Rechte an Daten – zum Stand der Diskussion

ALAIN SCHMID[*] / KIRSTEN JOHANNA SCHMIDT[**] / HERBERT ZECH[***]

In Zeiten von fortschreitender Digitalisierung, Big Data und «Internet of Things» werden Daten zunehmend als handelbares Gut verstanden. Deshalb werden mögliche Rechte an Daten und ihre Ausgestaltungsmöglichkeiten in der Wissenschaft und Politik vermehrt diskutiert. Der vorliegende Beitrag gibt einen Überblick über den Stand der Diskussion in der Schweiz[1].

À l'ère de la numérisation galopante, des mégadonnées et de l'Internet des objets, les données sont de plus en plus considérées comme un bien commercialisable. Par conséquent, les droits potentiels sur les données et les possibilités de les configurer en science et en politique sont de plus en plus discutés. Cet article donne un aperçu de l'état des discussions en Suisse[1].

I. Einführung

Die aktuelle Diskussion wurde durch technische Entwicklungen angestossen, die zahlreiche neue Geschäftsmodelle ermöglichen. Aus rechtlicher Sicht ist neben den ökonomischen Auswirkungen neuer Datentechnologien auch die Verwendung eines klar definierten Datenbegriffs wichtig, der für die rechtliche Analyse herangezogen werden kann.

1. Die Bedeutung von Rechten an Daten

Der technische Wandel hat in den letzten Jahren neue Erscheinungen wie selbst fahrende Autos («Smart Cars»), die Vernetzung physischer und virtueller Gegenstände («Internet of Things») oder die Verzahnung von industrieller Produktion mit modernster Informations- und Kommunikationstechnik («Industrie 4.0») hervorgebracht. Diesen Erscheinungen ist gemein, dass immer mehr Daten erzeugt

[*] MLaw, Advokat, wissenschaftlicher Assistent an der Juristischen Fakultät der Universität Basel.
[**] MLaw, Rechtsanwältin, LL.M. (Boston), wissenschaftliche Assistentin an der Juristischen Fakultät der Universität Basel.
[***] Prof. Dr. jur., Dipl.-Biol., Professor für Life Sciences-Recht und Immaterialgüterrecht an der Juristischen Fakultät der Universität Basel.
[1] Der vorliegende Beitrag entstand im Rahmen des Projektes «Legal Challenges in Big Data. Allocating benefits. Averting risks» des Nationalen Forschungsprogramms 75 «Big Data» (NFP 75 «Big Data»), welches durch den Schweizerischen Nationalfonds (SNF) finanziert wird. Die Autoren bedanken sich für die Förderung.
La présente contribution a été rédigée dans le cadre du Projet «Legal Challenges in Big Data. Allocating benefits. Averting risks» Du Programme national de recherche 75 «Big Data» (NFP 75 «Big Data») financé par le Fonds national suisse de la recherche scientifique (FNS). Les auteurs remercient le FNS pour son soutien.

werden[2]. Diese Daten können von Marktteilnehmern gesammelt, zu grossen unstrukturierten Datenbeständen zusammengeführt und auf wertvolle Erkenntnisse hin analysiert werden («Big Data Analytics»). Das zunehmende wirtschaftliche Interesse am Wert dieser Daten führte vor allem auf europäischer Ebene und in Deutschland zu grossen Diskussionen über die rechtliche Einordnung von Daten[3]. Es stellen sich Fragen wie: «Wem gehören Daten? Wie können Daten geschützt werden? Muss der Zugang zu Daten rechtlich gewährleistet werden?» Der vorliegende Aufsatz soll einen Überblick über den Stand der Diskussion zu Rechten an Daten in der Schweiz geben[4].

2. Datenbegriff

In Bezug auf Rechte an Daten interessiert die Frage, wie Daten als Rechtsobjekt erfasst werden können. Daten lassen sich als maschinenlesbar codierte Information (abgegrenzt auf der syntaktischen Ebene) definieren[5]. Sie können eine semantische Ebene (Bedeutung) aufweisen, aber müssen dies nicht notwendigerweise[6]. Zudem liegen Daten regelmässig auf physikalischer bzw. struktureller Ebene, d.h. auf einem Datenträger, vor, der die syntaktische Ebene ermöglicht[7]. Daten lassen sich demnach auch auf der Bedeutungsebene (semantische Information)[8] und auf der Zeichenebene (syntaktische Information)[9] abgrenzen[10].

Daten sind öffentliche Güter und als solche nicht rivalisierend, nicht exklusiv und nicht abnutzbar. Nicht rivalisierend bedeutet, dass die Nutzung des Gutes durch eine Person die Nutzung des Gutes durch eine andere Person nicht beeinträchtigt. Das Gut kann demnach von mehreren Personen gleichzeitig verwendet werden. Nicht exklusiv meint, dass die Nutzung des Gutes durch Dritte nicht verhindert werden kann[11]. Schliesslich unterliegen Daten keiner Abnutzbarkeit, da sie beliebig vervielfältigbar sind[12].

Daten werden in Personen- und Sachdaten unterteilt. Personendaten sind gemäss Art. 3 lit. b DSG alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Alle anderen Daten sind Sachdaten. Die Unterscheidung zwischen Personen- und Sachdaten spielt deshalb eine Rolle, da in ersterem Fall das Datenschutzrecht anwendbar ist und im letzteren Fall nicht. Die zunächst einfach erscheinende Abgrenzung stellt sich bei näherer Betrachtung als problematisch heraus. Denn die Beantwortung der Frage, ob sich einzelne Daten einer mindestens bestimmbaren Person zuordnen lassen, fällt je nach Kontext unterschiedlich aus und kann deshalb nicht starr festgelegt werden.

Gemäss dem Bundesgericht ist eine Person bestimmbar, wenn sie zwar allein durch die Daten nicht eindeutig identifiziert werden kann, aber aus dem Kontext einer Information oder aufgrund zusätzlicher Informationen auf sie geschlossen werden kann. Für die Bestimmbarkeit genügt jedoch nicht jede theoretische Möglichkeit der Identifizierung. Wenn aber nach der allgemeinen Lebenserfahrung damit gerechnet werden muss, dass ein Interessent den Aufwand für die Bestimmung der betroffenen Person auf sich nehmen wird, liegt Bestimmbarkeit vor. Bei der Beurteilung des Aufwands sind die aktuellen

---

2 R.G. BRINER, Big Data und Sachenrecht, Jusletter IT vom 21. März 2015, Rz. 14 f. erwähnt Schätzungen von 1,5 Exabytes für das Jahr 1999, 5 Exabytes für das Jahr 2003, 161 Exabytes für das Jahr 2006 und 1000 Exabytes für das Jahr 2010. Für das Jahr 2016 betrug die Menge an Daten gemäss einer Studie der International Data Corporation (IDC) 16,1 Zettabytes und wird bis ins Jahr 2025 auf 163 Zettabytes ansteigen. Siehe dazu: D. REINSEL/J. GANTZ/J. RYDNING, Data Age 2025: The Evolution of Data to Life-Critical. Don't Focus on Big Data; Focus on the Data That's Big, IDC White Paper, April 2017, 3, abrufbar unter <www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf> (17. Mai 2018).

3 Für eine Auflistung von ausländischer Literatur siehe Fn. 3 in R.H. WEBER/F. THOUVENIN, Dateneigentum und Datenzugangsrechte – Bausteine der Informationsgesellschaft?, ZSR 2018, 44.

4 Dementsprechend wurde nur die Schweizer Literatur berücksichtigt und nur, wo nötig, auf deutsche Literatur verwiesen. Nicht Gegenstand dieses Aufsatzes bilden auch eigentumsähnliche Rechte an Daten, die durch Vertrag oder Delikte begründet werden können.

5 H. ZECH, Information als Schutzgegenstand, Tübingen 2012, 32.

6 ZECH (Fn. 5), 32 f., 43.

7 ZECH (Fn. 5), 32.

8 So findet bspw. das DSG auf alle Daten, die sich auf eine bestimmte oder bestimmbare Person beziehen, Anwendung (Art. 3 lit. a DSG).

9 Wenn Informationen im binären Format gespeichert werden, resultiert daraus eine Kette von Einsen und Nullen.

10 D. HÜRLIMANN/H. ZECH, Rechte an Daten, sui generis 2016, N 3.

11 Die Daten können aber selbstverständlich faktisch durch technische Mittel (z.B. Verschlüsselung) vor dem Zugriff durch Dritte geschützt werden.

12 H. ZECH, Daten als Wirtschaftsgut – Überlegungen zu einem «Recht des Datenerzeugers», CR 2015, 139. Davon zu unterscheiden ist allenfalls eine Beeinträchtigung der Nutzung des Datenträgers durch wiederholtes Kopieren der sich darauf befindlichen Daten.

Möglichkeiten der Technik zu berücksichtigen. Nebst dem Aufwand spielt auch das Interesse des Dritten an der Identifizierung eine Rolle[13].

Als Beispiel: Die von einem Personenwagen aufgezeichneten Angaben, ob dessen Fahrer den Sicherheitsgurt angelegt hat oder nicht, können durch die Verknüpfung mit Lokalisierungsdaten zu Personendaten werden.

Erschwerend kommt hinzu, dass die Bestimmbarkeit relativ zum Wissen und den Möglichkeiten des jeweiligen Inhabers der Information beurteilt wird. Eine Person kann so für bestimmte Menschen identifizierbar sein, für andere hingegen nicht[14]. So können beispielsweise grosse Mengen von anonymisierten Daten gesammelt werden (Stichwort Big Data), mit welchen der Personenbezug durch die Kombination oder Analyse der Daten wiederhergestellt werden kann.

Ist eine Person aus Daten bestimmbar, liegen mithin Personendaten vor, so können diese durch Anonymisierung zu Sachdaten werden. Anonymisierte Daten liegen dann vor, wenn der irreversibel aufgehobene Personenbezug nicht ohne unverhältnismässigen Aufwand wiederhergestellt werden kann[15]. Wurden die Personendaten hingegen nur pseudonymisiert, d.h. der Personenbezug nur reversibel aufgehoben, da mittels eines aufbewahrten Schlüssels eine Re-Identifizierung möglich ist, so liegen aus der Sicht der Personen, die Zugang zum Schlüssel haben, weiterhin Personendaten vor, für Aussenstehende hingegen Sachdaten[16].

Es lässt sich festhalten, dass aufgrund der sehr weiten Definition des Begriffes «Personendaten» und der stetig zunehmenden technischen Möglichkeiten zur Wiederherstellung des Personenbezuges bei anonymisierten Daten oftmals keine Sachdaten, sondern Personendaten vorliegen dürften.

II. Eigentumsartige Rechte an Daten

Sachen werden im Rechtsverkehr mit der Rechtsfigur des Eigentums einer Person zugewiesen und geschützt. Für Daten wird deshalb diskutiert, ob de lege lata ebenfalls eine Zuweisung und ein Schutz durch eigentumsartige Rechte bestehen und, falls nicht, was de lege ferenda für eigentumsartige Rechte an Daten denkbar wären.

1. De lege lata

In Bezug auf Daten sind de lege lata vor allem das Sachen- und das Immaterialgüterrecht relevant.

a) Sachenrecht

Das Sachenrecht räumt dem Eigentümer einer Sache ein erga omnes wirkendes und umfassendes Herrschaftsrecht an einer Sache ein[17]. Dieses Herrschaftsrecht umfasst zwei Seiten: Im Rahmen der positiven Seite kann der Eigentümer einer Sache gemäss Art. 641 Abs. 1 ZGB «in den Schranken der Rechtsordnung über sie nach seinem Belieben verfügen». Die Sache wird demnach dem Eigentümer zugeordnet. Als Befugnisse stehen dem Eigentümer insb. der Besitz und die Nutzung (Gebrauch, Verbrauch, Veränderung und Vernichtung) der Sache zu. Der Eigentümer kann zudem Rechtsgeschäfte über die Sache abschliessen, um die Sache einem Dritten zur Nutzung zu überlassen, dingliche Rechte an der Sache begründen oder das Eigentum übertragen[18]. Die negative Seite in Art. 641 Abs. 2 ZGB räumt dem Eigentümer einer Sache das Recht ein, «sie von jedem, der sie ihm vorenthält, herauszuverlangen [rei vindicatio] und jede ungerechtfertigte Einwirkung abzuwehren [actio negatoria]»[19]. Diese durch das Eigentumsrecht gewährten Befugnisse verjähren nicht[20].

---

[13] BGE 138 II 346 ff. E. 6.1.
[14] B. BAERISWYL/K. PÄRLI, Datenschutzgesetz (DSG), Bern 2015, DSG 3 N 12.
[15] BAERISWYL/PÄRLI (Fn. 14), DSG 3 N 13.
[16] BAERISWYL/PÄRLI (Fn. 14), DSG 3 N 14.
[17] H. HONSELL/N.P. VOGT/T. GEISER, Basler Kommentar ZGB II, Basel 2015, ZGB 641 N 3.
[18] HONSELL/VOGT/GEISER (Fn. 17), ZGB 641 N 30 ff.
[19] HONSELL/VOGT/GEISER (Fn. 17), ZGB 641 N 40 ff.
[20] Eine Sache kann allerdings ersessen (Art. 728 ZGB) oder von einem Nicht-Berechtigten gutgläubig erworben werden (Art. 714 Abs. 2 und Art. 933 und 934 ZGB).

Als absolut geschütztes Rechtsgut wird das Eigentum an einer Sache zudem von Art. 41 OR erfasst. Wer ausservertraglich eine Sache beschädigt oder zerstört und dadurch deren Eigentümer einen Schaden zufügt, wird ihm schadenersatzpflichtig. Art. 41 OR schützt damit die Integrität einer Sache.

Strafrechtlich wird das Eigentum an einer Sache durch die Tatbestände der unrechtmässigen Aneignung (Art. 137 StGB), der Veruntreuung (Art. 138 StGB), des Diebstahls (Art. 139 StGB), des Raubs (Art. 140 StGB), der Sachentziehung (Art. 141 StGB), der Sachbeschädigung (Art. 144 StGB) und der Erpressung (Art. 156 StGB) geschützt.

Das Sachenrecht im Zivilgesetzbuch normiert allerdings keine Legaldefinition des Begriffes «Sache», sondern überlässt die Definition der Lehre und Rechtsprechung nach Massgabe der Verkehrsauffassung[21]. In der Lehre wird eine Sache definiert als «ein körperlicher, von anderen abgegrenzter Gegenstand, der tatsächlicher und rechtlicher Beherrschung zugänglich ist»[22]. Eigentum im Sinne des Sachenrechts kann demnach nur an körperlichen Sachen (und Naturkräften[23]) bestehen[24]. Da Daten jedoch immaterielle Güter darstellen, kann kein Eigentum im Sinne des Sachenrechts an Daten bestehen[25]. Eine Zuweisung der Daten an einen Eigentümer und der Schutz der Daten durch das Eigentum existieren deshalb nicht.

b) Immaterialgüterrecht

Nebst der Zuordnung und dem Schutz von Daten durch das Sachenrecht wird auch eine Zuordnung und ein Schutz von Daten als Werk durch das im URG normierte Urheberrecht diskutiert. Art. 2 Abs. 1 URG definiert Werke als geistige Schöpfungen der Literatur und Kunst, die individuellen Charakter haben, unabhängig von ihrem Wert oder Zweck. Bei Vorliegen dieser Schutzvoraussetzungen hat der Urheber gemäss Art. 10 Abs. 1 URG «das ausschliessliche Recht zu bestimmen, ob, wann und wie das Werk verwendet wird». Der Urheber kann insbesondere die Vervielfältigung und Nutzung seines Werkes untersagen[26] und das Urheberrecht gemäss Art. 16 Abs. 1 URG auf einen Dritten übertragen. Dem Rechtsinhaber wird damit sein Werk zugeordnet und ein umfassendes, erga omnes wirkendes Ausschliesslichkeitsrecht gewährt. Die Herrschaftsrechte ähneln damit, abgesehen vom Besitz, denjenigen des Eigentums[27]. Die umfassenden Ausschliesslichkeitsrechte werden durch die im 5. Kapitel des URG normierten Schranken des Urheberrechts eingeschränkt[28]. Der urheberrechtliche Schutz ist zudem zeitlich befristet: Gemäss Art. 29 Abs. 2 URG erlischt der Schutz 50 Jahre nach dem Tod des Urhebers von Computerprogrammen und 70 Jahre nach dem Tod des Urhebers von allen anderen Werken. Das Urheberrecht bietet keinen semantischen Schutz, sondern schützt die Art und Weise, wie Inhalt mitgeteilt wird[29].

Daten können demnach urheberrechtlich geschützt sein, wenn sie eine geistige Schöpfung mit individuellem Charakter sind. Bei von Maschinen generierten Daten fehlt es aber gerade an einer geistigen Schöpfung, weshalb solche Daten keinen urheberrechtlichen Schutz geniessen. Hingegen können Datenbanken als Sammelwerke urheberrechtlich geschützt sein, sofern es sich bezüglich der Auswahl oder Anordnung der gesammelten Daten um eine geistige Schöpfung mit individuellem Charakter handelt[30].

---

[21] HONSELL/VOGT/GEISER (Fn. 17), ZGB Vor Art. 641 ff. N 6.
[22] HONSELL/VOGT/GEISER (Fn. 17), ZGB Vor Art. 641 ff. N 6.
[23] Art. 713 ZGB.
[24] Vgl. Art. 641 und 713 ZGB; im Vergleich dazu die klaren §§ 90 des D-BGB, gemäss welchem «Sachen im Sinne des Gesetzes [...] nur körperliche Gegenstände [sind]», und 353 des AT-ABGB, gemäss welchem körperliche und unkörperliche Sachen Eigentum darstellen können.
[25] So auch U. HESS-ODONI, Die Herrschaftsrechte an Daten, Jusletter vom 17. Mai 2004, Rz. 7 ff.; BRINER (Fn. 2), Rz. 31; R.H. WEBER/L. CHROBAK, Rechtsinterdisziplinarität in der digitalen Datenwelt, Jusletter vom 4. April 2016, Rz. 16; HÜRLIMANN/ZECH (Fn. 10), N 8; G. FRÖHLICH-BLEULER, Eigentum an Daten?, Jusletter vom 6. März 2017, Rz. 13; F. THOUVENIN/A. FRÜH/A. LOMBARD, Eigentum an Sachdaten: Eine Standortbestimmung, SZW 2017, 26; WEBER/THOUVENIN (Fn. 3), 49.
[26] Art. 10 Abs. 2 URG enthält einen ganzen Katalog von Befugnissen, die dem Urheber zustehen.
[27] Siehe vorne II.1.a).
[28] So darf ein veröffentlichtes Werk beispielsweise nach Art. 19 Abs. 1 lit. a URG zum Privatgebrauch oder nach lit. b zu Unterrichtszwecken verwendet werden.
[29] BGE 113 II 306 ff. E. 3a.
[30] Art. 4 Abs. 1 URG; B.K. MÜLLER/R. OERTLI, Urheberrechtsgesetz (URG), Bundesgesetz über das Urheberrecht und verwandte Schutzrechte. Mit Ausblick auf EU-Recht, deutsches Recht, Staatsverträge und die internationale Rechtsentwicklung, Bern 2012, URG 4 N 4 ff.

c) Leistungsschutzrecht

Nebst dem Sachen- und Immaterialgüterrecht wird auch die Anwendung von Leistungsschutzrechten auf Daten diskutiert[31]. Leistungsschutzrechte räumen dem Berechtigten ein erga omnes wirkendes Ausschliesslichkeitsrecht an der eigenen Leistung zum Schutz vor unrechtmässiger Aneignung durch einen Dritten ein. Die Leistungsschutzrechte schützen damit Investitionen in die Erbringung von Leistungen, die ohne Leistungsschutz aufgrund des Risikos einer Aneignung der erbachten Leistung durch einen Dritten nicht getätigt werden würden[32]. Leistungsschutzrechte begründen jedoch kein Eigentum an Daten. Insbesondere Art. 5 lit. c UWG verbietet die Übernahme und Verwertung eines marktreifen Arbeitsergebnisses, wenn dies durch technische Reproduktionsverfahren und ohne angemessenen eigenen Aufwand erfolgt. Eine Big-Data-Analyse kann ein marktreifes Arbeitsergebnis darstellen und damit von Art. 5 lit. c UWG geschützt sein. Zur Beurteilung des angemessenen eigenen Aufwands wird der Aufwand des Erst- und des Zweitbewerbers verglichen. In Bezug auf Datensammlungen sind zwei Fälle zu unterscheiden: Die Datensammlung fällt als Haupt- oder als Nebenprodukt der gewerblichen Tätigkeit an. Während im ersten Fall der Aufwand des Erstbewerbers für die Erhebung der Daten berücksichtigt wird, wird im letzteren Fall nur der Aufwand für die Aufbereitung (nicht jedoch zur Erhebung) der Daten berücksichtigt[33]. Bei der Übernahme einer als Nebenprodukt der gewerblichen Tätigkeit entstandenen Datensammlung eines Dritten dürfte Art. 5 lit. c UWG deshalb kaum anwendbar sein.

d) Datenbankschutz (Schutz des Datenbankherstellers)

Die EU kennt mit der Richtlinie 96/9/EG des Europäischen Parlaments und des Rates vom 11. März 1996 (Datenbank-RL) ein Datenbankschutzrecht sui generis. Eine Datenbank ist gemäss Art. 1 Abs. 2 der Datenbank-RL eine Sammlung von Daten, die systematisch oder methodisch angeordnet und einzeln zugänglich sind. Als Schutzvoraussetzung verlangt Art. 7 Abs. 1 der Datenbank-RL eine qualitativ oder quantitativ wesentliche Investition in die Beschaffung, Überprüfung oder Darstellung des Inhalts einer Datenbank. Die Erzeugung der Daten berechtigt hingegen wohl nicht zum Schutz[34]. Bei Vorliegen dieser Schutzvoraussetzung steht dem Datenbankhersteller während 15 Jahren das Recht zu, die Entnahme und/oder Weiterverwendung der Gesamtheit oder eines qualitativ oder quantitativ wesentlichen Teils des Inhalts der Datenbank sowie die wiederholte und systematische Entnahme und/oder Weiterverwendung unwesentlicher Teile zu untersagen (Art. 7 Abs. 1 und 5 sowie Art. 10 Abs. 1 Datenbank-RL). Die Richtlinie schützt allerdings nur die Datenbank, aber nicht die Daten selbst und wurde von der Schweiz bis jetzt (noch) nicht nachvollzogen. Die Datenbank-RL begründet deshalb kein Eigentum an Daten.

2. De lege ferenda

Wie aufgezeigt[35] bestehen nach geltendem schweizerischem Recht keine eigentumsartigen Rechte an Daten. In der Literatur und öffentlichen Debatte werden deshalb verschiedene Lösungsansätze für die Einführung solcher Rechte an Daten diskutiert.

a) Sachenrecht

Um Daten den Eigentumsregeln des Sachenrechts unterstellen zu können, wird eine Anwendung des Sachenrechts auf Daten mittels eines erweiterten Sachbegriffes diskutiert.

ECKERT argumentiert anhand der für die Qualifikation als Sache massgebenden Verkehrsauffassung[36], dass Daten von der Wirtschaft bereits jetzt wie Sachen erworben, genutzt, verändert, veräussert, übertragen und zerstört werden. Zudem seien Daten durch die Speicherung auf einem Datenträ-

[31] WEBER/CHROBAK (Fn. 25), Rz. 31 f.
[32] Z.B. das Leistungsschutzrecht für Interpreten in Art. 33 ff. URG, für Hersteller von Ton- und Bildträgern in Art. 35 f. URG und für Sendeunternehmen in Art. 37 URG.
[33] Vgl. ZivGer Basel-Stadt, sic! 2004, 495 f. E. 3d, «Arzneimittel-Kompendium».
[34] EuGH vom 9. November 2004, C-338/02; EuGH vom 9. November 2004, C-444/02; EuGH vom 9. November 2004, C-46/02. Siehe dazu auch K.J. SCHMIDT/H. ZECH, Datenbankherstellerschutz für Rohdaten?, CR 2017, 417 ff.
[35] Siehe vorne II.1.
[36] Siehe vorne II.1.a.

ger verkörpert und von Menschen beherrschbar. Deshalb könnten Daten mithilfe eines der begrifflichen Klärung dienenden, leicht erweiterten Sachbegriffs als Sachen («res digitalis») qualifiziert werden[37].

Die Qualifizierung von Daten als Sachen würde zu einer Unterstellung der Daten unter die Regeln des sachenrechtlichen Eigentums und Besitzes führen. Dies hätte insb. zur Folge, dass die Daten einem Eigentümer zugeordnet werden könnten. Dem Eigentümer würden die vorne erwähnten[38] zwei Seiten des erga omnes wirkenden Herrschaftsrechts zustehen: Er könnte innerhalb der Rechtsordnung frei über die Daten verfügen (insb. nutzen, vervielfältigen, verändern und zerstören) und hätte einen unverjährbaren Herausgabe- und Abwehranspruch gegen ungerechtfertigte Einwirkungen.

Nach ECKERT wären sachenrechtliche Konzepte wie der selbständige und unselbständige Besitz (Art. 920 ZGB) und die Besitzdienerschaft an Daten sowie die Verarbeitung (Art. 726 ZGB), die Verbindung/Vermischung (Art. 727 ZGB) und die Ersitzung (Art. 728 ZGB) von Daten denkbar. Er erachtet auch den Besitzesschutz (Selbsthilfe sowie die Klage aus Besitzesentziehung und Besitzesstörung, Art. 926 ff. ZGB) als anwendbar[39].

Mit diesem Konzept wären Daten als absolut geschütztes Rechtsgut bei einer Beschädigung oder Zerstörung durch Art. 41 OR zivilrechtlich und durch die Art. 137 ff. StGB strafrechtlich geschützt.

ECKERT schlägt vor, dass das originäre Eigentum an Daten der Person zugewiesen werden soll, der technisch und wirtschaftlich die Erstspeicherung der Daten zugeordnet werden kann («Datenerzeuger»)[40]. Als Besitzer der Daten schlägt er die den Zugriff auf die Daten steuernde Person vor[41]. Der Besitzeserwerb soll bei Originaldaten durch Übergabe des Speichermediums und bei Kopien durch Übertragung einer Kopie der Originaldaten erfolgen[42]. Zur Eigentumsübertragung bedürfte es nebst dem Rechtsgrund noch der Besitzesübertragung nach einer der beiden vorerwähnten Arten.

Die Anwendung des Sachenrechts auf Daten erscheint u.E. jedoch nicht angemessen. Daten unterscheiden sich als öffentliche Güter grundlegend von Sachen. Der Datenträger wiederum unterliegt bereits heute den Regeln des Sachenrechts.

b) Sachenrechtsähnliche Lösung

HESS-ODONI schlägt die Einführung eines Eigentumsschutzes für Daten vor, der materiell teilweise auf der analogen Anwendung sachenrechtlicher Regelungen und teilweise auf neuem Richterrecht basieren soll. Der Berechtigte soll ebenfalls im Rahmen der rechtlichen Schranken frei über seine Daten verfügen bzw. Dritten die Verwendung seiner Daten untersagen können. Zudem soll er einen Herausgabe- und Löschungsanspruch sowie einen Abwehranspruch gegen ungerechtfertigte Einwirkungen auf seine Daten haben. Die Übertragung der Berechtigung an den Daten soll durch eine schriftliche Rechtsabtretung in Analogie zur Zession (Art. 164 f. OR) erfolgen. Bei gleichzeitiger Übergabe eines Datenträges ergebe sich die Übertragung der Datenberechtigung hingegen direkt aus der Eigentumsübertragung am Datenträger[43].

c) Neues Immaterialgüterrecht

Ein weiterer Lösungsansatz wäre ein neues Immaterialgüterrecht an Daten. Die Einführung eines neuen Immaterialgüterrechts an Daten bedürfte allerdings (wie alle Ausschliesslichkeitsrechte) der Rechtfertigung, da ein gemeinfreies Gut ausschliesslich an einen Rechtsträger zugewiesen werden würde und die Handlungs- bzw. Wettbewerbsfreiheit Dritter eingeschränkt wird. In der Literatur werden in Bezug auf Daten verschiedene Rechtfertigungsgründe angeführt: (1) ungenügender Anreiz für

[37] Zum Ganzen M. ECKERT, Digitale Daten als Wirtschaftsgut: digitale Daten als Sache, SJZ 2016, 247 ff.; HESS-ODONI (Fn. 25), Rz. 29 ff. diskutiert einen erweiterten Sachbegriff bzw. eine analoge Anwendung des Sachenrechts auf Daten ebenfalls, hält dies aber nicht für sinnvoll.
[38] Siehe vorne II.1.a).
[39] Zum Ganzen M. ECKERT, Digitale Daten als Wirtschaftsgut: Besitz und Eigentum an digitalen Daten, SJZ 2016, 267 ff.
[40] ECKERT (Fn. 39), 267, mit Hinweis auf ZECH (Fn. 12), 144.
[41] ECKERT (Fn. 39), 265.
[42] ECKERT (Fn. 39), 269 f.
[43] Zum Ganzen HESS-ODONI (Fn. 25), Rz. 38 ff.

Investitionen in die Datenerzeugung und -nutzung[44], (2) Rechtsunsicherheit, wem Daten zugewiesen sind[45], (3) Reduktion der Kosten bei der Erstellung, dem Abschluss und der Durchführung des Vertrags (sog. Transaktionskosten)[46], (4) Allokation des Nutzens und der Risiken beim gleichen Inhaber[47], sowie (5) Schutz zentraler Werte wie Freiheit, Würde und Autonomie von Individuen, die Nicht-Diskriminierung, das informationelle Selbstbestimmungsrecht und die Befähigung zur Selbstentfaltung[48].

Dem ersten Argument wird entgegengehalten, dass Daten bereits heute problemlos gehandelt werden und das Volumen an neuen Daten ständig zunehme[49]. Zum zweiten Argument wird angeführt, dass die Zuordnung von Daten vertraglich geregelt werden könne und damit keine Rechtsunsicherheit bestehe[50]. In Bezug auf das dritte Argument wird zumindest infrage gestellt, ob die Transaktionskosten wirklich sinken würden, und eine empirische Untersuchung der tatsächlich anfallenden Transaktionskosten gefordert[51]. Auch hinsichtlich des vierten Arguments wird angezweifelt, ob mit einem neuen Immaterialgüterrecht an Daten die ungleichmässige Verteilung des Nutzens und der Risiken zulasten einer schwächeren Partei behoben werde, da sich die stärkere Partei das Immaterialgüterrecht von der schwächeren Partei übertragen lassen könnte[52]. Hinsichtlich des letzten Arguments wird vorgebracht, dass die Einführung eines neuen Immaterialgüterrechts an Daten dem Schutz der zentralen Werte sogar zuwiderlaufen könnte[53].

Die Diskussion in der Literatur zeigt, dass der Idee eines neuen Immaterialgüterrechts an Daten zu Recht überwiegend kritisch entgegengetreten und zur genaueren Beurteilung eine vertiefte, insbesondere ökonomische, Forschung gefordert wird[54]. Im Übrigen lehnt das Bundesamt für Justiz das Schaffen eines Dateneigentums ab, da es mehr Probleme schaffen als lösen würde[55].

Bei der Definition eines neuen Immaterialgüterrechts an Daten müssten verschiedene «Parameter» definiert werden, so z.B. das Schutzobjekt, der originäre Rechtsinhaber, die Befugnisse und die Schutzausnahmen[56].

In Bezug auf das Schutzobjekt sind zwei mögliche (und miteinander kombinierbare) Abgrenzungen denkbar: Einerseits kann eine Abgrenzung anhand der Art der Daten (nur Sach- oder Personendaten oder alle Daten) und andererseits anhand der semiotischen Einordnung der Daten (semantisch oder syntaktisch) erfolgen.

Da in Deutschland ein neues Dateneigentumsrecht im Kontext der Industrie 4.0 diskutiert wird und das Datenschutzrecht mit der am 25. Mai 2018 in Kraft getretenen neuen DSGVO auf europäischer Ebene gerade reformiert wurde, schlägt die Europäische Kommission in Bezug auf die Art der Daten eine Eingrenzung auf Sachdaten vor[57]. Wie vorne aufgezeigt[58], ist die Abgrenzung zwischen Personen- und Sachdaten allerdings schwierig, weshalb als Schutzobjekt auch alle Arten von Daten vorgeschlagen werden[59].

---

[44] ZECH (Fn. 12), 144, welcher aber auch festhält, dass «die Kosten für die Erzeugung von Daten durch Aufnahme ständig sinken» und daher «das Bedürfnis nach entsprechenden rechtlichen Anreizen sinkt»; den ungenügenden Anreiz nicht für einzelne Daten, aber für ganze Datenbestände bejahend: FRÖHLICH-BLEULER (Fn. 25), Rz. 22.

[45] ZECH (Fn. 12), 145.

[46] H. ZECH, Data as a Tradeable Commodity, in: A. De Franceschi (Hg.), European Contract Law and the Digital Single Market, Cambridge 2016, 77.

[47] A. WIEBE, Protection of industrial data – a new property right for the digital economy?, GRUR Int. 2016, 881.

[48] Weber/Thouvenin (Fn. 3), 55.

[49] Siehe Fn. 2 und 44.

[50] Thouvenin/Früh/Lombard (Fn. 25), 32.

[51] Fröhlich-Bleuler (Fn. 25), Rz. 25 f.; Weber/Thouvenin (Fn. 3), 53 f.; Thouvenin/Früh/Lombard (Fn. 25), 33.

[52] Thouvenin/Früh/Lombard (Fn. 25), 33.

[53] Weber/Thouvenin (Fn. 3), 56.

[54] Hürlimann/Zech (Fn. 10), N 18; Thouvenin/Früh/Lombard (Fn. 25), 34; F. Thouvenin/R.H. Weber/A. Früh, Data ownership: Taking stock and mapping the issues, in: M. Dehmer/F. Emmert-Streib (Hg.), Frontiers in Data Science, Boca Raton 2017, 116.

[55] Bundesamt für Kommunikation, Medienrohstoff vom 9. Mai 2018, Eckwerte für eine Datenpolitik der Schweiz, 4, abrufbar unter <www.newsd.admin.ch/newsd/message/attachments/52302.pdf> (23. Mai 2018).

[56] Hürlimann/Zech (Fn. 10), N 18.

[57] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen «Aufbau einer europäischen Datenwirtschaft», COM(2017) 9 final, 14.

[58] Siehe vorne I.2.

[59] F. Thouvenin, Wem gehören meine Daten? Zu Sinn und Nutzen einer Erweiterung des Eigentumsbegriffs, SJZ 2017, 22.

In Bezug auf die semiotische Einordnung der Daten lässt sich festhalten, dass bei einer Anknüpfung an die semantische Ebene die in den Daten enthaltene Information geschützt würde. Die Normierung von Ausschliesslichkeitsrechten an Informationen als öffentliches Gut sollte jedoch nur restriktiv und begründet erfolgen[60]. Bei einer Anknüpfung an die syntaktische Ebene wäre nur der (binäre) Code der Information geschützt. Dritten könnte nur die Nutzung desselben Codes, nicht jedoch die unabhängige Generierung und Nutzung derselben Information untersagt werden.

Als originärer Rechtsinhaber werden u.a. der «Skribent», der inhaltlich Betroffene und der wirtschaftlich verantwortliche Erzeuger diskutiert[61]. Der Skribent ist die Person, welche die Daten speichert (Skripturakt). Inhaltlich betroffen wäre die Person, auf die sich die Daten beziehen. Im letzten Fall könnten nur Personendaten, nicht jedoch Sachdaten originär zugeordnet werden.

Als Befugnisse des Rechtsinhabers werden insb. das Recht auf Zugang zu den Daten, die Nutzung der Daten, die Beeinträchtigung der Integrität der Daten und die Übertragung des Rechts diskutiert[62].

Für die Schutzausnahmen könnte das Urheber- und Patentrecht[63] als Vorbild dienen. So werden in der Literatur u.a. die private oder wissenschaftliche Verwendung von Daten als vom Schutz ausgenommene Handlungen vorgeschlagen[64]. Als weitere Schutzschranken werden die Beschränkung der Schutzdauer (wie im Urheber- und Patentrecht) und die Eintragung in einem Register diskutiert[65].

III. Zugangsrechte an Daten

Datengetriebene Unternehmen erzeugen, sammeln und verarbeiten immer mehr Daten, was zu «Datensilos» führt. Nebst der Diskussion um eigentumsartige Rechte an Daten wird deshalb auch untersucht, was de lege lata für Zugangsrechte an Daten bestehen und was de lege ferenda für neue Zugangsrechte denkbar wären.

1. De lege lata

Im geltenden Recht gibt es kein allgemeines Zugangsrecht an Daten. In Bezug auf Personendaten besteht in Art. 8 Abs. 2 lit. a DSG ein Auskunftsrecht, wonach eine von einer Datenbearbeitung betroffene Person vom Inhaber einer Datensammlung verlangen kann, dass er alle über sie in der Datensammlung vorhandenen Daten mitteilt[66]. Bei elektronischen Daten bedeutet dies regelmässig die Herausgabe der Personendaten durch Übergabe eines Datenträges mit den verlangten Personendaten oder Übermittlung auf elektronischem Weg[67]. Hinsichtlich Personendaten besteht deshalb ein Zugangsrecht, nicht jedoch in Bezug auf Sachdaten. Als Rechtsgrundlage für Zugangsansprüche zu Daten könnte auch das Kartellrecht dienen. Dies wird in seiner derzeitigen Form jedoch nicht als geeignete Lösung für Zugangsprobleme angesehen[68].

2. De lege ferenda

Auf politischer Ebene wurde im Rahmen einer parlamentarischen Initiative vom Bundesrat verlangt, ein «Recht auf Kopie» von personenbezogenen Daten zu prüfen[69]. Im Rahmen der Revision des DSG hielt der Bundesrat in der Botschaft zum Entwurf des neuen Datenschutzgesetzes aber fest, dass die

---

60 Zech (Fn. 5), 149 und 201.
61 Hürlimann/Zech (Fn. 10), N 18.
62 ZECH (Fn. 12), 145 f.
63 Für Schutzausnahmen siehe 5. Kapitel des URG sowie Art. 9 und 9a PatG.
64 ZECH (Fn. 12), 146.
65 FRÖHLICH-BLEULER (Fn. 25), Rz. 26 f.; ZECH (Fn. 12), 146.
66 Auf europäischer Ebene ist das Auskunftsrecht in Art. 15 Abs. 2 DSGVO geregelt. Die DSGVO kennt in Art. 20 DSGVO (im Gegensatz zum DSG) zusätzlich ein Recht auf Datenübertragbarkeit (Datenportabilität). Das Recht ermöglicht der betroffenen Person, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und diese Daten einem anderen Verantwortlichen zu übermitteln, sofern die Verarbeitung auf einer Einwilligung oder auf einem Vertrag beruht und die Verarbeitung mithilfe automatisierter Verfahren erfolgt.
67 BAERISWYL/PÄRLI (Fn. 14), DSG 8 N 50.
68 A. FRÜH, Zum Bedarf nach Datenzugangsrechten, Jusletter IT Flash vom 11. Dezember 2017, Rz. 13.
69 Parlamentarische Initiative «Recht auf Nutzung der persönlichen Daten. Recht auf Kopie» von Fathi Derder, eingereicht am 25. September 2015, Geschäftsnr. 15.4045, abrufbar unter <www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20140434> (23. April 2018).

Einführung eines Rechts auf Datenportabilität «nicht wünschenswert» sei[70]. Zuerst sollen die Ergebnisse der Erfahrungen innerhalb der Europäischen Union abgewartet und danach die Einführung eines Rechts auf Datenportabilität im Rahmen der Strategie «Digitale Schweiz» (erneut) geprüft werden[71]. Es wird aber davon ausgegangen, dass bei der parlamentarischen Behandlung der Revision des DSG Vorschläge für ein Portabilitätsrecht im Bereich der Personendaten eingereicht werden[72].

In der Literatur wird (wenn auch noch vereinzelt) insbesondere wegen der zunehmenden Monopolisierung auf den Datenmärkten über neue Zugangsrechte an Daten diskutiert[73]. Ein Zugangsrecht wäre grundsätzlich auf horizontalen oder vertikalen Märkten denkbar, in denen Wettbewerber Dienstleistungen oder Güter nur mit den Daten eines anderen Wettbewerbers erbringen bzw. produzieren können, und würde dem freien Datenfluss[74] dienen. Als Rechtsinstrument werden u.a. Zwangslizenzen vorgeschlagen, mit denen ein Inhaber von Daten dazu bewegt werden soll, freiwillig einen Lizenzvertrag über die Nutzung der Daten mit einem Dritten abzuschliessen. Falls der Inhaber der Daten keinen Lizenzvertrag eingehen möchte, kann gerichtlich die Erteilung einer Zwangslizenz durchgesetzt werden[75]. Die Voraussetzungen und die Ausgestaltung (insb. Lizenzinhaber, Lizenzgegenstand und Entschädigung) eines solchen Zugangsrechts müssen aber noch näher untersucht werden[76]. Insbesondere erscheint der Konflikt mit dem Schutz von Unternehmensgeheimnissen problematisch[77].

IV. Datenschutzrecht

Nebst eigentumsartigen Rechten und Zugangsrechten an Daten wird auch über das Datenschutzrecht als Grundlage für die Zuordnung von Daten an Rechtssubjekte diskutiert.

1. De lege lata

Das Datenschutzrecht kommt immer dann zur Anwendung, wenn es sich bei den bearbeiteten Daten um Personendaten handelt[78]. Eine Datenbearbeitung stellt gemäss Art. 3 lit. e DSG jeder Umgang mit Personendaten dar, und zwar unabhängig von den angewandten Mitteln und Verfahren. So fallen insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten unter den Begriff der Datenbearbeitung. Das DSG erfasst gemäss dessen Art. 2 Abs. 1 lit. a und b nicht nur die Datenbearbeitung durch Bundesorgane, sondern auch durch private Personen.

Mögliche Rechtssubjekte, denen Daten durch das Datenschutzrecht zugewiesen werden könnten, sind nach geltendem Recht die von den Daten betroffenen natürlichen oder juristischen Personen[79]. Durch das Datenschutzrecht werden aber nicht die Daten selbst geschützt, sondern es wird die betroffene Person vor Eingriffen in ihr Persönlichkeitsrecht geschützt[80]. Die betroffenen Personen können zwar durch Erteilung ihrer Einwilligung der Bearbeitung und damit der Nutzung der sie betreffenden Daten zustimmen. In diesem Sinne können sie auch Verträge schliessen und darin ihre Daten als Gegenleistung hingeben[81]. Allerdings ist die erteilte datenschutzrechtliche Einwilligung jederzeit frei

---

70 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017, 7009.
71 Botschaft (Fn. 70), 6985.
72 Bundesamt für Kommunikation, Medienrohstoff vom 9. Mai 2018, Eckwerte für eine Datenpolitik der Schweiz, 4, abrufbar unter <www.newsd.admin.ch/newsd/message/attachments/52302.pdf> (23. Mai 2018).
73 WEBER/THOUVENIN (Fn. 3), 70 ff.
74 Siehe dazu Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen «Aufbau einer europäischen Datenwirtschaft», COM(2017) 9 final, 5 ff.; Europäische Kommission, Commission Staff Working Document on the free flow of data and emerging issues of the European data economy. Accompanying the document Communication Building a European data economy, SWD(2017) 2 final, 21 f.
75 WEBER/THOUVENIN (Fn. 3), 71 f.
76 FRÜH (Fn. 68), Rz. 10.
77 P.G. PICHT, Dateneigentum und Datenzugang, Schutz von Geschäftsgeheimnissen als Alternative?, Jusletter IT Flash vom 11. Dezember 2017, Rz. 7.
78 Siehe vorne I.2.
79 Vgl. Art. 3 lit. b DSG. Dies soll sich allerdings mit der Revision des Datenschutzgesetzes ändern, siehe Art. 2 Abs. 1 und Art. 4 lit. a und b E-DSG.
80 HÜRLIMANN/ZECH (Fn. 10), N 5.
81 L. SPECHT, Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen. Eine Erläuterung des gegenwärtigen Meinungsstands und Gedanken für eine zukünftige Ausgestaltung, CR 2016, 288, 289.

widerruflich, was dazu führt, dass die Empfänger der Einwilligung keine gesicherte Rechtsposition innehaben und darauf gestützte Verträge nicht bindend sind[82]. Die Möglichkeit der betroffenen Personen, die sie betreffenden Daten kommerziell zu verwerten, führt deshalb noch nicht dazu, dass ihnen ein eigentumsartiges Recht an den Daten zugewiesen wird[83].

So wird auch nicht für jede Datenbearbeitung eine Einwilligung verlangt. Die Datenbearbeitung kann gemäss Art. 13 Abs. 1 DSG auch durch ein Gesetz oder ein höheres öffentliches oder privates Interesse gerechtfertigt werden. Dann kann die Datenbearbeitung durch die betroffene Person kaum verhindert werden.

Die Rechtsansprüche bei widerrechtlichen Datenbearbeitungen durch private Personen richten sich nach Art. 15 DSG. Zum Schutz ihrer Persönlichkeit kann die betroffene Person gemäss Art. 15 Abs. 1 DSG die Klagen gemäss Art. 28, 28a und 28l ZGB erheben. Die betroffene Person kann auf diesem Weg insbesondere verlangen, dass die Datenbearbeitung gesperrt wird, keine Daten an Dritte bekannt gegeben oder die Personendaten berichtigt oder gelöscht werden. Ausserdem hat sie einen Gewinnherausgabeanspruch gemäss Art. 28a Abs. 3 ZGB entsprechend der Geschäftsführung ohne Auftrag, mit welchem geldmässige Vorteile durch den unrechtmässigen Eingriff in das Rechtsgut der Persönlichkeit, die Verletzung einer geschützten fremden Rechtssphäre, abgeschöpft werden können[84]. Eine widerrechtliche Datenbearbeitung zieht allerdings gemäss DSG keine strafrechtliche Konsequenz nach sich[85].

Insgesamt lässt sich also festhalten, dass das Datenschutzrecht den betroffenen Personen zwar eine Abwehrbefugnis gegen widerrechtliche Datenbearbeitungen mit erga-omnes-Wirkung einräumt, welche der Rechtsposition bei eigentumsartigen Rechten immerhin teilweise nahekommt, aber darüber hinaus keine ausschliessliche Zuweisung von Personendaten an ein Rechtssubjekt vornimmt[86].

2. De lege ferenda

Politisch wurde die Einführung eines Dateneigentums bereits im Jahr 2014 durch parlamentarische Initiativen in die Debatte eingebracht: So forderte die Parlamentarische Initiative 14.413 «Grundrecht auf informationelle Selbstbestimmung» vom 21. März 2014[87] die Änderung des Datenschutzes von einem Missbrauchsschutz hin zu einem festgeschriebenen Grundrecht auf informationelle Selbstbestimmung durch Anpassung des Art. 13 Abs. 2 BV. Mit der Parlamentarischen Initiative 14.434 «Schutz der digitalen Identität von Bürgerinnen und Bürgern» vom 20. Juni 2014[88] sollte in Art. 13 Abs. 2 BV mit dem Wortlaut «[d]ie Daten sind Eigentum der betroffenen Person […]» sogar ein Eigentumsrecht an Personendaten eingeführt werden. Beide Initiativen zielten darauf ab, das Datenschutzrecht von einem Abwehrrecht, zu einem Recht, welches Personen weitgehende Verfügungshoheit über die sie betreffenden Daten gewährt, weiterzuentwickeln[89]. Beide Initiativen wurden am 29. September 2017 vom Nationalrat mit dem Hinweis abgeschrieben, dass die bereits existierende Verfassungsbestimmung die «Forderungen der Initiativen obsolet» mache[90]. Zudem wurde durch die Staats-

---

[82] Vgl. P.G. PICHT (Fn. 77), Rz. 8, m.H. auf BAERISWYL/PÄRLI (Fn. 14), DSG 4 N 57.
[83] SPECHT (Fn. 81), 289; ZECH (Fn. 46), 69.
[84] Z.B. BGE 113 III 153 ff. E. 2.4. Dies ist alternativ auch durch die Eingriffskondiktion (Art. 62 Abs. 1 OR) möglich.
[85] Dies im Gegensatz zu ausländischen Rechtsordnungen, z.B. Deutschland. Siehe dazu § 44 des bis einschliesslich 24. Mai 2018 gültigen D-BDSG, sowie Art. 84 DSGVO und § 42 des neuen D-BDSG.
[86] ZECH (Fn. 12), 141; THOUVENIN (Fn. 59), 26; F. THOUVENIN/R.H. WEBER, Zum Bedarf nach einem Dateneigentum, Jusletter IT Flash vom 11. Dezember 2017, Rz. 9. Vgl. auch HÜRLIMANN/ZECH (Fn. 10), N 5; ähnlich HESS-ODONI (Fn. 25), Rz. 17.
[87] Eingereicht von Daniel Vischer, abrufbar unter <www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20140413> (23. April 2018).
[88] Eingereicht von Fathi Derder, abrufbar unter <www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20140434> (23. April 2018).
[89] Medienmitteilung der Staatspolitischen Kommission des Ständerates vom 20. August 2015, Ständeratskommission nach wie vor gegen vermehrte Mitsprache der Bundesversammlung bei Verordnungen des Bundesrates, abrufbar unter <www.parlament.ch/press-releases/Pages/2015/mm-spk-s-2015-08-20.aspx> (23. April 2018).
[90] Bericht der Staatspolitischen Kommission des Nationalrates vom 18. August 2017, 4, abrufbar unter <www.parlament.ch/centers/kb/Documents/2014/Kommissionsbericht_SPK-N_14.434_2017-08-17.pdf>; sowie Abschreibung der Initiativen durch den Nationalrat, abrufbar unter <www.parlament.ch/de/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=41225> (23. April 2018).

politischen Kommissionen darauf hingewiesen, dass derzeit eine Totalrevision des Datenschutzgesetzes durchgeführt werde, innerhalb welcher den Anliegen der beiden Initiativen Rechnung getragen werden sollte[91].

Der vom Bundesrat am 15. September 2017 zusammen mit der Botschaft verabschiedete Entwurf des revidierten Datenschutzgesetzes wird demnächst von National- und Ständerat beraten[92]. Im Zuge dieser Revision wurde noch nicht thematisiert, ob das Datenschutzrecht künftig zu einem eigentumsartigen Recht weiterentwickelt werden soll. Lediglich der Vorschlag, eigentumsartige Rechte an Daten generell zu schaffen, wurde als nicht umsetzbar beurteilt, da kein anderes europäisches Land solche Rechte vorsieht[93]. So hängen die meisten Neuerungen durch die Revision des Datenschutzgesetzes mit den Entwicklungen der Datenschutzgesetzgebung des Europarats und der Europäischen Union, insbesondere der DSGVO, zusammen[94].

In der Lehre wurde eine mögliche Weiterentwicklung des Datenschutzes hin zu einem eigentumsartigen Recht noch nicht umfassend erforscht. FLÜCKIGER fordert einen neuen Eigentumstypus für das Recht auf Selbstbestimmung über Personendaten[95]. Ein solches Ausschliesslichkeitsrecht an Daten wird in der Lehre ansonsten überwiegend kritisch gesehen[96]. THOUVENIN skizziert in einem Beitrag vier verschiedene Varianten der Ausgestaltung eines Eigentumsrechts an (Personen-)Daten, weist aber ebenfalls auf den noch bestehenden Forschungsbedarf hin[97]. Als erste Variante könnte den betroffenen Personen ein eigentumsartiges Recht an ihren Daten als immaterielle Güter eingeräumt werden, während die Unternehmen, welche diese Daten gesammelt und gespeichert haben, nur ein Recht an der Festlegung der Daten erhalten sollen[98]. Die Unternehmen könnten allerdings das eigentumsartige Recht der Betroffenen erwerben und anschliessend jedermann, also auch den Betroffenen, die Nutzung der Daten untersagen. Diese Variante wird deshalb zu Recht abgelehnt[99]. Bei der zweiten Variante schlägt THOUVENIN vor, sich bloss auf die Festlegung der Daten zu beschränken, an welcher sowohl die festlegenden Unternehmen als auch die betroffenen Personen ein Recht erhalten sollen[100]. Bezüglich der Nutzung dieser festgelegten Daten werden wiederum drei verschiedene Möglichkeiten erörtert, wobei die dritte Option klar favorisiert wird: Danach sollen die Betroffenen die sie betreffenden, festgelegten Daten frei nutzen können, während die Unternehmen die Einwilligung der Betroffenen einholen oder die vollen Eigentumsrechte an dieser Festlegung erwerben müssten[101]. Die positiven Konsequenzen sollen bei dieser Ausgestaltung eines Dateneigentums sein, dass (1) die Nutzung von Daten als immaterielle Güter nicht beschränkt würde, (2) durch die Konstruktion als Miteigentum sowohl Betroffene als auch Unternehmen Dritten die Nutzung der Daten untersagen könnten, wobei die Unternehmen die Daten nur mit der Einwilligung der Betroffenen nutzen könnten, und (3) dass die

---

[91] Bericht der Staatspolitischen Kommission des Nationalrates vom 18. August 2017, 4, abrufbar unter <www.parlament.ch/centers/kb/Documents/2014/Kommissionsbericht_SPK-N_14.434_2017-08-17.pdf>, sowie Medienmitteilung der Staatspolitischen Kommission des Ständerates vom 20. August 2015, Ständeratskommission nach wie vor gegen vermehrte Mitsprache der Bundesversammlung bei Verordnungen des Bundesrates, abrufbar unter <www.parlament.ch/press-releases/Pages/2015/mm-spk-s-2015-08-20.aspx> (23. April 2018).

[92] Siehe dazu <www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20170059> (12. April 2018).

[93] Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017, 6988.

[94] Botschaft (Fn. 93), 6943; vgl. S. HUSI-STÄMPFLI, Die DSG-Revision oder: Ein Beziehungsdrama in drei Akten, Jusletter vom 7. Mai 2018, Rz. 13; HÜRLIMANN/ZECH (Fn. 10), N 15. Für eine Übersicht siehe z.B. D. VASELLA, Revision des DSG: Entwurf und Botschaft veröffentlicht, swissblawg vom 15. September 2017, abrufbar unter <swissblawg.ch/2017/09/entwurf-des-datenschutzgesetzes.html> (24. April 2018); Medienmitteilung des Bundesrates vom 15. September 2017, Den Datenschutz verbessern und den Wirtschaftsstandort stärken, abrufbar unter <www.bj.admin.ch/bj/de/home/aktuell/news/2017/ref_2017-09-150.html> (24. April 2018). Für eine Übersicht der Auswirkungen der DSGVO auf die Schweiz siehe z.B. M. BERGAMELLI, Die Auswirkung der neuen DSGVO auf die Schweiz, Jusletter vom 30. April 2018. Kritisch zur DSG-Revision S. HUSI-STÄMPFLI (Fn. 94).

[95] A. 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.

[96] Vgl. HÜRLIMANN/ZECH (Fn. 10), N 13, 18 ff.; WEBER/THOUVENIN (Fn. 3), 56; Y. BENHAMOU/L. TRAN, Circulation des biens numériques: de la commercialisation à la portabilié, sic! 2016, 572 ff. schlagen stattdessen einen Weg über das Vertragsrecht vor. Vgl. A. FRÜH, Roboter und Privacy, AJP 2017, 149 und 151.

[97] THOUVENIN (Fn. 59), 27 ff.

[98] THOUVENIN (Fn. 59), 28.

[99] THOUVENIN (Fn. 59), 29.

[100] THOUVENIN (Fn. 59), 29 f.

[101] THOUVENIN (Fn. 59), 29 f.

betroffenen Personen für die Übertragung ihrer Rechte an die Unternehmen ein Entgelt verlangen könnten[102].

Im Vergleich zum geltenden Recht dürften sich dabei u.E. jedoch nur geringe Vorteile ergeben. Bereits heute können die betroffenen Personen für die Nutzung ihrer Daten eine Gegenleistung verlangen. Es ist umgekehrt jedoch eher unwahrscheinlich, dass Unternehmen in den Erwerb eines vollen Eigentumsrechts an der konkreten Festlegung von Daten investieren würden angesichts der Tatsache, dass die betroffenen Personen die gleichen Daten beliebig oft festlegen und verkaufen können. Denn da Personendaten auf der semantischen Ebene, d.h. auf der Bedeutungsebene, definiert werden, können sie auf syntaktischer Ebene, d.h. auf Zeichenebene, in unzähligen Varianten festgelegt werden[103]. Rein praktisch wird nach einer gewissen Zeit nicht mehr nachvollzogen werden können, welches Unternehmen die alleinigen Eigentumsrechte an welchen Daten hat und welches Unternehmen auf die Einwilligung der betroffenen Person angewiesen ist, denn Daten werden immerhin auch zwischen Unternehmen gehandelt und ausgetauscht. Ausserdem stünden auch Personendaten, welche aus der Analyse der festgelegten und erworbenen Personendaten entstehen, wieder originär im Miteigentum des Unternehmens, welches die Analyse durchgeführt hat, und der von den (neuen) Daten betroffenen Person. Schlussendlich wären die Unternehmen also trotz allem auf die Einwilligung der betroffenen Personen verwiesen. Der Umstand, dass die betroffenen Personen die sie betreffenden Daten beliebig oft festlegen können, führt aus offensichtlichen Gründen auch dazu, dass Unternehmen Dritte schlecht von der Nutzung der Daten ausschliessen können. Überdies ist fraglich, ob die Persönlichkeit der betroffenen Personen am Ende noch geschützt wäre und ob die betroffenen Personen ihre Rechte auch durchsetzen könnten[104].

Als weiteren Ansatz zur Rechtsentwicklung neben dem eines eigentumsartigen Rechts an (Personen-)Daten nennt FRÜH eine Neukonzeption des Schutzgegenstands «Privacy», welcher über den Begriff «Privatsphäre» hinausgehen soll, aber ansonsten (noch) nicht näher definiert wird[105]. Zumindest soll «Privacy» nicht als normative Konstante angesehen werden, sondern als dem gesellschaftlichen Wandel unterworfen, weshalb dieser Schutzgegenstand interdisziplinär erforscht werden soll[106].

Ferner könnte, angelehnt an den BGE 136 III 401 aus dem Jahre 2010 bezogen auf das Recht am eigenen Bild, angedacht werden, die freie Widerrufbarkeit der datenschutzrechtlichen Einwilligung einzuschränken, wenn bei der Erteilung derselben hauptsächlich wirtschaftliche Interessen massgeblich waren und der «höchstpersönliche Kernbereich der Persönlichkeit»[107] nicht betroffen ist[108]. Strukturell handelt es sich bei Rechtsgeschäften über Datenschutz, wie bei Verträgen über die Nutzung des eigenen Bilds oder des eigenen Namens, um Verträge über ein Persönlichkeitsrecht.

V. Sektorenspezifische Regelungen und Selbstregulierung

Neben den dargelegten Lösungsansätzen sind auch Lösungen jenseits von subjektiven Rechten, die in allen Lebensbereichen eingreifen, denkbar. So könnten sektorenspezifische Regelungen für Rechte an Daten entwickelt werden, beispielsweise für die Automobilindustrie und den Gesundheitssektor. Dieses Vorgehen könnte umfassende gesetzliche Lösungen ermöglichen, mit welchen trotzdem auf die Eigenheiten der jeweiligen Branche eingegangen werden kann.

Die Erzeugung von Daten kann auch als regulatorische Aufgabe – vergleichbar mit der Produktesicherheit – gesehen werden. Eine Möglichkeit, die Rechtspositionen und das Verantwortungsbewusstsein der verschiedenen Akteure in einer Datenwirtschaft zu stärken, wäre auch die Selbstregulierung durch die beteiligten Unternehmen[109]. Vorteile solcher Selbstregulierung sind unter anderem die Flexibilität sowie der hohe, branchenspezifische Differenzierungsgrad[110]. Bei der Selbstregulierung kann

[102] THOUVENIN (Fn. 59), 30; zusätzlich hält THOUVENIN dieses Modell auch für Sachdaten für passend, wobei hier die Unternehmen Alleineigentümer wären.
[103] Siehe zu den verschiedenen Informationsebenen ausführlich: ZECH (Fn. 5), § 2.
[104] So ist gemäss R.H. WEBER, Herausforderungen für das Datenschutzrecht, in: A. Epiney/D. Nüesch (Hg.), Big Data und Datenschutzrecht, Zürich 2016, 17, die Anerkennung eines Eigentumsrechts nur sinnvoll, wenn es auch tatsächlich durchsetzbar ist.
[105] FRÜH, (Fn. 96), 150 f.
[106] FRÜH, (Fn. 96), 151.
[107] BGE 136 III 401 ff. E. 5.4.
[108] THOUVENIN (Fn. 59), 31 f.
[109] Vgl. Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017, 7182.
[110] Ähnlich Botschaft (Fn.109), 6973, 7034 und 7172.

zwischen drei Arten unterschieden werden[111]: Erstens ist die freie Selbstregulierung zu nennen, welche rein privatautonom ausgestaltet ist und ohne gesetzliche Vorgaben und ohne Mitwirkung des Staates stattfindet. Zweitens diejenige Selbstregulierung, welche von einer gesetzlich vorgesehenen Behörde als Mindeststandard nicht nur für die Mitglieder der jeweiligen Selbstregulierungsorganisation, sondern auch für die übrigen Branchenzugehörigen anerkannt wird[112]. Die Einhaltung dieser Mindeststandards wird sowohl von den Selbstregulatoren als auch von der jeweiligen gesetzlich bestimmten Behörde sichergestellt. Drittens ist die obligatorische Selbstregulierung zu nennen, bei welcher der zu regulierende Bereich durch Gesetz oder Verordnung an den jeweiligen Selbstregulator delegiert und die ausgearbeitete Selbstregulierung unter den Genehmigungsvorbehalt einer Behörde gestellt wird[113].

Der Entwurf des revidierten Datenschutzgesetzes sieht in Art. 10 E-DSG für Branchen- und Wirtschaftsverbände im privaten Sektor sowie für Bundesorgane im öffentlichen Sektor die Möglichkeit vor, branchenspezifische Verhaltenskodizes zu schaffen, welche dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten vorgelegt werden können[114]. Dieser nimmt zu dem Verhaltenskodex Stellung und veröffentlicht seine Stellungnahme unabhängig von einer positiven oder negativen Beurteilung[115]. Durch den Weg über die Selbstregulierung kann der technologieneutrale Charakter der Datenschutzgesetzgebung beibehalten und gleichzeitig auf technologische Eigenheiten eingegangen werden[116]. Um die Selbstregulierung zu fördern, sollen Akteure, welche Verhaltenskodizes einhalten, gemäss Art. 20 Abs. 5 E-DSG unter bestimmten Voraussetzungen auf die Durchführung einer Datenschutz-Folgenabschätzung verzichten können[117]. Es irritiert jedoch eine Aussage in der Botschaft, nach welcher die Verhaltenskodizes nicht als bindend betrachtet werden sollen[118]. Denn einerseits hat die Stellungnahme des Beauftragten keinen Verfügungscharakter und stellt keine Genehmigung (oder Ablehnung) dar[119]. Dennoch soll davon ausgegangen werden, dass ein dem vorgelegten Verhaltenskodex entsprechendes Verhalten keine Verwaltungsmassnahmen nach sich zieht[120]. Diese Kompromisslösung erscheint u.E. wenig konsequent.

Beispiele für Selbstregulierung gibt es immerhin auch in anderen Bereichen. Dabei zu nennen ist die Selbstregulierung der Schweizerischen Bankiervereinigung, die von der FINMA als Mindeststandard anerkannt wird[121]. Solch ein Modell oder sogar das der obligatorischen Selbstregulierung könnte auch im Hinblick auf branchenspezifische Selbstregulierungen in der Datenwirtschaft sinnvoll sein. Gemäss der Botschaft zum Bundesgesetz über die Totalrevision des DSG hätte der Eidgenössische Daten-

[111] Für die folgenden drei Unterscheidungen siehe Eidgenössische Finanzmarktaufsicht FINMA, Selbstregulierung im Schweizerischen Finanzmarktrecht, abrufbar unter <www.finma.ch/de/dokumentation/selbstregulierung> (25. April 2018).
[112] Beispiel: Art. 7 Abs. 3 FINMAG.
[113] Beispiele für solche Regulierungsaufträge: Art. 37h BankG (Einlagensicherung), Art. 27 Abs. 1 FinfraG (angemessene Organisation), Art. 4 Abs. 3 KKV (Anforderungen an den vereinfachten Prospekt für strukturierte Produkte), Art. 25 GwG (Konkretisierung der Sorgfaltspflichten). Genehmigende Behörde ist in allen diesen Fällen die FINMA.
[114] Medienmitteilung des EJPD vom 15. September 2017, Den Datenschutz verbessern und den Wirtschaftsstandort stärken, abrufbar unter <www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2017/2017-09-150.html> (23. April 2018); Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017, 7035.
[115] Art. 10 Abs. 2 E-DSG; Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017, 6973 und 7035.
[116] Vgl. Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017, 7007 und 7034.
[117] Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017, 7035 und 7062.
[118] Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017, 6973.
[119] Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017, 7035. Interessant ist, dass offenbar mitunter die Kosten einer Verfügung durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten eine Rolle für diese Entscheidung gespielt haben.
[120] Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017, 7035.
[121] Art. 7 Abs. 3 FINMAG. Eidgenössische Finanzmarktaufsicht FINMA, Rundschreiben 2008/2010, Selbstregulierung als Mindeststandard, 4, abrufbar unter <www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2008-10.pdf?la=de> (17. Mai 2018).

schutz- und Öffentlichkeitsbeauftragte es denn auch vorgezogen, wenn die Berufs- und Wirtschaftsverbände dazu verpflichtet worden wären, ihm die entwickelten Verhaltenskodizes zur Genehmigung vorzulegen[122].

VI. Zuordnung an eine Mehrheit von Rechteinhabern und Konkurrenzen

Bei einer Mehrheit von Berechtigten an Daten ist der Zuordnungsmechanismus von Daten an mehrere Rechteinhaber noch nicht geklärt. Vorbilder finden sich in der Inhaberschaft von Immaterialgüterrechten.

ECKERT schlägt als Folge seines Konzeptes, Daten mittels eines erweiterten Sachbegriffes den Eigentumsregeln des Sachenrechts zu unterstellen[123], vor, dass es sowohl Miteigentum (Art. 646 ff. ZGB) wie auch Gesamteigentum (Art. 652 ff. ZGB) an Daten geben soll[124]. Auch HESS-ODONI erachtet die (wenn auch analoge) Anwendung der Regelungen über das Miteigentum und das Gesamteigentum als sachgerecht und sieht dabei keine «Argumente, welche dagegen sprechen könnten»[125]. THOUVENIN/WEBER sehen hier allerdings zu Recht praktische Schwierigkeiten[126].

Fragen, welcher Person einzelne Personendaten zugeordnet werden sollen, wenn sie sich auf mehrere Personen beziehen («Mehrrelationalität»[127]), oder wie der Interessenkonflikt zu lösen ist, wenn eine betroffene Person einzelne Daten wirtschaftlich nutzen möchte, während eine andere von den gleichen Daten betroffene Person dies jedoch ablehnt, können durch das Datenschutzrecht bisher nicht beantwortet werden[128]. THOUVENIN nennt hier, zumindest bei seinem Modell für ein Recht auf die konkrete Festlegung von Personendaten[129], ebenfalls die Möglichkeit der Anwendung der sachenrechtlichen Regeln über das Miteigentum sowie der Regelungen des Patent- und Urheberrechts für mehrere originär Berechtigte. Gleichzeitig beschreibt er jedoch auch die Schwierigkeiten einer solchen Lösung[130].

Bei den vorne dargestellten[131] Konzepten zu Eigentumsrechten an Daten ergeben sich ausserdem Konflikte mit bestehenden Rechtsgebieten: Wenn Personendaten vorliegen, ist der Datenschutz zu berücksichtigen, und wenn die Daten ein Werk enthalten, muss das Urheberrecht beachtet werden. Im Bereich des Urheberrechts ergäbe sich die paradoxe Situation, dass einzelne Daten wie Fakten und Tatsachen keinen urheberrechtlichen Schutz geniessen, für sie aber gleichzeitig ein sogar noch weitergehender eigentumsrechtlicher Schutz beansprucht werden könnte[132]. Auch ein Nebeneinander von Datenschutzrecht und einem Eigentumsrecht an Daten wäre problematisch: Wenn der datenschutzrechtlich Betroffene und der Eigentümer der Daten nicht dieselbe Person sind, könnten sie sich gegenseitig (Ersterer durch Widerruf der datenschutzrechtlichen Einwilligung zur Verarbeitung der Daten und Letzterer gestützt auf das Herrschaftsrecht) die Nutzung der Daten untersagen[133]. ECKERT schlägt deshalb vor, dass das Datenschutzrecht und das Urheberrecht einem allfälligen eigentumsartigen Recht an Daten jeweils als lex specialis vorgehen sollen[134]. FRÖHLICH-BLEULER zweifelt allerdings daran, dass sich der Wertungskonflikt dadurch beseitigen lässt[135]. THOUVENIN weist auf die Möglichkeit hin, das geltende Datenschutzrecht zu grossen Teilen durch ein Dateneigentum zu ersetzen, wofür aber ebenfalls noch Forschungsbedarf bestehe[136].

---

[122] Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017, 7035.
[123] Siehe vorne II.2.a).
[124] ECKERT (Fn. 39), 267.
[125] HESS-ODONI (Fn. 25), Rz. 43.
[126] THOUVENIN/WEBER (Fn. 86), Rz. 14; ebenso THOUVENIN (Fn. 59), 29.
[127] L. SPECHT/R. ROHMER, Zur Rolle des informationellen Selbstbestimmungsrechts bei der Ausgestaltung eines möglichen Ausschließlichkeitsrechts an Daten, PinG 2016, 130.
[128] N. HÄRTING, «Dateneigentum» – Schutz durch Immaterialgüterrecht?, CR 2016, 648.
[129] Siehe vorne IV.2.
[130] THOUVENIN (Fn. 59), 29.
[131] Siehe vorne II.2.
[132] FRÖHLICH-BLEULER (Fn. 25), Rz. 28.
[133] THOUVENIN (Fn. 59), 30; WEBER/THOUVENIN (Fn. 3), 62.
[134] ECKERT (Fn. 39), 273; kritisch dazu: FRÖHLICH-BLEULER (Fn. 25), Rz. 29.
[135] FRÖHLICH-BLEULER (Fn. 25), Rz. 29.
[136] THOUVENIN (Fn. 59), 30 f.; ebenso WEBER/THOUVENIN (Fn. 3), 62.

VII. Fazit

Der Überblick über die verschiedenen rechtlichen Instrumente de lege lata und de lege ferenda hat gezeigt, dass sich die Frage «Wem gehören Daten?» nicht auf einfache Weise beantworten lässt. Bereits die Frage, was juristisch unter «Gehören» zu verstehen ist, lässt sich unterschiedlich beantworten. De lege lata bestehen jedenfalls keine echten Ausschliesslichkeitsrechte an Daten. Das Datenschutzrecht gewährt dem Betroffenen zwar einen absolut wirkenden Persönlichkeitsschutz, dieser ist jedoch gerade nicht als Ausschliesslichkeitsrecht konzipiert. De lege ferenda wird die Schaffung eines generellen Dateneigentums in der Schweizer Literatur mehrheitlich und zu Recht abgelehnt. Im Bereich des Datenschutzes werden mögliche Weiterentwicklungen hin zu einer Beteiligung am Wert der Daten diskutiert. Hier ist die Diskussion, wie auch bei der Frage nach einem generellen Dateneigentum, erst im Entstehen. Dabei sollte jedenfalls die Kernfunktion des Datenschutzes, der Schutz des Betroffenen bzw. seiner Persönlichkeit, nicht ausser Acht gelassen werden. Es lässt sich festhalten, dass die Diskussion zu Rechten an Daten in der Schweiz noch nicht so lange und eingehend geführt wird wie z.B. in Deutschland und der EU. Insbesondere zu Zugangsrechten liegen kaum wissenschaftliche Untersuchungen vor. Zukünftig sollten nebst dem Dateneigentum auch weitere Rechte an Daten wie z.B. Zugangsrechte und die Rechtsentwicklung im Bereich des Datenschutzes vertiefter in die Diskussion miteinbezogen werden.

Zusammenfassung

Das zunehmende wirtschaftliche Interesse am Wert von Daten führte vor allem auf europäischer Ebene und in Deutschland zu grossen Diskussionen über die rechtliche Einordnung von Daten. Auch in der Schweiz wird dieses Thema in letzter Zeit vermehrt diskutiert. Daten lassen sich als maschinenlesbar codierte Information definieren (syntaktische Information), die zudem auf der Bedeutungsebene (semantische Information) und auf der Strukturebene (strukturelle Information) abgegrenzt werden können. Daten sind als öffentliche Güter zudem nicht rivalisierend, nicht exklusiv und nicht abnutzbar. Die Abgrenzung zwischen Sach- und Personendaten wird zunehmend schwieriger. Eine Zuweisung und der Schutz von Daten durch eigentumsartige Rechte besteht de lege lata weder durch das Sachen- noch durch das Datenschutzrecht. Auch das geltende Urheber- und Leistungsschutzrecht bietet kaum Schutz. De lege ferenda erscheint die (analoge oder erweiterte) Anwendung des Sachenrechts auf Daten als nicht sachgerecht. Auch die Einführung eines neuen Immaterialgüterrechts lässt sich kaum rechtfertigen. Denkbarer erscheinen Datenzugangsrechte, die Weiterentwicklung des Datenschutzes hin zu einem eigentumsartigen Recht und sektorspezifische Selbstregulierung. Diese Konzepte bedürfen aber, vor allem in der Schweiz, einer vertieften Diskussion.

Résumé

L'intérêt commercial croissant pour la valeur des données a suscité un débat considérable sur la classification juridique des données, en particulier au niveau européen et en Allemagne. En Suisse aussi, ce sujet a été de plus en plus discuté récemment. Les données peuvent être définies en tant qu'informations codées lisibles par machine (informations syntaxiques), qui peuvent également être délimitées au niveau de la signification (informations sémantiques) et au niveau de la structure (informations structurelles). De plus, en tant que biens publics, les données ne sont ni concurrentes, ni exclusives, ni périssables. La distinction entre données matérielles et données personnelles devient de plus en plus difficile. Une classification et la protection de données par des droits assimilables à la propriété ne découlent de lege lata ni des droits réels, ni du droit de la protection des données. Par ailleurs, la législation actuelle sur droit d'auteur et les droits voisins n'offre que peu de protection. De lege ferenda, l'application (analogue ou étendue) du droit de la propriété aux données semble inappropriée. L'introduction d'un nouveau droit de propriété intellectuelle est difficilement justifiable. Les droits d'accès aux données, l'évolution de la protection des données vers un droit de propriété et l'auto-régulation sectorielle semblent plus convaincants. Cependant, ces concepts nécessitent une discussion plus approfondie, particulièrement en Suisse.