaten und Bundesorganen einzuhalten sind. Diese sollen zwar den Interessen der Betroffenen dienen, vermitteln ihnen aber kein Recht selbst zu bestimmen, ob und zu welchen Zwecken Daten über sie bearbeitet werden.

2. Rechtmässigkeit der Datenbearbeitung

Die Bearbeitung von Personendaten ist nach der schweizerischen Konzeption des Datenschutzrechts zulässig, wenn die Grundsätze der Datenbearbeitung eingehalten werden. Für Bundesorgane bedeutet dies, dass die Bearbeitung auf einer gesetzlichen Grundlage beruhen muss. Das folgt aus dem datenschutzrechtlichen Grundsatz der Rechtmässigkeit (Art. 4 Abs. 1 aDSG; Art. 6 Abs. 1 DSG)⁵⁷ und wird mit dem Erfordernis der Rechtsgrundlage im DSG ausdrücklich normiert (Art. 17 aDSG; Art. 34 DSG), ergibt sich aber bereits aus dem Legalitätsprinzip der Bundesverfassung (Art. 5 Abs. 1 BV)⁵⁸. Für Private hat die Konzeption zur Folge, dass ihnen die Bearbeitung von Personendaten frei-

steht, wenn sie die Grundsätze der Datenbearbeitung einhalten. Anders als nach dem europäischen Datenschutzrecht, das auf dem Konzept des Verbots mit Erlaubnisvorbehalt⁵⁹ beruht, benötigen private Datenbearbeiter damit nur dann eine Rechtsgrundlage bzw. (in der Terminologie des DSG) einen Rechtfertigungsgrund, wenn sie gegen einen Grundsatz der Datenbearbeitung verstossen. Angesichts der grundlegenden Unterschiede ist für die Frage nach der Umsetzung der informationellen Selbstbestimmung im DSG zwischen der Bearbeitung von Personendaten durch Bundesorgane und Private zu unterscheiden.

2.1 Bearbeitung durch Bundesorgane

Die Bearbeitung von Personendaten durch Bundesorgane bedarf einer gesetzlichen Grundlage (Art. 17 aDSG; Art. 34 DSG). Von diesem Grundsatz bestanden unter bisherigem Recht keine Ausnahmen, das neue DSG sieht aber drei spezifische Ausnahmen vor. So dürfen Bundesorgane Daten nun auch ohne gesetzliche Grundlage bearbeiten, wenn der Bundesrat die Bearbeitung bewilligt hat, weil er die Rechte der betroffenen Personen für nicht gefährdet hält (Art. 34 Abs. 4 lit. a DSG), wenn die betroffene Person im Einzelfall in die Bearbeitung eingewilligt oder ihre Personendaten allgemein zugänglich gemacht und die Bearbeitung nicht ausdrücklich untersagt hat (Art. 34 Abs. 4 lit. b DSG) und wenn die Bearbeitung notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen und es nicht möglich ist, innert angemessener Frist eine Einwilligung einzuholen (Art. 34 Abs. 4 lit. c DSG). Weitere Ausnahmen bestanden im bisherigen und bestehen im geltenden Recht nur für die Bekanntgabe von Personendaten⁶⁰.

56 Zur Ableitung des Grundsatzes der Speicherbegrenzung aus dem Grundsatz der Verhältnismässigkeit unter dem aDSG siehe: MEIER (Fn. 4), § 4 Rz. 633; ferner EPINEY, in: Belser/Epiney/Waldmann (Fn. 3), § 9 Rz. 27; YVONNE PRIEUR, Datenschutz durch «Big-Data-Geschäfte» auf dem Prüfstand, AJP 2015, 1643 ff., 1649; FLORENT THOUVENIN, Forschung im Spannungsfeld von Big Data und Datenschutzrecht: eine Problemskizze, in: Volker Boehme-Nessler/Manfred Rehinder (Hrsg.), Big Data: Ende des Datenschutzes?, Gedächtnisschrift für Martin Usteri, Bern 2017, 27 ff., 33 f.

57 Ebenso: BRUNO BAERISWYL, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpfli Handkommentar., 2. Aufl., Bern 2023, DSG 6 N 5 und 9; EPINEY, in: Belser/Epiney/Waldmann (Fn. 3), § 9 Rz. 11; teilweise abweichend ROSENTHAL/JÖHRI (Fn. 4), DSG 4 N 11 f., der das Erfordernis der Rechtsgrundlage allein aus Art. 17 DSG ableitet.

58 Ebenso: BAERISWYL, in: Baeriswyl/Pärli/Blonski (Hrsg.) (Fn. 57), DSG 6 N 9; BALLENEGGER, in: Maurer-Lambrou/Blechte (Hrsg.) (Fn. 4), DSG 17 N 3.

59 Siehe dazu statt vieler: BENEDIKT BUCHNER/THOMAS PETRI, in: Jürgen Kühling/Benedikt Buchner (Hrsg.), Datenschutz-Grundverordnung, BDSG, Kommentar, München 2020, Art. 6 N 11 ff. In Anlehnung an die Konzeption der EU wird deshalb für die Schweiz teilweise von einer Erlaubnis mit Verbotsvorbehalt gesprochen; siehe dazu: DAMIAN GEORGE, Prinzipien und Rechtmässigkeitsbedingungen im privaten Datenschutzrecht, Kritische Betrachtungen zu Geschichte und Gegenwart eines Schutzkonzepts in der Schweiz und der Europäischen Union, Zürich/Basel/Genf 2021, 137; MARTIN STEIGER, Neues EU-Datenschutzrecht: Was gilt für Anwaltskanzleien?, Anwaltsrevue 2018, 205 ff., 207; DAVID VASELLA, Kapitel 7: Social Media und Datenschutz, in: Oliver Staffelbach/Claudia Keller (Hrsg.), Social Media und Recht für Unternehmen, Zürich/Basel/Genf 2015, 244.

60 Im Einzelnen: Bundesorgane dürfen im bisherigen und dürfen im geltenden Recht Personendaten an Dritte bekannt geben, wenn dafür eine Rechtsgrundlage besteht (Art. 19 Abs. 1 i.V.m. Art. 17 aDSG; Art. 36 Abs. 1 i.V.m. Art. 34 Abs. 1–3 DSG), die Daten für den Empfänger zur Erfüllung der gesetzlichen Aufgabe unentbehrlich sind (Art. 19 Abs. 1 lit. a aDSG; Art. 36 Abs. 2 lit. a DSG), wenn die betroffene Person in die Bekanntgabe eingewilligt hat (Art. 19 Abs. 1 lit. b aDSG; Art. 36 Abs. 2 lit. b DSG; für die Bekanntgabe ins Ausland: Art. 17 Abs. 1 lit. a DSG), wenn die betroffene Person die Daten allgemein zugänglich gemacht und ihre Bekanntgabe nicht ausdrücklich untersagt hat (Art. 19 Abs. 1 lit. c aDSG; Art. 36 Abs. 2 lit. d DSG) und wenn der

Das Erfordernis der gesetzlichen Grundlage deutet zwar an, dass die Bearbeitung von Personendaten durch ein Grundrecht der betroffenen Personen geschützt ist, das nur unter Einhaltung der Vorgaben von Art. 36 BV eingeschränkt werden kann⁶¹. Dabei kann es sich aber nicht um ein Grundrecht auf informationelle Selbstbestimmung handeln, dessen Gehalt, darin besteht, dass die betroffenen Personen grundsätzlich selbst bestimmen können, ob und zu welchen Zwecken Daten über sie bearbeitet werden dürfen⁶². Da Bundesorgane Personendaten nur bearbeiten dürfen, wenn eine gesetzliche Grundlage besteht und weil die betroffenen Personen beim Bestehen einer gesetzlichen Grundlage keine Möglichkeit haben, über die Bearbeitung der sie betreffenden Personendaten zu bestimmen, gibt es – abgesehen von den erwähnten Ausnahmen – keine Konstellationen, in denen ein Recht auf informationelle Selbstbestimmung bestehen könnte, in denen also Bundesorgane Personendaten bearbeiten dürfen und die betroffenen Personen zugleich über die Bearbeitung der sie betreffenden Personendaten bestimmen können. Ein Grundrecht auf informationelle Selbstbestimmung kann es damit nicht geben. Jedenfalls hätte ein solches Grundrecht keinen Anwendungsbereich. Denn: Beruht die Bearbeitung von Personendaten durch Bundesorgane auf einer gesetzlichen Grundlage, haben die betroffenen Personen keine Möglichkeit, über die Bearbeitung der sie betreffenden Daten zu bestimmen – fehlt hingegen eine gesetzliche Grundlage, dürfen Bundesorgane die Personendaten nicht bearbeiten.

An diesem Grundsatz vermögen auch die erwähnten Ausnahmen nichts zu ändern, zumal deren Bedeutung gering ist. Der überwiegende Teil der Ausnahmen betrifft nur die Bekanntgabe von Personendaten, nicht die anderen Formen der Bearbeitung, namentlich das Beschaffen, Speichern, Aufbewahren,

Empfänger glaubhaft macht, dass die betroffene Person die Einwilligung verweigert oder die Bekanntgabe sperrt, um ihm die Durchsetzung von Rechtsansprüchen oder die Wahrnehmung anderer schutzwürdiger Interessen zu verwehren (Art. 19 Abs. 1 lit. d aDSG; Art. 36 Abs. 2 lit. e DSG). Nach dem neuen Recht dürfen Bundesorgane Daten auch bekannt geben, wenn dies notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen und nicht innert angemessener Frist eine Einwilligung eingeholt werden kann (Art. 36 Abs. 2 lit. c DSG). Zudem dürfen Bundesorgane im bisherigen und dürfen im geltenden Recht auf Anfrage Name, Vorname, Adresse und Geburtsdatum einer Person bekannt geben, auch wenn dafür keine gesetzliche Grundlage besteht (Art. 19 Abs. 2 aDSG; Art. 36 Abs. 4 DSG). Ferner dürfen sie Personendaten im Rahmen der behördlichen Information der Öffentlichkeit bekannt geben, wenn die Personendaten im Zusammenhang mit der Erfüllung öffentlicher Aufgaben stehen und an deren Bekanntgabe ein überwiegendes öffentliches Interesse besteht (Art. 19 Abs. 1^{bis} aDSG; Art. 36 Abs. 3 DSG). Schliesslich sieht das neue Recht vor, dass die betroffene Person Widerspruch gegen die Bekanntgabe bestimmter Personendaten erheben kann, wenn sie ein schutzwürdiges Interesse glaubhaft macht (Art. 37 Abs. 1 DSG); das verantwortliche Bundesorgan weist ein solches Begehren aber ab, wenn eine Rechtspflicht zur Bekanntgabe besteht oder die Erfüllung seiner Aufgaben gefährdet würde (Art. 37 Abs. 2 DSG).

61 Siehe dazu hinten, D.1.

62 Siehe dazu vorn, A.

Verwenden und Löschen (Art. 3 lit. e aDSG; Art. 5 lit. d DSG). Für diese Bearbeitungen ist immer eine gesetzliche Grundlage erforderlich. Da Daten von einem Bundesorgan nur an Dritte bekannt gegeben werden können, wenn sie diese zuvor beschafft und gespeichert haben, führen die Ausnahmen für die Bekanntgabe nicht dazu, dass Bundesorgane Personendaten ohne gesetzliche Grundlage bearbeiten dürfen. Auch die neuen Ausnahmen vom Erfordernis der gesetzlichen Grundlage vermitteln den betroffenen Personen nur in zwei Konstellationen die Möglichkeit zur informationellen Selbstbestimmung, nämlich wenn sie im Einzelfall in die Bearbeitung eingewilligt oder ihre Personendaten allgemein zugänglich gemacht und die Bearbeitung nicht ausdrücklich untersagt haben (Art. 34 Abs. 4 lit. b DSG).

Damit ist klar, dass das DSG für die Bearbeitung von Personendaten durch Bundesorgane nicht auf einem Grundrecht auf informationelle Selbstbestimmung beruht. Das Bestehen eines solchen Grundrechts ist vielmehr eine Illusion.

2.2 Bearbeitung durch Private

Bei der Bearbeitung von Personendaten durch Private ist das Bild differenzierter. Diese ist, wie bereits erwähnt, stets zulässig, wenn die Grundsätze der Datenbearbeitung eingehalten werden. Das ist allerdings längst nicht immer der Fall, sodass sich regelmässig die Frage nach dem Vorliegen eines Rechtfertigungsgrundes stellt. In Frage kommen dabei die Einwilligung der betroffenen Person, ein überwiegendes öffentliches oder privates Interesse und das Gesetz (Art. 13 Abs. 1 aDSG; Art. 31 Abs. 1 DSG).

Der am prominentesten geregelte und am häufigsten diskutierte Rechtfertigungsgrund ist die Einwilligung der betroffenen Person (Art. 13 Abs. 1 i.V.m. Art. 4 Abs. 5 aDSG; Art. 31 Abs. 1 i.V.m. Art. 6 Abs. 6 f. DSG). Die Rechtfertigung durch Einwilligung lässt sich offensichtlich als unmittelbare Umsetzung der Idee der informationellen Selbstbestimmung verstehen. Sie hat im Datenschutzrecht allerdings längst nicht die Bedeutung, die betroffene Personen und datenschutzrechtliche Laien erwarten. Auch wenn die meisten Betroffenen davon ausgehen, dass die Bearbeitung der sie betreffenden Daten in der Regel (oder gar immer) auf ihrer Einwilligung beruht, ist die Einwilligung bei weitem nicht der wichtigste Rechtfertigungsgrund. Zwar gibt es keine vertieften empirischen Untersuchungen zur relativen Bedeutung der drei Rechtfertigungsgründe des DSG. Allen Fachpersonen – Datenschutzbeauftragten, Datenschutzanwäl:innen und Aufsichtsbehörden – ist jedoch klar, dass der mit Abstand wichtigste Rechtfertigungsgrund nicht die Einwilligung, sondern das Vorliegen eines überwiegenden Interesses ist, zu dem nach dem DSG auch die Bearbeitung von Personendaten im unmittelbaren Zusammenhang mit dem Abschluss

oder der Abwicklung eines Vertrags (Vertragserfüllung) gehört (Art. 13 Abs. 2 lit. a aDSG; Art. 31 Abs. 2 lit. a DSG). Dies zeigt auch eine im Winter 2023 durchgeführte Umfrage des Vereins Unternehmens-Datenschutz (VUD), an der sich 45 grosse Schweizer Unternehmen beteiligt haben⁶³. Die Umfrage zeigt zwar grosse Unterschiede zwischen verschiedenen Branchen, weshalb sich kaum Aussagen machen lassen, die für alle Unternehmen gleichermassen gelten. Die Erkenntnisse zur relativen Bedeutung der Rechtfertigungsgründe sind aber dennoch bemerkenswert. Zu beachten ist zunächst, dass mehr als die Hälfte der Unternehmen für mehr als die Hälfte der von ihnen durchgeführten Datenbearbeitungen das Vorliegen eines Rechtfertigungsgrundes im Sinn des DSG bzw. einer Rechtsgrundlage im Sinn der DSGVO prüft. Das bedeutet umgekehrt, dass weniger als die Hälfte der Unternehmen diese Prüfung für weniger als die Hälfte der Datenbearbeitungen vornimmt. Insgesamt prüfen die an der Umfrage beteiligten Unternehmen für etwa 60% der Datenbearbeitungen, ob ein Rechtfertigungsgrund bzw. eine Rechtsgrundlage vorliegt. Damit ist bereits klar, dass die übrigen 40% der Datenbearbeitungen nicht auf einer Einwilligung der betroffenen Personen beruht. Bei den Datenbearbeitungen, für die ein Rechtfertigungsgrund bzw. eine Rechtsgrundlage geprüft wird, liegt der Anteil der Einwilligung bei etwa zwei Dritteln der Unternehmen bei weniger als 20%, bei etwas mehr als 15% der Unternehmen bei 20–40% und bei je ca. 7,5% der Unternehmen bei 40–80% bzw. 80–100%. Von den Datenbearbeitungen, für die ein Rechtfertigungsgrund bzw. eine Rechtsgrundlage geprüft wird, beruht damit insgesamt etwas weniger als 25% auf einer Einwilligung. Mit Blick auf die gesamte Menge beträgt der Anteil der Datenbearbeitungen, der auf einer Einwilligung der betroffenen Personen beruht, damit weniger als 15%. Die übrigen Datenbearbeitungen beruhen entweder auf Gesetz oder – und dies vor allem – auf einem überwiegenden privaten oder öffentlichen Interesse unter Einschluss des Rechtfertigungsgrundes der Vertragserfüllung.

Die Interessenabwägung als bei weitem wichtigster Rechtfertigungsgrund des DSG beruht nicht auf der Idee der informationellen Selbstbestimmung, sondern auf der Notwendigkeit, Personendaten in einer Vielzahl von Situationen bearbeiten zu können – unabhängig vom (und bisweilen sogar entgegen dem) Willen der betroffenen Personen. Das DSG nennt selbst eine Reihe solcher Konstellationen, neben der Bearbeitung zur Vertragserfüllung (Art. 13 Abs. 2 lit. a aDSG; Art. 31 Abs. 2 lit. a DSG) die Bearbeitung zur Prüfung der Kreditwürdigkeit (Art. 13 Abs. 2 lit. c aDSG; Art. 31 Abs. 2 lit. c DSG) und diejenige zu nicht-personenbezogenen Zwecken, insb. für Forschung, Planung und Statistik (Art. 13 Abs. 2 lit. e aDSG; Art. 31 Abs. 2 lit. e DSG). Hinzu kommen

⁶³ Die Ergebnisse der vom VUD im Zusammenhang mit diesem Beitrag durchgeführten Umfrage sind in graphischer Darstellung auf der Webseite des VUD publiziert: <www.vud.ch>.

zahlreiche weitere Konstellationen, etwa die Bearbeitung zur Verhinderung von Straftaten, zum Erhalt der Gesundheit, zum Schutz von Eigentum oder zur Betrugsbekämpfung durch Banken, Versicherungen oder Kreditkartenunternehmen, oder die Bekanntgabe von Gesundheitsinformationen Verwandter im Rahmen einer medizinischen Behandlung⁶⁴. Auch rein wirtschaftliche Interessen können genügen, sogar schon das blosse Interesse, eine Datenbearbeitung möglichst effizient zu gestalten⁶⁵. Bei der Beurteilung des Vorliegens eines überwiegenden Interesses an der Datenbearbeitung werden die Interessen der betroffenen Person zwar berücksichtigt⁶⁶. Das ändert aber nichts daran, dass diese keine Möglichkeit hat, die Interessenabwägung zu beeinflussen, z.B. indem sie ihre eigene Sichtweise in die Beurteilung einbringt. Von einem Recht der Betroffenen, selbst zu bestimmen, ob und zu welchen Zwecken Daten über sie bearbeitet werden, kann damit in allen diesen Fällen nicht die Rede sein.

Immerhin haben die Betroffenen das Recht, Widerspruch gegen die Bearbeitung der sie betreffenden Daten zu erheben. Dieses Widerspruchsrecht ist zwar im DSG nicht als solches normiert⁶⁷, es ergibt sich aber aus der Bestimmung über die Persönlichkeitsverletzung, nach der insb. dann eine Persönlichkeitsverletzung vorliegt, wenn Private Personendaten gegen den ausdrücklichen Willen der betroffenen Person bearbeiten (Art. 12 Abs. 2 lit. b aDSG; Art. 30 Abs. 2 lit. b DSG). Die Bearbeitung kann allerdings selbst beim Vorliegen eines ausdrücklichen Widerspruchs gerechtfertigt werden. Das ergab sich im aDSG unmittelbar aus dem Wortlaut der Bestimmung (Art. 12 Abs. 2 lit. b aDSG «ohne Rechtfertigungsgrund Daten einer Person gegen deren ausdrücklichen Willen bearbeiten») und folgt im neuen DSG aus der Systematik des

⁶⁴ RAMPINI, in: Maurer-Lambrou/Blechta (Hrsg.) (Fn. 4), DSG 13 N 22; siehe BGer 6B_536/2009, E. 3.7 betreffend Überwachung am Arbeitsplatz zur Verhinderung von Straftaten durch Dritte; BGer 5A_57/2010, E. 2.2.3 und 4.1 betreffend Versicherungsleistungen; diese und zahlreiche weitere Beispiele aufführend MEIER (Fn. 4), § 12 Rz. 1615, 1621 ff. und 1630.

⁶⁵ BGE 138 II 346, 365; ebenso: RAMPINI, in: Maurer-Lambrou/Blechta (Hrsg.) (Fn. 4), DSG 13 N 22.

⁶⁶ Botschaft DSG, BBl 1988 II, 460; PFAFFINGER, in: Baeriswyl/Pärli/Blonski (Hrsg.) (Fn. 57), DSG 31 N 45; RAMPINI, in: Maurer-Lambrou/Blechta (Hrsg.) (Fn. 4), DSG 13 N 20; ROSENTHAL/JÖHRI (Fn. 4), DSG 13 N 16 und 20.

⁶⁷ Anders die DSGVO, die im Rahmen der Regelung der Rechte der betroffenen Person (Art. 12 ff. DSGVO) in Art. 21 DSGVO ein Widerspruchsrecht normiert. Im Gegensatz zum DSG besteht dieses Widerspruchsrecht allerdings nur, wenn die Verarbeitung der Personendaten auf dem berechtigten Interesse des für die Verarbeitung Verantwortlichen beruht (Art. 6 (f) DSGVO) oder wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt (Art. 6 (e) DSGVO). Darüber hinaus muss das Widerspruchsrecht aus Gründen ausgeübt werden, die sich aus der besonderen Situation der betroffenen Person ergeben (Art. 21 Abs. 1 Satz 1 DSGVO), z.B. aus Gründen, die sich auf das Familienleben beziehen, oder zum Schutz von Geschäftsgeheimnissen. Selbst wenn solche Gründe vorliegen, unterliegt das Widerspruchsrecht einer weiteren, weit gefassten Einschränkung, weil der Verantwortliche die Daten weiterhin bearbeiten darf, wenn er zwingende schutzwürdige Gründe nachweisen kann, welche die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen (Art. 21 Abs. 1 Satz 2 DSGVO).

Gesetzes (Art. 30 Abs. 2 lit. b i.V.m. Art. 31 DSG). Im Vordergrund steht auch hier die Rechtfertigung aus einem überwiegenden öffentlichen oder privaten Interesse⁶⁸. Wie die Einwilligung kann auch das Widerspruchsrecht der betroffenen Personen als Umsetzung der informationellen Selbstbestimmung verstanden werden. Dieses Recht wird allerdings in der Praxis nur selten ausgeübt und es entfällt, wie gerade ausgeführt, bei Vorliegen eines überwiegenden öffentlichen oder privaten Interesses. Die Bedeutung des Widerspruchsrechts ist damit gering.

Die Analyse der Bestimmungen zur Rechtmässigkeit der Bearbeitung von Personendaten durch Private zeigt, dass die Idee der informationellen Selbstbestimmung in diesem zentralen Bereich nur in Form der Einwilligung und des Widerspruchsrechts umgesetzt worden ist. Beide Konzepte sind zwar dogmatisch bedeutsam, in der Praxis aber nur von vergleichsweise geringer (Einwilligung) bzw. geringer (Widerspruchsrecht) Relevanz. Damit ist klar, dass sich die Bestimmungen über die Rechtmässigkeit der Datenbearbeitung, die zusammen mit den Grundsätzen der Datenbearbeitung den normativen Kern des privaten Datenschutzrechts ausmachen, nur punktuell, aber nicht insgesamt auf die Idee der informationellen Selbstbestimmung stützen lassen.

3. Rechte und Pflichten

Im Gegensatz zu den Grundsätzen und zur Rechtmässigkeit der Datenbearbeitung lassen sich die Rechte der Betroffenen eindeutig auf die Idee der informationellen Selbstbestimmung stützen. Das gilt für das Auskunftsrecht (Art. 8 f. aDSG; Art. 25 ff. DSG), das Recht auf Berichtigung (Art. 15 Abs. 1 aDSG; Art. 32 Abs. 1 und Art. 41 Abs. 2 lit. a DSG) und das Recht auf Löschung (Art. 15 Abs. 1 aDSG; Art. 32 Abs. 2 lit. b und Art. 41 Abs. 2 lit. a DSG) ebenso wie für das bereits erwähnte Widerspruchsrecht (Art. 12 Abs. 2 lit. b aDSG; Art. 30 Abs. 2 lit. b DSG)⁶⁹ und das mit der Totalrevision des aDSG neu geschaffene Recht auf Datenherausgabe und -übertragung (Art. 28 f. DSG). Ebendies gilt auch für die Informationspflichten des Verantwortlichen (Art. 14 und Art. 18a f. aDSG; Art. 25 ff. DSG), unter Einschluss der neu geschaffenen Pflicht zur Meldung von Verletzungen der Datensicherheit an die betroffenen Personen (Art. 24 Abs. 4 DSG), nicht aber für die weiteren Pflichten der Verantwortlichen, namentlich die bisherige Pflicht zur Meldung bestimmter Datensammlungen an den EDÖB (Art. 11a Abs. 3 aDSG) und die neuen Pflichten

zur Führung eines Verzeichnisses von Bearbeitungstätigkeiten (Art. 12 DSG), zur Durchführung einer Datenschutz-Folgenabschätzung (Art. 22 DSG) und zur Meldung von Verletzungen der Datensicherheit an den EDÖB (Art. 24 Abs. 1 f. DSG).

Zu beachten ist allerdings, dass die Informationspflichten und das Auskunftsrecht nur mittelbar der informationellen Selbstbestimmung dienen, indem sie den betroffenen Personen ermöglichen, sich Informationen über die Bearbeitung der sie betreffenden Daten zu beschaffen, ihnen aber nicht das Recht vermitteln, selbst über die Bearbeitung der Daten zu bestimmen. Hinzu kommt, dass teilweise gewichtige Ausnahmen von den Informationspflichten bestehen, namentlich wenn eine Bearbeitung gesetzlich vorgesehen ist (Art. 20 Abs. 1 lit. b DSG)⁷⁰, die Information nicht möglich ist oder einen unverhältnismässigen Aufwand erfordert (Art. 20 Abs. 2 DSG) oder überwiegende Interessen Dritter (Art. 20 Abs. 3 lit. a DSG) oder eines privaten Verantwortlichen (Art. 20 Abs. 3 lit. c DSG) vorliegen. Auch das Auskunftsrecht unterliegt einer Reihe von Einschränkungen, namentlich bei überwiegenden Interessen des Verantwortlichen (Art. 9 Abs. 4 aDSG; Art. 26 Abs. 2 lit. a DSG) oder Dritter (Art. 9 Abs. 1 lit. b; Art. 9 Abs. 1 lit. b aDSG; Art. 26 Abs. 1 lit. b DSG).

Die bedeutendste Einschränkung der Rechte der Betroffenen ergibt sich allerdings daraus, dass im DSG die Rechte gegenüber privaten Datenbearbeitern – anders als in der DSGVO⁷¹ – nicht als vorbehaltlos bestehende Betroffenenrechte normiert sind, sondern als Rechtsansprüche der Betroffenen, die nur bei einem Verstoss gegen die Vorgaben des DSG bestehen, insb. also beim Nichteinhalten eines Grundsatzes der Datenbearbeitung und gleichzeitigem Fehlen eines Rechtfertigungsgrundes. Das gilt namentlich für den Anspruch auf Unterlassung der Bearbeitung (Art. 15 Abs. 1 aDSG i.V.m. Art. 28a Abs. 1 Ziff. 1 ZGB; Art. 32 Abs. 2 lit. a DSG) und den Anspruch auf Löschung (Art. 15 Abs. 1 aDSG; Art. 32 Abs. 2 lit. b DSG) von Personendaten, aber nicht für den Anspruch auf Berichtigung (Art. 15 Abs. 1 aDSG;

70 Kritisch zu dieser Ausnahme: FLORENT THOUVENIN/NADJA BRAUN BINDER, Transparenz durch Datenschutzerklärungen von Behörden, ZSR 2022, 5–29, 20 f.

71 Siehe dazu Art. 15 ff. DSGVO. Allerdings werden auch die Betroffenenrechte der DSGVO nicht immer vorbehaltlos gewährt. So besteht das Recht auf Löschung nur, wenn einer von fünf in der DSGVO vorgesehenen Gründe vorliegt, bspw. wenn die personenbezogenen Daten für den Zweck, für den sie erhoben wurden, nicht mehr erforderlich sind (Art. 17 Abs. 1 Bst. a DSGVO), die betroffene Person ihre Einwilligung widerruft und es keinen anderen Rechtsgrund für die Rechtmässigkeit der Verarbeitung gibt (Art. 17 Abs. 1 Bst. b DSGVO) oder die Daten unrechtmässig bearbeitet wurden (Art. 17 Abs. 1 Bst. d DSGVO). Dasselbe gilt für das Recht auf Einschränkung der Bearbeitung, auch wenn die Situationen, in denen dieses Recht zum Tragen kommt, unterschiedlich sind (Art. 18 DSGVO).

68 In diesem Sinne in Bezug auf das Arbeitsrecht: SIMON WOLFER, Die elektronische Überwachung des Arbeitnehmers im privatrechtlichen Arbeitsverhältnis, Zürich/Basel/Genf 2008, 84.

69 Siehe dazu gerade vorstehend, C.2.2.2.

Art. 32 Abs. 1 DSGVO⁷². Als eigentliche Betroffenenrechte normiert sind einzig das Auskunftsrecht (Art. 8 ff. aDSG; Art. 25 ff. DSGVO) und das neue Recht auf Datenherausgabe und –übertragung (Art. 28 f. DSGVO). Anderes gilt zudem bei der Bearbeitung durch Bundesorgane, von denen die betroffenen Personen eine Berichtigung oder Löschung der Daten und ein Unterlassen der Bearbeitung verlangen können, wenn sie ein schutzwürdiges Interesse haben (Art. 25 Abs. 1 lit. a und Abs. 3 lit. b aDSG; Art. 41 Abs. 1 lit. a und Abs. 2 lit. a DSGVO). Auch die Betroffenenrechte vermitteln den Betroffenen damit nur sehr punktuell das Recht, selbst zu bestimmen, ob und zu welchen Zwecken Daten über sie bearbeitet werden dürfen.

4. Durchsetzung des Datenschutzrechts

Das Datenschutzrecht wird primär durch den EDÖB als Aufsichtsbehörde durchgesetzt. Die Aufgaben und Kompetenzen des EDÖB wurden mit der Totalrevision des DSGVO zwar erweitert, für die Frage nach der Umsetzung der informationellen Selbstbestimmung ergeben sich aber keine relevanten Unterschiede zum bisherigen Recht. Die Aufgabe des EDÖB besteht auch künftig vor allem darin, die Einhaltung der Vorgaben des DSGVO durch die Bundesorgane und die privaten Datenbearbeiter zu überwachen. Stellte der EDÖB einen Verstoß fest, konnte er unter bisherigem Recht Anpassungen oder ein Unterlassen der Bearbeitung lediglich empfehlen (Art. 27 Abs. 4 und Art. 29 Abs. 3 aDSG). Neu kann er auch Verfügungen erlassen und Anpassungen, Unterbrechungen oder ein Abbrechen der Bearbeitung anordnen (Art. 51 DSGVO).

Der EDÖB eröffnet von Amtes wegen oder auf Anzeige eine Untersuchung, wenn genügend Anzeichen für einen Verstoß gegen die Vorgaben des DSGVO oder anderer Datenschutzvorschriften vorliegen⁷³. Unter altem Recht hat er gegen Private nur eine Untersuchung eingeleitet, wenn eine Datensammlung

registriert werden musste (Art. 29 Abs. 1 lit. b aDSG), eine Informationspflicht bei einer grenzüberschreitenden Bekanntgabe von Personendaten bestand (Art. 29 Abs. 1 lit. c aDSG) oder – und das vor allem – wenn ein sog. Systemfehler vorlag, wenn also eine Datenbearbeitung geeignet war, die Persönlichkeit einer Vielzahl von Personen zu verletzen (Art. 29 Abs. 1 lit. a aDSG). Die Konzentration auf Systemfehler ist zwar entfallen, der EDÖB kann aber nach geltendem Recht von der Eröffnung einer Untersuchung absehen, wenn die Verletzung der Datenschutzvorschriften von geringfügiger Bedeutung ist (Art. 49 Abs. 2 DSGVO). Das Verfahren untersteht unter bisherigem und geltendem Recht der Official- und Untersuchungsmaxime, der EDÖB eröffnet eine Untersuchung also von sich aus und klärt den Sachverhalt von Amtes wegen ab⁷⁴. Partei des Verfahrens sind nur das Bundesorgan oder die private Person, gegen die eine Untersuchung eröffnet wurde, nicht die von der Datenbearbeitung betroffenen Personen⁷⁵. Diese haben keinen Einfluss auf das Verfahren und können kein Rechtsmittel gegen Verfügungen des EDÖB ergreifen⁷⁶. Hat eine betroffene Person Anzeige beim EDÖB erstattet, informiert er sie immerhin über die unternommenen Schritte und das Ergebnis einer allfälligen Untersuchung⁷⁷.

Die betroffenen Personen können ihre Rechte allerdings auch direkt gegenüber den Bundesorganen und den privaten Datenbearbeitern geltend machen und durchsetzen. Über die Ansprüche der Betroffenen entscheidet das verantwortliche Bundesorgan mit Verfügung (Art. 25 Abs. 4 aDSG; Art. 41 Abs. 5 DSGVO jeweils i.V.m. Art. 5 VwVG)⁷⁸; gegen diese kann Beschwerde beim Bundesverwaltungsgericht erhoben werden (Art. 47 Abs. 1 lit. b VwVG i.V.m. Art. 31 ff. VGG). Erfüllen private Datenbearbeiter die von den betroffenen Personen geltend gemachten Ansprüche nicht, verweigern sie also bspw. das Erteilen der Auskunft, müssen die Betroffenen Klage beim Zivilgericht erheben, um ihre Rechte durchzusetzen (Art. 15 aDSG; Art. 32 DSGVO). Das kommt allerdings in

⁷² Der Anspruch auf Berichtigung wird zwar im neuen DSGVO ebenfalls nur als Rechtsanspruch der Betroffenen und nicht als eigenständiges Betroffenenrecht normiert. Der Wortlaut von Art. 32 Abs. 1 DSGVO legt aber nahe und die Botschaft zum neuen DSGVO stellt klar, dass der Anspruch auf Berichtigung unabhängig vom Vorliegen einer Persönlichkeitsverletzung besteht und keine Rechtfertigungsgründe geltend gemacht werden können; Botschaft DSGVO, BBl 2017, 7076; DAVID ROSENTHAL, Das neue Datenschutzgesetz, Jusletter 16. November 2020, Rz. 139 f., der darin jedoch eine Fehlkonzeption sieht, die in der Praxis «bereinigt» werden müsse. Eine Persönlichkeitsverletzung fordernd hingegen: PFAFFINGER, in: Baeriswyl/Pärli/Blonski (Hrsg.) (Fn. 57), DSGVO 32 N 12; zum aDSG: ROSENTHAL/JÖHRI, (Fn. 4), DSGVO 15 N 18.

⁷³ Für das bisherige Recht: Art. 27 aDSG (für Bundesorgane) und Art. 29 aDSG (für Private). Siehe dazu auch ROSENTHAL/JÖHRI, (Fn. 4), DSGVO 27 N 6; BAERISWYL, in: Bruno Baeriswyl/Kurt Pärli (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, Bern 2015, DSGVO 29 N 1 ff. Für das geltende Recht: Art. 49 Abs. 1 DSGVO und dazu BRUNO BAERISWYL, in: Baeriswyl/Pärli/Blonski (Hrsg.) (Fn. 57), DSGVO 49 N 8.

⁷⁴ ROSENTHAL/JÖHRI, (Fn. 4), DSGVO 29 N 2 und 28 f.

⁷⁵ Für das bisherige Recht: ROSENTHAL/JÖHRI, (Fn. 4), DSGVO 29 N 21 und 42. Für das geltende Recht: Art. 52 Abs. 2 DSGVO; siehe dazu BAERISWYL, in: Baeriswyl/Pärli/Blonski (Hrsg.) (Fn. 57), DSGVO 53 N 6.

⁷⁶ Für das bisherige Recht in diesem Sinn ROSENTHAL/JÖHRI, (Fn. 4), DSGVO 29 N 42; ebenso BVGer A-7040/2009, E. 4.3.1 und BVGer A-3548/2018, E. 1.3. Für das geltende Recht: Das neue Datenschutzgesetz aus Sicht des EDÖB vom 9. Februar 2021, 7, abrufbar unter: <https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2021/revdsg.pdf.download.pdf/revDSG_DE.pdf> (zuletzt besucht am 20. Juni 2023).

⁷⁷ Art. 49 Abs. 4 DSGVO und dazu BAERISWYL, in: Baeriswyl/Pärli/Blonski (Hrsg.) (Fn. 57), DSGVO 49 N 24 ff. Auch unter bisherigem Recht wurde das Bestehen einer solchen Informationspflicht angenommen; siehe dazu HUBER, in: Maurer-Lambrou/Blechta (Hrsg.) (Fn. 4), DSGVO 27 N 6b und DSGVO 29 N 19.

⁷⁸ Siehe dazu: ROSENTHAL/JÖHRI, (Fn. 4), DSGVO 25 N 37 f.; STURNI, in: Baeriswyl/Pärli/Blonski (Hrsg.) (Fn. 57), DSGVO 25 N 45.

der Praxis kaum vor⁷⁹. Das gilt namentlich für die Ansprüche, die sich aus der Verletzung der Vorgaben des DSG ergeben (Art. 15 aDSG; Art. 32 DSG)⁸⁰. Zu diesen gibt es fast 30 Jahre nach Inkrafttreten des DSG keinen einzigen amtlich publizierten Entscheid des Bundesgerichts⁸¹. Das Bundesgericht hat sich zwar in den letzten Jahren mehrfach mit dem Auskunftsrecht gegenüber Privaten befasst. In den meisten Entscheiden ging es aber weniger um die Durchsetzung von datenschutzrechtlichen Ansprüchen, sondern um die teilweise missbräuchliche Verwendung des Auskunftsrechts⁸².

Der kurze Überblick macht deutlich, dass die Durchsetzung des DSG bisher ganz überwiegend durch den EDÖB als Aufsichtsbehörde erfolgte. Die betroffenen Personen machen ihre Rechte gegenüber den Verantwortlichen zwar durchaus geltend, setzen diese aber kaum je mit den zur Verfügung stehenden rechtlichen Mitteln durch. Auch wenn die Durchsetzung des Datenschutzrechts ohne eine hinreichend aktive Aufsichtsbehörde Illusion bleiben würde und der EDÖB sicherlich bestrebt ist, im besten Interesse der betroffenen Personen zu handeln, so ist doch offenkundig, dass sich die Durchsetzung der Vorgaben des Datenschutzrechts durch eine Aufsichtsbehörde nicht als Umsetzung der informationellen Selbstbestimmung verstehen lässt.

5. Zwischenerkenntnis

Die Analyse der Kernbestimmungen des bisherigen und des geltenden DSG hat gezeigt, dass die Idee der informationellen Selbstbestimmung für die Bearbeitung von Personendaten durch Bundesorgane überhaupt nicht und für die Bearbeitung durch Private nur punktuell umgesetzt worden ist.

Von zentraler Bedeutung ist die Erkenntnis, dass die betroffenen Personen die Bearbeitung von Personendaten durch Bundesorgane weder erlauben noch ver-

bieten können und (abgesehen von wenigen, kaum bedeutsamen Ausnahmen) auch sonst keine Möglichkeit haben, auf die Bearbeitung der sie betreffenden Daten Einfluss zu nehmen. Von der Umsetzung eines Grundrechts auf informationelle Selbstbestimmung kann damit nicht die Rede sein. Gegenüber Privaten haben die betroffenen Personen zwar die Möglichkeit, die Bearbeitung der sie betreffenden Personendaten in bestimmten Fällen durch Erteilen einer Einwilligung zu erlauben oder durch Erheben eines Widerspruchs zu verhindern. Da die weit überwiegende Zahl der Datenbearbeitungen durch Private aber nicht auf der Einwilligung der Betroffenen, sondern auf einer Interessenabwägung beruht, haben die Betroffenen auch hier nur beschränkte Möglichkeiten, selbst zu bestimmen, ob und zu welchem Zweck die sie betreffenden Daten bearbeitet werden. Auch die Regelung der Datenbearbeitung durch Private kann damit nicht als Umsetzung der Idee der informationellen Selbstbestimmung verstanden werden. Bei näherer Betrachtung der Kernbestimmungen des alten und neuen DSG wird vielmehr deutlich, dass die informationelle Selbstbestimmung eine blosse Illusion ist.

Die Analyse der Kernbestimmungen zeigt zwar, dass die betroffenen Personen nicht selbst bestimmen können, ob und zu welchem Zweck die sie betreffenden Daten bearbeitet werden. Zugleich wird aber auch deutlich, dass die Betroffenen nicht blosse Objekte der Datenbearbeitung sein sollen, sondern eine durchaus aktive Rolle einnehmen können, wenn sie möchten. Das zeigt sich namentlich im Grundsatz der Transparenz, bei den Informationspflichten, beim Auskunftsrecht und bei den weiteren Betroffenenrechten. Diese Normen vermitteln zwar kein Recht auf informationelle Selbstbestimmung, machen die betroffenen Personen aber immerhin zu Akteuren und Kontrolleuren der Bearbeitung der sie betreffenden Personendaten.

⁷⁹ In der Umfrage des VUD (siehe dazu vorn, Fn. 63) haben nur drei Unternehmen angegeben, dass betroffene Personen bereits einmal datenschutzrechtliche Ansprüche in einem Zivilverfahren gegen das Unternehmen geltend gemacht haben.

⁸⁰ Siehe dazu vorn, C.3.

⁸¹ Das Bundesgericht hat sich immerhin in zwei nicht amtlich publizierten Entscheiden (BGer 4A_188/2015 und BGer 5A_458/2018, E. 6) zu den Rechtsansprüchen nach Art. 15 aDSG geäußert. Bisweilen beschäftigen die kantonalen Gerichte zudem Unterlassungsklagen gegen die Bekanntgabe ihrer Daten an Dritte, meist im Kontext des Steuerstreits mit den USA; siehe dazu: AppGer BS, Urteil ZB.2019.3 vom 9. August 2019; OGer ZH Urteil HG160128-O vom 21. März 2018; OGer ZH Urteil HG140186-O vom 16. Dezember 2015 (geschützt vom BGer in BGer 4A_83/2016).

⁸² BGE 147 III 139; BGE 141 III 119; BGE 138 III 425. Eingehend zur rechtsmissbräuchlichen Ausübung des Auskunftsrechts zudem die nicht publizierten Entscheide BGer 4A_277/2020, E. 5.3; BGer 4A_506/2014 und 4A_524/2014, E. 8.

D. Normative Analyse: Implosion

Die Untersuchung der historischen Entwicklung⁸³ und der tatsächlichen Umsetzung des Grundrechts auf informationelle Selbstbestimmung im Datenschutzrecht⁸⁴ haben gezeigt, dass die Einführung eines solchen Grundrechts nie begründet und die Idee der informationellen Selbstbestimmung im DSG nur punktuell umgesetzt worden ist. Das lässt zwar grundlegende Zweifel an der Richtigkeit und Realisierbarkeit der Idee aufkommen, bedeutet aber noch nicht, dass ein solches Grundrecht nicht bestehen kann und aus einer normativen Perspektive das Grundprinzip des Datenschutzrechts bilden sollte. Es ist deshalb auch zu untersuchen, ob es eine überzeugende Begründung für die Anerkennung eines Grundrechts auf informationelle Selbstbestimmung gibt und das DSG als Folge dieser möglichen Erkenntnis künftig so ausgestaltet werden müsste, dass es den betroffenen Personen tatsächlich Selbstbestimmung über die sie betreffenden Daten vermittelt. Für diese Analyse ist zwischen der Bearbeitung von Personendaten durch Bundesorgane und Private zu unterscheiden.

1. Bearbeitung durch Bundesorgane

Der Bund ist für die Erfüllung seiner Aufgaben auf Daten über Einwohnerinnen und Einwohner angewiesen. Die erforderlichen Daten sind dabei ebenso vielfältig wie die Bundesaufgaben. Zu denken ist etwa an Stammdaten im Zivilstandsregister, Vermögensdaten für die Steuerverwaltung, Gesundheitsdaten für die obligatorische Kranken- und Unfallversicherung, Daten über die Ein- und Ausreise von Personen für die Aufgaben im Ausländer- und Asylrecht, Personaldaten von Bundesangestellten für das Arbeitsverhältnis und viele mehr⁸⁵. Da der Bund seine Aufgaben ohne diese Daten nicht zu erfüllen vermag, kann es nicht im Belieben der Einwohnerinnen und Einwohner sein, ob sie den Bundesorganen die erforderlichen Daten zur Verfügung stellen und zu welchem Zweck diese die Daten verwenden dürfen. Die Befugnis zur Bearbeitung von Personendaten ergibt sich vielmehr in fast allen Fällen⁸⁶ allein aus der gesetzlichen Grundlage, auf welche die Bundesorgane die Bearbeitung von Personendaten stützen müssen. Besteht eine solche Grundlage, hängt die Rechtmässigkeit der Datenbearbeitung allein vom Einhalten der Vorausset-

⁸³ Siehe dazu vorn, B.

⁸⁴ Siehe dazu vorn, C.

⁸⁵ Die Bundesbehörden müssen dem EDÖB die von ihnen durchgeführten Datenbearbeitungen melden (Art. 11a Abs. 2 aDSG/Art. 12 Abs. 4 DSG). Die Verzeichnisse der Bearbeitungstätigkeiten sind online abrufbar unter: <https://datareg.edoeb.admin.ch/>.

⁸⁶ Zu den wenigen Ausnahmen siehe vorn, C.2.2.1.

zungen der jeweiligen Bestimmung ab, nicht vom Willen der betroffenen Personen. Ein Grundrecht auf informationelle Selbstbestimmung, verstanden als Recht der betroffenen Personen, grundsätzlich selbst zu bestimmen, ob und zu welchem Zweck der Bund Daten über sie bearbeiten darf, kann und soll es deshalb nicht geben.

Das bedeutet allerdings nicht, dass es kein Grundrecht geben kann (und soll), welches der Bearbeitung von Personendaten durch den Bund Grenzen setzt und die Datenbearbeitung an das Einhalten der Voraussetzungen für Einschränkungen von Grundrechten knüpft. Denn nur ein solches Grundrecht vermag sicherzustellen, dass der Bund Personendaten nur bearbeiten darf, wenn eine gesetzliche Grundlage besteht (Art. 36 Abs. 1 BV), ein öffentliches Interesse vorliegt (Art. 36 Abs. 2 BV) und die Bearbeitung verhältnismässig ist (Art. 36 Abs. 3 BV). Denkbar wäre die Anerkennung eines Grundrechts auf Schutz personenbezogener Daten, wie es die Charta der Grundrechte der EU vorsieht (Art. 8 EU-Charta). Das liesse sich zwar über eine neue Auslegung von Art. 13 Abs. 2 BV erreichen, zumal ein Verständnis als Grundrecht auf Schutz von Personendaten näher am Wortlaut der Bestimmung liegen würde als die heutige Auffassung, die dieser ein Grundrecht auf informationelle Selbstbestimmung entnehmen will. Ein derart weitgehender Schritt scheint allerdings nicht erforderlich, zumal eine andere Auslegung von Art. 13 Abs. 2 BV ungleich näher liegt. Die Marginalie von Art. 13 BV stellt klar, dass mit dieser Norm ein Grundrecht auf Schutz der Privatsphäre garantiert wird. Damit lässt sich die Bestimmung zwanglos so verstehen, dass das Grundrecht nicht nur das Privat- und Familienleben, die Wohnung sowie den Brief-, Post- und Fernmeldeverkehr (Abs. 1), sondern auch die Bearbeitung von Personendaten (Abs. 2) umfasst. Dies dürfte auch der vom Bundesrat in der Botschaft zur Totalrevision der Bundesverfassung vertretenen Auffassung entsprechen, zumal er dort festgehalten hat: «Der Anspruch auf Datenschutz (Abs. 2) ist ein Teilaspekt des Rechts auf eine persönliche Geheimsphäre und soll deshalb im Zeitalter der Informationsgesellschaft in der Verfassung ausdrücklich erwähnt werden»⁸⁷. Mit Art. 13 Abs. 2 BV sollte damit kein neues Grundrecht geschaffen, sondern lediglich klargestellt werden, dass das Grundrecht auf Schutz der Privatsphäre auch bei der Bearbeitung von Personendaten besteht.

Dieses Verständnis wirft allerdings die Frage auf, weshalb die Bundesverfassung von einem «Anspruch auf Schutz vor Missbrauch» von Personendaten spricht. Man mag sich, wie ein Teil der Vertreter einer Auslegung im Sinn eines Grundrechts auf informationelle Selbstbestimmung, damit begnügen,

den Wortlaut von Art. 13 Abs. 2 BV als missglückt zu qualifizieren⁸⁸. Überzeugender erscheint allerdings, einen inhaltlichen Gleichlauf von Bundesverfassung und Datenschutzrecht herzustellen und einen Missbrauch von Personendaten durch den Staat immer dann anzunehmen, wenn Bundesorgane bei der Bearbeitung von Personendaten die Grundsätze des DSG nicht einhalten. Diese Grundsätze haben teilweise ohnehin Verfassungsrang, so namentlich das Erfordernis der gesetzlichen Grundlage, der im Grundsatz der Rechtmässigkeit zum Ausdruck kommt (Art. 5 Abs. 1 BV bzw. Art. 4 Abs. 1 aDSG und Art. 6 Abs. 1 DSG), der Grundsatz der Verhältnismässigkeit (Art. 5 Abs. 2 BV bzw. Art. 4 Abs. 2 aDSG und Art. 6 Abs. 2 DSG) und der Grundsatz von Treu und Glauben (Art. 5 Abs. 3 BV bzw. Art. 4 Abs. 2 aDSG und Art. 6 Abs. 2 DSG). Art. 13 Abs. 2 BV würde damit nur die spezifisch datenschutzrechtliche Ausprägung dieser Grundsätze rechtsstaatlichen Handelns enthalten. Bei diesem Verständnis würde das Grundrecht auf Schutz der Privatsphäre überdies die Rechte auf Transparenz der Datenbearbeitung, auf Einhalten der Zweckbindung, auf Richtigkeit der Personendaten und auf Gewährleistung einer angemessenen Datensicherheit umfassen. Dass diesen Grundsätzen Verfassungsrang zukommen kann, zeigt das Grundrecht auf Schutz personenbezogener Daten in der EU-Charta (Art. 8 EU-Charta), welches die Aspekte der Transparenz, der Zweckbindung und der Richtigkeit umfasst⁸⁹. Zu Recht misst ihnen auch ein Teil der schweizerischen Lehre Verfassungsrang zu⁹⁰. Anderes gilt nur für den Grundsatz der Datensicherheit. Da alle übrigen Vorgaben des Datenschutzrechts ins Leere gehen, wenn Personendaten nicht hinreichend gegen unbefugte Zugriffe geschützt sind, ist es allerdings naheliegend, auch einen grundrechtlichen Anspruch auf Gewährleistung einer angemessenen Datensicherheit anzuerkennen.

88 ROSENTHAL/JÖHRI (Fn. 4), DSG 17 N 30; MEIER (Fn. 4), § 1 Rz. 17; SCHWEIZER/STRIEGEL, in: Ehrenzeller/Egli/Hettich/Hongler/Schindler/Schmid/Schweizer (Fn. 4), BV 13 N 79; FRANZISKA SPRECHER, Datenschutz und Big Data im Allgemeinen und im Gesundheitsrecht im Besonderen / V.–VII., ZBJV 2018, 543; mit Verweis auf SCHWEIZER auch ROLF H. WEBER, Neue Grundrechtskonzeptionen zum Schutz der Privatheit, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Neuer Regulierungsschub im Datenschutzrecht?, Zürich/Basel/Genf 2012, 14.

89 Die Grundsätze der Zweckbindung und der Richtigkeit werden direkt, derjenige der Transparenz indirekt über den Grundsatz von Treu und Glauben und die Gewährleistung des Auskunftsrechts genannt. Siehe zum Ganzen: HEINRICH AMADEUS WOLFF, in: Matthias Pechstein/Carsten Nowak/Ulrich Häde (Hrsg.), Frankfurter Kommentar zu EUV, GRC und AEUV, Tübingen 2017, Art. 8 N 34; HANS D. JARASS, Charta der Grundrechte der Europäischen Union, 4. Aufl., München 2021, Art. 8 N 11.

90 EPINEY, in: Belser/Epiney/Waldmann (Fn. 3), § 9 Rz. 6; MAURER-LAMBROU/STEINER, in: Maurer-Lambrou/Blechte (Hrsg.) (Fn. 4), Vorbemerkungen zu DSG 4–11a N 1 f.; MARTIN SIGRIST, Staatsschutz oder Datenschutz?, Die Vereinbarkeit präventiver Datenbearbeitung zur Wahrung der inneren Sicherheit mit dem Grundrecht auf informationelle Selbstbestimmung, Zürich/Basel/Genf 2014, 22; BRUNO STERNATH/REINHARD ZWEIDLER, Einsatz von Video in der Evaluation – rechtlicher Rahmen, Datenschutz, Datensicherheit, SEVAL-Standards, LeGes 2014, 199 ff., 203.

87 Botschaft BV, BBl. 1997 I, 153.

2. Bearbeitung durch Private

Die Erkenntnis, dass es kein Grundrecht auf informationelle Selbstbestimmung geben kann, schliesst nicht aus, dass diese Idee die konzeptionelle Grundlage für die Regelung der Bearbeitung von Personendaten durch Private bilden könnte und allenfalls auch sollte. Dafür spricht, dass Personendaten als eine Emanation unseres Selbst verstanden werden können, quasi als (heute meist digitales) Abbild unseres Lebens. Aus der Idee der Bestimmung über das eigene Leben folgt dann – vermeintlich schlüssig – die Idee der Bestimmung über die Bearbeitung der Daten, die Informationen über das eigene Leben enthalten. Diese Perspektive dürfte denn auch dem intuitiven Verständnis der informationellen Selbstbestimmung entsprechen⁹¹. Eine zweite Begründung kann mit dem deutschen Bundesverfassungsgericht darin gesehen werden, dass Menschen für selbst bestimmtes Entscheiden und Handeln mit hinreichender Sicherheit wissen können sollten, «wer was wann und bei welcher Gelegenheit über sie weiss»⁹². Dieses Wissen erfordert allerdings kein Recht auf informationelle Selbstbestimmung, verstanden als «Recht der betroffenen Personen, grundsätzlich selbst zu bestimmen, ob und zu welchen Zwecken Daten über sie bearbeitet werden dürfen»⁹³. Vielmehr reichen hierfür Rechte und Pflichten zum Schaffen von Transparenz, wie sie das Datenschutzrecht als Grundsatz der Datenbearbeitung vorsieht und mit den Informationspflichten und dem Auskunftspflicht umsetzt⁹⁴. Im Gegensatz zur unzweifelhaft richtigen und für die betroffenen Personen wichtigen Gewährleistung von Transparenz vermag das intuitive Verständnis der informationellen Selbstbestimmung aus einer normativen Perspektive nicht zu überzeugen. Entscheidend sind drei Aspekte:

2.1 Menschliche Interaktion

Jede menschliche Interaktion beruht auf der Verarbeitung von Personendaten. Entsprechend verarbeiten wir in unseren Gehirnen ständig grosse Mengen an Daten über andere. Aber niemand käme auf die Idee, dass wir ein Recht darauf haben sollten, zu bestimmen, was andere über uns denken. Das gilt auch für Geschäftsbeziehungen, z.B. für Leser, die ihre Bücher bei der lokalen Buchhändlerin kaufen. Die Buchhändlerin wird mit der Zeit recht viele Informationen über die Gewohnheiten, Vorlieben und finanziellen Möglichkeiten ihrer

Kunden im Gedächtnis gespeichert haben, es würde aber niemand die Einführung eines Rechts fordern, das es den Kunden erlauben würde, über die Verarbeitung dieser Informationen im Gehirn der Buchhändlerin zu bestimmen. Warum sollte das grundlegend anders sein, wenn die Daten auf Papier oder auf einem elektronischen Datenträger erfasst, gespeichert und bearbeitet werden?

Zwischen der Verarbeitung von Daten im Gehirn eines Menschen und der Bearbeitung auf Papier oder elektronischen Datenträgern in privaten Organisationen bestehen zwar durchaus relevante Unterschiede. So sind die Verarbeitungskapazitäten von Menschen beschränkt, während die Bearbeitung in privaten Organisationen meist automatisiert erfolgt und damit nahezu beliebig skaliert werden kann. Auch die Weitergabe von Daten an Dritte ist bei einer Bearbeitung in Organisationen ungleich einfacher. Zudem besteht hier die Gefahr, dass sich Mitarbeitende oder Dritte unbefugten Zugang zu den Daten beschaffen. Diese Unterschiede mögen zwar Anlass für den Erlass von Rechtsregeln sein, die bei der Bearbeitung von Daten durch private Organisationen einzuhalten sind, bspw. in Form von Vorgaben zur Gewährleistung von Transparenz und Datensicherheit, sie vermögen aber kein Recht auf informationelle Selbstbestimmung zu begründen.

Wie die Analyse der tatsächlichen Umsetzung der informationellen Selbstbestimmung im DSGVO gezeigt hat, trifft es auch gar nicht zu, dass die betroffenen Personen ein umfassendes Recht hätten, über die Bearbeitung der sie betreffenden Daten durch private Organisationen zu bestimmen⁹⁵. Weil jede Interaktion – diejenige zwischen Menschen ebenso wie diejenige zwischen Menschen und Organisationen – auf der Bearbeitung von Personendaten beruht, kommen Gesetzgeber, Gerichte und Aufsichtsbehörden gar nicht umhin, eine Vielzahl von Fällen anzuerkennen, in denen Personendaten ohne die Einwilligung der betroffenen Person oder gar gegen deren Willen bearbeitet werden dürfen. Der Grund ist einfach: An einer Interaktion sind stets mindestens zwei Personen beteiligt, die betroffene Person und ihr Gegenüber. Die Idee der informationellen Selbstbestimmung berücksichtigt aber nur die Perspektive der betroffenen Person und blendet diejenige des Gegenübers aus. Sie negiert damit den Kern jeder Interaktion und der damit verbundenen Kommunikation, der im Senden und Empfangen von Information besteht. Dieser Vorgang ist zwar nicht notwendigerweise, aber meist reziprok, beide Beteiligten sind in der Regel Sender und Empfänger zugleich. Einem Beteiligten (oder bei einer Interaktion von zwei natürlichen Personen, beiden Beteiligten) ein Recht zuzugestehen, darüber zu bestimmen, ob und zu welchem Zweck das Gegenüber Informationen über sie bearbeiten darf, würde bedeuten, die Interaktion und die damit verbun-

⁹¹ Siehe dazu vorn, A.

⁹² BVerfGE 65, 1, 43. Das Bundesgericht hat dagegen schon vor Jahren festgehalten, dass «ein generelles Recht eines jeden [...], jederzeit zu wissen, wer was über ihn weiss [...] jedenfalls in dieser allgemeinen Form kaum praktikabel» wäre und «im Ergebnis jegliche Kommunikation zum Erliegen bringen» könnte; so BGE 124 I 176, 183.

⁹³ Siehe dazu vorn, A.

⁹⁴ Siehe dazu vorn, C.1 und C.3.

⁹⁵ Siehe dazu vorn, C.

dene Kommunikation in einzelne Informationsteile aufzuspalten und jeweils einem Beteiligten die Herrschaft über diese Teile zuzuweisen. Wird dieses Herrschaftsrecht ausgeübt und der einen Seite die Bearbeitung bestimmter Informationen verwehrt, funktioniert Kommunikation nicht mehr, weil sie im Austausch aufeinander bezogener Informationen besteht und dieser Austausch in sich zusammenfällt, wenn ihm einzelne Teile entzogen werden. Denkt man die Idee der informationellen Selbstbestimmung konsequent zu Ende, schafft sie Bedingungen, unter denen eine sinnvolle Kommunikation jedenfalls dann nicht mehr möglich ist, wenn das Recht auf informationelle Selbstbestimmung nicht nur als theoretisches Konstrukt im Raum steht, sondern auch tatsächlich ausgeübt wird⁹⁶. Damit scheint klar, dass es ein solches Recht weder geben kann noch geben soll.

2.2 Bedarf und Aufwand, Kosten und Nutzen

Die Idee der informationellen Selbstbestimmung beruht auf der Annahme, dass sich die betroffenen Personen für die Bearbeitung der sie betreffenden Daten interessieren und selbst bestimmen wollen, ob und zu welchen Zwecken diese Daten bearbeitet werden. Ob diese Annahme zutrifft, ist allerdings zweifelhaft. Empirische Untersuchungen gibt es, soweit ersichtlich, nur zur Frage, ob Menschen der Schutz ihrer Privatsphäre wichtig ist. Das wird in aller Regel bejaht⁹⁷. Diesen Aussagen lässt sich aber nichts über den Bedarf der befragten Personen nach informationeller Selbstbestimmung entnehmen, weil diese zwar dem Schutz der Privatsphäre dienen kann, der Schutz der Privatsphäre aber keine informationelle Selbstbestimmung erfordert, sondern auch anders gewährleistet werden kann. Ob die Annahme zutrifft, dass die betroffenen Personen selbst bestimmen wollen, ob und zu welchen Zwecken sie betreffende Daten bearbeitet werden, lässt sich derzeit empirisch nicht direkt beantworten. Die Frage kann allerdings offen bleiben. Denn ein Recht auf informationelle Selbstbestimmung macht jedenfalls nur Sinn, wenn die betroffenen Personen

nicht nur angeben, dass sie gerne selbst über die Bearbeitung der sie betreffenden Daten bestimmen möchten, sondern die auf der Grundlage eines solchen Rechts gewährten Ansprüche auch tatsächlich nutzen.

Die Ausübung eines Rechts auf informationelle Selbstbestimmung ist für die betroffenen Personen mit einem gewissen Aufwand verbunden. Die Gewährung eines solchen Rechts ist deshalb nur sinnvoll, wenn die Betroffenen bereit sind, diesen Aufwand auf sich zu nehmen. Das ist allerdings bei der weit überwiegenden Mehrheit nicht der Fall. Nur wenige Betroffene nutzen ihre Rechte, etwa das Auskunfts- oder Widerspruchsrecht⁹⁸, und Studien zeigen, dass Datenschutzerklärungen kaum gelesen werden⁹⁹. Das deckt sich auch mit der eigenen Erfahrung: Anstatt dass wir uns über die Bearbeitung der uns betreffenden Daten informieren und zumindest in denjenigen Fällen die Möglichkeit zur informationellen Selbstbestimmung nutzen, in denen sie besteht, klicken wir meist auf «Akzeptieren», wenn wir gefragt werden, ob wir mit der Bearbeitung der uns betreffenden Daten einverstanden sind. Das vermag kaum zu erstaunen, zumal die Bearbeitung von Personendaten heute omnipräsent ist und wir uns über eine Vielzahl von komplexen Bearbeitungsvorgängen Gedanken machen müssten, um einen informierten Entscheid über die Bearbeitung der uns betreffenden Personendaten zu fällen. Zugegeben, die heute bestehenden Mittel sind oft wenig nutzerfreundlich. Hilfreicher als das Anzeigen unzähliger «Cookie Banners» sind technische Mittel, die es erlauben, die eigenen Präferenzen in allgemeiner Weise festzulegen, bspw. durch entsprechende Einstellungen in Smartphones oder Browsern. Die beschränkte Nutzung der schon heute bestehenden Möglichkeiten zeigt dennoch, dass die betroffenen Personen in der Regel nicht bereit sind, den Aufwand zu betreiben, um darüber zu bestimmen, ob und zu welchen Zwecken sie betreffende Daten bearbeitet werden. Dies zeigt sich deutlich im fehlenden Interesse an der Nutzung bestehender Angebote zur Ausübung von informationeller Selbstbestimmung, die bisweilen als «*Personal Information Management Systems (PIMS)*»

⁹⁶ Zu einem ähnlichen Ergebnis ist das Bundesgericht schon vor Jahren in BGE 124 I 176, 183 gelangt; siehe dazu vorn, Fn. 92.

⁹⁷ In einer Studie des Beratungsunternehmens KPMG gaben 2021 86% der befragten Amerikaner an, dass der Datenschutz ihnen zunehmend Sorge bereitet («is a growing concern»); siehe dazu <https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2021/corporate-data-responsibility-bridging-the-consumer-trust-gap.pdf>. In einer im Herbst 2019 in Deutschland durchgeführten Studie gaben 82% der befragten Personen an, um den Schutz ihrer Daten im Internet «ein bisschen» oder «sehr» besorgt zu sein; siehe dazu ANASTASIA KOZYREVA/STEFAN HERZOG/PHILIPP LORENZ-SPREEN/RALPH HERTWIG/STEPHAN LEWANDOWSKY, Artificial Intelligence in online Environments, Representative Survey of public Attitudes in Germany, Berlin 2020, 12, abrufbar unter: https://pure.mpg.de/rest/items/item_3188061_4/component/file_3195148/content (beide zuletzt besucht am 20. Juni 2023). Siehe zudem die Übersicht bei HELEN NISSENBAUM, Privacy in Context, Stanford 2009, 104 f., m.w.H.

⁹⁸ Die Umfrage des VUD (siehe dazu vorn, Fn. 63) hat gezeigt, dass die meisten Unternehmen nur wenige Betroffenenrechtsanfragen erhalten. Ungefähr ein Drittel der Unternehmen erhält weniger als 10 Anfragen pro Jahr, ein zweites Drittel etwa 10–50 und ein drittes Drittel zwischen 50 und 1000. Vier der 44 Unternehmen, welche die Frage nach den Betroffenenrechten beantwortet haben, erhalten allerdings mehr als 1000 Anfragen pro Jahr.

⁹⁹ ALEECIA M. McDONALD/LORRIE FAITH CRANOR, The Cost of Reading Privacy Policies, I/S: A Journal of Law and Policy for the Information Society, Vol. 4/2008, 543 ff., 565, die davon ausgehen, dass ein amerikanischer Internetnutzer jährlich 201 Stunden mit dem Lesen von Datenschutzerklärungen verbringen müsste; NISSENBAUM (Fn. 97), 105; RAZIEH NOKHBEH ZAEEM/RACHEL L. GERMAN/K. SUZANNE BARBER, PrivacyCheck: Automatic Summarization of Privacy Policies Using Data Mining, ACM Transactions on Internet Technology, Vol. 18 No. 4 2018, 2, m.w.H.

bezeichnet werden, etwa die Dienste von POSMO oder MIDATA¹⁰⁰. Solche Angebote bestehen teilweise seit Jahren, sie werden aber kaum genutzt¹⁰¹.

Die geringe Nutzung der bestehenden Möglichkeiten zur informationellen Selbstbestimmung wirft die Frage auf, ob die (begrenzte) Kontrolle, welche das Datenschutzrecht den betroffenen Personen über die sie betreffenden Daten vermittelt, überhaupt von Nutzen ist. Selbst wenn man davon ausgeht, dass die Möglichkeit zur Selbstbestimmung für die Betroffenen einen Wert hat, müsste der Nutzen der Selbstbestimmung gegen die damit verbundenen Kosten abgewogen werden. Denn auch das Datenschutzrecht kann sich der für alle Rechtsnormen entscheidenden Frage nicht entziehen, ob es insgesamt einen gesellschaftlichen Nutzen schafft oder mehr Kosten verursacht als Nutzen stiftet.

Zu den gesellschaftlichen Kosten des Datenschutzrechts liegen kaum verlässliche Zahlen vor. Anekdotische Belege legen aber nahe, dass die Kosten für die Einhaltung der DSGVO für die grossen Technologie-Unternehmen (Big Tech) im dreistelligen Millionenbereich und für viele andere grosse Unternehmen, die Kunden in der EU haben, im zweistelligen Millionenbereich liegen¹⁰². Die im Winter 2023 durchgeführte Umfrage des VUD zeigt grosse

¹⁰⁰ Die Genossenschaft POSMO bezweckt den Aufbau einer Plattform für Mobilitätsdaten. Diese sollen externen Dienstleistern zur Verfügung gestellt werden und die Entstehung eines innovativen Ökosystems fördern. Die Genossenschaft MIDATA möchte zur Förderung der digitalen Selbstbestimmung eine sichere IT-Plattform zur Verwaltung von Gesundheits- und Bildungsdaten betreiben. Vertieft zum Ganzen: ROLF H. WEBER/FLORENT THOUVENIN, Gutachten zur Möglichkeit der Einführung eines Datenportabilitätsrechts im schweizerischen Recht und zur Rechtslage bei Personal Information Management Systems (PIMS) vom 22. Dezember 2017, 16 f., abrufbar unter: <https://www.itsl.uzh.ch/dam/jcr:26f84429-2aef-47b1-9ba1-6f6e8910c60d/180321%20BJ-Gutachten_final.pdf> (zuletzt besucht am 20. Juni 2023).

¹⁰¹ WEBER/THOUVENIN (Fn. 100), 39 f.

¹⁰² Konkrete und verlässliche Zahlen liegen nicht vor und die meisten Unternehmen werden nicht bereit sein, die sie betreffenden Zahlen zu veröffentlichen. Einige Hinweise lassen sich aber öffentlich zugänglichen Aussagen entnehmen. Nach einer Schätzung von Forbes bspw. kostet die Einhaltung der Anforderungen der DSGVO die Fortune-500-Unternehmen durchschnittlich je rund 16 Millionen Dollar; siehe dazu: OLIVER SMITH, The GDPR Racket: Who's Making Money From This \$9bn Business Shakedown, Forbes, 2. Mai 2018, abrufbar unter: <<https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/#4727a86434a2>>; ähnlich JEREMY KAHN/STEPHANIE BODONI/STEFAN NICOLA, It'll Cost Billions for Companies to Comply With Europe's New Data Law, Bloomberg Businessweek, 22. März 2018, abrufbar unter: <<https://www.bloomberg.com/news/articles/2018-03-22/it-ll-cost-billions-for-companies-to-comply-with-europe-s-new-data-law>>; RITA HEIMES/SAM PFEIFLE, Study: GDPR's global reach to require at least 75 000 DPOs worldwide, iapp, 9. November 2016, abrufbar unter: <<https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/>>. Eine Umfrage von PwC bei 200 Unternehmen mit jeweils mehr als 500 Angestellten ergab 2017, dass 77% der Teilnehmenden erwarteten, mehr als USD 1 Mio. für die *compliance* mit der DSGVO aufwenden zu müssen; siehe dazu: <<https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/pwc-gdpr-series-pulse-survey.pdf>>. Jüngere Untersuchungen haben gezeigt, dass Unternehmen, die der DSGVO unterstehen, einen Gewinnrückgang von 8% und einen Umsatzrückgang von 2% aufweisen; die grossen Technologieunternehmen waren von diesem Rückgang aber nicht betroffen, siehe

Unterschiede zwischen den befragten Unternehmen, mit Kosten von weniger als CHF 100 000 bis zu über CHF 1 Mio¹⁰³. Das sind allerdings nur die direkten Kosten für die *compliance*. Noch schwerer einzuschätzen, aber ungleich grösser dürften die indirekten Kosten für den entgangenen Nutzen sein, der mit der Bearbeitung von Personendaten geschaffen werden könnte, insb. in Forschung und Entwicklung, aber auch bei der Entwicklung und Einführung innovativer Geschäftsmodelle. Zwar lässt gerade das DSG viel Raum für eine sinnvolle und durchaus permissive Anwendung der gesetzlichen Vorgaben. Dennoch werden viele innovative Projekte erschwert, verteuert und verzögert, ohne dass dem ein klarer Nutzen entgegensteht.

Insgesamt kann damit kaum angenommen werden, dass eine Regulierung der Bearbeitung von Personendaten, die auf der Idee der informationellen Selbstbestimmung beruht, der Gesellschaft mehr Nutzen bringt als Kosten verursacht.

2.3 Daten als öffentliche Güter

Daten sind ihrer Natur nach öffentliche Güter¹⁰⁴. Das gilt nicht nur für Sach-, sondern auch für Personendaten. Diese Qualifikation mag zwar aus der Perspektive des Datenschutzrechts und der informationellen Selbstbestimmung geradezu ketzerisch klingen. Abwehrreflexe gegenüber dieser Erkenntnis vermögen an ihrer Richtigkeit aber nichts zu ändern.

Öffentliche Güter zeichnen sich dadurch aus, dass sie gleichzeitig von einer Vielzahl von Personen genutzt werden können, ohne dass die Nutzung durch eine Person diejenige durch eine andere beeinträchtigt (sog. nicht-rivalisierende

CHINCHIH CHEN/CARL BENEDIKT FREY/GIORGIO PRESIDENTE, Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally, Working Paper No. 2022-1, abrufbar unter: <<https://www.oxfordmartin.ox.ac.uk/downloads/Privacy-Regulation-and-Firm-Performance-Giorgio-WP-Upload-2022-1.pdf>> (alle zuletzt besucht am 20. Juni 2023).

¹⁰³ In der Umfrage des VUD (siehe dazu vorn, Fn. 63) haben nur 36 Unternehmen die Frage nach den Kosten für die Umsetzung der Anforderungen der DSGVO und/oder des neuen DSG beantwortet. Von diesen konnten oder wollten 12 Unternehmen keine Angaben zu den Kosten machen. Die übrigen 24 Unternehmen schätzten ihre Kosten wie folgt ein: 8 Unternehmen: weniger als CHF 100 000; 7 Unternehmen: CHF 100 000–500 000; 2 Unternehmen: CHF 500 000–1 Mio.; 7 Unternehmen über CHF 1 Mio.

¹⁰⁴ Statt vieler: RICHARD A. POSNER, Economic Analysis of Law, 9. Aufl., New York 2014, 402; ROBERT COOTER/THOMAS ULEN, Law and Economics, 6. Aufl., Boston 2016, 40; HANS-BERND SCHÄFER/CLAUS OTT, Lehrbuch der ökonomischen Analyse des Zivilrechts, 6. Aufl., Berlin 2020, 86 f.; HERBERT ZECH, Information als Schutzgegenstand, Tübingen 2012, 117 ff.; DERS., Daten als Wirtschaftsgut – Überlegungen zu einem «Recht des Datenerzeugers», CR 2015, 139; ROLF SCHWARTMANN/CHRISTIAN-HENNER HENTSCH, Parallelen aus dem Urheberrecht für ein neues Datenverwendungsrecht, PinG 2016, 121; THOMAS HEYMANN, Rechte an Daten, Warum Daten keiner eigentumsrechtlichen Logik folgen, CR 2016, 652 f.; FLORENT THOUVENIN, Wem gehören meine Daten?, SJZ 2017, 24; KEVIN MACCABE, Eigentum an digitalen Daten im sachenrechtlichen Sinne, Jusletter IT vom 26. September 2018, Rz. 12.

rende Nutzung)¹⁰⁵. Klassische Beispiele sind das Feuer eines Leuchtturms, das Bestehen von Frieden, Werke der Literatur und Kunst im Sinn des Urheberrechts oder Erfindungen im Sinn des Patentrechts. Regelmässig wird die Qualifikation als öffentliches Gut von einem zweiten Merkmal abhängig gemacht, das vorliegt, wenn Dritte nicht von der Nutzung des Gutes ausgeschlossen werden können (sog. nicht-ausschliessbare Nutzung)¹⁰⁶. Das Vorliegen dieses Merkmals hängt allerdings von den tatsächlichen und rechtlichen Möglichkeiten zur Einschränkung der Nutzung eines Gutes ab, nicht von der Natur des Gutes allein. Bei Daten stehen dabei die faktische Kontrolle, bspw. durch Speichern in proprietären Systemen oder Verschlüsselung, und die rechtlichen Möglichkeiten zum Ausschluss von Dritten im Vordergrund, insb. durch den Schutz als Fabrikations- und Geschäftsgeheimnisse. Ob Daten auch das zweite Merkmal öffentlicher Güter erfüllen, hängt damit massgeblich von der Ausgestaltung der Rechtsordnung ab. Für die vorliegende Frage, bei der gerade zu entscheiden ist, ob die betroffenen Personen durch die Gewährung eines Rechts auf informationelle Selbstbestimmung über die Bearbeitung der sie betreffenden Daten bestimmen können sollen, kann nicht auf dieses zweite Merkmal abgestellt werden, weil sonst die zweite Voraussetzung für die Qualifikation von Daten als öffentliches Gut mit der Folge dieser Qualifikation zusammenfallen würde (Zirkelschluss). Entscheidend ist damit allein das erste Merkmal öffentlicher Güter, die nicht-rivalisierende Nutzung. Dieses Merkmal liegt in der Natur von Daten begründet und bleibt damit der Verfügbarkeit der Rechtsordnung entzogen. Diesem zentralen Umstand wird hier Rechnung getragen, indem Daten als «ihrer Natur nach öffentliche Güter» bezeichnet werden¹⁰⁷.

Wegen der Möglichkeit zur nicht-rivalisierenden Nutzung ist der Nutzen eines seiner Natur nach öffentlichen Gutes für die Gesellschaft am grössten, wenn das Gut von jedermann genutzt werden kann. Rechte, die es einer Person erlauben, die Nutzung eines öffentlichen Gutes durch andere einzuschränken – bspw. ein Recht auf informationelle Selbstbestimmung – sollten deshalb nur gewährt werden, wenn diese Einschränkungen zur Erreichung anderer wichtiger Ziele erforderlich sind. Die Gewährung von Rechten an öffentlichen Gütern bedarf

damit stets der Rechtfertigung. Bei Personendaten stehen zwei Konstellationen im Vordergrund:

Die Zuweisung eines Rechts auf informationelle Selbstbestimmung wäre zum einen angezeigt, wenn ein Marktversagen vorliegen würde. Das ist namentlich der Fall, wenn ein für die Gesellschaft wertvolles Gut nicht (oder nicht im erwünschten Umfang) produziert wird, weil potentielle Produzenten nicht in der Lage sind, die von ihnen geschaffenen Güter am Markt zu verwerten. In diesem Fall könnte die Rechtsordnung mit der Gewährung von Ausschliesslichkeitsrechten Anreize für die Produktion der Güter setzen und die damit verbundene Beschränkung der Nutzung dieser Güter in Kauf nehmen¹⁰⁸. Dieser Begründungsansatz wurde im Zusammenhang mit der Forderung nach der Schaffung eines «Dateneigentums» diskutiert¹⁰⁹. Heute dürfte allerdings unbestritten sein, dass es bei der Produktion von Personendaten grundsätzlich kein Marktversagen gibt und der Gesetzgeber keine Anreize setzen sollte, um das Sammeln und Nutzen von Personendaten (noch) weiter zu fördern¹¹⁰.

Ein Eingreifen des Rechts wäre zum andern erforderlich, wenn die betroffenen Personen vor Schäden oder anderen rechtlich relevanten Nachteilen geschützt werden müssten, die von privaten Organisationen durch die Bearbeitung von Personendaten verursacht werden. Die Bearbeitung von Personendaten verursacht den Betroffenen zwar kaum je einen Schaden im Rechtssinn, die Gefahr von rechtlich relevanten Nachteilen besteht aber durchaus, insb. in Form von Diskriminierung oder Manipulation. Der Schutz gegen diese Nachteile erfordert allerdings kein Recht auf informationelle Selbstbestimmung. Ein solches Recht würde kaum helfen, weil die betroffenen Personen in aller Regeln nicht vorhersehen können, in welchen Konstellationen ihnen durch die Bearbeitung der sie betreffenden Personendaten ein Nachteil entstehen könnte. Ein indirekter Schutz gegen rechtlich relevante Nachteile durch die Gewährung eines

105 COOTER/ULEN (Fn. 104), 40; SCHÄFER/OTT (Fn. 104), 86. An der nicht-rivalisierenden Nutzung von Daten ändert nichts, dass der Wert von Daten für die Nutzer abnehmen kann, wenn eine Vielzahl von Personen die Daten nutzt. So ist es zwar richtig, dass der Wert von Daten über frei verfügbare Parkplätze in einer Stadt abnimmt, wenn viele Leute Zugang zu diesen Daten haben (FRANCIS CHENEVAL, Property rights of personal data and the financing of pensions, CRISPP 2018, 6). Das liegt aber nicht an der nicht-rivalisierenden Nutzung der Daten, sondern an der rivalisierenden Nutzung der Parkplätze.

106 COOTER/ULEN (Fn. 104), 40; SCHÄFER/OTT (Fn. 104), 86 f.

107 Näheres zum Ganzen: FLORENT THOUVENIN/ROLF H. WEBER/ALFRED FRÜH, Elemente einer Datenpolitik, Zürich/Basel/Genf 2019, 9 f.

108 Ein typisches Beispiel ist die Gewährung von Urheberrechten und Patenten, die wichtige Anreize setzen, damit Unternehmen in die Produktion und Vermarktung von Werken der Literatur und Kunst bzw. in Forschung und Entwicklung investieren; siehe dazu statt vieler: FLORENT THOUVENIN, Funktionale Systematisierung von Wettbewerbsrecht (UWG) und Immaterialgüterrechten, Köln/Berlin/München 2006, 288 f. (für das Patentrecht) und 322 f. (für das Urheberrecht), jeweils m.w.H.

109 Siehe dazu: THOUVENIN/WEBER/FRÜH (Fn. 107), 36 ff.

110 Von diesem Grundsatz bestehen allerdings gewichtige Ausnahmen. Namentlich hat sich gezeigt, dass die Nutzung von Daten in vielen Konstellationen mit Schwierigkeiten verbunden ist und das Potential von Daten nur ungenügend genutzt werden kann. Der Bund fördert deshalb das Entstehen von vertrauenswürdigen Datenräumen; siehe dazu: <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-87780.html> (zuletzt besucht am 20. Juni 2023) und der Gesetzgeber wird möglicherweise zeitnah ein Rahmengesetz für die Sekundärnutzung von Daten erlassen; zum Stand der Arbeiten siehe: <https://www.parlament.ch/de/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=61080> (zuletzt besucht am 20. Juni 2023).

Rechts auf informationelle Selbstbestimmung ist deshalb nicht sinnvoll. Notwendig sind vielmehr Normen, welche die rechtlich relevanten Nachteile direkt erfassen, insb. ein allgemeines Verbot von Diskriminierung aufgrund geschützter Merkmale, das auch für Private gilt¹¹¹, und ein Erfassen von Manipulation über die Generalklauseln des allgemeinen Persönlichkeitsrechts (Art. 28 ZGB) und des Bundesgesetzes gegen den unlauteren Wettbewerb (Art. 2 UWG).

3. Zwischenerkenntnis

Die normative Analyse hat gezeigt, dass es keine überzeugenden Gründe für die Gewährung eines Rechts auf informationelle Selbstbestimmung gibt. Die Idee der informationellen Selbstbestimmung fällt damit in sich zusammen – sie implodiert.

Die Bundesorgane sind für die Erfüllung ihrer Aufgaben in vielen Fällen auf Daten über die Einwohnerinnen und Einwohner angewiesen. Es kann deshalb nicht im Belieben der betroffenen Personen stehen, ob und zu welchen Zwecken Bundesorgane Daten über sie bearbeiten dürfen. Ein so verstandenes Grundrecht auf informationelle Selbstbestimmung kann und sollte es deshalb nicht geben.

Zugunsten eines Rechts auf informationelle Selbstbestimmung als konzeptionelle Grundlage für die Regelung der Bearbeitung von Personendaten durch Private lässt sich anführen, dass Personendaten als Emanation einer Person verstanden werden können und die Selbstbestimmung über die eigene Person auch die Selbstbestimmung über die sie betreffenden Daten umfassen müsse. Gegen diesen intuitiv überzeugenden Begründungsansatz sprechen allerdings gewichtige Gründe. Zum einen nimmt der Ansatz nur die betroffene Person in den Blick und blendet die Perspektive des Gegenübers aus. Dieses ist in vielen Fällen auf die Bearbeitung von Personendaten angewiesen, weshalb der betroffenen Person kein Recht gewährt werden sollte, dem Gegenüber die Bearbeitung der sie betreffenden Daten zu verbieten. Zudem beruht die menschliche Interaktion auf Kommunikation, die aus dem Senden und Empfangen aufeinander bezogener Informationen besteht. Diese Kommunikation kann nur funktionieren, wenn keiner der Beteiligten die Möglichkeit hat,

über die Bearbeitung der empfangenen Informationen durch den anderen zu bestimmen. Zum anderen hat sich gezeigt, dass die bestehenden Möglichkeiten zur informationellen Selbstbestimmung von den betroffenen Personen kaum genützt werden. Besteht aber kein relevanter Bedarf nach informationeller Selbstbestimmung, ist auch nicht ersichtlich, weshalb ein solches Recht gewährt werden sollte, zumal ein Datenschutzrecht, das auf der Idee der informationellen Selbstbestimmung beruht, der Gesellschaft hohe Kosten verursacht, weil private Organisationen einen erheblichen Aufwand für die *compliance* betreiben müssen und sinnvolle Nutzungen von Personendaten erschwert und verteuert oder gar verhindert werden. Hinzu kommt, dass Personendaten ihrer Natur nach öffentliche Güter sind. Der Nutzen solcher Güter ist für eine Gesellschaft dann am grössten, wenn sie frei verwendet werden können. Da ein Recht auf informationelle Selbstbestimmung die Nutzung von Personendaten stark einschränken würde, sollte ein solches Recht nur gewährt werden, wenn es erforderlich wäre, um andere wichtige Ziele zu erreichen, namentlich das Verhindern von Marktversagen oder von rechtlich relevanten Nachteilen der betroffenen Personen. Ein allgemeines Marktversagen liegt beim Sammeln und Nutzen von Personendaten allerdings nicht vor und das Eintreten von rechtlich relevanten Nachteilen kann nur mit spezifischen, auf den jeweiligen Nachteil ausgerichteten Normen wirksam verhindert werden, nicht durch ein Recht auf informationelle Selbstbestimmung.

¹¹¹ Denkbar sind drei Ansätze: (1) Der Gesetzgeber könnte ein allgemeines Gleichbehandlungsgesetz schaffen, das auch Diskriminierungen durch Private erfasst. (2) Da Diskriminierung in der Regel auf der Bearbeitung von Personendaten beruht, könnte sie durch einen neuen Grundsatz des Datenschutzrechts erfasst werden, nach welchem die Bearbeitung von Personendaten nicht zu einer Diskriminierung der betroffenen Personen führen darf. (3) Im Rahmen des geltenden Rechts könnten Gerichte eine Diskriminierung durch Private als Persönlichkeitsverletzung qualifizieren und über das allgemeine Persönlichkeitsrecht (Art. 28 ZGB) erfassen.

E. Erkenntnisse und Alternativen

Es fällt schwer, sich von einer Illusion zu verabschieden. Das gilt erst recht, wenn sie intuitiv überzeugt, (zumindest vermeintlich) den eigenen Interessen dient und über viele Jahre von Experten und Laien hochgehalten wurde. Wie die Analyse der historischen Entwicklung¹¹², der (fehlenden) tatsächlichen Umsetzung¹¹³ und die normative Betrachtung¹¹⁴ gezeigt haben, ist die Idee der informationellen Selbstbestimmung aber jedenfalls dann nicht haltbar, wenn sie so wie in der Schweiz verstanden wird, nämlich als «Recht der betroffenen Person, grundsätzlich selbst zu bestimmen, ob und zu welchen Zwecken Daten über sie bearbeitet werden dürfen». Man mag, wie das deutsche Bundesverfassungsgericht, am Begriff festhalten und ihn derart aushöhlen, dass der Gehalt des Grundrechts mit seiner Bezeichnung kaum noch etwas gemein hat¹¹⁵. Ehrlicher und zielführender ist es aber, den Begriff und die Idee der informationellen Selbstbestimmung ganz aufzugeben.

Löst man sich von dieser Illusion, wird der Blick frei für andere und sinnvollere konzeptionelle Grundlagen des Datenschutzrechts. Man braucht dabei weder erfinderisch zu sein noch weit zu suchen – ein Blick in die Bundesverfassung genügt: Das zentrale Konzept, das der rechtlichen Erfassung der Bearbeitung von Personendaten seit jeher zugrunde liegt, ist der Schutz der Privatsphäre. Das gilt für die Bearbeitung von Personendaten durch den Staat ebenso wie für diejenige durch Private. Die Bundesverfassung sieht in Art. 13 ein Grundrecht auf Schutz der Privatsphäre vor, das geeignet ist, alle Aspekte der Privatsphäre zu erfassen, den physischen Raum ebenso wie die persönlichen Beziehungen, die klassischen Kommunikationsformen ebenso wie die elektronischen und die Bearbeitung von Informationen ebenso wie diejenige von Daten. Die Gliederung in die beiden Absätze lässt sich dabei zwanglos so verstehen, dass das Grundrecht nicht nur das Privat- und Familienleben, die Wohnung sowie den Brief-, Post- und Fernmeldeverkehr (Abs. 1), sondern auch die Bearbeitung von Personendaten (Abs. 2) umfasst¹¹⁶. Über die mittelbare Drittwirkung der Grundrechte (Art. 35 Abs. 3 BV) lässt sich ableiten, dass der Gesetzgeber den Schutz der Privatsphäre auch unter Privaten sicherzustellen hat. Zum gleichen Resultat gelangt man über eine Auslegung des Zweckartikels des DSG. Dieser stellt klar, dass das DSG unter Privaten den Schutz der Persönlichkeit von Personen bezweckt, über die Personendaten bearbeitet werden (Art. 1 aDSG;

112 Siehe dazu vorn, B.

113 Siehe dazu vorn, C.

114 Siehe dazu vorn, D.

115 Siehe dazu vorn, B.3.

116 Siehe dazu vorn, D.1.

Art. 1 DSGVO). Der Begriff der Persönlichkeit ist zwar breiter als jener der Privatsphäre, er umfasst aber nach herrschender Auffassung den Schutz der Privatsphäre¹¹⁷. Jede Bearbeitung von Personendaten, welche die Privatsphäre der betroffenen Personen verletzt, kann damit als Persönlichkeitsverletzung qualifiziert und vom Zweck des DSGVO umfasst werden.

Mit dem Fokus auf den Schutz der Privatsphäre kommt der Frage nach deren Gehalt zentrale Bedeutung zu. Diese Frage erscheint heute mit Blick auf die vielfältigen digitalen Kontexte offener und komplexer denn je. Eine Klärung kann dieser Beitrag nicht leisten; dazu ist vertiefte interdisziplinäre Forschung erforderlich. Immerhin scheint es möglich, erste Grundlinien zu skizzieren: Der Privatsphäre kommt jedenfalls zwischen Menschen entscheidende Bedeutung zu. Für die meisten Menschen ist es zentral, grundsätzlich selbst entscheiden zu können, welche Informationen über sie oder ihn anderen Menschen zugänglich gemacht werden. Offen erscheint hingegen, ob es auch eine Privatsphäre gegenüber Maschinen geben kann. Die meisten Menschen scheinen es jedenfalls kaum als problematisch zu empfinden, wenn (oft auch intime) Daten auf einem Rechner in der Cloud gespeichert werden – solange sichergestellt ist, dass kein Mensch auf diese Informationen zugreifen kann. Diesem Aspekt tragen das bisherige und das geltende Datenschutzrecht denn auch bereits Rechnung, indem im Rahmen der Vorgaben für die Gewährleistung der Datensicherheit eine Zugriffskontrolle verlangt wird (Art. 8 Abs. 1 lit. e und Art. 9 Abs. 1 lit. g aDSV; Art. 3 Abs. 1 lit. a DSGVO)¹¹⁸. Neben dieser zwischenmenschlichen Konzeption von Privatsphäre mag man auch den Schutz gegen Überwachung durch den Staat und grosse Unternehmen als zentrale Komponente verstehen. Selbst wenn die Daten nie von einem Menschen eingesehen werden, führt die Kumulation von grossen Datenmengen bei einzelnen Akteuren zu einem potentiell «gläsernen Bürger», dessen Privatsphäre vielleicht noch nicht verletzt, wohl aber in hohem Mass gefährdet ist und deshalb geschützt werden sollte.

117 ANDREAS MEILI, in: Thomas Geiser/Christiana Fountoulakis (Hrsg.), Basler Kommentar zum Zivilgesetzbuch I, 7. Aufl., Basel 2022, ZGB 28 N 26; mit dem Hinweis auf die «informationelle» Privatsphäre ausdrücklich BGE 143 III 297, 311; HEINZ HAUSHEER/REGINA E. AEBI-MÜLLER, Das Personenrecht des Schweizerischen Zivilgesetzbuches, 5. Aufl., Bern 2020, Rz. 664f.; ANDREA BÜCHLER, in: Jolanta Kren Kostkiewicz/Stephan Wolf/Marc Amstutz/Roland Fankhauser (Hrsg.), Schweizerisches Zivilgesetzbuch, Orell Füssli Kommentar, 4. Aufl., Zürich 2021, ZGB 28 N 5; REGINA E. AEBI-MÜLLER, in: Peter Breitschmid/Alexandra Jungo (Hrsg.), Personen- und Familienrecht – Partnerschaftsgesetz, Handkommentar zum Schweizer Privatrecht, 3. Aufl., Zürich 2016, ZGB 28 N 22.

118 Regelungen über den Zugriff auf Personendaten finden sich zudem in den datenschutzrechtlichen Bestimmungen zahlreicher Erlasse, etwa in der Verordnung über die Informations- und Speichersysteme des Nachrichtendienstes des Bundes (SR 121.2; Art. 5 ff. sowie Anhänge), in der Verordnung über das elektronische Patientendossier (SR 816.11; Art. 2 ff.) oder in der Verordnung für die von der Ausgleichsstelle der Arbeitslosenversicherung betriebenen Informationssysteme (SR 837.063.1; Art. 9, 11, 20, 25 sowie Anhänge).

Neben dem Schutz der Privatsphäre sind zwei weitere Aspekte bedeutsam: Zum einen sollte die Rechtsordnung sicherstellen, dass niemand durch die Bearbeitung von ihm oder sie betreffenden Personendaten einen rechtlich relevanten Nachteil erleidet, insb. durch Diskriminierung oder Manipulation. Der Schutz gegen diese Nachteile sollte allerdings nicht im Datenschutzrecht, sondern in spezifischen Erlassen vorgesehen oder in Anwendung der Generalklauseln des allgemeinen Persönlichkeitsrechts (Art. 28 ZGB) und des UWG (Art. 2 UWG) sichergestellt werden. Zum andern haben Personendaten einen wirtschaftlichen Wert. Dieser wird allerdings nicht durch die betroffenen Personen selbst geschaffen, sondern im Zusammenwirken mit Unternehmen, welche die Daten sammeln, speichern, aufbereiten und auswerten. Damit die Betroffenen am Wert der sie betreffenden Daten partizipieren können, sollte die Rechtsordnung Ansprüche vorsehen, die es ihnen ermöglichen, eine Kopie der Daten zu erhalten und die Daten selbst zu nutzen oder an Dritte weiterzugeben. Soweit keine überwiegenden Interessen der Daten bearbeitenden Unternehmen entgegenstehen, sollten die Betroffenen zudem die Möglichkeit haben, der Nutzung der sie betreffenden Personendaten zu widersprechen oder sie gegen Bezahlung eines Entgelts oder Nutzung eines Dienstes zu erlauben. Entsprechende Rechte waren teils schon im bisherigen, sind aber jedenfalls im geltenden DSGVO mit dem Recht auf Kopie (Art. 8 Abs. 2 lit. a aDSG; Art. 25 Abs. 2 lit. b DSGVO), dem Recht auf Datenherausgabe und -übertragung (Art. 28 DSGVO) und dem Widerspruchsrecht (Art. 12 Abs. 2 lit. b aDSG; Art. 30 Abs. 2 lit. b DSGVO) vorgesehen. Ob diese Rechte von den Betroffenen künftig in relevantem Umfang genutzt werden, wird sich allerdings erst noch weisen müssen.

Neben der rechtlichen Umsetzung dieser drei Aspekte – dem Schutz der Privatsphäre, dem Schutz gegen Nachteile und der Möglichkeit der betroffenen Personen, am Wert der sie betreffenden Personendaten zu partizipieren – wird die Rechtsordnung weitere Regeln für die Bearbeitung von Personendaten bereitstellen müssen, denen allerdings nur eine dienende Funktion zukommt. Zentral sind dabei Normen zur Gewährleistung der Transparenz, weil die betroffenen Personen ihre Privatsphäre nur schützen, gegen Nachteile nur vorgehen und am Wert der sie betreffenden Personendaten nur partizipieren können, wenn sie über ausreichende Informationen verfügen, um zu erkennen, wer zu welchen Zwecken welche sie betreffenden Personendaten bearbeitet. Unverzichtbar sind schliesslich Vorgaben zur Datensicherheit, weil keiner der drei Aspekte ohne hinreichende Sicherheit der Personendaten erreicht werden kann.

Die skizzierten Grundlinien für eine differenzierte rechtliche Einfassung der Bearbeitung von Personendaten sind einstweilen nur Denkanstösse. Erst eine vertiefte Analyse wird zeigen, ob diese Ansätze belastbar sind und inwiefern sie modifiziert, differenziert und ergänzt – oder durch andere Konzepte ersetzt werden müssen.

Das Datenschutzrecht beruht nach weit verbreiteter Auffassung auf der Idee der informationellen Selbstbestimmung. Nach der Rechtsprechung des Bundesgerichts handelt es sich dabei gar um ein Grundrecht. Es versteht darunter das Recht der betroffenen Person, grundsätzlich selbst zu bestimmen, ob und zu welchen Zwecken Daten über sie bearbeitet werden dürfen. Diesem Verständnis hat sich der Bundesrat in der Botschaft zum neuen DSG angeschlossen. Die Idee der informationellen Selbstbestimmung leuchtet zwar intuitiv ein, hält einer näheren Betrachtung aber nicht stand. Eine Analyse des DSG zeigt, dass die Idee für die Bearbeitung von Personendaten durch Bundesorgane im DSG überhaupt nicht und für diejenige durch Private nur punktuell umgesetzt worden ist. Tatsächlich lässt sich eine «informationelle Selbstbestimmung» weder sinnvoll rechtlich umsetzen noch überzeugend normativ begründen. Die Idee sollte deshalb aufgegeben und das DSG auf eine tragfähige konzeptionelle Grundlage gestellt werden.

Der Autor

Florent Thouvenin, Prof. Dr. iur., Rechtsanwalt, Ordinarius für Informations- und Kommunikationsrecht und Vorsitzender des Leitungsausschusses des Center for Information Technology, Society, and Law (ITSLS) an der Universität Zürich

