

NIK R. ROEINGH

Geheime Daten

*Schriften zum
Recht der Digitalisierung*



Mohr Siebeck

Schriften zum Recht der Digitalisierung

Herausgegeben von

Florian Möslein, Sebastian Omlor und Martin Will

Band 53



Nik R. Roeingh

Geheime Daten

Staatlicher Datenzugang und
grundrechtlicher Geschäftsgeheimnisschutz

Mohr Siebeck

Nik R. Roeingh, geboren 1996; Studium der Rechtswissenschaft in Leipzig und Münster; 2021 Erstes Staatsexamen (OLG Hamm); 2023 Chercheur invité an der Université Paris 1 Panthéon-Sorbonne; 2022–2024 Deutsche Universität für Verwaltungswissenschaften Speyer; 2026 Promotion (Universität der Bundeswehr München); Rechtsreferendariat beim Kammergericht Berlin mit Stationen u. a. beim Bundesministerium für Digitales und Staatsmodernisierung sowie bei der Europäischen Kommission (DG CONNECT); 2022–2026 Forschungsreferent am Deutschen Forschungsinstitut für öffentliche Verwaltung Speyer.
orcid.org/0009-0007-1430-5146

ISBN 978-3-16-200653-0 / eISBN 978-3-16-200654-7
DOI 10.1628/978-3-16-200654-7

ISSN 2700-1288 / eISSN 2700-1296 (Schriften zum Recht der Digitalisierung)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind über <https://dnb.dnb.de> abrufbar.

Publiziert von Mohr Siebeck Tübingen 2026.

© Nik R. Roeingh.

Dieses Werk ist lizenziert unter der Lizenz „Creative Commons Namensnennung – Keine Bearbeitung 4.0 International“ (CC BY-ND 4.0). Eine vollständige Version des Lizenztextes findet sich unter: <https://creativecommons.org/licenses/by-nd/4.0/>.

Jede Verwendung, die nicht von der oben genannten Lizenz umfasst ist, ist ohne Zustimmung des Urhebers unzulässig und strafbar. Das Recht einer Nutzung der Inhalte dieses Werkes zum Zwecke des Text- und Data-Mining im Sinne von § 44b UrhG bleibt ausdrücklich vorbehalten.

Gedruckt auf alterungsbeständiges Papier. Satz: SatzWeise, Bad Wünnenberg.

Mohr Siebeck GmbH & Co. KG, Wilhelmstraße 18, 72074 Tübingen, Deutschland
www.mohrsiebeck.com, info@mohrsiebeck.com

*Meinen Eltern
Margit und Friedrich*

Vorwort

*„Knowledge and human power are synonymous,
since the ignorance of the cause frustrates the effect“
Bacon, Novum Organum (1620),
zit. nach 1902, Buch I, Aph. III.*

Die Effektivität staatlicher Steuerung steht und fällt mit der Qualität ihrer Entscheidungsgrundlagen; Erkenntnislücken schlagen in Wirkungsdefizite um. Je dichter die Wirklichkeit, desto vielfältiger und differenzierter müssen die zugrunde liegenden Informationsparameter sein. Davon ausgehend widmet sich die vorliegende Untersuchung den Grenzen und Möglichkeiten einer grundrechtsschonenden staatlichen Informationsbefriedigung. Sie entstand während meiner Tätigkeit als Forschungsreferent am Deutschen Forschungsinstitut für öffentliche Verwaltung und wurde von der Universität der Bundeswehr München im Herbsttrimester 2025 als Dissertation angenommen.

Mein herzlicher Dank gilt zunächst meinem Doktorvater, Herrn Professor Dr. Mario Martini, für die Übernahme der Betreuung dieser Arbeit, die überaus produktive Zusammenarbeit in den vergangenen Jahren sowie den stets konstruktiven und erkenntnisfördernden Austausch. Seine persönliche Begleitung, präzisen Nachfragen und weitsichtigen Hinweise haben maßgeblich dazu beigetragen, meine Überlegungen schrittweise zu schärfen, gewonnene Einsichten klarer zu konturieren und dem fortwährenden Ziel des Erkenntnisgewinns stetig näherzukommen.

Zu Dank verpflichtet bin ich ferner Professor Dr. Walther Michl, LL.M. (King's College London), für die Übernahme sowie die zügige Erstellung des Zweitgutachtens. Ebenso gilt mein Dank Professor Dr. Heiko Richter, LL.M. (Columbia), Dipl.-Kfm., dessen Vorarbeiten mein Interesse am Datenzugangs- und Datennutzungsrecht geweckt und der vorliegenden Untersuchung maßgebliche Impulse verliehen haben. Den Herausgeberinnen und Herausgebern der Schriften zum Recht der Digitalisierung danke ich für die Aufnahme in die Reihe.

Die vorliegende Arbeit ist über die Jahre hinweg von mehreren Institutionen großzügig gefördert worden. Dem Deutsch-Französischen Doktorandenkolleg danke ich herzlich für die Gewährung einer Mobilitätsbeihilfe im Rahmen meines Forschungsaufenthalts in Paris. Der Deutschen Vereinigung für gewerblichen Rechtsschutz und Urheberrecht (GRUR), der Johanna und Fritz Buch Gedächtnis-Stiftung sowie der Dr.-Giesing-Stiftung gilt mein besonderer Dank für die anteilige Übernahme der Druckkosten.

Das Verfassen einer Dissertation lässt sich vielleicht am treffendsten mit Hannah Arendts „Denken ohne Geländer“ beschreiben – ein Weg, der gleichermaßen durch große Freiheit in positiver wie in negativer Hinsicht gekennzeichnet ist. Die Möglichkeit, das eigene Denken in aller Konsequenz zu entfalten, kann beglückend, bisweilen aber auch beunruhigend sein. Umso bedeutsamer ist es, auf diesem Weg Mitstreiterinnen und Mitstreiter zu finden, die im wissenschaftlichen ebenso wie im persönlichen Austausch Orientierung und Halt geben. Mein besonderer Dank gilt daher David Wagner, der mich zu Beginn meiner Zeit am Institut in die Themen eingeführt hat, die mich bis heute bewegen. Herzlich danken möchte ich darüber hinaus Dr. Jonas Lange für die zahlreichen gemeinsamen Stunden in den Berliner Bibliotheken und Mensen, die von beinahe rituellen Tagesabläufen geprägt waren und auf meinen Denk- und Schreibprozess eine wohltuend ordnende Wirkung entfalteten. Mein Dank gilt ebenso meinen ehemaligen Kolleginnen und Kollegen an Institut und Lehrstuhl: Dr. Jonas Botta, Martin Feldhaus, Luci Haspinger, Dr. Carolin Kemper, Michael Kolain, Inken Kramme, Dr. Luise Lautenbach und Paul Seeliger.

Danken möchte ich schließlich auch jenen Determinanten eines Lebens, die sich jeder Planung entziehen: dem Glück und dem Zufall, die manches ermöglicht haben, was sich allein durch eigenes Zutun nicht hätte erreichen lassen.

Zuletzt – und doch an erster Stelle – gebührt mein tiefster Dank meiner Familie. Ihre unerschütterliche Unterstützung hat mich in allen Phasen meines Lebens getragen, bestärkt und immer wieder neu ausgerichtet.

Zwischen Brüssel und Berlin
Im Sommer 2026

Nik Reinhold Roeingh

Inhaltsübersicht

Vorwort	VII
Inhaltsverzeichnis	XIII
Abkürzungsverzeichnis	XXV
Prolegomena	1
<i>A. Der Zugang zu Daten als Elementarbaustein eines intelligenten Staates</i>	1
<i>B. Der staatliche Zugang zu Daten als Eingriff in die unternehmerische Geheimsphäre</i>	8
<i>C. Ziel der Untersuchung</i>	10
<i>D. Gang der Untersuchung</i>	12
Kapitel 1: Das Phänomen Business-to-Government-Data-Sharing	15
<i>A. Data – Daten als Zugangsobjekt</i>	16
I. Terminologische Grundlagen	17
II. Ökonomische Grundlagen	26
III. Rechtliche Grundlagen	31
IV. Kategorisierung von Daten...	42
V. Zwischenergebnis	56
<i>B. Government – Der Staat als Zugangsberechtigter</i>	58
I. Primärrechtlicher und verfassungsrechtlicher Handlungsrahmen staatlicher Datenzugangsrechte	58
II. Möglichkeiten staatlicher Informations- und Datenbefriedigung . . .	76
III. Typologie staatlicher Datenzugangsrechte	79
IV. Gesetzgeberische Ausgestaltungsmöglichkeiten staatlicher Datenzugänge	91
V. Zwischenergebnis	95
<i>C. Business – Private Unternehmen als Zugangsverpflichtete</i>	96
I. Subjektive Restriktion des Datenzugangs	96
II. Objektive Restriktion des Datenzugangs	109
III. Verhältnismäßigkeit staatlicher Datenzugangsrechte	116
IV. Zwischenergebnis	145

Kapitel 2: Die Datafizierung des Geschäftsgeheimnisschutzes	147
<i>A. Historische und wettbewerbliche Dimensionen wirtschaftlich motivierter Geheimhaltung von Informationen</i>	148
I. Von geheimen Handwerksverfahren zu geheimen Nullen und Einsen	148
II. Geheimnisse als Wettbewerbsfaktoren	151
<i>B. Das Geschäftsgeheimnis als Rechtsbegriff</i>	154
I. Das tradierte (dualistische) Verständnis	155
II. Das moderne (monistische) Verständnis	156
III. Annäherung an einen einheitlichen Begriff	159
<i>C. Geheimnisrechtliche Trennungslinien</i>	170
I. Wirtschaftsgeheimnisse	170
II. Know-how	170
III. Gewerbliche Schutzrechte	171
<i>D. Daten als Geschäftsgeheimnisse</i>	173
I. Daten als unternehmensbezogene Informationen	174
II. Nichtoffenkundigkeit von Daten	180
III. Wirtschaftlicher Wert von Daten	196
IV. Angemessene Geheimhaltungsmaßnahmen	205
V. Berechtigtes Geheimhaltungsinteresse	212
VI. Zwischenergebnis	214
Kapitel 3: Der staatliche Zugang zu geheimen Daten als materielle Grundrechtsbeschränkung	217
<i>A. Grundrechtsbetroffenheit des zugangsverpflichteten Unternehmens</i>	218
I. Geheimnisschutz der Grundrechtecharta (GRCh)	219
II. Geheimnisschutz des Grundgesetzes (GG)	226
III. Geheimnisschutz der Europäischen Menschenrechtskonvention (EMRK)	244
IV. Zwischenergebnis	247
<i>B. Der staatliche Zugang zu geheimen Daten als Eingriff</i>	248
I. Eingriffsqualität bei bipolaren Datenzugangsverhältnissen	249
II. Eingriffsqualität bei multipolaren Datenzugangsverhältnissen	253
III. Wesentlichkeit eines staatlichen Zugangs zu geheimen Daten	267
IV. Zwischenergebnis	268
<i>C. Grundrechtliche Rechtfertigung des staatlichen Zugangs zu geheimen Daten</i>	269
I. Vorgaben der Wesensgehaltsgarantie: Extensive Datenzugangsrechte als Aushöhlung des grundrechtlichen Geschäftsgeheimnisschutzes	270
II. Verhältnismäßigkeit des staatlichen Zugangs zu geheimen Daten	273
<i>D. Ausblick: Inklusive Datenräume</i>	325

Zusammenfassung	329
<i>A. (Rechts-)Ökonomische Einordnung von Daten als Zugangsobjekt</i>	<i>329</i>
<i>B. Daten als Grundlage und Ziel staatlicher Steuerung</i>	<i>332</i>
<i>C. Restriktionsmechanismen staatlicher Datenzugänge</i>	<i>334</i>
<i>D. Vom dualistischen zum monistischen Geschäftsgeheimnisbegriff</i>	<i>338</i>
<i>E. Die Datafizierung des Geschäftsgeheimnisses</i>	<i>339</i>
<i>F. Grundrechtsdimensionen des Geheimnisschutzes</i>	<i>339</i>
<i>G. Eingriffsqualität des staatlichen Zugangs zu geheimen Daten</i>	<i>340</i>
<i>H. Grundrechtliche Rechtfertigung des staatlichen Zugangs zu geheimen Daten</i>	<i>342</i>
<i>I. Gemeinsame europäische Datenräume als demokratische Wissensermächtigungsstrategie</i>	<i>346</i>
Bibliographie	347
Stichwortverzeichnis	395

Inhaltsverzeichnis

Vorwort	VII
Inhaltsübersicht	IX
Abkürzungsverzeichnis	XXV
Prolegomena	1
<i>A. Der Zugang zu Daten als Elementarbaustein eines intelligenten Staates</i>	1
<i>B. Der staatliche Zugang zu Daten als Eingriff in die unternehmerische Geheimsphäre</i>	8
<i>C. Ziel der Untersuchung</i>	10
<i>D. Gang der Untersuchung</i>	12
Kapitel 1: Das Phänomen Business-to-Government-Data-Sharing	15
<i>A. Data – Daten als Zugangsobjekt</i>	16
I. Terminologische Grundlagen	17
1. Daten – Information – Wissen	17
a) Daten	17
aa) Rechtliche Perspektive	18
bb) Etymologische Perspektive	19
cc) Informationstechnische Perspektive	20
dd) Ausgangsdefinition „Daten“	21
b) Information	21
aa) Syntax (Zeichenebene)	22
bb) Semantik (Bedeutungsebene)	23
cc) Pragmatik (Wirkungsebene)	24
dd) Ebenenrelation	24
c) Wissen	25
2. Zwischenergebnis	25
II. Ökonomische Grundlagen	26
1. Immaterialität	26
2. Nichtrivalität	27
3. Nichtexklusivität	28
4. Nichtabnutzbarkeit und universale Verwendungsmöglichkeiten . .	29
5. Zwischenergebnis	30

III. Rechtliche Grundlagen	31
1. Eigentum an Daten und Datenzuordnung	31
a) Sachenrechtliche Bewertung von Daten	31
b) Vermögensrechtliche Datenzuordnung durch das Strafrecht	32
c) Vermögensrechtliche Datenzuordnung durch das Daten- schutzrecht	33
d) „Datenimmaterialgüterrecht“	35
aa) Urheberrecht	36
bb) Datenbankherstellerrecht	37
2. Datenzugangsrechte	38
a) Datenzugang als Ausdruck ökonomischer Spezifika	38
b) Der Data Act als Markstein des Übergangs von exklusiver Zuordnung zu inklusivem Datenzugang	40
3. Zwischenergebnis	41
IV. Kategorisierung von Daten...	42
1. ...nach semantischem Inhalt	43
a) Personenbezug	43
b) Unternehmensbezug	44
c) Umweltbezug	44
aa) Unzulänglichkeiten bestehender Begriffe	45
bb) Begriffskonzeption de lege ferenda	46
2. ...nach Kontext	48
a) Primärdaten	48
b) Metadaten	48
3. ...nach Strukturierungsgrad	49
a) Strukturierte Daten	49
b) Unstrukturierte Daten und semi-strukturierte Daten	50
4. ...nach Schöpfungsakt	52
a) Nutzergenerierte Daten	52
b) Sensorgenerierte (Umwelt-)Daten und Maschinendaten	53
5. ...nach Zeit	54
a) Historische Daten	55
b) Echtzeitdaten	55
V. Zwischenergebnis	56
B. <i>Government – Der Staat als Zugangsberechtigter</i>	58
I. Primärrechtlicher und verfassungsrechtlicher Handlungsrahmen staatlicher Datenzugangsrechte	58
1. Daten- und Informationsbedarf staatlicher Aufgabenwahrnehmung	58
a) Legislative	59
aa) Erste Phase: Ermittlung	60
bb) Zweite und dritte Phase: Beobachtung und Nachbesserung	61

b) Exekutive	62
c) Judikative	64
2. Primärrechtliche und verfassungsrechtliche Legitimation des staatlichen Zugriffs auf private Daten	65
a) Rechtsstaatsinduzierter Datenzugang	65
aa) Datenzugang als Gesetzgebungsfaktor	66
bb) Korrektiv staatlicher Aufgabenwahrnehmungskompetenz	66
(1) Staatliche Aufgaben als Anwendungsfelder staatlicher Datenzugänge	67
(2) Umwelt- und Klimaschutz als Staatsaufgabe	68
cc) Auswirkungen auf die zweite und dritte Gewalt	70
b) Staatszielinduzierter Datenzugang	71
c) Schutzpflichtinduzierter Datenzugang	73
aa) Verdichtung der Schutzpflichtdimension durch Digitalisierung und Klimawandel	73
bb) Datenzugang zur Erfüllung staatlicher Schutzpflichten	75
3. Zwischenergebnis	75
II. Möglichkeiten staatlicher Informations- und Datenbefriedigung	76
1. Selbständige Informationsbefriedigung	76
2. Unselbständige Informationsbefriedigung	77
a) Aktive informationelle Inpflichtnahme Privater	78
b) Reaktive informationelle Inpflichtnahme Privater	78
III. Typologie staatlicher Datenzugsrechte	79
1. Datenzugang als Instrument konkreter staatlicher Aufgabenwahrnehmung und -planung	80
2. Datenzugang als Instrument staatlichen Datenbrokerings	83
a) Potenziale staatlichen Datenbrokerings	84
b) Herausforderungen staatlichen Datenbrokerings	86
3. Datenzugang als Instrument staatlicher Compliance	88
a) Datenzugang als direktes Complianceinstrument	88
b) Datenzugang als indirektes Complianceinstrument	89
IV. Gesetzgeberische Ausgestaltungsmöglichkeiten staatlicher Datenzugänge	91
1. Dynamischer Datenzugang	91
a) Infrastrukturbedürfnisse dynamischer Datenzugänge	92
b) Aktive oder reaktive Ausgestaltungsoptionen	93
2. Statischer Datenzugang	93
3. Dynamisch-statische Zwitterstellung des Data Act	94
V. Zwischenergebnis	95

C. <i>Business – Private Unternehmen als Zugangsverpflichtete</i>	96
I. Subjektive Restriktion des Datenzugangs	96
1. Grundrechtsbetroffenheit datenzugangsverpflichteter Unternehmen	97
a) Eigentum – Art. 17 GRCh, Art. 14 GG	97
aa) Einzeldaten	98
bb) Datensets	99
cc) Sozialgebundenheit von Information	100
b) Unternehmerische Freiheit und Berufsfreiheit – Art. 16 GRCh, Art. 12 GG	101
c) Datenzugang und Geschäftsgeheimnisse	102
2. Grundrechte Drittbetroffener	103
a) Eigentum – Art. 17 GRCh, Art. 14 GG	104
aa) Nutzerseitige Nutzungs- und Verfügungsrechte nach dem Data Act	104
bb) Schuldrechtliche Ansprüche Dritter	105
b) Unternehmerische Freiheit und Berufsfreiheit – Art. 16 GRCh, Art. 12 GG	105
c) Datenschutz – Art. 7, 8 GRCh, Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG	107
3. Zwischenergebnis	108
II. Objektive Restriktion des Datenzugangs	109
1. Grundsatz des fairen Verfahrens und Vertrauensschutz	109
2. Selbstbelastungsfreiheit	111
a) Schutz vor Selbstbelastung juristischer Personen	111
b) Gewährleistungsgehalte der Selbstbelastungsfreiheit bei staatlichem Datenzugang	113
3. Zwischenergebnis	116
III. Verhältnismäßigkeit staatlicher Datenzugangsrechte	116
1. Legitimer Zweck	117
a) Metazweck staatlicher Datenzugangsrechte	117
b) Berücksichtigung unionaler und nationaler Disparitäten	118
2. Datenzugang als Mittel der Wahl	119
3. Datenzugang als relativ mildestes Mittel	121
a) „Ob“ des Zugangs	121
aa) Eigengenerierung	122
bb) Datenerwerb	122
cc) Datenzugangspflicht	126
b) „Wie“ des Zugangs	126
aa) Für wen? – staatsinterne Perspektive	127
bb) Mit wem? – staatsexterne Perspektive	128
(1) Beschränkte Nutzung unternehmensinterner Daten durch Dritte	129

(2) Privilegierte Nutzung unternehmensinterner Daten durch Dritte	130
(3) Unbeschränkte Nutzung unternehmensinterner Daten durch Dritte	131
cc) Zweckbindung und Datenminimierung bei staatlichen Datenzugangsrechten	133
(1) Infizierung des Datenrechts	134
(2) Fehlende Vergleichbarkeit zwischen Persönlichkeits- und Unternehmensschutz	135
4. Angemessenheit	138
a) Auswirkungen des Datenverarbeitungsgrads auf die Eingriffsintensität	139
b) Abhängigkeit der Eingriffsintensität vom semantischen Informationsgehalt	140
aa) Einfache Daten	140
bb) Unternehmenssensible Daten	141
cc) Personenbezogene Daten	142
c) Maßgebliche Kriterien für Unternehmensdaten: Aktivlegitimierter Personenkreis und Nutzungsradius	144
IV. Zwischenergebnis	145
Kapitel 2: Die Datafizierung des Geschäftsgeheimnisschutzes	147
A. Historische und wettbewerbliche Dimensionen wirtschaftlich motivierter Geheimhaltung von Informationen	148
I. Von geheimen Handwerksverfahren zu geheimen Nullen und Einsen	148
II. Geheimnisse als Wettbewerbsfaktoren	151
B. Das Geschäftsgeheimnis als Rechtsbegriff	154
I. Das tradierte (dualistische) Verständnis	155
II. Das moderne (monistische) Verständnis	156
1. Geschäftsgeheimnis-RL	156
2. Geschäftsgeheimnisgesetz (GeschGehG)	157
3. Konfliktpunkte	158
III. Annäherung an einen einheitlichen Begriff	159
1. Begriffsdivergenzstützende Argumente	159
a) Entgegenstehender gesetzgeberischer Wille?	160
b) Disparate öffentlich-rechtliche und privatrechtliche Logiken?	160
2. Begriffskonvergenzstützende Argumente	161
a) Konnex zwischen öffentlichem und privatem Recht	162
b) Aspekt der Rechtsklarheit	164
c) Entwicklungsoffenheit der Rechtsprechung	165
aa) Bundesverfassungsgericht – BVerfGE 115, 205	165
bb) Bundesverwaltungsgericht – BVerwGE 167, 319	166

d) Unionsrechtliche Überformung des Daten- und Geschäfts- geheimnisrechts	168
3. Zwischenergebnis	169
C. <i>Geheimnisrechtliche Trennungslinien</i>	170
I. Wirtschaftsgeheimnisse	170
II. Know-how	170
III. Gewerbliche Schutzrechte	171
D. <i>Daten als Geschäftsgeheimnisse</i>	173
I. Daten als unternehmensbezogene Informationen	174
1. Informationen als Geheimnisgegenstand	174
2. Unternehmensbezug	175
3. (Umwelt-)Daten	176
a) Informationscharakter von Einzeldaten	177
b) Problemfall Rohdaten	177
c) Datensets	179
II. Nichtoffenkundigkeit von Daten	180
1. Bezugspunkt der Geheimhaltung	181
2. Geheimhaltungsgrad	181
a) Allgemeine Voraussetzungen	182
b) Auswirkungen der Offenlegung von Informationen gegenüber staatlichen Stellen	183
3. Maßgeblicher Verkehrskreis	184
4. Die Nichtoffenkundigkeit von Daten als neuralgischer Punkt ihrer Geschäftsgeheimnisqualität	185
a) Daten	185
aa) Einzeldaten	186
bb) Datensets	187
cc) Auswirkungen kooperativer Netzwerkstrukturen auf den Geheimnisschutz	188
b) Umweltdaten als geheime Daten	190
aa) Sensordaten über Umweltbestandteile und umweltrelevante Faktoren	190
bb) Historische Verkehrs- und Mobilitätsdaten	192
cc) Emissionsdaten	193
dd) Agrardaten	195
III. Wirtschaftlicher Wert von Daten	196
1. Wertermittlung geheimer Informationen	197
a) Prospektiv-schadenszentrierter Ansatz	198
b) Retrospektiv-investitionszentrierter Ansatz	198
c) Marktzentrierter Ansatz	199
d) Kombinatorischer Ansatz	200
2. Konnex zwischen Geheimhaltung und Werthaltigkeit	200

3. Daten	201
a) Einzeldaten	201
b) Datensets	203
IV. Angemessene Geheimhaltungsmaßnahmen	205
1. Differenz zum tradierten Verständnis	205
2. Ausgestaltung des Geheimnisschutzes	207
3. Geheimnisschutzmaßnahmen in öffentlich-rechtlichen Beziehungen	209
4. Geheimnisschutzmaßnahmen bei Daten	210
V. Berechtigtes Geheimhaltungsinteresse	212
VI. Zwischenergebnis	214
 Kapitel 3: Der staatliche Zugang zu geheimen Daten als materielle Grundrechtsbeschränkung	217
 A. Grundrechtsbetroffenheit des zugangsverpflichteten Unternehmens	218
I. Geheimnisschutz der Grundrechtecharta (GRCh)	219
1. Recht auf den Schutz personenbezogener Daten – Art. 7, 8 GRCh	219
2. Berufsfreiheit und unternehmerische Freiheit – Art. 15, 16 GRCh	221
3. Eigentum – Art. 17 GRCh	224
II. Geheimnisschutz des Grundgesetzes (GG)	226
1. Schutz der Unternehmenspersönlichkeit – Art. 2 Abs. 1 GG	226
a) Unternehmenspersönlichkeit	227
b) Geschäftsgeheimnisse als Ausprägung der Unternehmenspersönlichkeit	229
2. Berufsfreiheit – Art. 12 Abs. 1 GG	231
a) Geschäftsgeheimnisse als Ausprägung der Wettbewerbsfreiheit	231
aa) Funktionen der Wettbewerbsfreiheit	232
bb) Wettbewerbsliche Systemrelevanz von Geschäftsgeheimnissen	233
b) Geschäftsgeheimnisse als Ausprägung der Unternehmerfreiheit	234
3. Eigentum – Art. 14 Abs. 1 GG	235
a) Geschäftsgeheimnisse als eigenständige Vermögensposition i. S. d. Art. 14 Abs. 1 GG	236
aa) Geschäftsgeheimnisse als vermögenswerte Rechte	237
bb) Privatnützige Zuordnung von Geschäftsgeheimnissen nach Art eines Ausschließlichkeitsrechts	237
cc) Verfügungsbefugnis über Geschäftsgeheimnisse	240
b) Recht am eingerichteten und ausgeübten Gewerbebetrieb	242

III. Geheimnisschutz der Europäischen Menschenrechtskonvention (EMRK)	244
1. Recht auf Achtung des Privat- und Familienlebens – Art. 8 EMRK	245
2. Eigentum – Art. 1 EMRK-ZP 1	246
IV. Zwischenergebnis	247
B. <i>Der staatliche Zugang zu geheimen Daten als Eingriff</i>	248
I. Eingriffsqualität bei bipolaren Datenzugangsverhältnissen	249
1. Spannungslagen bei der Eingriffsqualität	250
2. Unterstützende Argumente für einen Eingriff	251
II. Eingriffsqualität bei multipolaren Datenzugangsverhältnissen	253
1. Begrenzte staatsinterne und staatsexterne Offenlegung geheimer Daten	254
2. Gezielte Offenlegung geheimer Daten an die Öffentlichkeit im Rahmen von Open Data	254
a) GG – Normative Trennlinien zwischen Inhalts- und Schrankenbestimmungen (Art. 14 Abs. 1 S. 2 GG) und Enteignung (Art. 14 Abs. 3 GG)	255
aa) Nichtrivalität von Daten als Ausschluss einer Enteignung	256
bb) Fehlende Rechtsübertragung	259
cc) Rechtspraktische Überlegungen	259
dd) Abgrenzung zur Sozialisierung (Art. 15 GG)	260
(1) Geheime Daten als sozialisierungsfähige Gegenstände	261
(2) Die Auflösung eines Geschäftsgeheimnisses als Spielart der Gemeinwirtschaft	262
b) EMRK – Normative Trennlinien zwischen Entziehung (Art. 1 Abs. 1 S. 2 EMRK-ZP 1), Nutzungsregelung (Art. 1 Abs. 2 EMRK-ZP 1) und sonstigem Eingriff (Art. 1 Abs. 1 S. 1 EMRK-ZP 1)	263
c) GRCh – Normative Trennlinien zwischen Entziehung (Art. 17 Abs. 1 S. 2 GRCh) und Nutzungsregelung (Art. 17 Abs. 1 S. 3 GRCh)	265
d) Schlussfolgerungen	266
III. Wesentlichkeit eines staatlichen Zugangs zu geheimen Daten	267
IV. Zwischenergebnis	268
C. <i>Grundrechtliche Rechtfertigung des staatlichen Zugangs zu geheimen Daten</i>	269
I. Vorgaben der Wesensgehaltsgarantie: Extensive Datenzugangsrechte als Aushöhlung des grundrechtlichen Geschäftsgeheimnisschutzes	270
II. Verhältnismäßigkeit des staatlichen Zugangs zu geheimen Daten	273
1. Legitimer Zweck – Leitidee eines Umweltdatenzugangsregimes	274
a) Erfüllung grundrechtlicher Schutzpflichten	274
b) Umweltschutz und Innovationsförderung	275

c) Herstellung von Transparenz	276
2. (Umwelt-)Datenzugang als Mittel der Wahl	276
3. Grundrechtsmildere Alternativen	277
a) Datenaskese als Leitprinzip	278
b) Abhängigkeit des Zugangs vom Nutzungszweck	278
c) Datenzugang geringerer Intensität als Ausschlussfaktor	279
d) Anonymisierung und Pseudonymisierung von Geschäfts- geheimnissen	281
aa) Anonymisierungs- und Pseudonymisierungsverfahren	281
bb) Beibehaltung des Datennutzwertes als Grenze von Anonymisierung und Pseudonymisierung	282
cc) Ausschluss von Anonymisierung und Pseudonymisierung nach Geheimnistyp	284
e) Entschädigungsausgleich als milderes Mittel	284
f) Zwischenergebnis	285
4. Angemessener Ausgleich zwischen staatlichem Zugangsinteresse und unternehmerischem Geheimhaltungsinteresse	285
a) Bipolares Datenzugangsverhältnis	286
aa) Konzeptualisierung der Eingriffsintensität	287
bb) Abwägung mit dem Datenzugangsinteresse	288
cc) Materielle und verfahrenstechnische Absicherungen	289
(1) Kennzeichnungspflicht	289
(2) Geheimhaltungspflicht	290
(3) Nutzungsbeschränkungen	290
dd) Erforderlichkeit eines Ausgleichs	291
ee) Zwischenergebnis	291
b) Multipolares (staatsinternes) Datenzugangsverhältnis	292
aa) Konzeptualisierung der Eingriffsintensität	292
bb) Abwägung mit dem Datenzugangsinteresse	293
cc) Materielle und verfahrenstechnische Absicherungen	293
dd) Erforderlichkeit eines Ausgleichs	294
ee) Zwischenergebnis	294
c) Multipolares (staatsexternes) Datenzugangsverhältnis	294
aa) Konzeptualisierung der Eingriffsintensität	295
bb) Abwägung mit dem Datenzugangsinteresse	295
cc) Materielle und verfahrenstechnische Absicherungen	296
dd) Erforderlichkeit eines Ausgleichs	296
ee) Zwischenergebnis	296
d) Multipolares (öffentliches) Datenzugangsverhältnis	297
aa) Konzeptualisierung der Eingriffsintensität	297
(1) Vorgaben der Berufsfreiheit	297
(a) Offener Datenzugang im Lichte der Drei-Stufen- Lehre	298

(b) Die Publikation geheimer Daten als „atypische Betroffenheit“	299
(2) Vorgaben des Eigentums	301
bb) Abstrakte Abwägung mit dem Datenzugangsinteresse	301
(1) Abstrakte Gewichtung der betroffenen Grundrechtsgüter	302
(2) Umweltdaten als eigentumssichernde Informationsgrundlage	303
(3) Innovationsanreize offener Daten	304
(4) Zwischenergebnis	305
cc) Feingranulare Abwägungskriterien zur grundrechtsschonenden Ausgestaltung staatlicher Zugangsrechte zu geheimen Daten	306
(1) Sozialbezug der Daten	306
(a) Umweltdaten als sozialbezogene Daten	307
(b) Öffentlich finanzierte Daten als sozialbezogene Daten	308
(2) Unternehmensinterner Kernbezug der Daten	310
(3) Alter der Daten	312
(4) Leistungsbezug	314
(5) Eigenständigkeit der Datengenerierung	315
(6) Nutzungszweck	317
(7) Zwischenergebnis	318
dd) Ausnahmetatbestände bei unbilliger Härte	318
ee) Erforderlichkeit eines Ausgleichs	320
(1) Finanzieller Ausgleich als Ausnahme	321
(2) Die Transition von geheimen zu öffentlichen Umweltdaten als ausgleichspflichtiger Härtefall	322
(a) Beibehaltung privatnütziger Verwertungsmöglichkeiten öffentlicher Daten	322
(b) Geheimnisschutz als zufälliges Schutzinstrument	323
(c) Einzelfallgerechtigkeit bei ungleicher Lastenteilung	324
ff) Zwischenergebnis	325
D. Ausblick: Inklusive Datenräume	325
Zusammenfassung	329
A. (Rechts-)Ökonomische Einordnung von Daten als Zugangsobjekt	329
B. Daten als Grundlage und Ziel staatlicher Steuerung	332
C. Restriktionsmechanismen staatlicher Datenzugänge	334
D. Vom dualistischen zum monistischen Geschäftsgeheimnisbegriff	338
E. Die Datafizierung des Geschäftsgeheimnisses	339

<i>F. Grundrechtsdimensionen des Geheimnisschutzes</i>	339
<i>G. Eingriffsqualität des staatlichen Zugangs zu geheimen Daten</i>	340
<i>H. Grundrechtliche Rechtfertigung des staatlichen Zugangs zu geheimen Daten</i>	342
<i>I. Gemeinsame europäische Datenräume als demokratische Wissensermächtigungsstrategie</i>	346
Bibliographie	347
Stichwortverzeichnis	395

Abkürzungsverzeichnis

a. F.	alte Fassung
Abl.	Amtsblatt der Europäischen Union
Abs.	Absatz
ACM	Association for Computing Machinery
AcP	Archiv für die civilistische Praxis (Zeitschrift)
AER	American Economic Review (Zeitschrift)
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
APr	Archiv für Presserecht (Zeitschrift)
Agr. Syst.	Agricultural Systems (Zeitschrift)
AI & Society	Artificial Intelligence & Society (Zeitschrift)
alt.	alternativ
AMG	Arzneimittelgesetz
AO	Abgabenordnung
AöR	Archiv des öffentlichen Rechts (Zeitschrift)
API	Application Programming Interface (Programmierschnittstelle)
Ariz. L. R.	Arizona Law Review (Zeitschrift)
Az.	Aktenzeichen
B2G	Business-to-Government
BAG	Bundesarbeitsgericht
BAGE	Amtliche Sammlung der Entscheidungen des BAG
BB	Betriebsberater (Zeitschrift)
Bd.	Band
Berkeley Tech. L. J.	Berkeley Technology Law Journal (Zeitschrift)
Beschl.	Beschluss
BGB	Bürgerliches Gesetzbuch
BGBI.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	Entscheidungen des BGH in Strafsachen
BGHZ	Entscheidungen des BGH in Zivilsachen
BH VERW	Die Verwaltung. Beihefte (Zeitschrift)
BMI	Bundesministerium des Innern
BMWK	Bundesministerium für Wirtschaft und Klimaschutz
BR	Bundesrat
BRD	Bundesrepublik Deutschland
BR-Drs.	Bundesratsdrucksache
BReg	Bundesregierung
BT-Drs.	Bundestags-Drucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Amtliche Sammlung der Entscheidungen des BVerfG
BVerwG	Bundesverwaltungsgericht
BVerwGE	Amtliche Sammlung der Entscheidungen des BVerwG
Cal. L. Rev.	California Law Review (Zeitschrift)

ChemG	Chemikaliengesetz
CLPD	Competition Law and Policy Debate (Zeitschrift)
CLSR	Computer Law & Security Review (Zeitschrift)
Col. J. T. L.	Columbia Journal of Transnational Law
COM	Dokument der Europäischen Kommission
CR	Computer und Recht (Zeitschrift)
DA	Data Act
DAR	Deutsches Autorecht (Zeitschrift)
DGA	Data Governance Act
DMA	Digital Markets Act
DSA	Digital Services Act
DB	Der Betrieb (Zeitschrift)
DesignG	Designgesetz
DIN	Deutsche Industrienorm
DNG	Datennutzungsgesetz
DÖV	Die öffentliche Verwaltung (Zeitschrift)
DS-GVO	Datenschutz-Grundverordnung
DuD	Datenschutz und Datensicherheit (Zeitschrift)
DVB1.	Deutsches Verwaltungsblatt (Zeitschrift)
DWD	Deutscher Wetterdienst
EBLR	European Business Law Review
ECL	European Competition Journal (Zeitschrift)
ECLI	European Case Law Identifier
EG	Europäische Gemeinschaft(en)
EGMR	Europäischer Gerichtshof für Menschenrechte
Einf.	Einführung
Einl.	Einleitung
EIPR	European Intellectual Property Review (Zeitschrift)
EJEG	Electronic Journal of e-Government (Zeitschrift)
EJLE	European Journal of Law and Economics (Zeitschrift)
EJRR	European Journal of Risk Regulation (Zeitschrift)
EL	Ergänzungslieferung
ELR	European Law Review (Zeitschrift)
EMRK	Europäische Menschenrechtskonvention
Environ. Res. Lett.	Environmental Research Letters (Zeitschrift)
EnWZ	Zeitschrift für das gesamte Recht der Energiewirtschaft
ErwGr.	Erwägungsgrund
et. al.	et alii (u. a.)
EU	Europäische Union
EuG	Gericht der Europäischen Union
EuGH	Europäischer Gerichtshof
EuGRZ	Europäische Grundrechte-Zeitschrift
EuR	Europarecht (Zeitschrift)
EurUP	Zeitschrift für Europäisches Umwelt- und Planungsrecht
EUV	Vertrag über die Europäische Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
EWG	Europäische Wirtschaftsgemeinschaft
EZB	Europäische Zentralbank
f., ff.	folgende
Flor. L. Rev.	Florida Law Review (Zeitschrift)
FM	First Monday (Zeitschrift)

Fn.	Fußnote
FS	Festschrift
FTC	Federal Trade Commission
GA	Generalanwalt/Generalanwältin am Europäischen Gerichtshof
GB	Gigabyte
GebrMG	Gebrauchsmustergesetz
GeolDG	Geologiedatengesetz
GeoZG	Geodatenzugangsgesetz
GeschGehG	Geschäftsgeheimnisgesetz
GewArch	Gewerbearchiv (Zeitschrift)
GG	Grundgesetz
GIQ	Government Information Quarterly (Zeitschrift)
GJ	Global Jurist (Zeitschrift)
GLJ	German Law Journal (Zeitschrift)
GmbH	Gesellschaft mit beschränkter Haftung
GPS	Global Positioning System
GRCh	Charta der Grundrechte der Europäischen Union
GRUR Int.	GRUR-International (Zeitschrift)
GRUR	Gewerblicher Rechtsschutz und Urheberrecht (Zeitschrift)
GRUR-Prax.	GRUR-Praxis im Immaterialgüter- und Wettbewerbsrecht (Zeitschrift)
GRUR-RR	GRUR-Rechtsprechungs-Report (Zeitschrift)
GSZ	Zeitschrift für das Gesamte Sicherheitsrecht
GVwR	Grundlagen des Verwaltungsrechts
GWB	Gesetz gegen Wettbewerbsbeschränkungen
Harv. D. Sc. Rev.	Harvard Data Science Review (Zeitschrift)
Harv. J. L. & Tech.	Harvard Journal of Law & Technology
Hrsg.	Herausgeber
hrsg.	herausgegeben
Hs.	Halbsatz
HStR	Handbuch des Staatsrechts
HVR	Handbuch des Verfassungsrechts
HVwR	Handbuch des Verwaltungsrechts
i. e. S.	im engeren Sinne
IDEA	The Intellectual Property Law Review (Zeitschrift)
IDPL	International Data Privacy Law (Zeitschrift)
IFG	Informationsfreiheitsgesetz (des Bundes)
IIC	International Review of Intellectual Property and Competition Law (Zeitschrift)
IJAIS	International Journal of Applied Information Systems (Zeitschrift)
IJIM	International Journal of Information Management (Zeitschrift)
Ind. J. G. L. S.	Indiana Journal of Global Legal Studies (Zeitschrift)
IoT	Internet of Things (Internet der Dinge)
IPCC	Intergovernmental Panel on Climate Change
IPR	Internet Policy Review (Zeitschrift)
IPRB	IP-Rechts-Berater (Zeitschrift)
JASIST	Journal of the Association for Information Science and Technology (Zeitschrift)
JEL	Journal of Environmental Law (Zeitschrift)
JEP	Journal of Economic Perspectives (Zeitschrift)
JICE	Journal of International Commerce and Economics (Zeitschrift)

JIPITEC	Journal of Intellectual Property, Information Technology and E-Commerce Law (Zeitschrift)
JME	Journal of Monetary Economics (Zeitschrift)
JIPL	University of Georgia Journal of Intellectual Property Law (Zeitschrift)
JZ	JuristenZeitung
JuS	Juristische Schulung (Zeitschrift)
JIPLP	Journal of Intellectual Property Law & Practice
JLPP	Harvard Journal of Law & Public Policy (Zeitschrift)
K&R	Kommunikation & Recht (Zeitschrift)
KG	Kammergericht
KI	Künstliche Intelligenz
KMU	Kleine und mittlere Unternehmen
KOM	Europäische Kommission; Dokument der Europäischen Kommission
KriPoZ	Kriminalpolitische Zeitschrift
L. Rev.	Law Review
LCP	Law and Contemporary Problems
Lfg.	Lieferung
LIBREAS	Library Ideas (Zeitschrift)
Lit.	Literatur
LLM	Largue Language Modell
Ltd.	Limited
Marq. L. Rev.	Marquette Law Review (Zeitschrift)
Min. L. Rev.	Minnesota Law Review (Zeitschrift)
Mio.	Millionen
MMR	Multimedia und Recht (Zeitschrift)
Mod. L. Rev.	The Modern Law Review (Zeitschrift)
MTS-K	Markttransparenzstelle für Kraftstoffe
MüKo	Münchener Kommentar
MuW	Markenschutz und Wettbewerb (Zeitschrift)
NC JOLT	North Carolina Journal of Law & Technology (Zeitschrift)
NIQ	Network Industries Quarterly (Zeitschrift)
NJW	Neue Juristische Wochenschrift (Zeitschrift)
No.	Nummer(n)
Notr. D. L. Rev.	Notre Dame Law Review (Zeitschrift)
NuR	Natur und Recht (Zeitschrift)
NVwZ	Neue Zeitschrift für Verwaltungsrecht
Nw. U. L. Rev.	Northwestern University Law Review (Zeitschrift)
N. Y. U. L. Rev.	New York University Law Review (Zeitschrift)
NZA	Neue Zeitschrift für Arbeitsrecht
NZKart	Neue Zeitschrift für Kartellrecht
OECD	Organisation for Economic Co-operation and Development
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
OWiG	Ordnungswidrigkeitengesetz
PatG	Patentgesetz
PBeG	Personenbeförderungsgesetz
PharmR	Pharmarecht (Zeitschrift)
PinG	Privacy in Germany (Zeitschrift)
PLoS ONE	Public Library of Sciences (Zeitschrift)

PSI	Public Sector Information
RAW	Recht Automobil Wirtschaft (Zeitschrift)
RdA	Recht der Arbeit (Zeitschrift)
RDi	Recht Digital (Zeitschrift)
REDC	Revue européenne de droit de la consommation (Zeitschrift)
RegE	Regierungsentwurf
Rev.	Review
RL	Richtlinie
Rn.	Randnummer
Rs.	Rechtssache
RW	Rechtswissenschaft (Zeitschrift)
Sci. Adv.	Science Advances (Zeitschrift)
SEC	Dokument der Europäischen Kommission
Sec.	Section
sic!	Zeitschrift für Immaterialgüter- Informations- und Wettbewerbsrecht
SIGMOD Rec.	Special Interest Group of Management of Data Record (Zeitschrift)
SJS-RSJ	Schweizerische Juristen-Zeitung, Revue Suisse de Jurisprudence
SMU L. Rev.	Southern Methodist University Law Review (Zeitschrift)
SozW	Soziale Welt (Zeitschrift)
st. Rspr.	ständige Rechtsprechung
Stanford L. Rev.	Stanford Law Review (Zeitschrift)
Stanford T. L. Rev.	Stanford Technology Law Review (Zeitschrift)
StGB	Strafgesetzbuch
SWD	Arbeitsunterlage der Kommissionsdienststellen
TRIPS	Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums
U. Ill. L. Rev.	University of Illinois Law Review (Zeitschrift)
U.S.	United States
UBC L. Rev.	University of British Columbia Law Review (Zeitschrift)
UC Davis L. Rev.	UC Davis Law Review (Zeitschrift)
UChi L. Rev.	University of Chicago Law Review (Zeitschrift)
UCLA L. Rev.	University of California Law Review (Zeitschrift)
UIG	Umweltinformationsgesetz
UPenn L. Rev.	University of Pennsylvania Law Review (Zeitschrift)
UrhG	Urhebergesetz
Urt.	Urteil
USB	Universal Serial Bus
VersR	Versicherungsrecht (Zeitschrift)
VerwArch	Verwaltungsarchiv (Zeitschrift)
VG	Verwaltungsgericht
VGH	Verwaltungsgerichtshof
VIG	Verbraucherinformationsgesetz
Vill. L. Rev.	Villanova Law Review (Zeitschrift)
Virg. J. L. Tech.	Virginia Journal of Law & Technology (Zeitschrift)
VO	Verordnung
Vorb.	Vorbemerkung
VVDStRL	Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer
VwGO	Verwaltungsgerichtsordnung (des Bundes)
Wash. L. Rev.	Washington Law Review (Zeitschrift)

WBGU	Wissenschaftlicher Beirat der Bundesregierung Globale Umweltveränderungen
WettbR	Wettbewerbsrecht
WM	Zeitschrift für Wirtschafts- und Bankrecht
WRP	Wettbewerb in Recht und Praxis
WuW	Wirtschaft und Wettbewerb
Yale J. L. & Tech.	Yale Journal of Law & Technology (Zeitschrift)
Yale L. J.	Yale Law Journal
ZD	Zeitschrift für Datenschutz
ZEuP	Zeitschrift für Europäisches Privatrecht
ZGE	Zeitschrift für geistiges Eigentum
ZGI	Zeitschrift für das gesamte Informationsrecht
ZHR	Zeitschrift für das gesamte Handelsrecht und Wirtschaftsrecht
ZIB	Zeitschrift für Internationale Beziehungen
Ziff.	Ziffer
ZIP	Zeitschrift für Wirtschaftsrecht
ZIS	Zeitschrift für Internationale Strafrechtsdogmatik
ZRP	Zeitschrift für Rechtspolitik
ZUM	Zeitschrift für Urheber- und Medienrecht
ZUR	Zeitschrift für Umweltrecht

Im Übrigen wird auf *Kirchner*, Abkürzungsverzeichnis der Rechtssprache, 11. Aufl. 2025, verwiesen.

Prolegomena

A. Der Zugang zu Daten als Elementarbaustein eines intelligenten Staates

Staatliche Dezision gründet sich auf einem Rationalitätsversprechen. Hoheitliche Entscheidungen folgen im modernen Rechtsstaat dem Ideal, präzise, nachvollziehbar und sachlich angemessen zu sein.¹ Sie sollen einen sachgerechten Bezug zur Tatsachenwelt herstellen.² Möglich ist dies nur, wenn sie auf zutreffenden Informationen beruhen. Erst dann können autoritative und verbindliche Entscheidungen ihren Geltungsanspruch gegenüber Bürgerinnen und Bürgern entfalten.

Ideengeschichtlich wurzelt die Vorstellung, dass sich staatliche Institutionen von nachvollziehbaren, vernünftigen (intersubjektiv vermittelbaren) Gründen leiten lassen sollen, bereits in *Thomas Hobbes'* „Leviathan“.³ Logikbasierte Regeln und nicht Intuition, Impuls und Willkür sollten zur Grundlage staatlichen Handelns werden.⁴ Seinen endgültigen Durchbruch feierte dieses Ideal in *Max Webers* Konzeption einer

¹ Bumke, Der Staat 49 (2010), 77 (77 ff.); Fassbender, in: Isensee/Kirchhof (Hrsg.), HStR IV, 3. Aufl., 2006, § 76 Wissen als Grundlage staatlichen Handelns, Rn. 1; Ellerbrok, in: Kahl/Ludwigs (Hrsg.), HVwR III, 2021, § 76 Rationalität und Effizienz, Rn. 20 ff.; Gusy, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), GVwR II, 2. Aufl., 2012, § 23 Informationsbeziehungen zwischen Staat und Bürger, Rn. 1; Guckelberger, VVDStRL 78 (2019), 235 (277 f.); Hesse, Der Rechtsstaat im Verfassungssystem des Grundgesetzes, in: Smend/Hesse/Reicke (Hrsg.), FS Smend, 1962, S. 83; Hong, Die Verwaltung 51 (2018), 367 (367); Isensee, in: Isensee/Kirchhof (Hrsg.), HStR II, 3. Aufl., 2004, § 15 Staat und Verfassung, Rn. 79; Isensee, AöR 140 (2015), 169 (170); Krüger, Allgemeine Staatslehre, 2. Aufl., 1966, S. 54 ff.; Martini/Roeingh, Die Verwaltung 59 (2026), 1 (30 f.); Mashaw, Reasoned Administration and Democratic Legitimacy, 2018, S. 2 ff., 163 ff.; Scherzberg, Die öffentliche Verwaltung als informationelle Organisation, in: Hoffmann-Riem/Schmidt-Aßmann (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, 2000, S. 195 (195 ff.); Schmidt-Aßmann, Die Forschung zwischen grundrechtlicher Freiheit und staatlicher Institutionalisierung, in: Broemel/Kuhlmann/Pilniok (Hrsg.), FS Trute, 2023, S. 3 (9); Trute, Governance des Wissens, in: Wagner/Weingart (Hrsg.), Wissenschaftliche Politikberatung im Praxistest, 2015, S. 115 (115).

² Augsberg, Informationsverwaltungsrecht, 2014, S. 41; Steinbach, Rationale Gesetzgebung, 2017, S. 53.

³ Voßkuhle, Das Konzept des rationalen Staates, in: Schuppert/Voßkuhle (Hrsg.), Governance von und durch Wissen, 2008, S. 13 (14).

⁴ „The skill of making, and maintaining commonwealths, consisteth in certain rules, as doth arithmetic and geometry; not (as tennisplay) on practice only: which rules, neither poor men have the leisure, nor men that have had the leisure, have hitherto had the curiosity, or the method to find out.“, *Hobbes, Leviathan*, 1965, S. 160.

rationalen staatlichen Verwaltung und ihrer „Herrschaft kraft Wissen“⁵. Niklas Luhmann führte diesen Gedanken später weiter und konstatierte: „Wer Autorität in Anspruch nimmt, muß diese auf Wissen gründen.“⁶

Im Laufe des 20. Jahrhunderts erlebte das Rationalitätskonzepts des modernen Staates indes einen deutlichen Bruch. Insbesondere im Bereich des Umwelt- und Klimaschutzes erfüllte sich das Leitbild einer exekutiven Wissensüberlegenheit und eines eindeutigen Fachwissens nie.⁷ Kausale Erklärungsmuster und falsifizierbare Voraussagen fielen innerhalb hochkomplexer Systeme wie der Umwelt und des Klimas immer schwerer.⁸ Naturwissenschaftliche Vorgänge erwiesen sich als zu dynamisch und vielschichtig, als dass sie sich vollständig erfassen ließen. Wo aber zukünftige Prozesse in der Gegenwart unberechenbar werden, keimt individuelle und kollektive Verunsicherung.⁹ Das stellt den modernen Staat vor Herausforderungen: Denn je mehr die Überzeugung an Kraft verliert, die Welt mit den Mitteln des Verstandes erfassen und beherrschen zu können, desto weniger kann sich staatliche Herrschaft auf unstrittiges Wissen berufen.¹⁰

Die technologischen Entwicklungen der letzten Jahrzehnte versprechen einen Ausweg aus dieser unbefriedigenden Situation und lassen das Rationalitätsversprechen des modernen Staates wieder aufleben. Sie gruppieren sich um die Schlagworte *Big Data*, *Künstliche Intelligenz*, *Machine Learning* & Co.¹¹ Die ihnen zugeschriebenen Potenziale sind immens, haben sich zum Teil auch schon bewahrheitet, sind vielfach jedoch erst als Verheißung am Horizont erkennbar. Ihre Hauptanwendungsdomäne liegt im Bereich prädiktiver Analysen und beruht auf ihrer Fähigkeit, schwer zugängliche, nicht erschlossene oder unbekannte Informationen über vergangene, gegenwärtige und zukünftige Ereignisse zu Tage zu fördern.¹²

⁵ Weber, *Wirtschaft und Gesellschaft*, 5. Aufl., 1976, S. 129.

⁶ Luhmann, *Die Wissenschaft der Gesellschaft*, 1992, S. 149.

⁷ Wehling, *Ungeahnte Risiken*, in: Collin/Horstmann (Hrsg.), *Das Wissen des Staates*, 2004, S. 309 (311); nach Wolf, *SozW* 39 (1988), 164 (171), wird dennoch „in vielen modernen Umweltgesetzen [...] die ‚Herrschaft kraft Wissen‘ zum archimedischen Punkt staatlicher Interventions-schwellen“.

⁸ Voßkuhle, *Das Konzept des rationalen Staates*, in: Schuppert/Voßkuhle (Hrsg.), *Governance von und durch Wissen*, 2008, S. 13 (17); Weingart, *Wissenschaftssoziologie*, 2003, S. 9; vor allem das hoch umstrittene Thema der Kernenergie legte im Laufe des 20. Jahrhunderts die Uneindeutigkeit und Unsicherheit auch naturwissenschaftlichen Wissens offen, Wehling, *Ungeahnte Risiken*, in: Collin/Horstmann (Hrsg.), *Das Wissen des Staates*, 2004, S. 309 (S. 312).

⁹ Spiecker gen. Döhmman, *Staatliche Entscheidungen unter Unsicherheit*, 2000, S. 1.

¹⁰ Siehe auch Voßkuhle, *Das Konzept des rationalen Staates*, in: Schuppert/Voßkuhle (Hrsg.), *Governance von und durch Wissen*, 2008, S. 13 (18).

¹¹ Valle-Cruz/Criado et al., *GIQ* 37 (2020), 1 (1 ff.); van der Voort/Klievink et al., *GIQ* 36 (2019), 27 (27).

¹² Alpaydin, *Maschinelles Lernen*, 3. Aufl., 2022, S. 2; Singh/Mishra et al., *Introduction to Data Analytics, Big Data, and Machine Learning*, in: Singh/Mishra/Garg (Hrsg.), *Data Analytics and Machine Learning*, 2024, S. 1 (1 ff.); zu den Wesensmerkmalen von Big Data aus rechtswissenschaftlicher Perspektive, Martini, *Big Data als Herausforderung für das Datenschutzrecht und den Persönlichkeitsschutz*, in: Hill/Martini/Wagner (Hrsg.), *Die digitale Lebenswelt gestalten*, 2015, S. 97 (101 ff.).

Der Staat kann sich diese Fähigkeiten zunutze machen, um das Gemeinwesen im Rahmen eines *Predictive Policing* vorausschauend zu steuern. Denn zahlreiche Bereiche staatlichen Handelns sind auf prospektive Informationen angewiesen – von Mobilitäts- und Gesundheitsfragen über Bildung und Energieversorgung bis hin zum Katastrophenschutz. Wer ein Mobilitätskonzept für die Verkehrswende entwickelt, eine Pandemie steuert oder die Energieversorgung von fossilen auf nachhaltige Technologien umstellt, muss Nah- und Fernprognosen erstellen, die nur auf der Basis von erschlossenen Informationen möglich sind. Gelingt es dem Staat, künftige Entwicklungen genauer zu antizipieren, eröffnen sich ihm neue Handlungsspielräume und damit verbundene Legitimationschancen.

Ein Sektor, der in diesem Zusammenhang besonders hervorsteicht, ist der Umwelt- und Klimaschutz. Nachhaltigkeit als übergeordnetes Ziel setzt immer das Wissen über gegenwärtige Zustände voraus, aber auch die Fähigkeit, die Auswirkungen aktueller Maßnahmen und zukünftiger Zustände zu prognostizieren.¹³ Nur wer Aufschluss über bestehende Problemlagen hat, kann zukunftsorientierte Lösungsstrategien entwickeln und auf dieser Grundlage umweltrelevante, rationale Entscheidungen in der Gegenwart treffen, die am Ende dem *Comte'schen* Leitmotiv des „savoir pour prévoir, prévoir pour pouvoir“¹⁴ Rechnung tragen.

So vielversprechend moderne Informationsanalysesysteme für das Gemeinwohl auch sein mögen, eines eint sie. Ihr Potenzial verpufft, wenn sie nicht auf ihr zentrales Stimulans zurückgreifen können: maschinenlesbar codierte Informationen, das heißt *Daten*. Sie bilden das Herzstück digitaler Technologien. Denn wie viel ein lernfähiges System tatsächlich leisten kann, hängt entscheidend davon ab, ob ihm qualitativ hochwertige und quantitativ ausreichende Daten bereitstehen. Die Erkenntniskraft seiner Prozesse beruht maßgeblich darauf, welche Daten in seinen Kreislauf einfließen.¹⁵ Ob sensor-, nutzer- oder maschinengeneriert – Daten bilden die Grundlage, große Vorhersagemodelle zu füttern. Erst auf ihrer Basis lassen sich Veränderungen, bisher verborgen gebliebene Muster, neue Erkenntnisse und wichtige Zusammenhänge an die Oberfläche tragen.

Die drängende Transformationsaufgabe des Umwelt- und Klimaschutzes¹⁶ ist dabei vor allem auf solche Daten angewiesen, die einen semantischen Bezug zur Umwelt aufweisen – seien es zum Beispiel die Umgebungsdaten eines PKW oder die

¹³ Vgl. nur *Appel*, Staatliche Zukunfts- und Entwicklungsvorsorge, 2005, S. 55 ff., 85 ff., 360 ff.; *Eifert*, Nachhaltigkeit durch Innovation und Wissensgenerierung, in: Kahl (Hrsg.), Nachhaltigkeit durch Organisation und Verfahren, 2016, S. 371 (372); *Roeingh*, Unlocking (Environmental) Data – State of Play and Challenges, <https://www.juwiss.de/58-2024/> (6.1.2026); krit. aus technisch-tatsächlicher Perspektive im Hinblick auf die Möglichkeiten von Datenanalysen als Governance-Instrument, *Leonelli*, Harv. D. Sc. Rev. 2021, 1 (1 ff.).

¹⁴ Dt.: „Wissen, um vorherzusehen, vorhersehen, um handeln zu können“; zitiert nach *Khondoss*, Auguste Comte Cours de Philosophie Positive, 1997, S. 35.

¹⁵ *Martini/Ruscheimer*, ZUR 32 (2021), 515 (529); *Martini/Roeingh*, Die Verwaltung 59 (2026), 1 (29 f.).

¹⁶ Siehe etwa den Bericht von *IPCC*, 1,5 °C Globale Erwärmung, 2018, S. 1 ff., auf den auch das Bundesverfassungsgericht in seinem Klimabeschluss Bezug nimmt, BVerfGE 157, 30 (50 f.) – Klimaschutz.

Auslastungsdaten einer Windenergieanlage. Sie transportieren Informationen über die sie umgebende Welt. Wer sie auswertet, kann faktenbasierte und damit evidente und effiziente Maßnahmen zum Schutz der natürlichen Lebensgrundlagen ergreifen.¹⁷ Bessere Prognosen und Simulationen werden möglich,¹⁸ Fehlsteuerungen minimiert. So kann der Staat politisch gesetzte Nachhaltigkeitsziele erreichen, das Umweltmonitoring optimieren und Gefahren von und für die Umwelt, wie sich häufende extreme Wetterereignisse, früher erkennen und begegnen¹⁹ – nicht zuletzt, um seinen grundrechtlichen Schutzpflichten gegenüber Bürgerinnen und Bürgern nachzukommen.

Doch der Staat, dem beim Gemeinwohl die Leitentscheidungskompetenz zukommt, steht vor einer unbefriedigenden Ausgangslage. Er kann selbst häufig nur auf eine defizitäre Datenbasis zurückgreifen.²⁰ Der Großteil von *Big Data* liegt hochgranular gefangen in den Silos privater Unternehmen, die nicht dem *bonum commune*, sondern vorwiegend ökonomischen Logiken unterworfen sind.²¹ Sie betrachten die potenziell wichtigen Informationen primär als wirtschaftlich verwert-

¹⁷ Nicht zu vernachlässigen sind jedoch die von den Science and Technology Studies (STS) sowie den aus ihnen hervorgegangenen Critical Data Studies (CDS) formulierten Einwände gegen das Versprechen einer datengetriebenen Governance. Daten stellen keine neutralen Abbilder der physischen Welt dar; zwischen Repräsentation und Objekt verbleibt stets eine Distanz. Daten sind daher nicht Realität selbst, sondern deren Interpretation. Bereits der Prozess der Datenerhebung ist notwendigerweise selektiv und exkludierend; auch ihre spätere Auswertung hängt maßgeblich vom Erhebungskontext und den verfolgten Erkenntniszielen ab. STS und CDS bezeichnen vermeintlich neutrale Darstellungen deshalb als „view from nowhere“, um auf die jeder Repräsentation inhärente Unmöglichkeit eines neutralen Standpunkts hinzuweisen. Daten können folglich zu größerer Rationalität staatlicher Entscheidungsfindung beitragen, garantieren diese jedoch nicht, da sie stets kontextabhängig und relational sind. Vgl. insg. *Beaulieu/Leonelli*, *Data and Society*, 2021, S. 40 ff.; *Helmreich*, *Social Research* 78 (2011), 1211 (1229); *Kitchin/Lauriault*, *Toward Critical Data Studies*, in: Thatcher/Eckert/Shears (Hrsg.), *Thinking Big Data in Geography*, 2018, S. 3 (5 ff.); *Lambach*, *Die Datafizierung der Welt*, in: Augsburg/Düwell/Müller (Hrsg.), *Daten Zugangsregeln*, 2024, S. 139 (146); *Leonelli*, *Harv. D. Sc. Rev.* 2021, 1 (6 f.); *Ricaurte*, *Televisions & New Media* 20 (2019), 350 (352 ff.); *Thylstrup*, *Big Data & Society* 6 (2019), 1 (1 ff.).

¹⁸ *Landesregierung Rheinland-Pfalz*, *Digitalstrategie für das Land Rheinland-Pfalz*, 2023, S. 83.

¹⁹ *Martini/Rusche-meier*, *ZUR* 32 (2021), 515 (515 ff.), zeigen die Potenziale lernfähiger Technologien für den Umweltschutz auf.

²⁰ *Europäische Kommission*, *Eine europäische Datenstrategie*, COM(2020) 66 final, 19.2.2020, S. 9.

²¹ Die *Europäische Kommission*, *Eine europäische Datenstrategie*, COM(2020) 66 final, 19.2.2020, S. 4 verzeichnet „beträchtliche Konzentrationseffekte“; *Martini/Fritzsche et al.*, *Digitalisierung als Herausforderung für Staat und Gesellschaft*, 2016, S. 33 weisen darauf hin, dass das Gemeinwohlprinzip als „übergreifender Leitmaßstab jeglichen staatlichen Handelns [...] auch das digitale staatliche Handeln in die Pflicht [nimmt]“. Für private Unternehmen gilt dies hingegen nicht; im EUV tritt der Gemeinwohlgedanke besonders deutlich in Art. 3 Abs. 2 EUV hervor: Die Union verfolgt das Ziel, „das Wohlergehen ihrer Völker“ zu fördern.

bares Gut,²² das umso wertvoller ist, je exklusiver der Zugang zu ihnen ist.²³ Ihre gemeinwohlrelevanten Datenbestände legen Unternehmen daher zu selten freiwillig offen, obwohl ca. 85 % dieser Daten ungenutzt bleiben.²⁴

Das Resultat ist eine asymmetrisch gezeichnete Datenlandschaft, in der informationsbasierte Interventionschancen zwischen Staat und Privat ungleich verteilt sind.²⁵ Die Rolle des Staates wandelt sich vom ehemals zentralen Informationsbereitsteller zum nachfragenden Datennutzer.²⁶ Die Hauptrolle nimmt der Privatsektor ein, der über Technologien wie das Internet-of-Things (IoT) und moderne Sensorik jeden Lebensbereich durchdringt und in binäre Codes überführt.²⁷ Die voranschreitende Digitalisierung fungiert angesichts der Fähigkeiten moderner Datenverarbeitungssysteme, exponentiell mehr Informationen digital zu erfassen und zu speichern, als Triebmittel. Privaten Unternehmen ist es heute möglich, ein akkurateres Bild der sie umgebenden und von ihnen beeinflussten Welt zu zeichnen und die von ihr ausgehenden Signale einzuordnen.²⁸ Damit gerät auch das *Weber'sche* Diktum von der Wissensüberlegenheit des Staates ins Wanken. Die dem englischen Lordkanzler *Francis Bacon* zugeschriebene Wendung „scientia est potentia“,²⁹ wonach Wissen gleich Macht ist, verschiebt sich auf den Privatsektor.

Seit jeher ist aber der Zugang zu Informationen *conditio sine qua non* jedes Gemeinwesens, seiner originären Aufgabe nachzukommen, das Gemeinwohl zu fördern. In der heutigen algorithmischen Gesellschaft verschiebt sich das Interesse auf

²² Die Ökonomie bezeichnet als „Güter“ Mittel zur Bedürfnisbefriedigung. Damit verweist der Begriff nicht auf eine Substanz, sondern auf eine Relation. Konkret kommt es auf den Nutzen einer Sache für die Zwecke eines wirtschaftlichen Akteurs an, *Linde*, Ökonomie der Information, 2008, S. 7.

²³ *Abrahamson*, Yale L. J. 124 (2014), 867 (873); *Fia*, GJ 21 (2021), 181 (187); *Gill/Zolna et al.*, Data Sharing for Collective Interests – Moving Beyond Exclusive Control, in: Heine/Budziniski (Hrsg.), FS Kerber, 2024, S. 225 (225); *Kitchin*, The Data Revolution, 2014, S. 14.

²⁴ *Ramge/Mayer-Schönberger*, Machtmaschinen, 2020, S. 24; *Tarkowski/Vogelezang et al.*, Public Data Commons, 2022, S. 3.

²⁵ *Valli Buttow*, EJRR 15 (2024), 1 (1): „While the private sector is leading the way in digital transformation, the public sector is perceived as missing the opportunity“; *WBGU*, Ein europäischer Weg in unsere gemeinsame digitale Zukunft, 2019, S. 17 spricht von einem „Informationsgefälle“.

²⁶ Galt früher noch der Staat als größter Informationsbesitzer (vgl. *Storher*, Informationspflichten Privater gegenüber dem Staat in Zeiten von Privatisierung, Liberalisierung und Deregulierung, 2007, S. 57), sind es heute private Unternehmen, die Zugriff auf die meisten die Gesellschaft betreffenden Daten haben, *Shkabatur*, Stanford T. L. Rev. 22 (2019), 354 (357); *Spiecker gen. Döhmman*, in: Kischel/Kube (Hrsg.), HStR I, 2023, § 20 Digitalisierung, Informationsgesellschaft, Massendaten, Rn. 7; siehe auch *Martini*, in: Kahl/Ludwigs (Hrsg.), HVwR I, 2021, § 28 Digitalisierung der Verwaltung, Rn. 72 ff.

²⁷ *Leopoldina/acatech et al.*, Digitalisierung und Demokratie, 2021, S. 19 f.; *Shkabatur*, Stanford T. L. Rev. 22 (2019), 354 (357); *Spiecker gen. Döhmman*, in: Kischel/Kube (Hrsg.), HStR I, 2023, § 20 Digitalisierung, Informationsgesellschaft, Massendaten, Rn. 7.

²⁸ Zur Datafizierung der Umwelt, *Lambach*, Die Datafizierung der Welt, in: Augsberg/Düwell/Müller (Hrsg.), Datenzugangsregeln, 2024, S. 139 (155).

²⁹ *Bacon*, Neues Organ der Wissenschaften, 1990, S. 26.

die vorgelagerte Ebene der Daten. Wo sie nicht in ausreichendem Maße verfügbar sind, schwindet die Möglichkeit staatlicher Stellen, drängende Aufgaben und Transformationsprozesse evidenzbasiert bewältigen zu können – und damit das Vertrauen in den Staat selbst.³⁰ Vorausschauend war es bereits *Max Weber*, der festgestellt hat, dass einzig die Sachkenntnis privater Unternehmen auf dem Gebiet der Wirtschaft derjenigen des Staates aus strukturellen Gründen überlegen sei, da für private Unternehmen die „genaue Tatsachenkenntnis auf ihrem Gebiet direkt[e] wirtschaftliche Existenzfrage“ sei.³¹ Heute potenziert sich diese Überlegenheit und es bleibt bisher unklar, welche Rolle der Staat in einer datengetriebenen Gesellschaft einnehmen soll und inwieweit er eine informatorische Gegenmacht bilden kann.³² Angesichts des Bedarfs an umfangreichen Datenmengen für gemeinwohlrelevante staatliche Entscheidungsprozesse sowie der mangelnden Bereitschaft des privaten Sektors, freiwillige Datenspenden zu leisten,³³ kommt insofern immer häufiger die Frage auf, wie der Staat sein Datendefizit wieder ausgleichen und Informationsvielfalt schaffen kann.³⁴

In den letzten Jahren hat sich vor allem ein Ansatz etabliert, der darauf setzt, dass sich der Staat kraft seiner demokratisch legitimierten Autorität Zugang zu relevanten privat gehaltenen Daten verschafft (*Business-to-Government-Data-Sharing*).³⁵ Im Fokus stehen vornehmlich nicht personenbezogene, maschinengenerierte Daten. Dabei macht sich der Staat ihr zentrales Charakteristikum zunutze, ihre Nichtrivali-

³⁰ *Löfgren/Webster*, *Big Data & Society* 7 (2020), 1 (1). *Tarkowski/Vogelezang et al.*, *Public Data Commons*, 2022, S. 4, konstatieren: „[T]he integrity and capacities of the public sector are questioned“; unter dem Begriff „*evidence-based public policy*“ hat sich in den letzten Jahren eine internationale Bewegung etabliert, die darauf abzielt, Regulierung und politische Prozesse auf theoretisch fundierte empirische Analysen zu stützen, um bessere Ergebnisse zu erzielen und Regulierungsversagen zu vermeiden. Staatliche Datenzugangsrechte sind Teil dieses größeren Bildes, *Valli Buttow*, *EJRR* 15 (2024), 1 (4); vgl. insg. *Strassheim*, *Trends towards evidence-based policy formulation*, in: Howlett/Mukherjee (Hrsg.), *Handbook of Policy Formulation*, 2017, S. 504 (504 ff.).

³¹ *Weber*, *Wirtschaft und Gesellschaft*, 5. Aufl., 1976, S. 574 ff.

³² *Richter*, *ZRP* 2020, 245 (245 f.).

³³ *Alemanno*, *EJRR* 9 (2018), 183 (185); *Greef*, *Staat und Staatlichkeit im digitalen Zeitalter*, 2023, S. 12 ff.; *Ramge/Mayer-Schönberger*, *Machtmaschinen*, 2020, S. 179.

³⁴ Vgl. z.B. *High-Level Expert Group on Business-to-Government Data Sharing*, *Towards a European strategy on business-to-government data sharing for the public interest*, 2020 sowie *Europäische Kommission*, *Eine europäische Datenstrategie*, COM(2020) 66 final, 19.2.2020, S. 9.

³⁵ Die Idee, öffentlichen Stellen systematisch Zugang zu privaten Daten zu gewähren, um die Erfüllung öffentlicher Aufgaben zu ermöglichen oder zu verbessern, stammt ursprünglich aus öffentlich-privaten Kooperationen in Entwicklungsländern. Innerhalb der EU hat erstmals Frankreich in seinem 2016 erlassenen „*Loi Lemaire*“ (insbesondere die Regelungen zu den „*données d'intérêt général*“ gem. Art. 17–24 *LOI n° 2016–1321 pour une République numérique* v. 7.10.2016) spezifische Regelungen zur Datenbereitstellung von privaten Akteuren an den Staat getroffen; ausführlich, *Richter*, *The Law and Policy of Government Access to Private Sector Data* („*B2G Data Sharing*“), in: Bundesministerium für Justiz und Verbraucherschutz/Max-Planck-Institut für Innovation und Wettbewerb (Hrsg.), *Data Access, Consumer Interests and Public Welfare*, 2021, S. 529 (529 ff.).

tät.³⁶ Teilt ein Unternehmen seine bisher exklusiv gehaltenen Daten mit einer staatlichen Stelle, können sie weiterhin in kommerzielle Auswertungen fließen, während sie simultan digitale Analysen im öffentlichen Interesse antreiben. Die asymmetrisch gezeichnete Datenlandschaft zwischen Staat und Privat soll so zu größerer Balance finden.

Zugleich erweitern sich die durch digitale Technologien eröffneten Handlungsspielräume und damit verbundenen Legitimationschancen. Datenanalysen können fluktuierendes Entscheidungswissen ordnen – gerade in informationsintensiven Bereichen staatlichen Handelns, die von Infrastruktur und Raumplanung über Mobilitäts- und Gesundheitsbelange bis hin zur Energieversorgung reichen. Der Umwelt- und Klimaschutz tritt hierbei als paradigmatisches Referenzfeld hervor, das durch eine besonders ausgeprägte Wissensabhängigkeit und eine erhebliche staatliche Informationsnachfrage gekennzeichnet ist.³⁷

Datenzugangsrechte gegenüber Privaten adressieren insofern die Herausforderung unzureichender Informations- und Wissensstände in zahlreichen dieser Bereiche. Sie zielen darauf ab, Entscheidungssicherheit herzustellen und das Rationalitätsversprechen des modernen Staates einzulösen. Damit stellen sie entscheidende Weichen für die Frage, wie der Staat in vielen bisher von Unsicherheit geprägten Feldern künftig zu mehr Sicherheit finden kann.³⁸ Versetzen gesetzliche Zugangsrechte den Staat in die Lage, eigene und bisher privat gehaltene Daten zu kombinieren, um auf dieser Basis relevante Sachverhalte digital zu erfassen, zu analysieren und abzubilden, so besteht die Hoffnung, wieder zu verlässlicheren und genaueren Erkenntnissen zu gelangen. Das Ideal der „Herrschaft kraft Wissen“ lebt aus dieser Perspektive neu auf.³⁹

³⁶ Gill/Zolna et al., Data Sharing for Collective Interests – Moving Beyond Exclusive Control, in: Heine/Budzinski (Hrsg.), FS Kerber, 2024, S. 225 (226).

³⁷ Zum besonders hohen Informationsbedarf innerhalb des Umweltrechts, vgl. u. a. Klopfer, Umweltrecht, 4. Aufl., 2016, S. 445; Ladeur, Das Umweltrecht der Wissensgesellschaft, 1995, S. 69 ff.; BT-Drs. 11/1152, S. 11; gleichzeitig sind der Umwelt- und Klimaschutz in den letzten Jahren durch ein Nichtwissen des Staates geprägt. Wehling, Ungeahnte Risiken, in: Collin/Horstmann (Hrsg.), Das Wissen des Staates, 2004, S. 309 (310), führt dabei die Erosion des Ideals der rationalen „wissensbasierten“ politischen Herrschaft auf zwei Entwicklungslinien zurück: zum einen die wachsende Abhängigkeit von externem wissenschaftlichen Expertenwissen, zum anderen die Überlegenheit des lokalen Wissens wirtschaftlicher und sozialer Akteure.

³⁸ Zu Information als Mittel zur Bewältigung von Unsicherheit, Spiecker gen. Döhmman, in: Kahl/Ludwigs (Hrsg.), HVwR I, 2021, § 23 Informationsverwaltung, Rn. 36 ff.

³⁹ Vgl. auch Martini, Big Data als Herausforderung für das Datenschutzrecht und den Persönlichkeitsschutz, in: Hill/Martini/Wagner (Hrsg.), Die digitale Lebenswelt gestalten, 2015, S. 97 (109).

B. Der staatliche Zugang zu Daten als Eingriff in die unternehmerische Geheimsphäre

Auch wenn die datengestützte Erfüllung öffentlicher Aufgaben zu den bedeutendsten Hoffnungsträgern gegenwärtiger Transformationsprozesse gehört, immunisiert sie dies nicht gegen grundrechtlich garantierte Freiheitsräume (Art. 6 Abs. 1 EUV; Art. 1 Abs. 3 GG). Sie bewegt sich in einem Spannungsfeld zweier konfligierender Pole: Einerseits bedarf die öffentliche Hand eines weitreichenden Zugangs zu den Daten privater Unternehmen, um ihre Gemeinwohlziele zu erreichen.⁴⁰ Andererseits genießen unternehmensinterne Daten einen besonderen Schutz. In den meisten Fällen halten Unternehmen ihre kommerziell wertvollen Daten exklusiv, womit sich diese als Geschäftsgeheimnis qualifizieren können.⁴¹ Der Gesetzgeber spricht Unternehmen insoweit exklusive Rechte an ihrem über lange Zeit und mit hohen Investitionen erworbenen Wissen zu, um Anreize zu schaffen, wertvolle Informationen zu generieren und darauf aufbauend Innovationen zu erzeugen.⁴² Da sich in diesen Daten die bisherige Leistung eines Unternehmens ausdrückt und sie zugleich die Grundlage seines künftigen wettbewerblichen Handelns bilden,⁴³ partizipieren sie am Schutz durch die Wirtschaftsgrundrechte (Art. 16, 17 GRCh; Art. 12 Abs. 1, 14 Abs. 1 GG). Nicht nur private Konkurrenten, sondern auch der Staat darf nicht ohne Weiteres auf sie zugreifen. Der grundrechtlich verbürgte Schutz von Geschäftsgeheimnissen stellt ein legitimes subjektives Restriktionsinteresse dar, sich staatlicher Datenzugangsrechte zu erwehren.⁴⁴

Dem Interesse der Wirtschaft, die unternehmerische Geheimsphäre vor staatlichen Übergriffen zu schützen,⁴⁵ stehen Stimmen gegenüber, die das Ideal des „*free flow of data*“ proklamieren.⁴⁶ Sie verweisen darauf, dass sich der Geheimnisschutz in den letzten Jahren immer weiter ausgedehnt hat: Die offene Definition von Geschäftsgeheimnissen ermöglicht es unter den Bedingungen der digitalen Wirtschaft,

⁴⁰ Gailhofer/Franke, ZUR 32 (2021), 532 (537).

⁴¹ Zu den einzelnen Voraussetzungen des Geschäftsgeheimnisschutzes Kap. 2 D.

⁴² Siehe Kap. 3 A.

⁴³ ErwGr. 1 Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates v. 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung (im Folgenden: Geschäftsgeheimnis-RL).

⁴⁴ Fetzner, The constitutional framework for data access rights, in: Bundesministerium für Justiz und Verbraucherschutz/Max-Planck-Institut für Innovation und Wettbewerb (Hrsg.), *Data Access, Consumer Interests and Public Welfare*, 2021, S. 155 (171); Richter, The Law and Policy of Government Access to Private Sector Data („B2G Data Sharing“), in: Bundesministerium für Justiz und Verbraucherschutz/Max-Planck-Institut für Innovation und Wettbewerb (Hrsg.), *Data Access, Consumer Interests and Public Welfare*, 2021, S. 529 (550).

⁴⁵ Vgl. u. a. Bundesverband der Deutschen Industrie e.V., Geschäftsgeheimnisschutz im Data Act, 2023; DIGITALEUROPE/European Round Table for Industry, Joint Statement on the Data Act, 2023.

⁴⁶ Ramge/Mayer-Schönberger, *Machtmaschinen*, 2020, S. 159 ff.; dazu auch Fisher/Strein, Col. J. T. L. 60 (2022), 829 (867 ff.).

nahezu alle unternehmensbezogenen Daten als Geheimnis zu deklarieren.⁴⁷ Aufgrund seiner Flexibilität ist der Geheimnisschutz so zum Schlüsselinstrument der Datenökonomie avanciert, Daten exklusiv zu halten als auch zu handeln⁴⁸ – obwohl er ursprünglich nicht auf Big-Data-Sachverhalte zugeschnitten war.⁴⁹

Diejenigen, die Daten aus ihrer Exklusivität befreien wollen, betonen ihre Gemeinwohlrelevanz. Offene Daten können nicht nur Innovationen fördern, sondern auch unmittelbar Leib und Leben schützen. Anfang 2024 formulierte der US-amerikanische Klimatologe *Justin Menkin* in einem Aufsehen erregenden Essay in der *New York Times* seine Forderung: „People Have a Right to Climate Data“.⁵⁰ Solche Daten sollten ihm zufolge als öffentliches Gut gelten, also nicht rival und vor allem nicht exklusiv sein. Das steht konträr zum tatsächlichen Status von Daten in Wettbewerbsprozessen, ihrer geheimnisrechtlichen Exklusivität und ihrer ungleichen Akkumulation zwischen Staat und Privat.⁵¹ Welche verheerenden Folgen es haben kann, wenn gemeinwohlrelevante Umwelt- und Klimadaten hinter verschlossenen Türen bleiben, macht *Menkin* an einem Beispiel aus den von Tornados heimgesuchten USA deutlich. Dort verkaufen kommerzielle Forecasting-Dienste präzisere Klima- und Wetterdaten an private Unternehmen, damit diese ihre geschäftlichen Aktivitäten an die sich verändernden extremen Umweltbedingungen anpassen können. Doch die Exklusivität dieser Daten fordert ihre Opfer, wie der CEO des umsatzstärksten Anbieters AccuWeather, *Joel Myers*, in einem Interview selbst verrät. Er macht auf ein Beispiel aufmerksam, in dem das private Verkehrsunternehmen Union Pacific auf diese Daten zugreifen konnte, die Stadtverwaltung einer Kleinstadt jedoch nicht:

„Two trains stopped two miles apart, they watched the tornado go between them, [...] unfortunately, it went into a town that didn't have our service and a couple of dozen people were killed. But the railroad did not lose anything.“⁵²

Angesichts des fortschreitenden Klimawandels, wachsender Umweltbelastungen und tiefgreifender gesellschaftlicher Transformationsprozesse stellt sich daher zu-

⁴⁷ *Dean*, Cal. L. Rev. 109 (2021), 2423 (2428); *Fia*, IIC 53 (2022), 917 (923 ff.); *Fisher/Strein*, Col. J. T. L. 60 (2022), 829 (886); *Fromer*, N. Y. U. L. Rev. 94 (2019), 706 (723); *Kapczynski*, Yale L. J. 129 (2020), 1460 (1466, 1503, 1509); *Levine*, Flor. L. Rev. 59 (2007), 135 (150, 156); *Pistor*, LCP 83 (2020), 101 (107); siehe auch *Dreyfuss*, Trade Secrets and Deep Secrets, 2024, S. 2 f., welche konstatiert: „[T]rade secrecy claims have become more popular [...], the types of knowledge that can fall outside the standard fields have expanded“.

⁴⁸ *Vatanparast*, Juridikum 2021, 98 (104).

⁴⁹ Krit. *Drexler*, JIPITEC 8 (2017), 257 (268); *Wiebe/Schur*, GRUR Int. 68 (2019), 746 (747).

⁵⁰ *Menkin*, The People Have a Right to Climate Data, <https://www.nytimes.com/2024/01/20/opinion/climate-risk-disasters-data.html> (6.1.2026).

⁵¹ Die Datafizierung der Umwelt hat zu einem fundamentalen Wertekonflikt geführt, bei dem auf der einen Seite die Überführung unseres „Weltwissens“ in die Sphäre eines Gemeinguts steht und auf der anderen Seite die proprietär-orientierte Sichtweise, Daten in Privateigentum zu überführen, *Lambach*, Die Datafizierung der Welt, in: *Augsberg/Düwell/Müller* (Hrsg.), Datenzugangsregeln, 2024, S. 139 (141).

⁵² *Wells/Chemi*, The business of weather forecasting, <https://www.cnn.com/video/2018/03/07/full-interview-the-business-of-weather-forecasting.html> (6.1.2026), ab Minute 10:13.

nehmend die rechtspolitische Frage, in welchem Ausmaß gemeinwohlrelevante Daten rechtlich vermittelte Exklusivität genießen dürfen und inwieweit der Staat kraft seiner Autorität auf diese Daten zugreifen können muss.⁵³

Voraussetzungslos lassen sich geheime, grundrechtssensible Daten allerdings nicht einer inklusiven Nutzung zuführen. Gesetzliche Datenzugangsrechte stellen einen empfindlichen Eingriff in die grundrechtlich garantierte unternehmerische Geheimosphäre dar. Greift eine öffentliche Stelle auf geheime Daten zu und treten diese aus der unternehmerischen in die staatliche Sphäre über, verschwimmt ihre Exklusivität. Im Extremfall löst der Staat sie aufgrund überwiegender Gemeinwohlinteressen auf, indem er die Daten der Öffentlichkeit als *Open Data* bereitstellt. Die Rechtsposition „Geschäftsgeheimnis“ geht vollständig unter und die unternehmerische Freiheit (Art. 16 GRCh), die Berufsfreiheit (Art. 12 Abs. 1 GG) sowie das Eigentum (Art. 17 GRCh; Art. 14 Abs. 1 GG) sind empfindlich berührt.

Aus grundrechtlicher Perspektive ist es daher essenziell zu klären, wie weit der Schutz von Geschäftsgeheimnissen den staatlichen Zugang zu geheimen Daten begrenzt und wie sich der Antagonismus zwischen dem gemeinwohlbezogenen Zugangsinteresse der Allgemeinheit und privaten, wirtschaftlich motivierten Restriktionsinteressen auflösen lässt.⁵⁴

C. Ziel der Untersuchung

Die Problematik des Schutzes von Geschäftsgeheimnissen im Kontext von Datenzugang und Datenökonomie ist einer breiten Diskussion ausgesetzt, jedoch vornehmlich im horizontalen Verhältnis zwischen Privaten.⁵⁵ Die Perspektive gegenüber dem Staat und damit auch die Grundrechte bleiben zumeist außen vor.

Dieser Befund lässt sich maßgeblich darauf zurückführen, dass die datengetriebene Wirtschaft enorme Wachstums- und Effizienzpotenziale verspricht und Daten primär als handelbares Gut versteht. Damit richtet sich der Blick typischerweise auf private Nutzungskonflikte, die Gegenstand des Privatrechts, insbesondere des Wettbewerbsrechts, sind. Die Verbindung von „Geschäftsgeheimnisschutz“ und „staatlichem Datenzugang“ hat daher in der Rechtswissenschaft bislang wenig bis gar keine Beachtung gefunden, obwohl der Schutz von Geschäftsgeheimnissen das

⁵³ Vgl. etwa *Datenethikkommission der Bundesregierung*, Gutachten der Datenethikkommission der Bundesregierung, 2019, S. 154; *Europäische Kommission*, Eine europäische Datenstrategie, COM(2020) 66 final, 19.2.2020, S. 14; *CDU/CSU/SPD*, Verantwortung für Deutschland, 2025, S. 69 f.

⁵⁴ *Dreyfuss*, Trade Secrets and Deep Secrets, 2024, S. 4.

⁵⁵ *Antoine*, CR 40 (2024), 73 (73 ff.); *Aplin/Radauer et al.*, IIC 54 (2023), 826 (826 ff.); *Graptin*, RDi 3 (2023), 173 (173 ff.); *Grützmacher*, CR 40 (2024), 281 (281 ff.); *Leistner/Antoine*, IPR and the use of open data and data sharing initiatives by public and private actors, 2022, S. 58 f., 64 f., 76 f.; *Lorenzen*, ZGE 14 (2022), 250 (250 ff.); *Mylly*, IIC 55 (2024), 368 (368 ff.); *Pauly/Wichert et al.*, MMR 27 (2024), 211 (211 ff.); *Radauer/Bader et al.*, Study on the Legal Protection of Trade Secrets in the Context of the Data Economy, 2022; *Wunner*, ZUM 68 (2024), 424 (424 ff.).