Universität Zürich[UZH]

CENTER FOR INFORMATION TECHNOLOGY SOCIETY AND LAW — ITSL

Center for Information Technology, Society, and Law (ITSL)

Zuordnung von Sachdaten
Eigentum, Besitz und Nutzung bei nicht-personenbezogenen Daten

Wissenschaftliche Studie im Auftrag des
Eidgenössischen Instituts für Geistiges Eigentum (IGE)

Prof. Dr. Florent Thouvenin
Dr. Alfred Früh

Zürich, 18. August 2020

Inhaltsverzeichnis

A. Gegenstand

Im Frühling 2020 wurden Prof. Dr. Florent Thouvenin und das Center for Information Technology, Society and Law (ITSL) vom Eidgenössischen Institut für Geistiges Eigentum (IGE) damit beauftragt, eine rechtswissenschaftliche Studie zum Thema "Besitz, Eigentum und Nutzung nicht-persönlicher Daten" zu verfassen.

Ziel dieses Beitrags ist es, die aktuelle Rechtslage in der Schweiz und der Europäischen Union (EU) zusammenzufassen und zu künftigen möglichen Rechtsentwicklungen, insbesondere zur Schaffung eines Eigentumsrechts an Daten oder Datenbanken, Stellung zu nehmen.

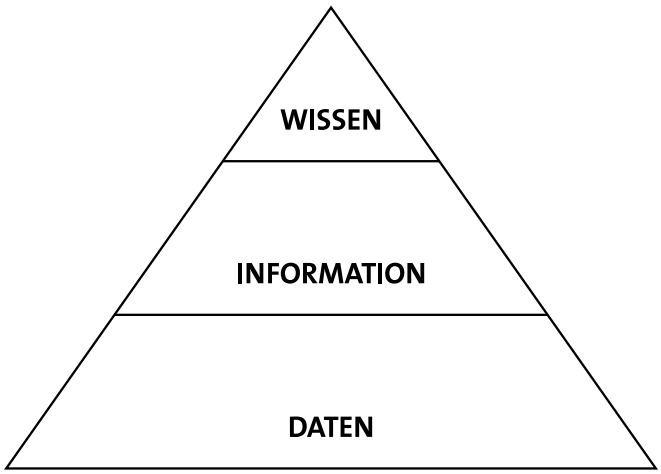
Vor diesem Hintergrund widmet sich die Studie in umfassender Weise der Fragestellung, wie Daten den verschiedenen Rechtsträgern (Unternehmen und Privaten, aber auch dem Staat) *de lege lata* zugeordnet werden können und *de lege ferenda* zugeordnet werden sollen. Diese breite Perspektive erfasst namentlich auch den rechtlichen Schutz einer faktischen Zuordnung von Daten, insbesondere durch Geheimhaltung, und die Zuordnung durch Verträge. Die Untersuchung geht damit über die im Auftrag genannten Begriffe von Eigentum, Besitz und Nutzung hinaus und ermöglicht gleichzeitig deren Einordnung.

Gemeinsam mit weiteren Beiträgen bildet der vorliegende Beitrag die Grundlage für die Ausarbeitung eines Berichts des IGE an den Bundesrat.

B. Begriffe

I. Daten

Um untersuchen zu können, ob und inwiefern Daten Gegenstand rechtlicher Zuordnung sind oder sein sollen, ist zunächst zu klären, was unter dem Begriff «Daten» zu verstehen ist. Hilfreich ist dabei die sog. *Informationspyramide*, anhand der das Verhältnis von Daten, Information und Wissen dargestellt werden kann:



In der Informationspyramide bilden Daten die Basis, bspw. die Geo-Lokalisationsdaten eines Mobiltelefons. Aus diesen Daten kann auf einer zweiten Stufe Information abgeleitet werden, bspw. die Information, an welchem Ort sich der Inhaber des Mobiltelefons zu einer bestimmten Zeit aufgehalten hat. Aus dieser Information lässt sich auf einer dritten Stufe sodann Wissen gewinnen, bspw. über den Wohn- und Arbeitsort dieser Person[1].

Dieses Bild mag helfen, um das Verhältnis von Daten, Information und Wissen zu veranschaulichen. Es kann aber nicht darüber hinwegtäuschen, dass bis heute kein einheitliches Verständnis dieser Begriffe besteht und sie oft undifferenziert verwendet werden[2]. Zwar wurden verschiedene Versuche unternommen, den Begriff der Information zu erfassen – gerade auch in den Rechtswissenschaften[3]. Die Ergebnisse dieser intellektuell anspruchsvollen und differenzierten Analysen konnten sich aber bisher kaum durchsetzen. Diese Studie unternimmt denn auch nicht den Versuch, einen Beitrag zu diesem Diskurs zu leisten. Sie kommt aber nicht umhin, den Gegenstand ihrer Analyse – die Daten – zumindest so genau zu umreissen, dass die Ergebnisse der Analyse nicht nur nachvollziehbar und plausibel, sondern (gegebenenfalls) auch falsifizierbar sind. 5

Ausgangspunkt bildet dabei die (allerdings implizit) an der Informationspyramide orientierte Strukturierung und Begrifflichkeit, die in der Rechtswissenschaft, namentlich in der Literatur zum Dateneigentum, entwickelt worden ist. Regelmässig werden dabei drei, bisweilen aber auch vier Ebenen unterschieden[4]:

- Die *syntaktische Ebene* bezieht sich auf die Struktur der Daten, also auf eine Folge von (elementaren) Zeichen. Bei digitalen Daten bestehen diese Zeichen oft in einer endlichen Folge von Nullen und Einsen, andere Repräsentationen sind etwa Gruben *(pits)* und Flächen *(lands)* in der Spiralspur einer CD. Auf der syntaktischen Ebene sind Daten damit maschinenlesbar[5] und sie werden durch eine bestimmte *Festlegung* in einer physikalisch existenten Form[6] erfasst. In der englischsprachigen Literatur wird diese Ebene bisweilen (etwas irreführend) auch als *«Code Layer»* bezeichnet[7].

- Auf der *semantischen Ebene* werden Daten als Information betrachtet. Diese Ebene bezieht sich auf die Bedeutung der Daten, also auf den informativen Gehalt, der durch die Daten vermittelt wird[8]. Diese Ebene erfasst Daten als immaterielle Güter[9]. In der

1 Zu dieser Verwendung der Begriffe Pombriant, CRi 2013, 97 ff.; Specht, CR 2016, 290 f. und Wiebe, GRUR Int. 2016, 881, jeweils m.w.H. Teilweise wird bei der Informationspyramide auch noch eine vierte Stufe unterschieden, die meist als Weisheit bezeichnet wird, siehe bspw. Succi/Coveney, Philos. Trans. Royal Soc. A 2019, 10.

2 Hildebrandt, 50. Für einen soziologischen Zugang zum Informationsbegriff siehe Marx, 9 ff.

3 Druey, 3 ff.; Zech, 11 ff.; ders., JIPITEC 2015, insb. 194 f.; Weber/Laux/Oertly, 5 ff.; Thouvenin/Weber/Früh, Datenpolitik, 120 f.; Janeček, CLSR 2018, 1042.

4 Für einen Überblick siehe Weber/Thouvenin, ZSR 2018 I, 46 f. Zu den Ebenen am Beispiel von Netzwerken auch Lessig, 23 f. und Abegg-Vaterlaus, 321.

5 Schmid/Schmidt/Zech, sic! 2018, 628, die Daten auf der syntaktischen Ebene als «maschinenlesbar codierte Information» bezeichnen; ebenso Amstutz, AcP 2018, 469.

6 Thouvenin, SJZ 2017, 28.

7 Zech, JIPITEC 2015, 194; siehe auch Schiele/Laux/Connolly, IJAIS 2014, 159 f., die zusätzlich zwischen einem *«Code Layer»* und einem *«Syntactic Layer»* unterscheiden.

8 Specht, CR 2016, 290; Wiebe, GRUR Int. 2016, 881; Kerber, GRUR Int. 2016, 992; Zech, 51 f.; ders., CR 2015, 138; Heymann, CR 2016, 650; Abegg-Vaterlaus, 322.

9 Thouvenin, SJZ 2017, 28.

englischsprachigen Literatur kommt der Fokus auf den Gehalt der Daten in der Bezeichnung als «*Content Layer*» zum Ausdruck[10]. Zentrales Merkmal von Information ist die Wahrnehmbarkeit durch die menschlichen Sinne[11]. Im Unterschied zu Daten richtet sich die Information stets an einen Adressaten mit den sinnlichen und kognitiven Fähigkeiten eines Menschen[12]. Der Übergang von der syntaktischen zur semantischen Ebene erfordert deshalb den Einsatz einer Maschine, welche die Daten interpretiert und «übersetzt», um die Information aus den Daten zu extrahieren und für Menschen wahrnehmbar zu machen[13].

- Auf der *pragmatischen Ebene* kann Information für sich allein oder in Kombination mit anderen Informationen Wissen bilden. Die pragmatische Ebene bezieht sich dabei auf nützliches Wissen, verstanden als Information, die einen bestimmten Effekt hat oder einem bestimmten Zweck dient[14].

- Gewisse Autoren unterscheiden noch eine weitere, nämlich die *strukturelle Ebene*, die sich auf die physikalische Festlegung der Daten auf einem Träger bezieht[15]. In der englischsprachigen Literatur wird daher auch der Begriff des «*Physical Layer*» verwendet[16]. Diese Ebene wird in der Informationspyramide nicht abgebildet.

- Für die rechtliche Betrachtung ist entscheidend, auf welcher Ebene die Rechtsordnung anknüpft. Die bestehenden rechtlichen Instrumente knüpfen für die Frage der Zuweisung von Rechten an Daten hauptsächlich auf der semantischen Ebene an, also dort, wo Daten in der Form von Information auftreten. Das gilt insbesondere für die Immaterialgüterrechte[17], aber auch für den Geheimnisschutz[18]. Auf der strukturellen Ebene sind Daten sodann dem Schutz durch das Sacheigentum zugänglich[19].

2. Personendaten

Diese Studie untersucht die Frage der Zuordnung von Sachdaten. Der Begriff der Sachdaten lässt sich allerdings nicht autonom, sondern nur aus der Abgrenzung gegenüber dem Begriff der Personendaten bestimmen. Denn Sachdaten sind nach Rechtsprechung und Lehre alle Daten, die nicht als Personendaten zu qualifizieren sind[20].

Als Personendaten gelten im schweizerischen Recht alle Daten, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 3 lit. a DSG; Art. 4 lit. a E-DSG). Dieser Begriff entspricht demjenigen des europäischen Rechts (Art. 4 Ziff. 1 DSGVO). Auf eine bestimmte Person beziehen sich Daten, wenn die Person direkt aufgrund der Daten identifiziert werden kann[21], bspw. durch den Namen und das Geburtsdatum. Solche Daten sind «als solche» – also unabhängig vom Kontext der Verwendung und von einer allfälligen Verknüpfung mit weiteren Daten – als Personendaten zu qualifizieren. Die meisten Daten beziehen sich allerdings nicht in einer derart direkten Weise auf eine bestimmte Person. Vielmehr lässt sich die Person, auf die sich die Daten beziehen, oft nur aus dem Kontext und aus der Verknüpfung mit anderen Daten bestimmen, bspw. aus der Verknüpfung des Surfverhaltens einer Internetnutzerin und der dabei verwendeten IP-Adresse mit den Angaben eines Telekom-Providers über die Zuteilung von IP-Adressen an seine Kunden[22].

In Lehre und Rechtsprechung wurde der ohnehin schon weite Begriff der Personendaten immer weiter

10 Siehe dazu Weber/Laux/Oertly, 7 mit Nachweisen in Fn. 31.
11 Weber/Laux/Oertly, 5 f.
12 Specht, CR 2016, 290.
13 Pombriant, CRi 2013, 98.
14 Specht, CR 2016, 290; Wiebe, GRUR Int. 2016, 881.
15 Zech, 41 ff.; ders., CR 2015, 138; Heymann, CR 2016, 650; Abegg-Vaterlaus, 324 f.
16 Zech, JIPITEC 2015, 194.
17 Siehe dazu hinten, C.II.2.
18 Siehe dazu hinten, C.III.3.
19 Siehe dazu hinten, C.II.1.
20 Statt vieler: BSK-DSG, Blechta, Art. 3 N 3. Siehe dazu auch Art. 3 Ziff. 1 Verordnung 2018/1807.
21 BSK-DSG, Blechta, Art. 2 N 9; Botschaft DSG 1988, BBl 1988 II 444; Passadelis/Rosenthal/Thür, Gerschwiler, Rn. 3.29.
22 BGE 136 II 508, E. 3; EuGH vom 19.10.2016, Rs. C-582/14, Rn. 45 ff.

ausgedehnt[23]. Dies zeigt sich insbesondere bei der Auslegung der Bestimmbarkeit der betroffenen Person: Nach der Rechtsprechung des Bundesgerichts reicht hierfür zwar nicht jede theoretische Möglichkeit der Identifizierung, es soll aber genügen, wenn die Identifizierung einer bestimmten Person ohne unverhältnismässigen Aufwand möglich ist[24]. Als unverhältnismässig gilt der Aufwand, wenn nach der allgemeinen Lebenserfahrung nicht damit zu rechnen ist, dass ein Interessent ihn auf sich nehmen wird[25]. Ähnliches gilt im europäischen Recht, für welches der EuGH sowie insbesondere die (ehemalige) Art. 29-Datenschutzgruppe den Begriff der Personendaten ebenfalls sehr weit auslegen[26]. Neben dem breiten Begriffsverständnis führt auch die Digitalisierung dazu, dass immer mehr Daten als Personendaten zu qualifizieren sind. Denn durch die Vereinfachung der Kombination und Verknüpfung verschiedener Daten können immer mehr Daten einer bestimmten Person zugeordnet werden, auch wenn die Daten für sich allein keinen Personenbezug aufweisen. Dieser Trend wird mit *Big Data* noch erheblich verstärkt. Denn die für solche Anwendungen typische Kombination sehr grosser Datenmengen macht es zunehmend unmöglich, das Risiko auszuschliessen, dass ein Bezug zwischen bestimmten Daten und der Person, auf die sich diese beziehen, erstmals oder erneut (Re-Identifikation) hergestellt wird[27]. Auch Daten, die als solche keinen Personenbezug aufweisen, sind deshalb häufig als Personendazu zu qualifizieren.

Das folgende *Beispiel* mag der Veranschaulichung dienen: Die Angaben über die Zusammensetzung einer Tafel Schokolade (bspw. 23% Haselnüsse) ist an sich ein Sachdatum. Liegen aber Daten darüber vor, wer diese Art von Schokolade gekauft (und damit wohl auch gegessen) hat und ist damit zu rechnen, dass diese Daten mit den Angaben über die Zusammensetzung der Schokolade verknüpft werden, wird die Angabe über den Anteil der Haselnüsse zu einem Personendatum, weil dann eine Aussage darüber besteht, dass eine (oder mehrere) bestimmte Person(en) eine bestimmte Menge Haselnüsse zu sich genommen hat (bzw. haben).

Dieser *relative Begriff* der Personendaten hat zur Folge, dass es in den meisten Fällen nicht möglich ist, ein bestimmtes Datum «als solches» für alle möglichen Verwendungen als Personen- oder als Sachdatum zu qualifizieren. Vielmehr kann diese Qualifikation immer nur im konkreten Einzelfall vorgenommen werden. Ein- und dasselbe Datum kann also, je nach Kontext und Verwendung, als Personen- oder als Sachdatum zu qualifizieren sein.

3. Sachdaten

Anders als der Begriff der Personendaten ist derjenige der «Sachdaten» im Gesetz nicht vorgesehen. Der Begriff der Sachdaten entstammt vielmehr der deutschsprachigen juristischen Diskussion, insbesondere jener zum Dateneigentum[28]. Die Lehre – vor allem ausserhalb des deutschsprachigen Raums – spricht auch von nichtpersonenbezogenen Daten[29]. Dies entspricht dem Begriff, welchen die EU in ihrer kürzlich in Kraft getretenen Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union verwendet[30].

Die negative Definition des Begriffs der Sachdaten («alle Daten, die keine Personendaten sind») und der relative Begriff der Personendaten[31] haben zur Folge, dass der Begriff der Sachdaten nicht in einer Weise definiert werden kann, die es erlauben würde, bestimmte Daten «als solche» als Sachdaten zu qualifizieren. So können etwa auch Daten, die eigentlich als solche keinen Personenbezug aufweisen – bspw. von Sensoren

23 Für die Rechtsprechung: BGE 136 II 508, E. 3; EuGH vom 19.10.2016, Rs. C-582/14, Rn. 23 ff. Für die Lehre statt vieler: Probst, AJP 2013, 1431 ff.; Meyerdierks, MMR 2009, 10.
24 BGE 138 II 346, E. 6.1; BGE 136 II 508, E. 3.2.
25 Statt vieler Belser/Epiney/Waldmann, § 7 Rn. 40; Rosenthal, Art. 3 N 24; Thouvenin, Forschung, 32.
26 Siehe dazu: EuGH vom 19.10.2016, Rs. C-582/14, Rn. 31 ff.; Art. 29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff «personenbezogene Daten» (WP 136), 6 ff.; Purtova, LIT 2018, 45 ff.
27 Thouvenin, Forschung, 33.
28 Siehe etwa Thouvenin/Früh/Lombard, SZW 2017, *passim*; Schmid/Schmidt/Zech, sic! 2018, *passim*; ferner Früh, digma 2019, *passim*; Sprecher, ZBJV 2018, *passim*; Weber/Laux/Oertly, *passim*.
29 Die englische Literatur verwendet den Begriff «non-personal data», die französische «données non-personelles».
30 Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates vom 14. November 2018 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union, ABl L 303 vom 28. November 2018, 59 ff.; siehe auch Europäische Kommission, Aufbau einer Europäischen Datenwirtschaft, insb. 9 ff.
31 Siehe dazu gerade vorstehend, B.2.

gemessene Wetterdaten oder anonymisierte Daten – im Einzelfall durch die Verknüpfung bzw. Re-Identifikation (erstmals oder erneut) zu Personendaten werden.

Für diese Studie hat dies zur Folge, dass sich der *Geltungsbereich* der Aussagen und Erkenntnisse nicht *ex ante* auf bestimmte Typen von Konstellationen eingrenzen, sondern nur *ex post* für konkrete Konstellationen bestimmen lässt. Während viele der nachfolgenden Aussagen für Personen- und Sachdaten gelten (bspw. zur Vermittlung absoluter Rechte durch das Urheberrecht[32] oder das europäische *sui-generis*-Recht an Datenbanken[33]), gelten andere Aussagen nur, wenn es sich bei den in Frage stehenden Daten tatsächlich um Sachdaten handelt (bspw. Aussagen zur freien Nutzung von Daten[34]). Dieses Problem steht der nachfolgenden, abstrakten Untersuchung der Rechtsfragen zur Zuordnung von Sachdaten zwar nicht entgegen. Bei der Anwendung der Erkenntnisse auf eine konkrete Fragestellung ist aber immer erst zu prüfen, ob es sich bei den in Frage stehenden Daten um Personen- oder Sachdaten handelt.

32 Siehe dazu hinten, C.II.2.
33 Siehe dazu hinten, C.II.4.
34 Siehe dazu hinten, C.I.

C. Rechtslage *de lege lata*

I. Datennutzung

Die Nutzung von Daten durch Staat und Private ist *grundsätzlich frei.* Wer also über Daten verfügt oder auf diese zugreifen kann, darf diese auch verwenden. Eine Rechtsgrundlage ist hierfür nicht erforderlich. Von diesem Grundsatz bestehen allerdings zwei gewichtige Ausnahmen:

Zum einen gilt diese Aussage nur für Sachdaten, weil das *Datenschutzrecht* der Nutzung von Personendaten[35] Grenzen setzt: Die Bearbeitung von Personendaten durch den Staat erfordert eine gesetzliche Grundlage (für den Bund: Art. 17 Abs. 1 DSG; Art. 30 Abs. 1 EDSG). Zudem muss die Bearbeitung in Übereinstimmung mit den Grundsätzen der Datenbearbeitung erfolgen (Art. 4, 5 und 7 DSG; Art. 5 und Art. 7 EDSG), also insbesondere mit dem Grundsatz der Erkennbarkeit (Art. 4 Abs. 4 DSG; Art. 5 Abs. 3 EDSG), der Zweckbindung (Art. 4 Abs. 3 DSG; Art. 5 Abs. 3 EDSG), der Verhältnismässigkeit (Art. 4 Abs. 2 DSG; Art. 5 Abs. 2 EDSG), der Datenrichtigkeit (Art. 5 Abs. 1 DSG; Art. 5 Abs. 5 EDSG) und der Datensicherheit (Art. 7 Abs. 1 DSG; Art. 7 Abs. 1 und 2 EDSG). Die Bearbeitung von Personendaten durch Private ist nach Schweizer Recht zulässig, wenn die Grundsätze der Datenbearbeitung eingehalten werden. Wird aber einer dieser Grundsätze verletzt oder widerspricht die von der Datenbearbeitung betroffene Person ausdrücklich (Art. 12 Abs. 2 lit. b DSG; Art. 26 Abs. 2 lit. b EDSG), muss der Private die Datenbearbeitung auf einen Rechtfertigungsgrund stützen können (Art. 12 Abs. 2 lit. a i.V.m. Art. 13 Abs. 1 DSG; Art. 27 Abs. 1 EDSG), insbesondere auf ein überwiegendes privates oder öffentliches Interesse oder auf die Einwilligung der betroffenen Person (Art. 13 Abs. 1 DSG; Art. 27 EDSG). In diesem Punkt unterscheidet sich das schweizerische grundlegend vom europäischen Datenschutzrecht. Denn nach der DSGVO ist die Bearbeitung von Personendaten nur zulässig, wenn eine Grundlage für deren Rechtmässigkeit (Art. 6 DSGVO) besteht. Die Bedingungen für die Rechtmässigkeit der Datenbearbeitung nach der DSGVO stimmen allerdings weitgehend mit den Rechtfertigungsgründen des schweizerischen Rechts überein; im Vordergrund stehen auch hier die berechtigten und überwiegenden Interessen des Bearbeiters an der Bearbeitung (Art. 6 Abs. 1 Bst. f DSGVO) und die Einwilligung der betroffenen Person (Art. 6 Abs. 1 Bst. a DSGVO).

Zum andern kann die Nutzung von Daten die *Rechte Dritter* an diesen Daten verletzen. Im Vordergrund steht dabei die Zuweisung von Rechten an den in den Daten repräsentierten Informationen, insbesondere durch Immaterialgüterrechte. Die Nutzung von Daten kann aber auch unzulässig sein, weil die Daten auf unrechtmässige Weise beschafft worden sind, etwa durch eine Verletzung von Fabrikations- oder Geschäftsgeheimissen (Art. 162 StGB; Art. 6 UWG) oder durch ein unbefugtes Eindringen in ein Datenverarbeitungssystem, sog. *Hacking* (Art. 143bis StGB). Bestehen Rechte Dritter an Daten, ist die Zuordnung dieser Daten für die Frage der Nutzung von entscheidender Bedeutung, weil derjenige, dem die Daten zugeordnet sind, in aller Regel auch über deren Nutzung bestimmen kann. Dabei stehen drei Konstellationen im Vordergrund:

- Eine Zuordnung durch die Zuweisung bestimmter *Rechte an Daten* bzw. an den in diesen Daten repräsentierten Informationen[36]. Die Nutzung der Daten durch (unberechtigte) Dritte kann in diesem Fall vom Berechtigten ausgeschlossen werden, sofern nicht bestimmte Schranken oder Ausnahmen des Schutzes greifen.

- Daten können einem Rechtsträger auch lediglich durch dessen *faktische Kontrolle* zugeordnet sein, namentlich durch die Speicherung in proprietären Systemen oder durch Verschlüsselung. Diese faktische Kontrolle ist bisweilen rechtlich abgesichert, namentlich durch den Schutz von Betriebs- und Geschäftsgeheimnissen (Art. 162 StGB und Art. 6 UWG) sowie durch Normen, welche das Durchbrechen der Kontrolle sanktionieren, insbesondere spezifische Straftatbestände[37]. Dritte sind in solchen Fällen zunächst einmal insoweit von der Nutzung ausgeschlossen, als sie keinen Zugang zu den Daten haben. Verschaffen sie sich aber Zugang und verstossen sie dabei gegen eine Rechtsnorm, welche die faktische Kontrolle absichert, wird dadurch in aller Regel

35 Zu diesem Begriff siehe vorn, B.2.
36 Siehe dazu hinten, C.II.
37 Siehe dazu hinten, C.III.

auch die Nutzung der Daten durch diese Dritten rechtlich unzulässig. Sind die Daten hingegen (etwa infolge eines Gewahrsamsbruchs oder wegen des Verlusts des Geheimnischarakters) frei verfügbar geworden, ist ihre Nutzung durch unbeteiligte Dritte typischerweise frei.

- Daten können schliesslich auch durch *vertragliche Vereinbarungen* einem bestimmten Berechtigten zugeordnet werden[38]. Eine solche Zuordnung bindet allerdings nur die Vertragsparteien, wirkt also nur *inter partes*, und vermittelt keinen Schutz gegen die Nutzungen durch Dritte, wirkt also nicht *erga omnes*.

Darüber hinaus ist zu beachten, dass auch das Datenschutzrecht als Zuordnungsinstrument aufgefasst werden kann, weil dessen Bestimmungen (bspw. das Widerspruchsrecht oder das Auskunftsrecht) den betroffenen Personen eine Rechtsstellung vermitteln, die einem Eigentum an Personendaten durchaus recht nahekommt[39]. Da sich die vorliegende Studie aber auf die Frage der Zuordnung von Sachdaten beschränkt[40], wird im Folgenden nicht weiter auf das Datenschutzrecht eingegangen.

In Bezug auf die Nutzung von Daten können sodann vier Aspekte unterschieden werden:

- Der *Zugang* zu Daten, d.h. die Möglichkeit, überhaupt auf Daten zugreifen zu können. Dabei handelt es sich um den wichtigsten Aspekt der Nutzung, weil dieser Voraussetzung für alle weiteren Nutzungshandlungen ist. Der Zugang zu Sachdaten wird deshalb in einer weiteren Studie vertieft untersucht[41].

- Das *Vervielfältigen* von Daten[42], also das Erstellen eines identischen Datensatzes auf einem eigenen Speicher, das die Kontrolle über die Daten und spätere (beliebige) weitere Nutzungen ermöglicht.

- Die *Verwendung* der Daten, in aller Regel erfolgt, um aus den Daten Erkenntnisse zu gewinnen. Zum Zweck der Analyse werden Daten oft bearbeitet, adaptiert und mit anderen Daten zusammengeführt. Die Verwendung setzt zwar Zugang zu den Daten, nicht aber zwingend das Herstellen einer Vervielfältigung des Datensatzes voraus, denn Daten können auch dezentralisiert oder auf fremden Systemen verwendet werden[43].

- Die Sicherstellung der *Vertraulichkeit, Verfügbarkeit und Integrität* der Daten gehört ebenfalls zu den Nutzungshandlungen in einem weiteren Sinn. Deren Kehrseite ist die Offenbarung, Löschung oder Veränderung der Daten[44].

II. (Absolut-)Rechtliche Zuordnung von Daten

Bei der Zuordnung von Daten stellt sich zunächst die Frage, ob bestehende Ausschliesslichkeitsrechte *erga omnes* wirkende Rechtspositionen an Daten vermitteln, also Rechte, die von den Rechteinhabern gegenüber jedermann geltend gemacht werden können.

Solche Ansprüche vermitteln den Rechteinhabern grundsätzlich umfassenden Schutz: Geht es um physische Gegenstände, untersagen sie nicht nur die Wegnahme, sondern gewähren auch einen Anspruch auf Wiedererlangung des jeweiligen Gegenstandes. Bei immateriellen Gütern ist eine vergleichbare Wegnahme und Wiedererlangung zwar aufgrund der ubiquitären Natur der Güter nicht möglich; *erga omnes* wirkende Unterlassungsansprüche vermitteln aber ebenfalls eine weitgehende Kontrolle des Rechteinhabers über das Schutzgut. Ähnlich verhält es sich bei den Leistungsschutzrechten und dem (diesen zuzuordnenden) europäischen *sui-generis*-Recht der Datenbankenhersteller.

38 Siehe dazu hinten, C.IV.
39 Früh, digma 2019, 174; Thouvenin/Weber/Früh, Datenpolitik, 28 und 89.
40 Siehe dazu vorn, B.2.
41 De Werra, *passim*.
42 Thouvenin/Weber/Früh, Data Ownership, 130 ff.
43 Thouvenin/Weber/Früh, Data Ownership, 132.
44 Thouvenin/Weber/Früh, Data Ownership, 132.

Dort ist jeweils die immaterielle Leistung oder das immaterielle Ergebnis einer bestimmten Leistung geschützt, indem die Leistung oder deren Ergebnis dem Rechteinhaber ausschliesslich vorbehalten bleibt und er jedem Dritten die Nutzung verbieten kann[45].

1. Sacheigentum

Das sachenrechtliche Eigentum gewährt seinem Inhaber umfassende Rechte, die *erga omnes* wirken[46]. Dabei lassen sich zwei Komponenten unterscheiden:

Die *positive Seite* des Sacheigentums vermittelt dem Rechteinhaber die grundsätzlich umfassende Herrschaft über die Sache (Art. 641 Abs. 1 ZGB)[47]. Schranken dieses Herrschaftsrechts können sich allerdings aus der übrigen Rechtsordnung ergeben, bspw. aus dem Nachbarrecht[48]. In den Schranken der Rechtsordnung umfasst das Herrschaftsrecht an der Sache namentlich den Besitz, den Gebrauch und den Genuss der Sache sowie die Möglichkeit, die Sache auf einen Dritten zu übertragen oder sie zu belasten, bspw. durch eine Verpfändung[49].

Die *negative Seite* des Sacheigentums gewährt dem Rechteinhaber zwei Arten von Rechten: Zum einen kann er die Sache von jedem Dritten herausverlangen (*rei vindicatio*) und zum andern alle Einwirkungen Dritter abwehren (*actio negatoria*, Art. 641 Abs. 2 ZGB)[50].

Das *Sachenrecht* ist zwar – auf der strukturellen Ebene[51] – ein wichtiges Zuordnungsinstrument für Datenträger. Denn das Sacheigentum an einem Datenträger, einem Server oder einer Serverfarm ermöglicht dem Eigentümer, (vertragliche) Bedingungen zur Nutzung der auf diesen Trägern gespeicherten Daten aufzustellen, an die sich Dritte halten müssen. Das Sachenrecht vermag aber keine Reche an Daten zu vermitteln, weil Daten nicht körperlicher Natur sind und damit – nach weitgehend einhelliger und richtiger Auffassung – das konstituierende Merkmal des Sacheigentums nicht erfüllen[52].

2. Immaterialgüterrechte

Immaterialgüterrechte verleihen dem Rechteinhaber Ausschliesslichkeitsrechte an immateriellen Gütern, die einem umfassenden Herrschaftsrecht zumindest nahekommen. Gegenstand dieser Rechte sind bestimmte immaterielle Güter, die nach Auffassung des Gesetzgebers eines besonderen Schutzes bedürfen; es gilt der sog. *numerus clausus* der Immaterialgüterrechte[53].

Wie das Sachenrecht wirken auch die Immaterialgüterrechte *erga omnes* (Art. 8 PatG; Art. 10 URG; Art. 9 DesG; Art. 13 MSchG)[54] und hier wie dort lassen sich zwei Komponenten unterscheiden:

Die Immaterialgüterrechte sind in erster Linie als Verbotsrechte konzipiert. Sie vermitteln ihrem Inhaber damit die Möglichkeit, jedermann die Nutzung der geschützten immateriellen Güter zu verbieten (Art. 8 PatG; Art. 10 URG; Art. 9 DesG; Art. 13 MSchG). Hierzu gehört namentlich das Recht, Dritten die Herstellung oder Vervielfältigung sowie die Nutzung des geschützten Gutes zu untersagen (Art. 8 PatG; Art. 10 URG; Art. 9 Abs. 1 DesG; Art. 13 MSchG).

Der Inhaber von Immaterialgüterrechten hat aber auch positive Verfügungsrechte; insbesondere kann er die Rechte belasten, bspw. durch eine Verpfändung (für das Urheber- und Patentrecht: Art. 899 Abs. 1 ZGB i.V.m. Art. 33 Abs. 1 PatG bzw. Art. 16 Abs. 1 URG; für das Design- und Markenrecht: Art. 16 DesG; Art. 19 MSchG)[55], auf Dritte übertragen (Art. 33 Abs. 1 PatG; Art. 16 Abs. 1 URG; Art. 14 DesG; Art. 17 MSchG) und Lizenzen zur

45 Thouvenin, Systematisierung, 376 ff.
46 Siehe dazu statt vieler: Schmid/Hürlimann-Kaup, Rn. 654; CHK-ZGB, Arnet, Art. 641 N 14.
47 ZK-ZGB, Haab, Art. 641 N 4; BSK-ZGB II, Wolf/Wiegand, Art. 641 N 3; KUKO-ZGB, Domej/Schmidt, Art. 641 N 2 & 5; Portmann, Rn. 220.
48 ZK-ZGB, Haab, Art. 641 N 3 und N 8 ff.; BSK-ZGB II, Wolf/Wiegand, Art. 641 N 35 ff.; KUKO-ZGB, Domej/Schmidt, Art. 641 N 9 ff.; CHK-ZGB, Arnet, Art. 641 N 29; Kren Kostkiewicz et al., Wolf, Art. 641 N 6; Tuor et al., § 96 N 4 ff.
49 ZK-ZGB, Haab, Art. 641 N 6; BSK-ZGB II, Wolf/Wiegand, Art. 641 N 30 ff.; KUKO-ZGB, Domej/Schmidt, Art. 641 N 8; CHK-ZGB, Arnet, Art. 641 N 28; Kren Kostkiewicz et al., Wolf, Art. 641 N 1 und N 5; Tuor et al., § 96 Rn. 3; Portmann, Rn. 222.
50 ZK-ZGB, Haab, Art. 641 N 7; BSK-ZGB II, Wolf/Wiegand, Art. 641 N 40 ff.; KUKO-ZGB, Domej/Schmidt, Art. 641 N 16 ff.; CHK, Arnet, ZGB 641 N 31 ff.; Kren Kostkiewicz et al., Wolf, Art. 641 N 8 f.; Tuor et al., § 96 N 10; Portmann, Rn. 223 und Rn. 229 ff.
51 Siehe dazu vorn, B.1.
52 Für die Schweiz: ZK-ZGB, Haab, Einleitung Art. 641–729 N 21; BSK-ZGB II, Wolf/Wiegand, Vor Art. 641 ff. N 5; BSK-ZGB II, Wolf/Wiegand, Art. 641 N 29; KUKO-ZGB, Domej/Schmidt, Vor Art. 641–654a N 4; Tuor et al., § 87 N 2; CHK-ZGB, Arnet, Art. 641 N 6, 10; Kren Kostkiewicz et al., Wolf, Art. 641 N 3; Zogg, recht 2019, 101; s.a. Hürlimann/Zech, sui generis 2016, 92, m.H. auf die für nicht-rivalisierende Güter unpassende zeitlich unbegrenzte Schutzdauer. Für Deutschland: Heymann, CR 2016, 656; Specht, CR 2016, 289. Anderer Meinung sind Ritter/Mayer, Duke L. & Tech. Rev. 2018, 255 ff. welche Daten als physische Materie behandeln wollen und Eckert, SJZ 2016, 246, wonach digitale Daten die Voraussetzung der Körperlichkeit erfüllen und deswegen als Sache *(res digitalis)* qualifiziert werden können.
53 Berger, 3; Thouvenin, Systematisierung, 518 f. m.w.H. in Fn. 52; SIWR I/1, Dessemontet, 21; David, AJP 1995, 1404.
54 Marbach/Ducrey/Wild, Rn. 3; SIWR I/1, Dessemontet, 16.
55 BSK-ZGB II, Bauer, Art. 899 N 50; CHK-ZGB, Reetz/Graber, Art. 899 N 16.

Nutzung der geschützten immateriellen Güter erteilen (Art. 34 PatG; implizit: Art. 62 Abs. 3 URG[56]; Art. 15 DesG; Art. 18 MSchG). Positive Nutzungsrechte vermitteln die Immaterialgüterrechte hingegen nicht. Die Möglichkeit zur Nutzung dieser Güter ergibt sich für den Rechteinhaber vielmehr daraus, dass ihm diese niemand verbieten kann[57].

Zu beachten ist, dass Immaterialgüterrechte verschiedenen *Schranken* unterworfen sind, die gewisse Nutzungen des geschützten Gutes entweder unentgeltlich oder gegen Zahlung einer Gebühr vom Verbotsrecht freistellen. Für die Nutzung von Sachdaten besonders relevant sind die Schranken zugunsten des Eigengebrauchs (Art. 19 und 20 URG) und die Schranke für die Verwendung von Werken zum Zweck der wissenschaftlichen Forschung (Art. 24d URG) im Urheberrecht sowie das Forschungsprivileg im Patentrecht (Art. 9 Abs. 1 lit. b PatG). Schliesslich sind Immaterialgüterrechte grundsätzlich zeitlich befristet (Art. 14 PatG; Art. 29 ff. URG; Art. 5 Abs. 2 f. DesG). Die einzige Ausnahme bildet das Markenrecht, dessen Schutz bei anhaltendem Gebrauch der Marke beliebig oft verlängert werden kann (Art. 10 MSchG)[58].

12

Die Immaterialgüterrechte vermitteln Ausschliesslichkeitsrechte an immaterielle Gütern, also bestimmten Informationen (semantische Ebene[59]), bspw. an Erfindungen als Lehren zum technischen Handeln (Art. 1 Abs. 1 PatG) oder an Werken der Literatur und Kunst (Art. 2 Abs. 1 URG). Die immaterialgüterrechtlich geschützten Informationen können durch die menschlichen Sinne wahrgenommen werden und sie sind auch gerade für die Wahrnehmung durch Menschen bestimmt. Der Schutz umfasst jede Ausprägung dieser Information und damit namentlich auch deren Festlegung in Form von Daten (syntaktische Ebene[60]). Soweit Immaterialgüterrechte bestehen, vermitteln sie damit auch Ausschliesslichkeitsrechte an denjenigen Daten, welche die geschützten Informationen in einer physikalisch existenten und maschinenlesbaren Form festlegen[61]. Die Zuweisung von Immaterialgüterrechten an Informationen hat demnach zur Folge, dass *Daten durch diese Rechte zwar nicht als solche geschützt* sind, dass der Schutz der Information (semantische Ebene) die Repräsentation der geschützten immateriellen Güter in Form von Daten (syntaktische Ebene) aber mitumfasst. Im Ergebnis vermitteln Immaterialgüterrechte damit *erga omnes* wirkende Rechte an Daten.

Das gilt auch für *Datenbanken*, die als Sammelwerke urheberrechtlich geschützt sind, sofern es sich hinsichtlich Auswahl und Anordnung der Inhalte um geistige Schöpfungen mit individuellem Charakter handelt (Art. 4 Abs. 1 URG)[62]. Der Schutz bezieht sich dabei allein auf die individuelle Struktur der Datenbank[63] und erfasst damit Informationen über die Auswahl und Anordnung von Daten sowie die Repräsentation dieser Informationen als Daten, nicht aber die in der Datenbank enthaltenen Daten[64] – und zwar weder auf der semantischen noch auf der syntaktischen Ebene.

3. Leistungsschutzrechte

Die Leistungsschutzrechte, die auch als verwandte Schutzrechte oder Nachbarrechte bezeichnet werden, verleihen dem Rechteinhaber der Struktur nach vergleichbare, *erga omnes* wirkende Herrschaftsrechte an bestimmten Leistungen[65]. Anders als bei den Immaterialgüterrechten bestehen bei den Leistungsschutzrechten massgebliche Unterschiede zwischen verschiedenen Rechtsordnungen. Während die Schweiz und die meisten anderen Länder (nur) die Leistungen der ausübenden Künstler (Art. 33 ff. URG), der Hersteller von Ton- und Tonbildträgern (Art. 36 URG) und der Sendeunternehmen

56 Auch ohne ausdrückliche gesetzliche Regelung ist unbestritten, dass Urheberrechte Gegenstand von Lizenzverträgen sein können. Siehe dazu statt vieler Hilty, Lizenzvertragsrecht, 21 ff.; ferner Barrelet/Egloff, Egloff, Art. 10 N 7; CR-LDA, Cherpillod, Art. 10 N 8 f.; SHK-URG, Pfortmüller, Art. 10 N 1.

57 Thouvenin, Systematisierung, 267 f.

58 Siehe dazu statt vieler Marbach/Ducrey/Wild, Rn. 772.

59 Siehe dazu vorn, B.1.

60 Siehe dazu vorn, B.1.

61 Dies verkennt Amstutz, AcP 2018, 488, nach welchem Immaterialgüterrechte «keinerlei eigentumsmässige oder eigentumsähnliche Rechte an Daten [verleihen], welche gesetzlich oder jurisprudentiell geschützte Information enthalten».

62 Ebenso das europäische Recht: Art. 3 Abs. 1 Datenbanken-RL.

63 Barrelet/Egloff, Egloff Art. 4 N 6; Hilty, Urheberrecht, Rn. 126.

64 SHK-URG, Cherpillod, Art. 4 N 5 f.; Kübler, 161 f.; ferner auch Barrelet/Egloff, Egloff, Art. 4 N 6, nach welchem der sui-generis-Schutz im schweizerischen URG ein Fremdkörper wäre, «da er nicht die Verwendung von Werken regelt, sondern Inhalte monopolisiert. So für den urheberrechtlichen Schutz von Datenbanken ausdrücklich Art. 3 Abs. 1 Datenbanken-RL.

65 Barrelet/Egloff, Egloff, Art. 33 N 18; Hilty, UFITA 1994, 43.

(Art. 37 URG) schützen, kennen einige Länder noch weitere Leistungsschutzrechte, etwa für Fotografen[66] oder Hersteller von Presseerzeugnissen[67].

Wie im Sachen- und Immaterialgüterrecht sind auch bei den Leistungsschutzrechten *zwei Komponenten* zu unterscheiden: Die Leistungsschutzrechte sind, wie die Immaterialgüterrechte, in erster Linie als Verbotsrechte konzipiert. Anders als jene verleihen diese den Rechteinhabern allerdings keine umfassenden, sondern nur bestimmte, gesetzlich abschliessend aufgezählte Verbotsrechte[68]. Kern aller Leistungsschutzrechte sind dabei das Verbot der Vervielfältigung der geschützten Leistung und das Recht des Zugänglichmachens (Art. 33 Abs. 2 lit. a und lit. c URG; Art. 36 lit. a und lit. b URG; Art. 37 lit. c und lit. e URG). Der Inhaber von Leistungsschutzrechten hat zudem positive Verfügungsrechte; insbesondere kann er die Rechte belasten[69], auf Dritte übertragen (Art. 38 i.V.m. Art. 16 Abs. 1 URG) und Lizenzen zur Nutzung der geschützten Leistungen erteilen (implizit: Art. 62 Abs. 3 URG[70]). Positive Nutzungsrechte vermitteln die Leistungsschutzrechte aber nicht; die Möglichkeit zur Nutzung der Leistung ergibt sich für den Rechteinhaber vielmehr daraus, dass ihnen niemand die Nutzung verbieten kann.

Auf die Leistungsschutzrechte finden die *Schranken* des Urheberrechts sinngemäss Anwendung (Art. 38 URG) und der Schutz ist auch hier zeitlich befristet (Art. 39 URG).

Gegenstand von Leistungsschutzrechten sind immaterielle Leistungen, der Schutz erfasst allerdings deren Ergebnisse, die sich in verschiedenen Formen materialisieren, etwa in der Festlegung der Aufnahme eines Musikstücks auf einer CD, in einem Sendesignal, das über Funk oder Kabel ausgestrahlt wird oder (wenn ein entsprechendes Leistungsschutzrecht besteht) in der auf einem Webserver gespeicherten Datei einer Fotografie[71]. Ihrem Gegenstand nach kommen Leistungsschutzrechte einem Ausschliesslichkeitsrecht an Daten damit sehr nahe; denn indem diese Rechte die *Festlegung der Leistungen in elektronischer Form* erfassen, lassen sie sich auch als *Ausschliesslichkeitsrechte an den entsprechenden Daten* verstehen. Allerdings reichen die Schutzwirkungen bei den Leistungsschutzrechten weniger weit als bei den Immaterialgüterrechten. Denn zum einen sehen die Leistungsschutzrechte, wie erwähnt, nur bestimmte Verbotsrechte vor. Zum andern erfassen sie immer nur die konkrete Festlegung der jeweiligen Leistung und vermitteln damit nur Schutz gegen die identische Übernahme der Leistung, nicht aber gegen deren Nachahmung oder Nachmachung[72].

4. *Sui-generis*-Recht an Datenbanken

Mit der Einführung eines Schutzes von Datenbanken durch Erlass der Richtlinie 96/9/EG über den rechtlichen Schutz von Datenbanken (Datenbanken-RL) erhoffte man sich in Europa Mitte der 90er Jahre Impulse für die (Daten-)Wirtschaft[73]. Die Datenbanken-RL verfolgte im Wesentlichen zwei Ziele: Zum einen sollten die sehr unterschiedlichen europäischen Schutzregime für Datenbanken harmonisiert werden, zum andern sollten mit der Einführung eines *sui-generis*-Schutzes von Datenbanken Investitionen in Aufbau und Produktion von Datenbanken begünstigt[74] und damit Anreize für deren Produktion geschaffen werden, um so den Rückstand gegenüber den USA aufzuholen.

Mit der Umsetzung der Datenbanken-RL haben alle Mitgliedstaaten der damaligen EG in ihrem nationalen Recht einen urheberrechtlichen Schutz von Datenbanken und ein sog. *sui-generis*-Recht für die Hersteller von Datenbanken geschaffen[75]. Das Schweizer Recht kennt kein

66 Für Deutschland § 72 D-UrhG und für Österreich § 73 ff. A-UrhG.
67 Für Deutschland § 87f ff. D-UrhG; für Spanien Art. 32.2 LPI. Ein solches Leistungsschutzrecht werden alle Mitgliedstaaten in Umsetzung von Art. 15 der Richtlinie des Europäischen Parlaments und des Rates über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG vom 17. April 2019 einführen müssen.
68 Marbach/Ducrey/Wild, Rn. 402; SIWR II/1, Mosimann, Rn. 1086; Barrelet/Egloff, Egloff, Art. 33 N 17.
69 Gemäss SIWR I/1, von Büren, 288, können an Urheberrechten Pfandrechte bestellt werden. Eine Ausnahme bilden die Urheberpersönlichkeitsrechte, die aufgrund der mangelnden Übertragbarkeit ausscheiden (Art. 899 Abs. 1 ZGB). Leistungsschutzrechte sind wie die Urheberrechte übertragbar, SIWR II/1, Mosimann, Rn. 1170, daher muss die Belastung (z.B. Verpfändung) eines Leistungsschutzrechts rechtlich zulässig sein; siehe hierzu auch Picht, 144. Für die Verwertbarkeit von Leistungsschutzrechten siehe Barrelet/Egloff, Egloff, Art. 38 N 10.
70 Auch ohne ausdrückliche gesetzliche Regelung ist unbestritten, dass Leistungsschutzrechte Gegenstand von Lizenzverträgen sein können; siehe dazu statt vieler Hilty, Lizenzvertragsrecht, 50 ff. insb. 52.
71 Thouvenin, Systematisierung, 372 ff.; siehe dazu auch SIWR II/1, Mosimann, Rn. 1008 ff., insb. Rn. 1009 und Hilty, Urheberrecht, Rn. 343.
72 Thouvenin, Systematisierung, 378 f.; SIWR II/1, Mosimann, Rn. 1008; weniger klar hingegen Weber, 588; Podszun, 369.
73 Zur Entstehungsgeschichte der Datenbanken-RL siehe Gaster, Rn. 5–12.
74 Erw. 9–12 Datenbanken-RL; Köklü, 306.
75 Art. 7 ff. Datenbanken-RL; zur Begründung insb. Erw. 38 Datenbanken-RL.

sui-generis-Recht, wohl aber einen urheberrechtlichen Schutz von Datenbanken[76]. Allerdings enthält das Wettbewerbsrecht (UWG) Instrumente, die einem *sui-generis*-Recht an Datenbanken zumindest teilweise nahekommen, so namentlich die Bestimmung von Art. 5 lit. c UWG[77], welche die unmittelbare Übernahme eines marktreifen Arbeitsergebnisses verbietet, wenn diese mit einem technischem Reproduktionsverfahren und ohne angemessenen eigenen Aufwand erfolgt[78].

Zweck des *sui-generis*-Rechts an Datenbanken ist der
14 Schutz der Investitionen der Hersteller von Datenbanken[79]. Als Datenbank gilt dabei eine Sammlung von Werken, Daten oder anderen unabhängigen Elementen[80], die systematisch oder methodisch angeordnet und einzeln mit elektronischen Mitteln oder auf andere Weise zugänglich sind (Art. 1 Abs. 2 Datenbanken-RL)[81]. Voraussetzung für die Gewährung des Schutzes ist, dass der Hersteller in die Beschaffung, Überprüfung oder Darstellung des Inhalts einer Datenbank eine in qualitativer oder quantitativer Hinsicht erhebliche Investition getätigt hat. Als mit der Datenbank verbundene Investition gilt dabei allerdings nur derjenige Mitteleinsatz, welcher der Beschaffung oder der Zusammenstellung von Elementen dient, nicht aber die Investition in die Erzeugung dieser Elemente, also der Daten als solcher[82].

Das *sui-generis*-Recht vermittelt seinem Inhaber das Recht, Dritten die *Entnahme und/oder Weiterverwendung der Gesamtheit oder eines* in qualitativer und quantitativer Hinsicht *wesentlichen Teils des Inhalts einer Datenbank* zu untersagen[83]. Entnahme bedeutet dabei die ständige oder vorübergehende Übertragung der Inhalte einer Datenbank auf einen anderen Datenträger, ungeachtet der dafür verwendeten Mittel und der Form der Entnahme (Art. 7 Abs. 2 Bst. a Datenbanken-RL). Als Weiterverwendung gilt jede Form der öffentlichen Verfügbarmachung (Art. 7 Abs. 2 Bst. b Datenbanken-RL)[84]. Von einem «wesentlichen Teil» kann ausgegangen werden, wenn im Verhältnis zum Gesamtvolumen der Datenbank ein *quantitativ* grosser Teil entnommen und/oder weiterverwendet wird. Ein *qualitativ* wesentlicher Teil liegt vor, wenn die Investition, die für das oder die entnommene(n) Element(e) getätigt worden ist, im Verhältnis zur Investition in die gesamte Datenbank erheblich ist[85]. Unzulässig ist auch die Entnahme und Weiterverwendung unwesentlicher Teile, sofern diese wiederholt und systematisch erfolgt und einer norma-

76 Siehe dazu vorn, C.II.2.

77 Die Einführung eines sui-generis-Rechts an Datenbanken wurde teilweise gerade unter Verweis auf Art. 5 lit. c UWG als unnötig angesehen: Tissot, Medialex 1996, 198; Heizmann/Loacker, Weber/Chrobak, Art. 5 lit. c N 17, auch mit Hinweis auf verbleibende Differenzen; Hilty, Leistungsschutz, 654 f.; Kübler, 322. Bemerkenswert ist in diesem Zusammenhang ein Entscheid des EuGH, der die Zulässigkeit einer Metasuchmaschine nach Art. 7 Datenbanken-RL untersucht. Diese Suchmaschine erlaubt es ihren Nutzern, mit einer Suchanfrage mehrere Datenbanken abzufragen und zeigt den Nutzern auch direkt die Ergebnisliste an, worin der EuGH eine Weiterverwendung der Gesamtheit der Datenbank sah (EuGH vom 19. Dezember 2013, Rs. C-202/12 – Innoweb vs. Wegener, Rn. 49 ff., insb. 53). Die zu beurteilende Handlung scheint dem sog. «Spidering», das in der Schweiz soweit ersichtlich schon zweimal mit Blick auf Art. 5 lit. c UWG gerichtlich beurteilt worden ist, zumindest recht nahezukommen (s. dazu KGer Fribourg, sic! 2017, 228 ff. – Spidering, Verstoss bejaht; BGE 131 III 384 – Suchspider, Verstoss verneint).

78 Siehe dazu hinten, C.III.5.

79 Erw. 39 f. sowie Erw. 48 Datenbanken-RL, wonach der Hersteller der Datenbank «die ihm zustehende Vergütung» erhalten soll; EuGH vom 09.10.2008, Rs. C-304/07 – Directmedia vs. Albert-Ludwigs-Universität, Rn. 33; EuGH vom 9. November 2004, Rs. C-444/2, Fixtures Marketing vs. OPAP, Rn. 41; EuGH vom 19. Dezember 2013, Rs. C-202/12, Innoweb vs. Wegener, Rn. 36 f.; siehe auch Thouvenin, Systematisierung, 402.

80 Unabhängig sind die Elemente, wenn sie sich «voneinander trennen lassen, ohne dass der Wert ihres informativen, literarischen, künstlerischen, musikalischen oder sonstigen Inhalts dadurch beeinträchtigt wird», wobei keine Beeinträchtigung vorliegt, wenn das Element nach der Trennung noch einen eigenständigen Informationsgehalt besitzt (EuGH vom 9. November 2004, Rs. C-444/2 – Fixtures Marketing vs. OPAP, Rn. 29 sowie 33 f.; EuGH vom 29. Oktober 2015, C-490/14 – Freistaat Bayern vs. Verlag Esterbauer GmbH, Rn. 17 und 22; s. dazu auch Sendrowski, 370; Witte, Rn. 15; Wiebe, GRUR 2017, 339).

81 Nach dem EuGH impliziert das Erfordernis der systematischen und methodischen Anordnung resp. das «einzeln zugänglich sein», dass es möglich sein muss, «jedes in der Sammlung enthaltene unabhängige Element zu lokalisieren». Dies kann durch technische Mittel oder durch einen Index, ein Inhaltsverzeichnis o.ä. gewährleistet werden (EuGH vom 9. November 2004, Rs. C-444/2 – Fixtures Marketing vs. OPAP, Rn. 30; s. auch Erw. 13 f., 17 und 21 Datenbanken-RL; Sendrowski, GRUR 2005, 370; Wiebe, GRUR 2017, 340; Gaster, Rn. 28).

82 EuGH vom 09.11.2004, Rs. C-203/02 – British Horseracing vs. Hill Organization, Rn. 38; EuGH vom 9. November 2004, Rs. C-444/2 – Fixtures Marketing vs. OPAP, Rn. 39 ff., insb. 47; Thouvenin, Systematisierung, 392; Gaster, Rn. 82 ff. m.w.H.; Sendrowski, GRUR 2005, 371 f., allerdings kritisch gegenüber der Abgrenzung zur Nichtberücksichtigung von Investitionen zur Erzeugung der Daten. Mit dem Versuch einer Abgrenzung zwischen erzeugten und gesammelten Daten Wiebe, GRUR 2017, 341.

83 Thouvenin, Systematisierung, 393.

84 Nach dem EuGH sind die Begriffe «Entnahme» und «Weiterverwendung» weit zu fassen. Darunter sei jede Handlung zu verstehen, «die darin besteht, sich ohne die Zustimmung der Person, die die Datenbank erstellt hat, die Ergebnisse ihrer Investition anzueignen bzw. sie öffentlich verfügbar zu machen und ihr damit die Einkünfte zu entziehen, die es ihr ermöglichen sollen, die Kosten dieser Investition zu amortisieren», EuGH vom 09.11.2004, Rs. C-203/02 – British Horseracing vs. Hill Organization, Rn. 51; Sendrowski, GRUR 2005, 374; Gaster. Rn. 127 ff. Zur Weiterverwendung: EuGH vom 19. Dezember 2013, Rs. C-202/12 – Innoweb vs. Wegener, Rn. 37; zur Entnahme: EuGH vom 05.03.2009, Rs. C-545/07 – Apis-Hristovich vs. Lakorda, Rn. 40 ff.; EuGH vom 09.10.2008, Rs. C-304/07 – Directmedia vs. Albert-Ludwigs-Universität, Rn. 34 ff., insb. 47.

85 EuGH vom 05.03.2009, Rs. C-545/07 – Apis-Hristovich vs. Lakorda, Rn. 56 ff., insb. 59, 66 und 74; EuGH vom 09.11.2004, Rs. C-203/02 – British Horseracing vs. Hill Organization., Rn. 70 f.; Sendrowski, GRUR 2005, 375; Wiebe, GRUR 2017, 343 f.

len Nutzung der Datenbank durch den Hersteller entgegensteht oder dessen Interessen unzumutbar beeinträchtigt (Art. 7 Abs. 5 Datenbanken-RL).

Während das Urheberrecht die Auswahl und Anordnung der Daten in einer Datenbank, also deren Struktur, schützt[86], erfasst das *sui-generis*-Recht den *Inhalt von Datenbanken*, also eine Mehrheit von Daten, indem es die Entnahme einzelner oder mehrerer Elemente aus einer Datenbank erfasst, unabhängig davon, ob auch die Struktur der Datenbank übernommen wurde[87]. Der Hersteller einer Datenbank kann Dritten damit die Entnahme und Weiterverwendung der darin enthaltenen Daten in jeglicher Form verbieten, sofern es sich dabei um quantitativ oder qualitativ wesentliche Teile handelt. Das *sui-generis*-Recht vermittelt damit zwar Ausschliesslichkeitsrechte an Inhalten von Datenbanken und damit an gewissen Datenbeständen, nicht aber an einzelnen, in der Datenbank enthaltenen Daten.

III. Rechtlicher Schutz der faktischen Zuordnung von Daten

1. Vorbemerkungen

Eine rechtlich relevante Zuordnung von Daten kann nicht nur durch die Gewährung von Ausschliesslichkeitsrechten[88] erfolgen, sondern auch durch einen *rechtlichen Schutz der faktischen Zuordnung, also der tatsächlichen Herrschaft über Daten*. Ein solcher Schutz geht zwar weniger weit als bei Ausschliesslichkeitsrechten, er kann aber unter Umständen zu vergleichbaren Ergebnissen führen und einen allenfalls bestehenden Schutzbedarf hinreichend abdecken.

Die Rechtsordnung kennt eine Reihe von *erga omnes* wirkenden Bestimmungen, die *Eingriffe in die faktische Herrschaft* über Daten sanktionieren. Im Vordergrund stehen dabei der Besitz[89] sowie die Bestimmungen über den Schutz von Fabrikations- und Geschäftsgeheimnissen[90] und der Amts- und Berufsgeheimnisse[91]. Relevant sind aber auch gewisse Vermögensdelikte[92] und die Bestimmungen des UWG[93]. In Kombination mit technischen Massnahmen, welche den Zugang zu und die Nutzung von Daten verhindern, kann damit eine effektive Kontrolle über Daten erreicht werden, die einem Eigentumsrecht im Ergebnis recht nahekommt.

Anders als Ausschliesslichkeitsrechte vermitteln die Ansätze für einen rechtlichen Schutz der faktischen Zuordnung von Daten keine grundsätzlich umfassenden Rechtspositionen. Namentlich weisen sie den Berechtigten kein bestimmtes (materielles oder immaterielles) Gut zu, über das diese im Rahmen der Rechtsordnung verfügen könnten, bspw. indem sie das Gut auf Dritte übertragen. Vielmehr qualifizieren diese Ansätze ein bestimmtes Verhalten als unzulässig (bspw. den Verrat von Fabrikations- und Geschäftsgeheimnissen nach Art. 162 StGB und Art. 6 UWG) und vermitteln den Berechtigten dadurch gewisse Rechtsansprüche, mit denen sie gegen ein solches Verhalten vorgehen können.

Diese Rechtsansprüche sind teilweise ausdrücklich gesetzlich vorgesehen, so namentlich der Anspruch auf Unterlassung (bspw. nach Art. 9 Abs. 1 UWG), teilweise lassen sie sich aber (nur) aus dem *allgemeinen Deliktsrecht* (Art. 41 ff. OR) ableiten. Denn dieses vermittelt nicht nur einen Anspruch auf Schadenersatz, sondern richtigerweise auch einen *Anspruch auf Unterlassung und Naturalrestitution*[94]. Dass ein solcher Anspruch besteht, ist im Zusammenhang mit Personendaten in der Lehre auch schon vertreten worden[95]. Für Sachdaten wurde die Frage zwar bisher, soweit ersichtlich, noch nicht erörtert; es sind aber keine Gründe ersichtlich, weshalb ein solcher Anspruch nicht auch hier gegeben sein sollte.

Deliktsrechtliche Ansprüche nach Art. 41 OR entstehen nur, wenn die in Frage stehende Handlung widerrechtlich im Sinn der objektiven Widerrechtlichkeitstheo-

86 Erw. 15 und 39 Datenbanken-RL.
87 Siehe dazu auch Erw. 58, wonach das Urheberrecht die Struktur, das Sui-generis-Recht dagegen den Inhalt schützt; EuGH vom 05.03.2009, Rs. C-545/07 – Apis-Hristovich vs. Lakorda, Rn. 55.
88 Siehe dazu vorn, C.II.
89 Siehe dazu hinten, C.III.2.
90 Siehe dazu hinten, C.III.3.
91 Siehe dazu hinten, C.III.3.
92 Siehe dazu hinten, C.III.4.
93 Siehe dazu hinten, C.III.5.
94 BSK-OR I, Kessler, Art. 43 N 4; in diese Richtung auch Eckert, SJZ 2016, 272 und Hess-Odoni, Jusletter 17. Mai 2004, Rz. 39.
95 HK-DSG, Rosenthal, Art. 15 N 41.

rie ist. Dies setzt die Verletzung absolut geschützter Rechtsgüter (sog. Erfolgsunrecht) oder den Verstoss gegen eine Schutznorm voraus, die nach ihrem Zweck (auch) vor Schädigungen der konkret eingetretenen Art schützen sollen (sog. Verhaltensunrecht)[96]. Da Daten *(de lege lata)* keine absolut geschützten Rechtsgüter sind, wird die Person, die durch einen Eingriff in ihrer faktischen Herrschaft über Daten beeinträchtigt wird, die Widerrechtlichkeit gestützt auf eine *Schutznorm* begründen müssen. Als solche Schutznormen kommen vor allem vermögensstrafrechtliche Bestimmungen[97], aber auch Normen aus dem übrigen Strafrecht in Frage[98]. Für die Widerrechtlichkeit ist dabei stets vorausgesetzt, dass sowohl der subjektive als auch der objektive Tatbestand der jeweiligen Strafnorm erfüllt ist[99].

16

Soweit ein bestimmtes Verhalten, das in die tatsächliche Herrschaft über Daten eingreift, durch die Rechtsordnung als widerrechtlich qualifiziert wird, verschaffen die bei einem widerrechtlichen Verhalten vorgesehenen Sanktionen und die allgemeinen deliktsrechtlichen Ansprüche den Berechtigten insgesamt eine Rechtsposition, welche der *negativen Seite von Eigentumsrechten* entspricht[100], indem sie einen *Anspruch auf Unterlassung* des Einwirkens auf die Daten und einen *Anspruch auf Herausgabe* der Daten vermitteln. Grundlegende Unterschiede zu einem vollen Eigentumsrecht bestehen allerdings bei der positiven Seite des Eigentums[101]. Diese ist hier nicht rechtlich abgesichert, sondern besteht nur faktisch, indem der Inhaber der tatsächlichen Herrschaft die Daten selbst nutzen, Dritten die Nutzung erlauben oder diesen die Daten übertragen kann.

2. Datenbesitz

Einen rechtlichen Schutz der faktischen Herrschaft vermittelt insbesondere der *Besitz* (Art. 919 ff. ZGB). Wie das Eigentum besteht aber auch der Besitz nach herrschender Lehre und Rechtsprechung vorab an körperlichen Sachen[102]. Daneben sieht Art. 919 Abs. 2 ZGB zwar auch einen Rechtsbesitz an Grunddienstbarkeiten und Grundlasten vor, den die Lehre auf Personaldienstbarkeiten und teilweise sogar auf Immaterialgüterrechte und Forderungen ausweitet[103]. Unabhängig von der Frage, worin der rechtlich relevante Gehalt des Besitzes an Immaterialgüterrechten oder Forderungen überhaupt bestehen würde, bezieht sich der Rechtsbesitz in all diesen Fällen stets auf die jeweiligen Rechte und nicht auf die mit diesen allenfalls verbundenen Daten. Daten sind damit weder Gegenstand des Sach- noch des Rechtsbesitzes.

In der (deutschen) Lehre finden sich vereinzelte Stimmen, die einen zivilrechtlichen Datenbesitz als sachgerecht einstufen und für die sinngemässe Anwendung «zivilrechtlicher Vorschriften des Besitzesschutzes» auf Daten einstehen[104]. Neben verschiedenen Einzelheiten scheint indes bei einem solchen Datenbesitz auch die zentrale Frage ungeklärt, welcher Person die Daten zuzuordnen wären und wem damit die aus dem Datenbesitz fliessenden Rechte zustehen würden. Das vorgeschlagene Abstellen auf den Skripturakt, verstanden als Erstellungsakt bzw. Datenspeicherung, hätte erhebliche Schwächen; namentlich würde dieser Ansatz dazu führen, dass der Datenbesitz nicht übertragen werden könnte: Da nämlich der Erstellungsakt für einen bestimmten Datensatz nicht wiederholt werden kann, liesse sich der an einem Datensatz begründete Besitz daran nicht mehr übertragen[105], sondern nur durch erneute Skriptur neu begründen. Damit würde mit jeder Verviel-

96 Statt vieler BGE 133 III 323, E. 5.1; BGE 132 III 122, E. 4.1; BGE 123 III 306, E. 4a.
97 BSK-OR I, Kessler, Art. 41 N 35. Siehe dazu auch hinten, C.III.4.
98 Solche Schutznormen sind etwa Art. 239 Abs. 2 (Schutz auch der Stromverbraucher: BGE 102 II 85, E. 5; sog. Kabelbruchfälle), Art. 305bis StGB (Geldwäscherei; BGE 133 III 323 E. 5.1) und Art. 159 StGB (Missbrauch von Lohnabzügen; BGer 4A_428/2014 vom 12. Januar 2015, E. 6.2).
99 BGE 133 III 323, E. 5.2; BSK-OR I, Kessler, Art. 41 N 35.
100 Siehe dazu vorn, C.II.1.
101 Siehe dazu vorn, C.II.1.
102 CR-CC II, Pichonnaz, Art. 919 N 16 f.; siehe auch Schmid/Hürlimann-Kaup, Rn. 118 f.; Steinauer, Rn. 204.
103 Schmid/Hürlimann-Kaup, Rn. 119; Steinauer, Rn. 213; CR-CC II, Pichonnaz, Art. 919 N 70; offen gelassen in Bezug auf Forderungen in BGer 4A_634/2012 vom 15. Januar 2013, E. 1.2.2; ablehnend: Fuchs, 35; Arnet/Eitel, Art. 919 N 6; ablehnend in Bezug auf Immaterialgüterrechte: BK-KGB, Stark/Lindenmann, Art. 919 N 71; Mauerhofer, 116; siehe auch Hilty, Lizenzvertragsrecht, 775, Fn. 206.
104 Hoeren, Jusletter 11. Mai 2020, insb. Rz. 24 f. und 37; ders., MMR 2019, 7 f.; s.a. Michl, NJW 2019, 2730 f.; s. aber auch das Urteil des Oberlandesgerichts Brandenburg vom 6. November 2019, in: NJW-RR 2020, 54, Rz. 42, wonach eine analoge Anwendung des Besitzesschutzes auf Daten nicht überzeugt; für die Schweiz: Eckert, SJZ 2016, 245 ff.
105 Siehe dazu Hoeren, Jusletter 11. Mai 2020, Rz. 16 ff. und 28 ff.; ders., MMR, 6 f.; demgegenüber will Eckert, SJZ 2016, 266, darauf abstellen, wer den Zugriff auf die zu beurteilenden, auf einen spezifischen Datenträger gespeicherten digitalen Daten auch tatsächlich steuern kann.

fältigung des Datensatzes ein neuer Datenbesitz entstehen, der Besitz würde also dupliziert[106], mit der Folge, dass eine potentiell unbegrenzte Vielzahl von Personen Besitz an einem inhaltlich identischen Datensatz hätte. Ein so verstandener Datenbesitz würde sich stark vom Konzept des Besitzes als faktische Herrschaft an einer Sache unterscheiden und es erscheint äusserst fraglich, ob sich die aus dem Besitz fliessenden Ansprüche – etwa der Anspruch auf Rückgabe der Sache nach Art. 927 ZGB – noch sinnvoll anwenden liessen[107]. Die Anwendung der Regeln des Besitzes auf Daten ist deshalb abzulehnen.

Für die Analyse der Zuordnung von Sachdaten im geltenden Recht scheidet der Besitz damit aus. Auf das Rechtsinstitut des Besitzes ist allerdings bei der Analyse der Rechtslage *de lege ferenda* näher einzugehen, zumal in der Lehre vereinzelt die Schaffung eines Datenbesitzes propagiert wird und nicht von vornherein ausgeschlossen werden kann, dass ein solches Rechtsinstitut geeignet sein könnte, eine angemessene Zuordnung von Sachdaten zu schaffen[108].

3. Geheimnisschutz

Die Bestimmungen über den Schutz von Fabrikations- und Geschäftsgeheimnissen (Art. 6 UWG und Art. 162 StGB) sowie Amts- und Berufsgeheimnissen (insb. Art. 320 ff. StGB) sanktionieren bei gegebenen Voraussetzungen Eingriffe in die faktische Herrschaft über Daten und dienen dadurch der rechtlichen Absicherung der tatsächlichen Kontrolle über diese Daten[109].

Nach **Art. 6 UWG** handelt unlauter, wer Fabrikations- oder Geschäftsgeheimnisse, die er ausgekundschaftet oder sonstwie unrechtmässig erfahren hat, verwertet oder anderen mitteilt. Als Geheimnis gilt dabei – in Übereinstimmung mit dem strafrechtlichen Geheimnisbegriff – die «besondere Kenntnis von Tatsachen, die nicht offenkundig oder allgemein zugänglich sind, an deren Geheimhaltung der Hersteller oder Geschäftsmann ein berechtigtes Interesse hat und die er tatsächlich geheim halten will»[110]. Ein solches Geheimnis muss ausserdem einen potentiellen Einfluss auf das Geschäftsergebnis des Unternehmens haben, es muss mithin «fabrikations- oder geschäftsrelevant» sein, damit es von Art. 6 UWG erfasst ist[111]. Allerdings schützt die Bestimmung nicht Unternehmensgeheimnisse an sich, sondern gewährt nur Ansprüche gegen deren Verwertung oder Mitteilung, nachdem die Geheimnisse ausgekundschaftet oder auf eine andere Weise unrechtmässig in Erfahrung gebracht worden sind[112]. Nach einer solchen unzulässigen Kenntniserlangung ist gemäss Art. 6 UWG zusätzlich eine Handlung erforderlich, die objektiv geeignet ist, den Wettbewerb zu beeinflussen[113]. Sind diese Voraussetzungen erfüllt, kann der Berechtigte den gesetzlich vorgesehenen Unterlassungs- und Beseitigungsanspruch (Art. 9 Abs. 1 lit. a und b UWG) geltend machen. Zudem bedroht Art. 23 Abs. 1 UWG die Verletzung von Art. 6 UWG auf Antrag mit Strafe.

Nach **Art. 162 StGB** wird auf Antrag mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft, wer ein Fabrikations- oder Geschäftsgeheimnis, das er infolge einer gesetzlichen oder vertraglichen Pflicht bewahren sollte, verrät, oder den Verrat für sich oder einen andern ausnützt. Der strafrechtliche Tatbestand ist mit Ausnahme der hier erforderlichen *vertraglichen oder gesetzlichen Geheimhaltungspflicht* weitgehend mit demjenigen von Art. 6 i.V.m. Art. 23 Abs. 1 UWG identisch[114]. Insbesondere stimmt, wie bereits erwähnt, der Begriff des Fabrikations- und Geschäftsgeheimnisses in Art. 6 UWG mit demjenigen in Art. 162 StGB überein[115]. Ein Verstoss gegen Art. 162 StGB indiziert die Widerrechtlichkeit einer Handlung im Sinn von Art. 41 OR[116] und kann damit dem Geschädigten die deliktsrechtlichen Ansprüche auf Unterlassung und Naturalrestitution vermitteln[117].

Im europäischen Recht wurde der Schutz von Geschäftsgeheimnissen mit der Richtlinie 2016/943 des

106 Hoeren, Jusletter 11. Mai 2020, Rz. 29.
107 Ebenso Hoeren, Jusletter 11. Mai 2020, Rz. 30.
108 Siehe dazu hinten, D.II.
109 Früh, digma 2019, 173.
110 SHK-UWG, Mabillard, Art. 6 N 8; BSK-UWG, Frick, Art. 6 N 162; BGer 4A_78/2014 vom 23. September 2014, E. 11.1; OGer ZH UE140269 vom 19. März 2015, E. 2.c.
111 SHK-UWG, Mabillard, Art. 6 N 13; BSK-UWG, Frick, Art. 6 N 15, je m.w.H.
112 BSK-UWG, Frick, Art. 6 N 5; siehe auch SHK-UWG-Mabillard, Art. 6 N 21.
113 SHK-UWG, Mabillard, Art. 6 N 21; BSK-UWG, Frick, Art. 6 N 53, je m.w.H.
114 BSK-StGB, Niggli/Hagenstein, Art. 162 N 52; SHK-UWG, Mabillard, Art. 6 N 5 m.w.H.
115 SHK-UWG, Mabillard, Art. 6 N 8; BSK-UWG, Frick, Art. 6 N 13; CHK-UWG, Ferrari Hofer/Vasella, Art. 6 N 3.
116 BK-OR, Brehm, Art. 41 N 39.
117 Siehe dazu vorn, C.III.1.

Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung harmonisiert *(Geschäftsgeheimnis-RL)*. Art. 2 Nr. 1 Geschäftsgeheimnis-RL definiert den Begriff «Geschäftsgeheimnis» als Informationen, die geheim sind und deshalb einen kommerziellen Wert haben und Gegenstand von den Umständen angemessenen Geheimhaltungsmassnahmen sind. Als geheim gelten dabei alle Informationen, die weder in ihrer Gesamtheit noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne weiteres zugänglich sind. Auch wenn dies in der Legaldefinition nicht explizit zum Ausdruck kommt, ist ausserdem erforderlich, dass das Geheimnis einen Unternehmensbezug aufweist und der Inhaber die Kontrolle rechtmässig inne hat[118]. Zwar muss auch unter Schweizer Recht der Geheimhaltungswille durch ausdrückliches oder konkludentes Verhalten wahrnehmbar sein[119], doch dürfte das Erfordernis der Richtlinie, dass das betreffende Unternehmen aktiv Geheimhaltungsmassnahmen ergreifen muss, darüber hinausgehen und mithin den Kreis der geschützten Geheimnisse stärker einschränken[120]. Gegen den rechtswidrigen Erwerb, die rechtswidrige Nutzung und die rechtswidrige Offenlegung von Geschäftsgeheimnissen[121] müssen die Mitgliedstaaten einen zivilrechtlichen Schutz vorsehen, der aus Massnahmen, Verfahren und Rechtsbehelfen bestehen muss (Art. 6 ff. Geschäftsgeheimnis-RL). Im Rahmen von Sachentscheiden müssen die Gerichte der Mitgliedstaaten zudem verschiedene Anordnungen und Abhilfemassnahmen erlassen, die inhaltlich der Durchsetzung von Beseitigungs- und Unterlassungsansprüchen entsprechen, und auch Schadenersatz zusprechen können (Art. 12 ff. Geschäftsgeheimnis-RL).

Weitere Straftatbestände zum Schutz von Geheimnissen finden sich im Schweizer Recht unter den strafbaren Handlungen gegen die Amts- und Berufspflicht, namentlich die *Verletzung des Amts- bzw. Berufsgeheimnisses* (Art. 320 f. StGB). Der Geheimnisbegriff ist dabei ähnlich wie derjenige bei Art. 6 UWG und Art. 162 StGB zu verstehen. Als Geheimnisse gelten auch nach Art. 320 f. StGB alle nicht allgemein bekannten oder zugänglichen Informationen, deren Schutz vor Preisgabe der Berechtigte will und an deren Geheimhaltung ein objektives Interesse besteht[122]. Geschützt sind dabei allerdings nur Geheimnisse, die einem Geheimnisträger in seiner amtlichen oder dienstlichen Eigenschaft bzw. infolge seines Berufes anvertraut worden sind oder die er in seiner Stellung bzw. Berufsausübung wahrgenommen hat. Zwar nicht immer, aber doch sehr oft, wird es sich bei Amts- und Berufsgeheimnissen um Personendaten handeln, die nicht Gegenstand dieser Studie sind. Ausserdem bedrohen diese Straftatbestände als *echte Sonderdelikte* ausschliesslich Geheimnisträger mit besonderen Eigenschaften mit Strafe. Die praktische Relevanz dieser Straftatbestände für die rechtliche Absicherung der tatsächlichen Kontrolle über Sachdaten ist deshalb gering. Sollten die Tatbestandsmerkmale einer dieser Strafnormen indes in einem konkreten Fall erfüllt sein, so ist davon auszugehen[123], dass die entsprechende Handlung auch widerrechtlich im Sinn von Art. 41 OR ist und damit deliktsrechtliche Ansprüche begründet.

4. Strafbare Handlungen gegen das Vermögen

Das Vermögensstrafrecht enthält eine Reihe von Bestimmungen, welche der rechtlichen Absicherung der faktischen Kontrolle über Daten dienen. Das gilt insbesondere für die Tatbestände der *unbefugten Datenbeschaffung* (Art. 143 StGB; sog. «Datendiebstahl»), des *unbefugten Eindringens in ein Datenverarbeitungssystem* (Art. 143bis StGB; sog. *Hacking*), der *Datenbeschädigung* (Art 144bis StGB) und des *betrügerischen Missbrauchs einer Datenverarbeitungsanlage* (Art. 147 StGB; sog. «Automatenbetrug»). Alle diese Bestimmungen wollen die Durchbrechung der faktischen Kontrolle verhindern, indem sie die entsprechenden Handlungen unter Strafe stellen[124].

118 Trebeck/Schulte-Wissermann, NZA 2018, 1177.
119 SHK-UWG, Mabillard, Art. 6 N 12; BSK-UWG, Frick, Art. 6 N 37, je m.w.H.
120 Siehe zum deutschen Recht Trebeck/Schulte-Wissermann, NZA 2018, 1177.
121 Art. 4 RL Geschäftsgeheimnis-RL definiert, was unter «rechtswidrigem Erwerb», «rechtswidriger Nutzung» und «rechtswidrige Offenlegung» von Geschäftsgeheimnissen zu verstehen ist.
122 BSK-StGB, Oberholzer, Art. 320 N 8; Donatsch, Isenring, Art. 320 N 3, je m.w.H.
123 Siehe mit Bezug auf Art. 321 StGB: BK-OR, Brehm, Art. 41 N 56g.
124 In der Lehre werden diese Bestimmungen auch «Computerstraftatbestände» genannt; siehe zu diesem Begriff BSK-StGB, Weissenberger, Art. 143 N 1.

Diesen Straftatbeständen ist gemeinsam, dass sie über vermögensstrafrechtliche Vorbilder im analogen Bereich verfügen wie z.B. den Diebstahl, die Sachbeschädigung oder den Hausfriedensbruch, die der Gesetzgeber unter den gebotenen Adaptierungen in den digitalen Bereich übertragen hat, nicht zuletzt um Strafbarkeitslücken zu schliessen[125].

So macht sich etwa strafbar, wer sich oder einem andern mit Bereicherungsabsicht[126] elektronisch gespeicherte oder übermittelte Daten beschafft, die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind (Art. 143 Abs. 1 StGB); dasselbe gilt für jedermann, der unbefugt solche Daten verändert, löscht oder unbrauchbar macht (Art. 144bis Ziff. 1 StGB). Daten sind nicht für eine Person bestimmt, wenn diese weder nach zivil- noch nach öffentlich-rechtlichen Bestimmungen über die Daten verfügen oder über ihre Verwendung bestimmen kann und die Daten auch nicht (unter bestimmten Bedingungen) benützen darf[127]. Gegen den unbefugten Zugriff gesichert sind Daten, wenn die getroffenen Sicherungsmassnahmen unter den Umständen des konkreten Falles üblicherweise ausreichen, um Unbefugte von den Daten fernzuhalten[128]. Nach demselben Massstab beurteilt sich bei Art. 143bis Abs. 1 StGB, ob ein Datenverarbeitungssystem besonders gegen den Zugriff gesichert ist[129]; auf Antrag bestraft wird nach dieser Bestimmung, wer über Datenübertragungseinrichtungen[130] unbefugterweise in ein fremdes und in diesem Sinn gesichertes Datenverarbeitungssystem eindringt. Strafbar macht sich sodann auch, wer mit Bereicherungsabsicht durch unrichtige, unvollständige oder unbefugte Verwendung von Daten auf einen elektronischen Datenverarbeitungs- oder Datenübermittlungsvorgang, etwa denjenigen eines Bankomaten, einwirkt und dadurch eine Vermögensverschiebung zum Schaden eines andern herbeiführt oder eine Vermögensverschiebung unmittelbar darnach verdeckt (Art. 147 Abs. 1 StGB); im Sinn eines ungeschriebenen Tatbestandsmerkmals ist dabei erforderlich, dass die Datenverarbeitung durch diese Einwirkung zu einem unzutreffenden Ergebnis gelangt[131], bspw. indem der Täter an einem Bankomaten mit einer gefälschten Bankkarte zu Lasten eines Dritten Geld bezieht.

Ein Verstoss gegen die hier angesprochenen Straftatbestände dürfte aufgrund ihrer Zugehörigkeit zum Vermögensstrafrecht regelmässig die Widerrechtlichkeit im Sinn von Art. 41 OR begründen[132]. Bei Vorliegen der übrigen Voraussetzungen stehen dem Geschädigten damit deliktsrechtliche Ansprüche auf Unterlassung und Naturalrestitution zu[133].

5. Verwertung fremder Arbeitsergebnisse

Neben dem Schutz von Fabrikations- und Geschäftsgeheimnissen (Art. 6 UWG)[134] vermittelt das UWG auch über die Tatbestände zur Verwertung fremder Leistungen (Art. 5 UWG) Rechtspositionen, die den Berechtigten eine rechtliche Absicherung der faktischen Herrschaft über Daten ermöglichen:

Art. 5 lit. a UWG erfasst die unbefugte Verwertung anvertrauter Arbeitsergebnisse wie Offerten, Berechnungen und Plänen, was als *direkte Vorlagenausbeutung* bezeichnet wird[135]. Der Tatbestand setzt voraus, dass das Arbeitsergebnis dem Verwertenden anvertraut und von diesem unbefugt verwertet worden ist. Als Arbeitsergebnisse werden in materialisierter Form fixierte Ergebnisse erfasst, die auf einer gewissen geistigen Anstrengung oder auf einem materiellen Aufwand beruhen[136]. Nicht erforderlich ist, dass das Arbeitsergebnis marktreif ist oder eine besondere Leistungshöhe erreicht[137]. Erfasst sind damit auch Entwürfe oder andere primär vorbereitende Arbeitsergebnisse. Als anvertraut gilt das Arbeits-

125 Siehe dazu etwa BSK-StGB, Weissenberger, Art. 143 N 1 und Art. 143bis N 1.
126 Eine Bereicherungsabsicht liegt etwa vor, wenn die Daten einen Verkehrswert haben, der Täter für die Datenbeschaffung bezahlt wird oder wenn die Daten auch nur einen vermögensrelevanten Gebrauchswert haben (BSK-StGB, Weissenberger, Art. 143 N 29 m.w.H.).
127 BSK-StGB, Weissenberger, Art. 143 N 15 m.w.H.; Schmid, § 2 N 68 und § 4 N 20 ff.
128 BSK-StGB, Weissenberger, Art. 143 N 19 m.w.H.; Schmid, § 4 N 30.
129 BSK-StGB, Weissenberger, Art. 143bis N 14.
130 Gemeint sind damit drahtverbundene Wege (Telefonnetz, elektrische Leitungen) oder drahtlose Kanäle der Datenfernübermittlung, z. B. UMTS, Funkverbindungen (BSK-StGB, Weissenberger, Art. 143bis N 17).
131 BSK-StGB, Fiolka, Art. 147 N 36.
132 Siehe dazu dazu Rey/Wildhaber, Rz. 860; BK-OR, Brehm, Art. 41 N 39; BSK-OR I, Kessler, Art. 41 N 35.
133 Siehe dazu vorn, C.III.1.
134 Siehe dazu vorn, C.III.3.
135 Heizmann/Loacker, Fahrländer, Vor Art. 5 N 1; BSK-UWG, Frick, Art. 5 N 26 f.
136 Heizmann/Loacker, Fahrländer, Art. 5 lit. a und b N 7; BSK-UWG, Frick, Art. 5 N 24.
137 BSK-UWG, Frick, Art. 5 N 26 und 28 Heizmann/Loacker, Fahrländer, Art. 5 lit. a und b N 9 f.

ergebnis, wenn es wissentlich und willentlich übergeben wurde[138]. Das unbefugte Verwerten beschreibt die wirtschaftliche (auch teilweise) Nutzbarmachung ohne Einverständnis des Erzeugers[139]. Weder das Anvertrauen noch das Verbot der Verwertung muss explizit erfolgen, beide Aspekte können sich auch aus den Umständen ergeben[140]. Sind Arbeitsergebnisse allgemein zugänglich oder allgemein bekannt, können sie nach der herrschenden Lehre nicht mehr anvertraut werden[141]. Ein Geheimnis im Sinn des straf- und wettbewerbsrechtlichen Geheimnisschutzes muss aber nicht vorliegen[142]. Aus den allgemeinen Anwendungsvoraussetzungen des UWG (Art. 1 und Art. 2 UWG) ergibt sich sodann, dass die Handlung objektiv geeignet sein muss, den Wettbewerb zu beeinflussen[143].

Art. 5 lit. b UWG erweitert den Anwendungsbereich von Art. 5 lit. a UWG auf die sog. *indirekte Vorlagenausbeutung*. Erfasst wird dabei die Verwertung fremder Arbeitsergebnissen im gerade vorstehend beschriebenen Sinn[144] durch Personen, die das Arbeitsergebnis nicht vom Erzeuger, sondern von einem Vermittler erhalten haben[145]. Voraussetzung ist, dass der Erzeuger das Arbeitsergebnis dem Vermittler anvertraut hat[146] und der Vermittler das Erzeugnis ohne Einverständnis des Erzeugers dem Verwertenden weitergegeben hat. Der Tatbestand ist nur erfüllt, wenn der Verwertende von der fehlenden Befugnis des Vermittlers zur Weitergabe Kenntnis hat oder haben müsste[147].

Art. 5 lit. c UWG erfasst die unmittelbare Übernahme und Verwertung marktreifer Arbeitsergebnisse Dritter, wenn diese als solche, ohne angemessenen eigenen Aufwand und durch ein technisches Reproduktionsverfahren erfolgt. Seit der Einführung dieser Norm im UWG von 1986 haben sich Lehre und Rechtsprechung eingehend mit den Tatbestandselementen auseinandergesetzt und es hat sich ein gewisser Grundkonsens herausgebildet[148].

Der Tatbestand erfasst nur die unmittelbare Übernahme mittels *technischer Reproduktionsverfahren*. Der Anwendungsbereich der Norm soll damit auf die typischen und besonders problematischen Erscheinungsformen des Erstellens identischer Kopien fremder Arbeitsergebnisse eingeschränkt werden[149]. Die erfassten Reproduktionsverfahren werden nicht definiert, die Norm erfasst aber selbstverständlich auch (und gerade) die Vervielfältigung digitaler Inhalte, etwa das Kopieren von Daten und Datenbanken[150].

Als *marktreif* gelten alle *Arbeitsergebnisse*, die sich ohne weiteres Zutun gewerblich verwerten lassen[151]. Verlangt wird ein materialisiertes Arbeitsergebnis, das aber auch unkörperlicher Natur sein kann[152], womit verschiedenartige Leistungsergebnisse (etwa Ton- und Bildaufnahmen, Fernsehsendungen und Computerprogramme, aber auch Daten und Datenbanken) erfasst sind. Das Tatbestandsmerkmal der Marktreife wird allerdings oft (zu) eng verstanden. Besonders deutlich zeigt dies ein jüngerer Entscheid des Handelsgerichts des Kantons Bern, nach welchem die unmittelbare Übernahme einer Zusammenstellung von Fragen für die Theorieprüfung für Motorfahrzeuglenker nach Art. 5 lit. c UWG nicht unzulässig sein soll, weil erst die unter Verwendung dieser Fragen entwickelte Lernsoftware für die Theorieprüfung marktreif sei[153]. Da Datenbestände zwar wirtschaftlich und strategisch äusserst wertvoll sein können, für sich genommen aber kaum je marktreife Arbeitsergebnisse im derart eng verstandenen Sinn darstellen, wird die Übernahme

138 Heizmann/Loacker, Fahrländer, Art. 5 lit. a und b N 14.
139 Heizmann/Loacker, Fahrländer, Art. 5 lit. a und b N 18 u. 20; BSK-UWG, Frick, Art. 5 N 49 und 53 f.
140 Heizmann/Loacker, Fahrländer, Art. 5 lit. a und b N 16; BSK-UWG, Frick, Art. 5 N 45.
141 Heizmann/Loacker, Fahrländer, Art. 5 lit. a und b N 17; SHK-UWG, Brauchbar Birkhäuser, Art. 5 N 15; BSK-UWG, Frick, Art. 5 N 46 f.; Jecklin, 109; Pedrazzini/Pedrazzini, Rn. 9.09.
142 Heizmann/Loacker, Fahrländer, Art. 5 lit. a und b N 17; BSK-UWG, Frick, Art. 5 N 29.
143 Siehe dazu auch Heizmann/Loacker, Fahrländer, Art. 5 lit. a und b N 21; BSK-UWG, Frick, Art. 5 N 53; BGE 131 III 384, E. 3.
144 Heizmann/Loacker, Fahrländer, Art. 5 lit. a und b N 26; zur deckungsgleichen Anwendung des Merkmals bei lit. a und lit. b auch SHK-UWG, Brauchbar Birkhäuser, Art. 5 N 21 f.
145 Heizmann/Loacker, Fahrländer, Art. 5 lit. a und b N 24.; BSK-UWG, Frick, Art. 5 N 58; SHK-UWG, Brauchbar Birkhäuser, Art. 5 N 17.
146 Dies ergibt sich zwar nicht unmittelbar aus dem Wortlaut des Gesetzes, ist in der h.L. aber anerkannt; siehe dazu Heizmann/Loacker, Fahrländer, Art. 5 lit. a und b N 25; BSK-UWG, Frick, Art. 5 N 58; SHK-UWG, Brauchbar Birkhäuser, Art. 5 N 17; Jecklin, 109.
147 Heizmann/Loacker, Fahrländer, Art. 5 lit. a und b N 26; BSK-UWG, Frick, Art. 5 N 59; SHK-UWG, Brauchbar Birkhäuser, Art. 5 N 18.
148 Thouvenin, sic! 2018, 598.
149 BSK-UWG, Arpagaus, Art. 5 N 81; Thouvenin, sic! 2018, 599.
150 BSK-UWG, Arpagaus, Art. 5 N 84; Heizmann/Loacker, Weber/Chrobak, Art. 5 lit. c N 15.
151 BGE 131 III 384, 389.
152 Thouvenin, sic! 2018, 598, m.w.H.
153 HGer, Bern, sic! 2016, 56 ff., 60, „Theorieprüfung für Motorfahrzeugfahrer".

und Verwertung von Daten regelmässig an diesem Tatbestandsmerkmal scheitern. Einen rechtlichen Schutz der faktischen Zuordnung von Daten vermag Art. 5 lit c UWG deshalb nur zu vermitteln, wenn man den Begriff der Marktreife – anders als die bisherige Rechtsprechung[154] – nicht allein am Markt für Endverbraucher ausrichtet, sondern auch vorgelagerte Märkte erfasst. Denn zwischen Unternehmen werden Daten und Datenbanken durchaus gehandelt, um mit ihrer Hilfe auf nachgelagerten Märkten Dienste und Produkte anzubieten. Im Verhältnis zwischen Unternehmen sind Daten und Datenbanken damit ohne weiteres regelmässig als marktreife Arbeitsergebnisse zu qualifizieren. Auch wenn Lehre und Rechtsprechung diesen Weg bisher nicht eingeschlagen haben, spricht vieles für eine solche, auch vorgelagerte Märkte einschliessende Auslegung des Tatbestandsmerkmals[155]. Folgt man diesem Ansatz, gewährt Art. 5 lit. c UWG einen weitgehenden rechtlichen Schutz der faktischen Zuordnung von Daten.

Die *Übernahme und Verwertung als solche* stand regelmässig im Fokus von Lehre und Rechtsprechung[156]. Dieses Tatbestandsmerkmal dient in erster Linie dazu, nur die unmittelbare Übernahme fremder Arbeitsergebnisse zu erfassen, blosse Nachahmungen von Leistungsergebnissen aber vom Zugriff des UWG auszuschliessen[157]. Wird das Kriterium des marktreifen Arbeitsergebnisses wie vorstehend ausgeführt auch auf vorgelagerte Märkte ausgedehnt, wird auch dieses Tatbestandsmerkmal regelmässig erfüllt sein.

Beim *angemessenen eigenen Aufwand* gilt es, den Aufwand des Unternehmens, welches die Daten faktisch kontrolliert, mit dem Aufwand des Dritten zu vergleichen, der die Daten übernommen und verwertet hat. Für die Prüfung dieses Tatbestandsmerkmals hat sich in Lehre und Rechtsprechung der sog. doppelte Aufwandvergleich etabliert[158]. Hierzu ist in einem ersten Schritt der Aufwand des Erstbewerbers für die Herstellung des Arbeitsergebnisses zu bestimmen und mit dem Aufwand des Zweitbewerbers für die Herstellung der Reproduktion zu vergleichen[159]. In einem zweiten Schritt ist der effektive Aufwand des Zweitbewerbers mit seinem hypothetischen Aufwand zu vergleichen, also mit dem Aufwand, den er gehabt hätte, wenn er das Arbeitsergebnis nicht übernommen, sondern selbst hergestellt hätte[160]. Ein angemessener eigener Aufwand des Zweitbewerbers fehlt, wenn sein effektiver Aufwand unangemessen geringer als der Aufwand des Erstbewerbers (erster Vergleich) und als sein hypothetischer Aufwand (zweiter Vergleich) ist[161]. Dies dürfte bei der Übernahme von Daten und Datenbanken regelmässig der Fall sein, zumal der Aufwand für das Sammeln und Aufbereiten von Daten sowie das Erstellen von Datenbanken meist beträchtlich, jener der Reproduktion hingegen in aller Regel gering ist. Anderes gilt allerdings auch hier, wenn man die Anwendung des Tatbestands mit der herrschenden Lehre und Rechtsprechung auf Arbeitsergebnisse einschränkt, die sich an Endverbraucher richten. Da derart eng verstandene Arbeitsergebnisse nur selten aus Daten oder Datenbanken bestehen, wird ein Unternehmen, das Daten von Dritten übernommen hat, regelmässig einen beträchtlichen Aufwand betreiben, um mithilfe der Daten ein Arbeitsergebnis zu produzieren, das den Endverbrauchern angeboten wird.

Damit ist klar, dass Art. 5 lit. c UWG nur, aber immerhin dann einen weitgehenden rechtlichen Schutz der faktischen Zuordnung von Daten vermittelt, wenn *Daten und Datenbanken selbst als markreife Arbeitsergebnisse verstanden* werden. Fokussiert man hingegen allein auf Produkte, die sich an Endverbraucher richten, wird der Tatbestand regelmässig nicht erfüllt sein, weil es an der

154 Thouvenin, sic! 2018, 606.

155 Thouvenin, sic! 2018, 606 und 609 f.; dazu auch BSK-UWG, Arpagaus, Art. 5 N 36, der Datenbanken zwar als Arbeitsergebnis im Sinn von Art. 5 lit. c UWG qualifiziert, als Beispiel allerdings auf ein Arzneimittelkompendium und auf online publizierte Immobilieninserate verweist, welche sich direkt an Endverbraucher richten und damit auch nach bestehender Praxis als marktreif qualifiziert werden können. S. zu den konkreten Fällen auch ZivGer Präs. BS, sic! 2004, E. 3b; BGE 131 III 384, E. 4.2.

156 Im Detail Thouvenin, sic! 2018, 599; Heizmann/Loacker, Weber/Chrobak, Art. 5 lit. c N 23 ff.

157 Heizmann/Loacker, Weber/Chrobak, Art. 5 lit. c N 23 m.w.H.; zum Grundsatz der Nachahmungsfreiheit siehe: BGE 139 IV 17, 20; BGE 131 III 384, 394; Jenny, Rn. 210 ff.; SHK-UWG, Brauchbar Birkhäuser, Art. 5 N 1.

158 BGE 131 III 384 E. 4.4.1; BSK UWG-Arpagaus, Art. 5 N 92; SHK-UWG, Brauchbar Birkhäuser, Art. 5 N 29; kritisch dazu Thouvenin, sic! 2018, 611 f.

159 Botschaft UWG, BBl 1983 II 1071; Baudenbacher, Baudenbacher, Art. 5 N 54; ähnlich Pedrazzini/Pedrazzini, Rn. 9.31; CR-LCD, Nussbaumer, Art. 5 N 84, 86.

160 Botschaft UWG, BBl 1983 II 1071; Heizmann/Loacker, Weber/Chrobak, Art. 5 lit. c N 54; Pedrazzini/Pedrazzini, Rn. 9.34; Baudenbacher, Baudenbacher, Art. 5 N 53, 55; ähnlich auch CR-LCD, Nussbaumer, Art. 5 N 84, 98.

161 SHK-UWG, Brauchbar Birkhäuser, Art. 5 N 29; Heizmann/Loacker, Weber/Chrobak, Art. 5 lit. c N 55; BSK-UWG, Arpagaus, Art. 5 N 101; CR-LCD, Nussbaumer, Art. 5 N 100; Pedrazzini/Pedrazzini, Rn. 9.35, wobei für sie auch ein „nur gerade minimaler Reproduktionsaufwand" für einen Verstoss gegen Art. 5 lit. c UWG spricht.

Übernahme eines marktreifen Arbeitsergebnisses fehlt und der Übernehmer einen hinreichenden Aufwand betreiben und das Arbeitsergebnis nicht als solches unmittelbar verwerten wird.

Neben den Spezialtatbeständen von Art. 5 und Art. 6 UWG ist stets auch die **Generalklausel des UWG (Art. 2 UWG)** anwendbar[162]. Diese mag in bestimmten Konstellationen greifen, in welchen die spezifischen Voraussetzungen der beiden Spezialtatbestände nicht erfüllt sind. Namentlich ist denkbar, die Generalklausel auf diejenigen Fälle anzuwenden, die von Art. 5 lit. c UWG wegen des einschränkenden Verständnisses des marktreifen Arbeitsergebnisses in der herrschenden Lehre und Rechtsprechung nicht erfasst werden. Im Übrigen sind für Daten und Datenbanken aber keine typischen Fallkonstellationen ersichtlich, die regelmässig nur mit der Generalklausel erfasst werden können.

22

IV. Vertragliche Zuordnung von Daten

Die Zuordnung von Daten kann auch durch vertragliche Vereinbarungen erfolgen. Solche Vereinbarungen wirken zwar nur *inter partes*, die Vertragsfreiheit ermöglicht aber, zwischen den Vertragsparteien eine Rechtslage zu schaffen, die – im Verhältnis zwischen diesen Parteien – einem Eigentum an Daten nahekommt. Das gilt in besonderem Mass für Sachdaten, weil Nutzung und Verfügung hier – im Gegensatz zu den Personendaten – grundsätzlich keinen Einschränkungen unterliegen.

Viele Verträge, welche die Übertragung und Nutzung von Daten zum Gegenstand haben, behandeln Daten im Vertrag wie Sachen[163]. Häufig halten Vertragsklauseln fest, dass das «Eigentum an den Daten» von einer Partei auf die andere «übertragen» werde oder dass «das Eigentum an den Daten beim Verkäufer» bleibe. Selbst wenn diese Klauseln rechtlich falsche Begriffe verwenden, beeinträchtigt dies ihre Gültigkeit nicht[164] und die Terminologie vermittelt klare Hinweise auf den Willen der Vertragsparteien, namentlich zur Frage, wer über vertraglich nicht geregelte, also residuale Nutzungen der Sachdaten entscheiden können soll.

V. Fazit

Die Analyse der Rechtslage *de lege lata* hat gezeigt, dass das geltende Recht eine Reihe von Normen enthält, die eine Zuordnung von Sachdaten ermöglichen und den Inhabern von Sachdaten eine weitgehende Kontrolle über «ihre» Daten vermitteln. Das heutige Recht ist zwar durch das Bestehen und Überlappen verschiedenartiger Schutzinstrumente geprägt, diese vermitteln den Inhabern von Sachdaten in der Summe aber eine Rechtsposition, die einem Eigentum an Sachdaten recht nahekommt. Zu unterscheiden ist dabei zwischen der Zuordnung durch absolute Rechte, dem rechtlichen Schutz der faktischen Zuordnung und einer Zuordnung durch vertragliche Vereinbarungen:

Bei den *absoluten Rechten* ist zunächst klarzustellen, dass das *Sachenrecht* keine Rechte an Sachdaten gewährt. Es bezieht sich nur, aber immerhin, auf die strukturelle Ebene und gewährt Eigentumsrechte an physischen Datenträgern. Die *Immaterialgüterrechte*, insb. das Patent- und Urheberrecht, gewähren dagegen einen weitgehenden, erga omnes wirkenden Schutz für gewisse Daten auf der semantischen Ebene, nämlich für diejenigen Informationen, welche die Schutzvoraussetzungen der jeweiligen Immaterialgüterrechte erfüllen. Die Repräsentation dieser Informationen in Form von Daten auf der syntaktischen Ebene ist vom immaterialgüterrechtlichen Schutz mitumfasst. Die *urheberrechtlichen Leistungsschutzrechte* bieten ebenfalls einen *erga omnes* wirkenden Schutz für die Ergebnisse bestimmter Leistungen. Indem die Leistungsschutzrechte auch die Festlegung der Leistungen in elektronischer Form erfassen, lassen sie sich (auch) als Ausschliesslichkeitsrechte an den entsprechenden Daten verstehen. In der Schweiz sind auf diese Weise (digitale) Festlegungen von Darbietungen ausübender Künstler,

162 Zur Anwendung der Generalklausel neben Art. 5 UWG: SHK-UWG, Brauchbar Birkhäuser, Art. 5 N 6; so wohl auch David/Jacobs, Rn. 365. Mit Blick auf Art. 5 lit. c UWG a.A. BSK-UWG, Arpagaus/Frick, Art. 5 N 112 ff., insb. N 114, die der Ansicht sind, Art. 5 lit. c UWG sei derart präzise formuliert, dass die Generalklausel bei Wegfallen eines Tatbestandsmerkmales nicht zum Tragen kommen könne; so auch Jecklin, 140; ZivGer Präs, sic! 2004, E. 3e. Weniger strikt aber BGE 131 III 384, E. 5.1. Zur Anwendung der Generalklausel neben Art. 6 UWG: SHK-UWG, Mabillard, Art. 6 N 4; kritisch BSK-UWG, Frick, Art. 6 N 56.

163 Siehe Zech, CR 2015, 140, zu den Vor- und Nachteilen des Status Quo.

164 Art. 18 Abs. 1 OR; siehe auch: Wiebe, GRUR Int. 2016, 878.

Aufnahmen auf Ton- oder Tonbildträgern und Sendungen geschützt. Ein *sui-generis*-Recht an Datenbanken gibt es in der Schweiz dagegen nicht.

Die *faktische Zuordnung* von Daten wird im schweizerischen Recht durch eine Reihe verschiedenartiger Bestimmungen rechtlich abgesichert. Im Vordergrund stehen dabei der Geheimnisschutz (Art. 162 StGB und Art. 6 UWG) und der Schutz gegen die unmittelbare Übernahme von Arbeitsergebnissen durch Art. 5 lit. c UWG. Ergänzend können verschiedene Bestimmungen des Strafrechts (insb. Art. 143 StGB und Art. 143bis StGB) zur Anwendung kommen. In allen diesen Fällen stehen dem Inhaber der Sachdaten weitgehende Rechtsansprüche zu, die teils gesetzlich vorgesehen sind (Art. 9 UWG) und sich teils durch eine geeignete Auslegung und Anwendung von Art. 41 OR ergeben. Der rechtliche Schutz der faktischen Zuordnung von Daten ist im geltenden Recht damit weit ausgebaut – auch wenn er sich nicht als kohärentes Gefüge, sondern als Flickenteppich präsentiert.

Eigentumsähnliche Rechtspositionen an Sachdaten lassen sich auch durch *vertragliche Vereinbarungen* schaffen. Diese wirken aber immer nur unter den Vertragsparteien *(inter partes)* und sie erfordern eine geeignete Gestaltung der entsprechenden Verträge.

Bei einer geeigneten Anwendung dieser Schutzmechanismen können die Inhaber von Sachdaten die *Nutzung dieser Daten in ähnlicher Weise kontrollieren wie beim Bestehen eines Eigentums an Sachdaten*. Zentrale Bedeutung kommt dabei dem Geheimnisschutz zu (insb. Art. 6 UWG und Art. 162 StGB), der es den Inhabern von Sachdaten erlaubt, die faktische Kontrolle über nicht allgemein zugängliche Sachdaten rechtlich abzusichern.

Werden die *Sachdaten* aber *öffentlich zugänglich* gemacht sei es durch die Inhaber selbst oder durch Dritte und greifen keine anderen Schutzinstrumente (insbesondere Urheberrechte, Leistungsschutzrechte oder das Verbot der unmittelbaren Verwertung von Art. 5 lit. c UWG), dann ist die Kontrolle über die Sachdaten «verloren» und kann nicht mehr wiedererlangt werden, weil der Geheimnisschutz nur greift, solange die Sachdaten auch geheim sind. Für öffentlich zugängliche Sachdaten mag damit ein gewisser Schutzbedarf bestehen, der nicht durch die Anpassung spezifischer Rechtsnormen abgedeckt werden kann. Ob dieser Bedarf ausgewiesen ist, erscheint allerdings fraglich. Es sind zwei Konstellationen zu unterscheiden: Hat der *Inhaber der Sachdaten diese selbst öffentlich zugänglich gemacht*, ist kaum einzusehen, weshalb die Rechtsordnung Mittel zur (Wiedererlangung der) Kontrolle dieser Daten zur Verfügung stellen soll, obwohl der Inhaber die Kontrolle freiwillig aufgegeben hat[165]. Sind die *Sachdaten von Dritten gegen den Willen des Inhabers öffentlich zugänglich gemacht* worden, erlauben es die Bestimmungen über den Geheimnisschutz nur, gegen diejenigen Personen vorzugehen, welche die Daten unrechtmässig offenbar haben; nach Offenbarung der Sachdaten erfolgende Nutzungen Dritter können aber nicht erfasst werden. Diese «Schutzlücke» könnte durch ein Eigentum an Sachdaten geschlossen werden. Diese Konstellation dürfte allerdings äusserst selten sein. Da der Wert von Sachdaten in aller Regel darin liegt, dass die Daten nicht öffentlich zugänglich sind, kann derjenige, welcher die Daten durch Geheimnisbruch erlangt hat, deren Wert auch nur realisieren, wenn er die Daten weiterhin geheim hält. In aller Regel dürfte deshalb schon die Interessenlage der Beteiligten sicherstellen, dass Sachdaten nicht gegen den Willen des Inhabers öffentlich zugänglich gemacht werden. Auch mit Blick auf diese Konstellationen besteht damit aus heutiger Sicht kein ausreichender Bedarf, welcher die Einführungen eines Eigentums an Sachdaten rechtfertigen könnte.

Sollte ein Schutzbedarf dennoch bejaht werden und sollte man (zugleich) Anreize für das öffentliche Zugänglichmachen von Sachdaten setzen wollen, könnte die Rechtsordnung – ähnlich wie im Patentrecht, aber unter Verzicht auf eine Prüfung und Registrierung – einen Schutz von Sachdaten dann (aber nur dann) gewähren, wenn diese Daten öffentlich zugänglich gemacht werden. Ob und inwiefern ein solcher Ansatz einen Beitrag zu einer besseren Kontrolle und Nutzung von Sachdaten leisten könnte, wäre allerdings ebenfalls erst noch näher zu untersuchen.

165 S. hierzu immerhin D.I.1.c).

D. Rechtslage *de lege ferenda*

Vor dem Hintergrund des geltenden Rechts stellt sich die Frage, ob die Zuordnung von Sachdaten zu den verschiedenen Rechtsträgern *de lege ferenda* angepasst werden sollte. Die Frage ist dabei breit zu verstehen, es geht also nicht nur um die Zuordnung eines einzelnen Sachdatums oder einer beschränkten Zahl von Sachdaten, sondern auch um die Zuordnung grosser Datenmengen, insbesondere von (strukturierten oder unstrukturierten) Datenbanken.

24

I. Dateneigentum

In der Rechtswissenschaft, aber auch in der Öffentlichkeit, wird seit einiger Zeit die Einführung eines Dateneigentums diskutiert. Die Debatte wurde in der Lehre durchaus lebhaft und kontrovers geführt[166], sie scheint aber mittlerweile ihren Kulminationspunkt überschritten, eine gewisse Reife erreicht und zu einem überwiegend geteilten Erkenntnisstand geführt zu haben. In der Schweiz ist aus heutiger Sicht jedenfalls einstweilen nicht mit der Einführung eines allgemeinen Dateneigentums zu rechnen[167]. Die vom Bundesrat eingesetzte Expertenkommission «Zukunft der Datenbearbeitung und Datensicherheit» hat sich nach dreijähriger Arbeit in ihrem ausführlichen Gesamtbericht vom 17. August 2018 gegen die Einführung eines Dateneigentums ausgesprochen[168] und der Bundesrat ist dieser Einschätzung bisher auch gefolgt[169].

Die Diskussion um die Einführung eines Dateneigentums betrifft verschiedene Arten von Daten, namentlich Personen- und Sachdaten. Es stellt sich deshalb die Frage, ob das Thema für unterschiedliche Daten differenziert anzugehen ist. Tatsächlich beschäftigen sich die meisten Publikationen denn auch (implizit oder explizit) entweder mit Personen- oder mit Sachdaten[170]. Das gilt auch für diese Studie, die sich auf die Frage nach der Zuordnung von Sachdaten konzentriert. Wie die Ausführungen zur Abgrenzung von Personen- und Sachdaten gezeigt haben, wären mit der Gewährung von Eigentumsrechten allein an Personen- oder an Sachdaten allerdings weitreichende Schwierigkeiten verbunden, weil Daten nicht als solche, sondern immer nur im jeweiligen Kontext als Personen- oder Sachdaten qualifiziert werden können[171]. Dies hat zur Folge, dass es bei der Gewährung von Eigentumsrechten an Sachdaten kaum möglich wäre, *ex ante* über das Bestehen von Eigentumsrechten an den jeweils in Frage stehenden Daten zu entscheiden und solche Rechte könnten auch – je nach Kontext – bestehen, fehlen, begründet werden oder wieder entfallen. Allein dies zeigt, *dass der Gesetzgeber mit der Einführung eines Eigentums an Sachdaten mehr Probleme schaffen als lösen würde*.

Hinzu kommt, dass sich die Einführung von Eigentumsrechten an Sachdaten angesichts der transversalen Bedeutung des Eigentums in der Rechtsordnung auf eine Vielzahl anderer Normen und Regelungen auswirken würde. Zu denken ist nicht nur an die Verflechtung

166 Für die Einführung eines Dateneigentums: Amstutz, AcP 2018, 438 ff.; Cheneval, CRISPP 2018, 1 ff.; Fezer, 28 ff.; ders., ZD 2017, 99 ff.; Säcker et al., Wagner, BGB § 823 N 294 ff.; Eckert, SJZ 2016, 245 ff.; ders., SJZ 2016, 265 ff.; Flückiger, AJP 2013, 837 ff.; Zech, GRUR 2015, 1159 f.; ders., CR 2015, 144 ff.; in der Tendenz ebenso: Schwartmann/Hentsch, PinG 2016, 120 ff.; Specht/Rohmer, PinG 2016, 127 ff.; Hoeren, MMR 2013, 486 ff.; Hess-Odoni, Jusletter 17. Mai 2004, Rz. 38 ff. Gegen die Einführung eines Dateneigentums: Bull, CR 2018, 425 ff.; Determann, ZD 2018, 503 ff.; ders., MMR 2018, 277 f.; ders., Hastings L. J. 2018, 1 ff.; Hugenholtz, Against ‚data property', 48 ff.; Janeček, CLSR 2018, 1039 ff.; Jentzsch, 1 ff.; Kühling/Sackmann, 7 ff.; Schmid/Schmidt/Zech, sic! 2018, 627 ff.; Schweitzer/Peitz, NJW 2018, 275 ff.; Stender-Vorwachs/Steege, NJOZ 2018, 1361 ff.; Ursic, 55 ff.; Weber/Thouvenin, ZSR 2018 I, 43 ff.; Paal/Hennemann, NJW 2017, 1697 ff.; Specht, ZGE 2017, 411 ff.; Spindler, ZGE 2017, 399 ff.; Schlinkert, ZRP 2017, 222 ff.; Benhamou/Tran, sic! 2016, 571 ff.; Drexl et al., Rz. 4 ff.; Hürlimann/Zech, sui generis 2016, 89 ff.; Kerber, IIC 2016, 759 ff.; ders., GRUR Int. 2016, 645 f.; ders., GRUR Int. 2016, 989 ff.; Wiebe, GRUR Int. 2016, 881 ff.; Hornung/Goeble, CR 2015, 271 ff.; Dorner, CR 2014, 626 ff.; für Sachdaten ebenso Kohler, sic! 2020, 412; in der Tendenz ebenso: Berberich/Golla, PinG 2016, 175 f.; Specht, CR 2016, 294 ff.; Żdanowiecki, 28 f.

167 Gegen die Einführung eines Dateneigentums in der Schweiz: UVEK/BAKOM, 3 f.; Economiesuisse, 5 ff.; Botschaft DSG 2017, 6988; scheinbar anders aber die Ergebnisse einer Studie des BAKOM (Jarchow/Estermann, 52), worin sich 75% der Befragten für neue Eigentums- oder Nutzungsrechte im Bereich der personenbezogenen Daten aussprechen.

168 EFD, Datenbearbeitung und Datensicherheit, 107 ff.

169 Bundesrat, Blockchain-Bericht, 47.

170 Spezifisch für Sachdaten: Thouvenin/Früh/Lombard, SZW 2017, *passim*; Kohler, sic! 2020, *passim*; Wiebe/Schur, ZUM 2017, *passim*; Europäische Kommission, Aufbau einer Europäischen Datenwirtschaft, insb. 9 ff.; Żdanowiecki, *passim*; Hugenholtz, System of Intellectual Property Law, *passim*; Kerber, IIC 2016, *passim*. Spezifisch für Personendaten: Schmidt, *passim*; dies., digma 2019, *passim*; Cheneval, CRISPP 2018, *passim*; Naumer, *passim*; Esken, *passim*. Ebenfalls mit einem Schwerpunkt auf den Personendaten Jentzsch, *passim*; Sattler, *passim*; Richter, insb. 552 ff.; Richter/Hilty, 251 ff.; Bull, CR 2018, *passim*; Ethics Advisory Group, *passim*; Landreau et al., *passim*; Janeček, CLSR 2018, *passim*; Hagen, APuZ 2018, *passim*; Sprecher, ZBJV 2018, *passim*; Horn/Reinhardt, insb. 3 ff., in Bezug auf Datenhoheit; Thouvenin, SJZ 2017, *passim*; Fezer, ZD 2017, *passim*; Buchner, ZGE 2017, *passim*; Wandtke, MMR 2017, *passim*; Purtova, LIT 2015, *passim*.

171 Siehe dazu vorn, B.2.

des Eigentums mit unzähligen Fragen des Zivilrechts, sondern auch an das Verfassungsrecht (Eigentumsgarantie), Strafrecht (Vermögensdelikte), Verwaltungsrecht (Enteignung), Zivilprozessrecht (Zuständigkeiten) sowie Schuldbetreibungs- und Konkursrecht (Aussonderung). Allein die unzähligen Folgewirkungen der Einführung eines Dateneigentums zeigen deutlich, dass eine solche Rechtsfigur nur geschaffen werden sollte, wenn ein entsprechender Bedarf ausgewiesen ist und keine weniger eingreifenden Alternativen erkennbar sind.

Dieser Bedarf lässt sich aus zwei Perspektiven untersuchen: Einerseits kann die Frage auf einer theoretischen Ebene angegangen werden. Für die Einführung eines Dateneigentums werden im Schrifttum denn auch überwiegend theoretische Argumente angeführt, etwa die Internalisierung externer Effekte und die damit verbundene Förderung der Effizienz von Märkten[172], das Schaffen von Rechtssicherheit durch die Zuweisung von Eigentumsrechten[173] und die Stärkung der Autonomie der Bürger[174]. Andererseits lässt sich die Frage auch aus einer praktischen Perspektive betrachten. Im Vordergrund stehen dabei konkrete Probleme, die mit den bestehenden Rechtsregeln nicht überzeugend gelöst werden können.

Für eine umfassende Analyse sind beide Perspektiven unverzichtbar. Entscheidend muss aber letztlich die praktische Perspektive sein, weil die lediglich theoretische Wünschbarkeit eines Eigentums an Sachdaten keinen hinreichenden Handlungsbedarf zu begründen vermag. Dies gilt umso mehr, als ein solches Eigentum angesichts seiner weitreichenden Bedeutung nicht mittels analoger Anwendung bestehender Rechtsregeln durch die Gerichte, sondern nur durch den Gesetzgeber geschaffen werden könnte. Und dieser wird eine solche Rechtsfigur nicht allein wegen einer allfälligen theoretischen Wünschbarkeit einführen.

1. Theoretische Perspektive

a) Überblick

Als Ausgangspunkt der nachfolgenden Analyse ist klarzustellen, dass ein Dateneigentum nicht propagiert werden kann, ohne die Einführung einer solchen Rechtsfigur zu rechtfertigen. Zwar könnte ein Dateneigentum für die Rechteinhaber positive Wirkungen haben. Ein solches Eigentumsrecht kann sich aber nicht nur für diejenigen, denen es entgegengehalten wird, sondern auch für die Gesellschaft insgesamt als nachteilig erweisen, weil die Nutzung von Daten durch Eigentumsrechte erschwert oder gar verunmöglicht wird. Die *Einführung eines Dateneigentums bedarf deshalb einer vertieften Rechtfertigung*. Die theoretischen Argumente, die in der Literatur für (und gegen) ein Dateneigentum ins Feld geführt werden, lassen sich dabei wie folgt gruppieren und bewerten:

Einige Autoren erblicken die Rechtfertigung eines Dateneigentums darin, dass *Daten einen Wert* haben, der zu schützen sei[175]. Dieses Argument vermag aber nicht zu überzeugen, weil es die fundamentale Frage offen lässt, wie dieser Wert am besten genutzt werden soll. Für die Einführung eines Eigentumsrechts würde der Wert von Daten nur sprechen, wenn sich ein solches Recht positiv auf deren Schaffung und Nutzung auswirken würde. Dies ist allerdings durchaus zweifelhaft und bedarf der näheren Untersuchung[176].

Andere Autoren machen in Anlehnung an die Arbeitstheorie von John Locke[177] geltend, Daten seien Arbeitsprodukte und der Hersteller des Produkts müsse deshalb ein Recht an den produzierten Daten haben[178]. Diesem Ansatz ist entgegen zu halten, dass Daten meist als Folge einer anderen Tätigkeit (bspw. das Fahren eines Autos oder die Nutzung eines *Social Media*-Dienstes) anfallen, in den meisten Fällen aber nicht spezifisch «produ-

172 Wiebe, GRUR Int. 2016, 881; Jentzsch, 15. In diesem Sinn ist auch die von der Europäischen Kommission präsentierte Option zu verstehen, zum Aufbau einer Europäischen Datenwirtschaft, ein Recht des «Datenerzeugers» einzuführen, Europäische Kommission, Aufbau einer Europäischen Datenwirtschaft, 9 ff. Umfassend zur Problematik, aber grundsätzlich gegen eine Einführung eines Dateneigentums zudem Schweitzer/Peitz, NJW 2018, 275 ff.

173 Fezer, 58; Zech, CR 2015, 145.

174 Amstutz, AcP 2018, 524 ff.; Fezer 21 ff.; Landreau et al., 25; Cheneval, CRISPP 2018, 10 f.; Bauer et al., 22.

175 Briner, Jusletter IT 21. Mai 2015, *passim*; Hoeren, EIPR 2014, 753; ders, sic! 2014, 217; Eckert, SJZ 2016, 246.

176 Siehe dazu hinten D.I.1.b)(ii).

177 Locke, 29 ff. (Kapitel 5. Das Eigentum); Thouvenin, Systematisierung, 321.

178 Amstutz, AcP 2018, 525 f.; Fezer, 45 ff., insb. 49 ff., welcher von «verhaltensgenerierten Daten» spricht. Moore/Himma, Kapitel 3.3, bezeichnen dies als Locke'sche Begründung.

ziert» werden. Daten sind damit meist Nebenprodukte einer anderen Tätigkeit und nur relativ selten zielgerichtet erstellte Produkte im Sinn der Arbeitstheorie[179].

Drei weitere Ansätze sind ungleich differenzierter und gewichtiger: Zum einen wird geltend gemacht, ein Eigentumsrecht an Daten stärke die Autonomie der Bürger, welche durch die neuen Nutzungsformen von Daten bedroht sei und die Einführung eines solchen Rechts würde zu einem fairen Ausgleich der mit Daten generierten Werte zwischen Bürgern und Unternehmen führen[180]. Dieses Argument greift allerdings, wenn überhaupt, dann jedenfalls nur für Personendaten[181], weshalb es nachfolgend nicht aufgegriffen wird. Zum andern wird argumentiert, dass Unternehmen den Profit aus der Nutzung von Daten internalisieren, während sie die Kosten dieser Nutzung – insbesondere die damit verbundenen Eingriffe in die Privatsphäre – auf die betroffenen Personen überwälzen und damit externalisieren[182]. Dies führe zu einer Fehlallokation von Kosten und Nutzen und damit zu einem Marktversagen[183]. Beklagt wird dabei namentlich, dass die Nutzer von den Unternehmen kein angemessenes Entgelt für das Überlassen ihrer Daten erhalten[184]. Auch dieser Ansatz kann allerdings, wenn überhaupt, nur als Argument für die Einführung von Eigentumsrechten an Personendaten dienen[185], weshalb auch dieses Argument hier nicht untersucht wird. Schliesslich wird drittens vertreten, dass ein Eigentum an Daten nur eingeführt werden sollte, wenn ein solches Recht ein Marktversagen verhindern oder korrigieren könnte. Dieser Ansatz greift auch für Sachdaten und ist deshalb nachfolgend näher zu untersuchen.

b) Marktversagen

Die Begründung der Einführung eines Dateneigentums als Mittel zur Korrektur von Marktversagen folgt klassischen rechtstheoretischen Überlegungen: Die Frage, ob ein subjektives Recht ein Marktversagen korrigieren kann, ist in der europäischen Rechtstradition längst zur wichtigsten Begründung von Eigentumsrechten geworden[186]. Dieser utilitaristische Ansatz[187] wird insbesondere im Zusammenhang mit Immaterialgüterrechten angerufen[188], ist aber auch auf alle anderen Eigentumsrechte anwendbar[189]. Dieser Begründungsansatz steht deshalb nachfolgend im Vordergrund.

(i) Allgemein

Ein Marktversagen liegt vor, wenn der Markt ein bestimmtes Gut nicht oder nicht im erwünschten Umfang produziert oder nutzt, obwohl dies im Interesse der Gesellschaft liegen würde. Bei Daten besteht die Gefahr eines solchen Marktversagens, weil es sich um *ihrer Natur nach öffentliche Güter* handelt, die am Markt typischerweise nur produziert werden, wenn die Rechtsordnung ausreichende Anreize für entsprechende Investitionen setzt, insbesondere durch die Gewährung von Ausschliesslichkeitsrechten[190].

Als öffentliche Güter werden Güter bezeichnet, die in ihrer Nutzung nicht rivalisierend und nicht ausschliessbar sind[191]. *Nicht-rivalisierend* bedeutet, dass die Nutzung des Gutes durch eine Person diejenige durch eine (oder mehrere) andere Person(en) nicht beeinträchtigt[192]. Gerade dies trifft auf Daten zu, die gleichzeitig von einer Vielzahl von Personen genutzt werden können, ohne dass einem Nutzer aufgrund der Nutzung durch einen anderen ein Nachteil entstehen würde. *Nicht ausschliessbar* bedeutet, dass niemand die Nutzung des in

179 Als Beispiel zu nennen sind etwa Forschungsdaten, die bspw. im Rahmen von Experimenten produziert werden oder spezifische Messdaten.
180 Cheneval, CRISPP 2018, 2 ff,
181 Thouvenin/Weber/Früh, Datenpolitik, 42 ff.
182 Purtova, LIT 2015, 84; Dorner, CR 2014, 626 m.w.H. in Fn. 117.
183 So Swire/Litan, 8; Laudon, Communications of the ACM 1996 No. 9, 99; Kilian, CRi 2012, 172.
184 Horn/Reinhardt, 4 f.; Denga, NJW 2018, 1375; Kühling/Sackmann, 25 ff. möchten eine gerechtere Partizipation durch eine «stärkere Akzentuierung der datenschutzrechtlichen Einwilligung erzielen». Auch Cohen, 26 f., vertritt diese Position, sieht aber ein Dateneigentum nicht als Lösung. In der Studie des BAKOM (Jarchow/Estermann, 50) gaben über 90% der Befragten an, keine faire Gegenleistung für ihre Daten zu erhalten.
185 Näheres dazu: Thouvenin/Weber/Früh, Datenpolitik, 42 ff.
186 Siehe dazu Dorner, CR 2014, 625 f.
187 Moore/Himma, *passim*.
188 Siehe dazu statt vieler: Thouvenin, Systematisierung, 287 ff., 322 ff., 337 ff., 358 ff., 385, 402 ff., jeweils m.w.H.
189 Für Know-How, Dorner, 373 ff.
190 Statt vieler Heller, Harv. L. Rev. 1998, 621 ff.; Heller/Eisenberg, Science 1998, 698 ff. und Ullrich, GRUR Int. 1996, 565.
191 Thouvenin/Weber/Früh, Datenpolitik, 9.
192 Thouvenin/Weber/Früh, Datenpolitik, 9.

Frage stehenden Gutes verhindern kann[193]. Dies gilt für Daten allerdings nur, wenn die Rechtsordnung den betroffenen Personen keine Rechte zuweist, die es ihnen ermöglichen, Dritte von der Nutzung der Daten auszuschliessen. Für Personendaten vermittelt das Datenschutzrecht den betroffenen Personen in vielen Konstellationen die Möglichkeit, die Nutzung «ihrer» Daten durch Erteilung einer Einwilligung zu erlauben oder durch deren Verweigerung oder das Erheben von Widerspruch zu verbieten[194]. Die Nutzung von Sachdaten kann dagegen in vielen Fällen nicht allein durch rechtliche, sondern nur durch eine Kombination von faktischen und rechtlichen Mitteln verhindert werden, namentlich durch Geheimhaltung[195].

Weil ihrer Natur nach öffentliche Güter von einer Vielzahl von Personen genutzt werden können, ohne dass die Nutzung durch eine Person diejenige durch eine andere beeinträchtigt, sollten Eigentumsrechte an Daten nur geschaffen werden, wenn ein Marktversagen vorliegt, das sich durch die Einführung eines Dateneigentums beheben lässt. Ein solches Marktversagen kann auf zwei Ebenen bestehen: bei der Produktion von Daten und bei Transaktionen von Daten[196].

(ii) Produktion von Daten

Das Argument, dass ein Eigentum an Daten eingeführt werden müsse, um ausreichende Anreize für die Produktion von Daten zu setzen, findet so gut wie keine Stütze im Schrifttum. Nur vereinzelt wird die Meinung vertreten, dass ein Dateneigentum Anreize für das Sammeln von Daten setzen würde[197]. In der Tat gibt es denn auch keine Hinweise darauf, dass sich das Fehlen eines Dateneigentums in nachteiliger Weise auf die Produktion oder das Sammeln von Daten auswirken würde. Vielmehr wird zu Recht darauf hingewiesen, dass das Sammeln und Produzieren von Daten keiner besonderen Anreize bedarf, weil Daten in aller Regel als Nebenprodukt anderer Aktivitäten anfallen[198].

Dass die Rechtsordnung keine Anreize für die Produktion von Daten setzen muss, zeigt auch das seit Jahren ungebremst anhaltende Wachstum der Datenmenge: Während im Jahr 2010 weltweit erst 0.2 Zettabytes an Daten produziert wurden, wird angenommen, dass diese Zahl im Jahr 2015 schon 15.5 Zettabytes erreicht hat. Schätzungen gehen davon aus, dass im Jahr 2020 59 und nur vier Jahre später sogar 149 Zettabytes produziert werden[199]. Gemäss einer Studie von IDC wird der Markt für *Big Data Analytics* bis zum Jahr 2022 ein Volumen von 274.3 Milliarden Dollar erreicht haben, bei einem jährlichen Wachstum von schätzungsweise 13.2 % zwischen 2019 und 2022[200].

Damit erscheint klar, dass hinsichtlich der Produktion von Daten kein Marktversagen besteht.

(iii) Transaktion von Daten

Die Einführung eines Eigentumsrechts an Daten könnte sich positiv auf Transaktionen von Daten auswirken. Die Befürworter eines solchen Rechts argumentieren jedenfalls, dass bei einer Zuordnung der Daten durch Eigentumsrechte ein klarer Ausgangspunkt für Verhandlungen geschaffen und damit die *Rechtssicherheit* erhöht werden könnte[201]. So mögen sich bspw. Nutzer und Hersteller von Geräten bisweilen darüber streiten, wer Zugang zu den von einem Gerät gesammelten Daten hat und die Daten nutzen darf. Beispiele solcher Konfliktsituationen finden sich etwa bei Sachdaten, die von Autos oder Landwirtschaftsgeräten erzeugt werden.

Allerdings wird die Ausgangslage bei Vertragsverhandlungen in aller Regel bereits durch die *faktische Herrschaft* einer potentiellen Vertragspartei über die in Frage stehenden Daten bestimmt. Eine rechtliche Zuordnung mithilfe eines Eigentumsrechts könnte die

193 Thouvenin/Weber/Früh, Datenpolitik, 9.
194 Thouvenin/Weber/Früh, Datenpolitik, 27.
195 Thouvenin/Weber/Früh, Datenpolitik, 9.
196 Zudem wird bisweilen darauf hingewiesen, in der bereits erwähnten (D.I.1.a)) ungerechten Allokation von Kosten und Nutzen der Daten, könne man ebenfalls eine Art Marktversagen erkennen, siehe dazu Thouvenin/Weber/Früh, Datenpolitik, 42 ff. Weil dieses Argument aber ausschliesslich im Kontext von Personendaten vorgebracht wird, muss hier nicht weiter darauf eingegangen werden.
197 Zech, CR 2015, 144.
198 Bull, CR 2018, 428; Wiebe, GRUR Int. 2016, 883.
199 Arne Holst: Volume of data/information created worldwide from 2010 to 2024 (in zetabytes), <https://www.statista.com/statistics/871513/worldwide-data-created/>. Zuletzt besucht am 10. August 2020.
200 IDC Forecasts Revenues for Big Data and Business Analytics Solutions Will Reach $189.1 Billion This Year with Double-Digit Annual Growth Through 2022, 4. April 2019, < https://www.idc.com/getdoc.jsp?containerId=prUS44998419>, zuletzt besucht am 14. August 2020.
201 Zech, CR 2015, 145.

Transaktionskosten deshalb nur senken, wenn keine faktische Herrschaft besteht. In diesen Fällen würde ein Dateneigentum allerdings den Bedarf nach einer Transaktion überhaupt erst begründen, weil die Sachdaten ohne ein solches Recht frei genutzt werden könnten. Von einer Reduktion von Transaktionskosten kann deshalb auch (und gerade) beim Fehlen einer faktischen Herrschaft keine Rede sein.

Die Befürworter eines Dateneigentums machen bisweilen geltend, dass Eigentumsrechte zu einer gewissen Standardisierung führen und damit die *Verhandlungskosten*, namentlich die Kosten der Aushandlung und Formulierung von Verträgen, reduzieren könnten[202]. Dieses Argument lässt sich zwar nicht von der Hand weisen. Allerdings kann diese Wirkung auch durch die Verwendung von standardisierten Verträgen erreicht werden[203]. Viele Unternehmen stützen die Nutzung von Daten, insbesondere aber nicht nur bei Personendaten, denn auch längst auf Standardverträge, namentlich in Form von Allgemeinen Geschäftsbedingungen (AGB). Eine weitere Senkung der Verhandlungskosten durch Einführung eines Dateneigentums erscheint deshalb nicht erforderlich.

Begründet wird ein erhoffter positiver Effekt eines Dateneigentums auf Transaktionen von Daten teilweise auch mit dem sog. *«disclosure paradox»*[204]. Dieses besteht, wenn Informationen vor dem Abschluss einer Vereinbarung über ihre Veräusserung oder Lizenzierung zumindest bis zu einem gewissen Grad offenbart werden müssen, damit der Erwerber oder Lizenznehmer den Wert der Informationen einschätzen kann. Durch die Offenbarung erlangt der potentielle Vertragspartner allerdings bereits Kenntnis von den Informationen, womit kein Grund mehr besteht, für den Erwerb oder das Recht zur Nutzung der Informationen ein Entgelt zu zahlen. Anders als bei geheimem Know-how verhindert oder erschwert das *«disclosure paradox»* den Rechtsverkehr bei Daten allerdings kaum, weil bei der Vertragsverhandlung in aller Regel die Daten nicht zugänglich gemacht werden müssen, sondern lediglich deren Art und Gehalt hinreichend genau zu umschreiben ist. Hinzu kommt, dass die Nutzung von Daten – anders als bei Know-how – in aller Regel einen tatsächlichen Zugriff auf die Daten erfordert. Das Argument, dass Daten zur Überwindung des *«disclosure paradox»* eines rechtlichen Schutzes bedürfen, überzeugt deshalb nicht.

Selbst wenn man annehmen würde, dass die Einführung eines Dateneigentums Transaktionen von Daten in bestimmten Konstellationen vereinfachen und damit fördern könnte[205], würde eine Reduktion von Transaktionskosten jedenfalls nur eintreten, wenn klar wäre, wer *Inhaber der Eigentumsrechte* und damit potentieller Transaktionspartner ist. Gerade dieser zentrale Punkt ist bisher aber ungeklärt, nicht nur, aber auch für Sachdaten[206]. Selbst wenn sich diese zentrale Frage theoretisch entscheiden und gesetzlich regeln liesse, dürfte in der Praxis oft umstritten bleiben, wem die Rechte an den Daten in einer konkreten Konstellation zustehen, weil regelmässig eine Vielzahl von Akteuren beim Sammeln, Speichern und Aufbereiten von Daten beteiligt ist[207]. Die Einführung von Eigentumsrechten an Daten dürfte deshalb zu *Streitigkeiten* über die Frage der Rechteinhaberschaft führen, die jedenfalls dann hohe Kosten verursachen würden, wenn sie vor Gericht ausgetragen werden[208].

Zudem würde die Einführung eines Dateneigentums dazu führen, dass die potentiellen Nutzer jeden Eigentümer der zu nutzenden Daten identifizieren und mit diesem eine Vereinbarung über die Nutzung der Daten aushandeln müssten. Dies hätte enorme *Such- und Verhandlungskosten* zur Folge[209] und könnte dazu führen, dass mögliche Nutzungen wegen der prohibitiv hohen Transaktionskosten unterbleiben würden.

Zusammenfassend erscheint es damit zwar nicht ausgeschlossen, dass ein Dateneigentum in bestimmten

202 Fairfield, Boston Univ. L. Rev. 2005, 1051.
203 Hinzuweisen ist bspw. auf die von Michel Jaccard und Juliette Ancelle ausgearbeiteten Musterverträge, welche die Transaktionskosten beim Handel mit Sachdaten zwischen KMU senken sollen. Zusammen mit der vorliegenden Studie (und weiteren Beiträgen) bilden diese Musterverträge die Grundlage für die Ausarbeitung eines Berichts des IGE an den Bundesrat.
204 Zech, CR 2015, 145; siehe hierzu grundlegend Arrow, *passim*, sowie Dorner, 415.
205 Fairfield, Boston Univ. L. Rev. 2005, 1051, wobei der Fokus hier auf virtuellem Eigentum liegt.
206 Siehe dazu: Weber/Thouvenin, ZSR 2018 I, 60; Wiebe, GRUR Int. 2016, 883; Bräutigam/Klindt, 23 ff.
207 Hierzu statt vieler Wiebe, GRUR Int. 2016, 883; betr. Personendaten Schmidt, digma 2019, 181.
208 Fröhlich-Bleuler, Jusletter 6. März 2017, Rz. 23.
209 Samuelson, Stanford L. Rev. 2000, 1135; Fröhlich-Bleuler, Jusletter 6. März 2017, Rz. 25, mit dem Hinweis, dass dies eher für die Einführung eines Haftungsregimes als eines Dateneigentums spräche.

Konstellationen einen Beitrag zur Reduktion von Transaktionskosten zu leisten vermag, zumindest wenn es gelingen sollte, die Frage der Rechteinhaberschaft überzeugend zu lösen. Diesem Potential zur Reduktion steht allerdings auch eine Erhöhung der Transaktionskosten gegenüber, namentlich weil Sachdaten nach Einführung eines Dateneigentums nicht mehr frei, sondern nur noch mit Zustimmung des jeweiligen Rechteinhabers genutzt werden können.

Insgesamt lässt sich die Einführung eines Eigentums an Sachdaten deshalb nicht durch eine allfällige Reduktion von Transaktionskosten und eine damit einhergehende, bessere Nutzung von Sachdaten rechtfertigen. Dass Daten auf dem Markt längst im grossen Umfang übertragen und für Nutzungen durch Dritte lizenziert werden, macht vielmehr deutlich, dass solche Transaktionen auch ohne Eigentumsrechte durchgeführt werden können. Die faktische Ausschliessbarkeit scheint hierfür offenbar zu genügen[210].

c) Offenlegung von Daten und Datenbanken und *data sharing*

Ein weiterer Begründungsansatz für ein – wie auch immer geartetes – Eigentum an Sachdaten könnte darin liegen, dass die Gewährung von Eigentumsrechten die Inhaber von Sachdaten (und damit v.a. die Unternehmen der Datenwirtschaft) dazu bringen könnte, ihre Sachdaten öffentlich zugänglich zu machen. Die Rechtsordnung könnte bspw. – ähnlich wie im Patentrecht, aber unter Verzicht auf eine Prüfung und Registrierung – einen Schutz von Sachdaten dann – aber nur dann – gewähren, wenn diese Daten von deren Inhabern öffentlich zugänglich gemacht werden. Dadurch würde aus Sicht der Unternehmen die Geheimhaltung der Daten weniger attraktiv und die Offenlegung könnte eine breitere Nutzung der Sachdaten ermöglichen, wie dies verschiedentlich unter dem Stichwort des *data sharing* gefordert wird[211]. Solche gesetzgeberischen Massnahmen sollte jedoch erst in Erwägung gezogen werden, wenn sich erweisen würde, dass Sachdaten trotz aller möglicher Fördermassnahmen[212] nicht im erwünschten Mass zugänglich gemacht werden. Zudem müsste vorab vertieft wissenschaftlich untersucht werden, ob sich die Einführung von Eigentums- oder anderen Ausschliesslichkeitsrechten an (öffentlich zugänglich gemachten) Sachdaten rechtfertigen lässt.

Der Vollständigkeit halber sei darauf hingewiesen, dass derselbe Effekt auch durch die Gewährung von Datenzugangsrechten erzielt werden könnte, mit denen der Allgemeinheit oder bestimmten Dritten die Nutzung – an sich faktisch kontrollierter – Sachdaten ermöglicht würde[213].

2. Praktische Perspektive

a) Vorbemerkung

Der Bedarf nach einem Eigentum an Sachdaten wäre ausgewiesen, wenn das bestehende Recht konkrete praktische Probleme nicht angemessen lösen und nur die Einführung eines Eigentumsrechts Abhilfe schaffen könnte. Angesichts der transversalen Bedeutung des Eigentums[214] für die Rechtsordnung erscheint ein derart weitreichender Schritt allerdings nur angezeigt, wenn so viele und bedeutsame praktische Probleme bestehen sollten, dass sich diese nur durch das Schaffen eines Eigentums an Sachdaten überzeugend lösen liessen.

Bei einer solchen Annahme ist allerdings eine gewisse Zurückhaltung geboten, zumal die nachfolgende Analyse deutlich macht, wie schwierig es ist, die heute schon bestehenden Probleme umfassend und hinreichend genau zu identifizieren. Ungleich schwieriger erscheint es, die Folgen der Einführung eines Eigentums an Sachdaten für alle möglicherweise betroffenen Bereiche der Rechtsordnung zu beurteilen. Es besteht deshalb die Gefahr, das Potential eines Eigentums an Sachdaten zur Lösung der erkennbaren Probleme zu überschätzen und die neuen Probleme, die sich durch die Einführung eines solchen Eigentumsrechts ergeben, zu unterschätzen oder gar ganz zu übersehen.

In der Lehre werden verschiedene praktische Probleme diskutiert, die sich allenfalls durch die Einführung eines Dateneigentums lösen liessen. Im Vordergrund stehen dabei die Datenportabilität, der Verlust von Daten, der Umgang mit Daten im Erbgang und im

210 Drexl et al., Rz. 7.
211 In diesem Sinn bereits Europäische Kommission, Aufbau einer Europäischen Datenwirtschaft, 12 ff., insb. 14.
212 S. hierzu ausführlich Golliez, *passim*.
213 Thouvenin/Weber/Früh, Datenpolitik, 93 ff.; zu den Zugangsrechten für Sachdaten insb. auch de Werra, *passim*.
214 Siehe dazu vorn, D.I.

Konkurs, das *Web-Scraping* und die Übertragung von Wertrechten auf der *Blockchain*.

b) Datenportabilität

Die Inhaber von Daten haben regelmässig ein Interesse daran, «ihre» Daten von Dritten herausverlangen und entweder selbst nutzen oder an andere Dritte weitergeben zu können. Dies gilt besonders für Daten, die bei Anbietern von Internetdiensten gespeichert sind, etwa bei *Social Media-* oder *Cloud*-Anbietern. Ein Dateneigentum würde den Inhabern von Daten einen Herausgabeanspruch vermitteln[215] und könnte dem Bedarf nach einem Anspruch auf Herausgabe der «eigenen» Daten damit gerecht werden.

30

Die Einführung eines Dateneigentums ist hierzu aber nicht erforderlich. Vielmehr reicht dazu ein Recht auf Datenportabilität, wie es Art. 20 DSGVO für Personendaten vorsieht. Der Entwurf für ein totalrevidiertes schweizerisches Datenschutzgesetz enthielt zwar anfänglich noch keinen entsprechenden Regelungsvorschlag. Auf Empfehlung der SPK-NR hat der Nationalrat aber in der Herbstsession 2019 ein Recht auf Datenportabilität in den Entwurf aufgenommen und diese Änderung ist vom Ständerat in der Wintersession 2019 auch angenommen worden[216]. Es ist deshalb davon auszugehen, dass auch die Schweiz in naher Zukunft über ein Recht auf Portabilität von Personendaten verfügen wird.

Für Sachdaten sind in der EU erste vergleichbare Bestrebungen erkennbar. Mit der Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates vom 14. November 2018 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union setzt der europäische Gesetzgeber aber vorerst auf regulierte Selbstregulierung, um unerwünschte *Lock-in*-Effekte zulasten der ursprünglichen Dateninhaber zu verhindern[217]. Diese Bestrebungen zeigen, dass es denkbar ist, auch dem analogen Bedürfnis der Inhaber von Sachdaten durch die Einführung spezifischer Portabilitäts- und/oder Zugangsrechte Rechnung zu tragen[218].

c) Verlust von Daten

Mit dem Verlust von Daten, etwa durch Hacking oder wegen des Verlustes eines Datenträgers, ist regelmässig der Verlust gewisser Werte verbunden, jedenfalls wenn die Daten nicht anderweitig gespeichert wurden und damit weiterhin verfügbar sind[219]. Das geltende Recht vermag dieses Problem zwar nur teilweise und lediglich indirekt, in den meisten Konstellationen aber durchaus angemessen zu lösen[220].

Rechtlich weitgehend unproblematisch erscheinen die Konstellationen, in welchen der Dateninhaber «seine» Daten auf Grundlage eines Vertrags bei einem Dritten gespeichert hat. Ein solcher Vertrag wird stets – zumindest implizit – die Pflicht enthalten, dem Dateninhaber die Daten herauszugeben und deren Verlust zu vermeiden. Dies gilt selbst dann, wenn eine solche Pflicht oder das Bestehen von Ansprüchen aus deren Verletzung in AGB wegbedungen worden sein sollte. Denn eine solche Klausel gilt entweder als Folge der Ungewöhnlichkeitsregel als nicht vom Konsens erfasst und ist damit unwirksam[221] oder sie ist wegen eines erheblichen und ungerechtfertigten Missverhältnisses der vertraglichen Rechte und Pflichten als Verstoss gegen Art. 8 UWG und damit als nichtig zu qualifizieren[222]. Aller-

215 Siehe dazu hinten, Weber/Thouvenin/Früh, Datenpolitik, 75.

216 Staatspolitische Kommission des Nationalrates (SPK-NR), Kommission schliesst Beratung der Revision des Datenschutzgesetzes ab, 16. August 2019 Bern, abrufbar unter <https://www.parlament.ch/press-releases/Pages/mm-spk-n-2019-08-16-a.aspx>, zuletzt besucht am 4. Mai 2020; Nationalrat, Herbstsession 2019, 25. September 2019, AB 2019 N 1819, Abstimmung zum Recht auf Datenherausgabe und Übertragung, Art. 25a ff.; Ständerat, 18. Dezember 2019, Wintersession 2019, AB 2019 S 1245, Annahme des Antrages der Kommission und Zustimmung zum Beschluss des Nationalrates, Art. 25, 25a, 25b. Die Chronologie des Geschäfts 17.059, Datenschutzgesetz, Totalrevision und Änderung weiterer Erlasse zum Datenschutz ist abrufbar unter: <https://www.parlament.ch/de/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=47369>, zuletzt besucht am 4. Mai 2020. Aus dem Schrifttum auch Laux, digma 2019, 166 ff.; siehe zu den Abklärungen betr. die Einführung eines Rechts auf Datenportabilität auch Weber/Thouvenin, *passim*; sowie Bericht Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit, 105 ff., insb. 106 f., wonach die Expertenkommission empfiehlt, dass der Bund für Personendaten «unter Berücksichtigung der internationalen Entwicklungen das Datenschutzrecht um das Element der Datenportabilität» ergänzt», Anknüpfungspunkt soll dabei das bestehende Auskunftsrecht sein. Ferner wird empfohlen, eine Regelung für die Portabilität von Sachdaten zu prüfen. Zur Ergänzung des Datenschutzrechts um das Element der Datenportabilität siehe auch UVEK, Datenbearbeitung und Datensicherheit, 9 f.

217 Siehe dazu Thouvenin/Weber/Früh, Datenpolitik, 46 f.

218 De Werra, *passim*.

219 Eingehend dazu Bühler, Jusletter IT Flash 11. Dezember 2017, Rz. 1.

220 Insb. zu den strafrechtlichen Anknüpfungspunkten siehe Bühler, Jusletter IT Flash 11. Dezember 2017, Rz. 5 ff.

221 Siehe dazu statt vieler: BSK-UWG, Thouvenin, Art. 8 N 53 f., m.w.H.; SHK-UWG, Probst, Art. 8 N 181, m.w.H.

222 Siehe dazu statt vieler: BSK-UWG, Thouvenin, Art. 8 N 143 ff., m.w.H.; SHK-UWG, Probst, Art. 8 N 291, m.w.H.; Heizmann/Loacker, Heiss, Art. 8 N 242 ff.

dings werden die vertraglichen Ansprüche in diesen Konstellationen kaum helfen, weil der Vertragspartner bei einem Verlust der Daten gar nicht mehr in der Lage ist, die Daten herauszugeben. Daran würde freilich auch ein Dateneigentum nichts ändern.

Fehlt es an einem Vertragsverhältnis, vermittelt das Sachenrecht dem Eigentümer des Datenträgers zwar einen Anspruch auf Herausgabe des Trägers. Dieser Anspruch führt aber nicht weiter, wenn der Verlust der Daten nicht auf dem Verlust eines Datenträgers beruht oder die Daten auf dem Träger nicht mehr vorhanden sind. Möglich ist immerhin, das allgemeine Deliktsrecht dahingehend auszulegen, dass bei Vorliegen von Widerrechtlichkeit nicht nur ein Anspruch auf Schadenersatz und Unterlassung, sondern auch ein Anspruch auf Naturalrestitution, also auf Herausgabe der Daten besteht. Ein solcher Anspruch ist denn im schweizerischen Recht auch grundsätzlich anerkannt[223] – er müsste in der Praxis nur noch auf Daten angewendet werden. Dieser an sich vielversprechende Ansatz hilft allerdings nur, wenn eine widerrechtliche Handlung vorliegt, etwa bei einem *Hacking* oder einem Diebstahl eines Datenträgers[224], nicht aber, wenn der Berechtigte seinen Datenträger schlicht verloren hat. Einen neuen Weg im Umgang mit abhanden gekommenen Daten sieht der Bundesrat einzig im Kontext der Technik verteilter elektronischer Register *(Distributed Ledger Technology)* vor. Mit der Ergänzung des OR will er neu eine Bestimmung einführen, die – entsprechend zum Wertpapierrecht – eine Kraftloserklärung von *Token* ermöglichen soll (Art. 973g VE-OR)[225].

Mit Blick auf die wenigen, nicht mit dem geltenden Recht erfassbaren Konstellationen erscheint allerdings fraglich, ob ein Eigentum an Sachdaten eingeführt werden muss. Eine punktuelle Lösung durch spezifische Normen, namentlich für das blosse Verlieren von Datenträgern, wäre angemessener[226]. Angesichts der zunehmenden Loslösung der Datennutzung von körperlichen Trägern erscheint der Bedarf nach einem Einschreiten des Gesetzgebers allerdings als gering.

d) Daten im Erbgang

Das Erbrecht basiert auf der Annahme, dass die Erbmasse aus Sacheigentum und Forderungen besteht. Daten standen beim Erlass der geltenden Regeln vor mehr als 100 Jahren nicht im Fokus. Solange Informationen überwiegend auf Papier festgehalten oder auf physischen Datenträgern gespeichert wurden, vermittelte der Übergang des Eigentums an diesen Datenträgern den Erben in der Regel auch die faktische Herrschaft über die entsprechenden Daten. Mit der Speicherung von Daten bei Dritten, insbesondere bei Anbietern von *Social Media-* oder *Cloud*-Diensten, stellt sich nun aber die Frage, wer auf die Daten eines Verstorbenen zugreifen und über diese verfügen darf[227].

Diese Entwicklung wirft eine Reihe erbrechtlicher Fragen auf, die es zu lösen gilt[228]. Diese Fragen lasen sich allerdings nicht durch die Einführung eines Eigentums an Sachdaten lösen, sondern müssen durch andere gesetzgeberische Vorkehren geregelt werden, die zwar Personen- und Sachdaten erfassen, zwischen diesen aber wohl differenzieren müssen. Während ein umfassender Übergang von Sachdaten auf die Erben durchaus denkbar erscheint, würde dieselbe Rechtsfolge bei Personendaten dazu führen, dass die Erben einen mit der fortschreitenden Digitalisierung aller Lebensbereiche

223 Siehe bereits vorn Fn. 94 und 95. Auch in Deutschland scheint diese Frage weitgehend geklärt zu sein, siehe Hoeren, MMR 2013, 490 f.; Hau/Poseck, Flume, BGB § 249 N 55 ff.; Stürner, Teichmann, BGB § 249 N 1; Prütting/Wegen/Weinreich, Luckey, BGB § 249 N 3.

224 Siehe dazu vorn, C.III.4.

225 Bundesrat, Bericht Elektronische Register, 35 f.

226 Bühler, Jusletter IT Flash 11. Dezember 2017.

227 Weber/Chrobak, Jusletter 4. April 2016, Rz. 22; zum Thema der Daten im Erbgang nun auch eingehend Eigenmann/Fanti, SJ 2017 II 193 ff.; Chrobak, Jusletter IT Flash 11. Dezember 2017, Rz. 2 ff.; für einen rechtsvergleichenden Überblick siehe Budzikiewicz, AcP 2018, 558 ff. Siehe z.B. zur Frage, ob Eltern auf Daten der verstorbenen Tochter zugreifen dürfen: Urteil des Deutschen Bundesgerichtshof vom 12. Juli 2018 – III ZR 183/17 wonach ein «Vertrag über ein Benutzerkonto bei einem sozialen Netzwerk grundsätzlich im Wege der Gesamtrechtsnachfolge auf die Erben des ursprünglichen Kontoberechtigten übergeht und diese einen Anspruch gegen den Netzwerkbetreiber auf Zugang zu dem Konto einschliesslich der darin vorgehaltenen Kommunikationsinhalte haben». (Bundesgerichtshof, Mitteilung der Pressestelle Nr. 115/2018, abrufbar unter <http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2018&Sort=3&nr=85390&pos=0&anz=115>.

228 Chrobak, Jusletter IT Flash 11. Dezember 2017, Rz. 5 ff. Schon 2014 wurde der Bundesrat mit dem Postulat 16.3416 Schwaab, Richtlinien für den digitalen Tod, vom 24. September 2014, aufgefordert, zu prüfen, ob das Erbrecht ergänzt werden muss. Eine entsprechende Prüfung sollte im Rahmen der Revision des Erbrechts geschehen. Der Bundesrat hat nun aber beschlossen, die «eher technischen Revisionsanliegen», zu denen offenbar auch dieses Postulat gehört, zu «einem späteren Zeitpunkt» zu behandeln (Botschaft Erbrecht, BBl 2018 5826). Mit Verweis auf die bereits laufenden Arbeiten an der Revision des Erbrechts und speziell das Postulat 14.3782 Schwaab lehnt es das EJPD denn auch ab, wie im Bericht Expertengruppe, Datenbearbeitung und Datensicherheit, 155, empfohlen, tätig zu werden, um Lücken im Erbrecht zu schliessen (UVEK, Datenbearbeitung und Datensicherheit, 22).

immer umfassenderen Zugriff auf und Einblick in die Aktivitäten der verstorbenen Person erhalten würden. Dies lässt sich mit dem Schutz der Privatsphäre und der Persönlichkeit der Verstorbenen nicht vereinbaren und dürfte in aller Regel nicht im Interesse des oder der Verstorbenen sein. Der Entwurf für ein totalrevidiertes Datenschutzgesetz[229] enthielt deshalb eine Bestimmung zum Umgang mit Daten verstorbener Personen, die gewisse Mechanismen zum Schutz der Persönlichkeit der Verstorbenen vorsah. Diese Bestimmung, die ohnehin nur für Personendaten Geltung erlangt hätte, wurde vom Parlament im Zuge der Beratungen aber gestrichen[230].

e) Daten im Konkurs

Wenn Private oder Unternehmen «ihre» Daten bei einem Dritten, namentlich bei einem Anbieter von *Cloud*-Diensten oder von *Token Wallets* speichern und dieser in Konkurs fällt, stellt sich die Frage, ob und wie die Betroffenen «ihre» Daten wieder erlangen können. Das heutige Schuldbetreibungs- und Konkursrecht ist auf die Aussonderung von Sachen ausgerichtet (Art. 242 SchKG), Daten sind nicht Gegenstand der Regelung.

Eine angemessene Lösung erscheint hier zwingend erforderlich[231]. Die Einführung eines Dateneigentums wäre zwar ein möglicher Ansatz, würde für sich allein aber nicht ausreichen, weil das SchKG eine Aussonderung ausdrücklich nur für Sachen vorsieht (Art. 242 Abs. 1 SchKG). Eine Anpassung des Gesetzes wäre damit selbst bei Einführung eines Eigentums an Sachdaten unumgänglich, sofern sich die Rechtsprechung nicht für eine analoge Anwendung der heutigen Regelung auf Sachdaten aussprechen sollte. Dies wäre hier – im Gegensatz zu einer analogen Anwendung der Regeln des Sacheigentums auf Sachdaten – zwar durchaus möglich, weil die Tragweite eines solchen Analogieschlusses klar umrissen und eingegrenzt wäre. Eine gesetzliche Lösung, die *ex ante* Rechtssicherheit schafft, wäre aber vorzuziehen.

Angesichts der grossen praktischen Bedeutung der Frage überrascht es wenig, dass die Einführung eines Anspruchs auf Datenherausgabe im Konkurs von Providern schon anfangs 2017 mit einer parlamentarischen Initiative verlangt worden ist[232]. Der Bundesrat ist diesem Anliegen denn auch nachgekommen: Nach Ankündigung im Bericht «Rechtliche Grundlagen für *Distributed Ledger*-Technologie und *Blockchain* in der Schweiz» vom 14. Dezember 2018[233] und einem dahingehenden Vorschlag des Bundesrates im Vernehmlassungsbericht vom 22. März 2019[234] ist im Entwurf für ein Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register vom 27. November 2019 nun vorgesehen, das SchKG durch eine neue Bestimmung (Art. 242a E-SchKG) zu ergänzen, welche die Herausgabe kryptobasierter Vermögenswerte regeln soll[235]. Darüber hinaus soll auch eine allgemein gefasste Bestimmung zum Zugang zu Daten geschaffen werden, die sich in der Verfügungsmacht der Konkursmasse befinden (Art. 242b E-SchKG). Da das Gesetz keinen Unterschied macht[236], werden sowohl Personen- als auch Sachdaten erfasst. Nach dieser Norm soll Zugang zu Daten erhalten, wer eine gesetzliche oder vertragliche Berechtigung an diesen nachweisen kann (Art. 242b Abs. 1 E-SchKG)[237]. Die Kosten für den Zugang muss dabei tragen, wer Zugang verlangt (Art. 242b Abs. 3 SchKG). Sollte das Parlament dem Vorschlag des Bundesrates folgen und diese Bestimmungen ins SchKG aufnehmen, ist aus heutiger Sicht davon auszugehen, dass sich damit die Probleme beim Zugang zu Sachdaten im Konkurs angemessen lösen lassen. Der Nationalrat hat am 17. Juni 2020 als Erstrat den Entwurf angenommen, einschliesslich des neuen Art. 242b SchKG. Ende August berät die ständerätliche Kommission für Wirtschaft und Abgaben das Geschäft, bevor es voraussichtlich im Herbst vom Ständerat behandelt wird.

229 E-DSG, Art. 16 (Daten von verstorbenen Personen).
230 Zur Behandlung im Nationalrat vom 25. September 2019, s. AB 2019 NR 1809; zur Behandlung im Ständerat vom 18. Dezember 2019, s. AB 2019 SR 1242.
231 Für einen Überblick siehe Neuenschwander/Oeschger, Jusletter IT Flash 11. Dezember 2017, Rz. 16 ff.
232 Siehe. dazu Parlamentarische Initiative Dobler 17.410, Daten sind das höchste Gut privater Unternehmen. Datenherausgabe beim Konkurs von Providern regeln, vom 7. März 2017.
233 Bundesrat, Blockchain-Bericht, 69 ff.
234 Bundesrat, Bericht Elektronische Register, 37 ff.
235 Bundesrat, Botschaft Elektronische Register, BBl 2020 291 ff.
236 Bundesrat, Botschaft Elektronische Register, BBl 2020 295.
237 Bundesrat, Botschaft Elektronische Register, BBl 2020 295 f.

f) Web-Scraping

Als *Scraping* von Webseiten oder *Web-Scraping* wird ein Vorgehen bezeichnet, bei dem Daten mit technischen Mitteln gezielt von einer Webseite extrahiert werden. Im Vordergrund steht dabei die Frage, ob der Betreiber einer Webseite das *Scraping* als solches und die anschliessende Verwertung der so gewonnenen Daten mit rechtlichen Mitteln verhindern kann. Beide Aspekte, das Extrahieren und das anschliessende Verwerten der Daten, könnten durch die Einführung eines Dateneigentums erfasst werden[238].

Zumindest für ein Vorgehen gegen die *wirtschaftliche Verwertung der Daten* erscheint ein Eigentumsrecht allerdings kaum erforderlich. Vielmehr bietet Art. 5 lit. c UWG schon heute eine Handhabe, um ein solches Verhalten zu erfassen[239]. Dies gilt allerdings nur, wenn die in Frage stehenden Daten als marktreifes Arbeitsergebnis verstanden werden und die Norm nicht nur auf horizontale, sondern auch auf vertikale Marktverhältnisse angewendet wird[240]. Die Regelung im UWG hat zudem den Vorteil, dass nur die wirtschaftliche Verwertung der durch *Scraping* erlangten Daten erfasst wird, die Nutzung zu privaten Zwecken oder für die Forschung aber möglich bleibt.

Anders zu behandeln ist das *Scraping als solches*. Dieses kann über Art. 5 lit. c UWG nicht erfasst werden, weil diese Bestimmung auch ein Verwerten des mit technischen Reproduktionsverfahren übernommenen Arbeitsergebnisses vorsieht.

Für das Erfassen des *Scraping* erscheint die Einführung eines Dateneigentums allerdings nicht zwingend erforderlich. Denn wenn der Betreiber einer Webseite das *Scraping* der Daten als solches verhindern will, steht es ihm frei, den Nutzern seiner Webseite in AGB das *Scraping* zu untersagen. Einzuräumen ist allerdings, dass bisher ungeklärt ist, ob das blosse Abrufen einer Webseite mit einem Rechtsbindungswillen des Anbieters und des Nutzers erfolgt. Dieser ist Voraussetzung für das Bestehen eines Vertragsverhältnisses und damit für die Möglichkeit zur Vereinbarung von AGB. Die Frage kann hier zwar nicht geklärt werden[241]. Geht man aber davon aus, dass es dem Betreiber einer Webseite durchaus möglich ist, deren Nutzung den eigenen AGB zu unterwerfen, dann stehen ihm bei entsprechender Ausgestaltung der AGB gegen das *Scraping* zwar keine deliktischen oder wettbewerbsrechtlichen, wohl aber vertragliche Ansprüche auf Unterlassung und Schadenersatz zu. Auch zur Lösung dieses Problems erscheint die Einführung eines Eigentums an Sachdaten deshalb nicht erforderlich.

g) Übertragung von Wertrechten auf der Blockchain

Bei der Übertragung von Wertrechten (sog. *Token*) auf der *Blockchain* ist nach den möglichen Qualifikationen solcher Wertrechte und den damit verbundenen Übertragungsformen zu unterscheiden[242]:

Ist das Wertrecht in einer Forderung ausgedrückt, was oft zutreffen dürfte, erfolgt die Übertragung traditionell durch Abtretung der Forderung (Art. 164 OR). Die Problematik liegt in der Praxis allerdings darin, dass Art. 165 Abs. 1 OR die Schriftform für die Abtretung verlangt. Diese Formerfordernis lässt sich zwar auch digital erfüllen, doch sind die Voraussetzungen des Bundesgesetzes über die elektronische Signatur so komplex, dass ein solcher Übertragungsvorgang aus praktischen Gründen regelmässig nicht in Frage kommt. Sind die Wertrechte in (traditionellen) Wertpapieren verurkundet (Art. 965 OR), erfolgt die Übertragung durch Übergabe des Besitzes (Art. 922 ZGB). Die Verurkundung von Wertrechten in Wertpapieren ist in der heutigen Welt aber nicht mehr üblich. Denkbar ist weiter die Ausgestaltung der Wertrechte als nicht verurkundete Rechte nach Art. 973c OR oder dem Bucheffektengesetz (BEG). Danach ergibt sich die Berechtigung des Eigentums aus einen zentral zu führenden Register. In der heutigen gesetzgeberischen Konzeption widerspricht aber das

238 Für einen Überblick siehe Stauber, Jusletter IT Flash 11. Dezember 2017, Rz. 1 ff.

239 Dies zeigt ein jüngerer Entscheid des Kantonsgerichts Fribourg, welcher das sog. «*Spidering*» von *Online*-Inseraten, das nichts anderes als ein *Web-Scraping* darstellt, als Verstoss gegen Art. 5 lit. c UWG qualifiziert, wenn sich der Übernehmer der Inserate relevante Arbeitsschritte erspart (KGer FR, sic! 2017, 228 ff.). Dieser Entscheid steht allerdings im Gegensatz zu einem nun schon etwas älteren Entscheid des Bundesgerichts, das bei einer gleich gelagerten Frage die Voraussetzungen von Art. 5 lit. c UWG als nicht gegeben erachtete (BGE 131 III 384); siehe dazu auch Stauber, Jusletter IT Flash 11. Dezember 2017, Rz. 8 ff.

240 Siehe dazu vorn C.III.5 sowie Thouvenin, sic! 2018, 609 ff.

241 Zur (offenen) Frage, ob durch das blosse Abrufen einer Webseite konkludent ein Vertrag zustande kommt, auch Stauber, Jusletter IT Flash 11. Dezember 2017, Rz. 13 f. m.w.H. und Kaiser, 189 m.w.H.; siehe weiter den Entscheid «Immobilien-Suchmaschine» des Bezirksgerichts Freiburg vom 24. Januar 2005, Akten-Nr. PZ 04-506 (FR), abgedruckt in sic! 2005, 675 ff., E. 2.3. Für das deutsche Recht Elteste, CR 2015, 450 f. und Kreutz, ZUM 2018, 163 ff.

242 Für einen umfassenden Überblick siehe Weber/Iacangelo, Jusletter IT Flash 24. Mai 2018, Rz. 7 ff. m.w.H.

gemäss BEG zentral zu führende Wertrechtebuch der dezentralen Struktur der *Blockchain*-Technologie. Zudem ist nach Art. 973c Abs. 4 OR wie bei der Abtretung die Schriftform erforderlich.

Bei der Übertragung digitaler Wertrechte besteht damit gesetzgeberischer Handlungsbedarf. Auf diesen wurde im Bericht der *Blockchain*-Arbeitsgruppe und in der Lehre hingewiesen[243] und der Bundesrat ist diesem Anliegen auch nachgekommen: Nach der Ankündigung im Bericht zur *Distributed Ledger*-Technologie vom 14. Dezember 2018[244] und einem ersten dahingehenden Vorschlag im Vernehmlassungsbericht vom 22. März 2019[245] ist im Entwurf zum Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register vom 27. November 2019 nun vorgesehen, eine neue Regelung zur Übertragung digitaler Wertrechte zu schaffen (Art. 973d ff. E-OR)[246]. Die praktischen Probleme bei der Übertragung digitaler Wertrechte dürften sich mit diesen neuen, rechtstechnisch allerdings durchaus komplexen Gesetzesbestimmungen angemessen lösen lassen[247]. Auch hier besteht damit kein Bedarf nach Einführung eines Dateneigentums.

3. Zwischenfazit

Die vorstehende Analyse umfasst die praktischen Probleme, die heute erkennbar und in der Literatur teilweise auch diskutiert worden sind, sie kann aber nicht Anspruch auf Vollständigkeit erheben. Dies gilt umso mehr, als künftig wohl weitere Probleme entstehen werden, zu deren Lösung ein Dateneigentum beitragen könnte.

Der Überblick über die praktischen Probleme zeigt aber, dass die Rechtsordnung ohne ein Eigentum an Sachdaten nicht vor grundlegenden und allgemeinen, sondern nur (aber immerhin) vor einigen spezifischen Problemen steht. Umgekehrt ist schon heute klar, dass der Gesetzgeber mit der Einführung eines Dateneigentums das Entstehen neuer Probleme in Kauf nehmen würde. Eines dieser Probleme ist die Besteuerung dieses neuen Eigentumswerts[248]; andere sind derzeit noch nicht vorhersehbar. Gerade mit Blick auf diese potentiellen, derzeit aber kaum einzuschätzenden negativen Auswirkungen eines allfälligen Eigentums an Sachdaten drängt es sich deshalb auf, den spezifischen Problemen – soweit erforderlich – mit dem Erlass spezifischer Regeln zu begegnen. Die Einführung eines Eigentums an Sachdaten ist hingegen abzulehnen[249].

II. Datenbesitz

Sollte man zum Schluss kommen, dass zwar kein Eigentum an Sachdaten einzuführen ist, dass der bestehende Rechtsrahmen und punktuelle Anpassungen aber nicht in der Lage sind, den Schutzbedarf abzudecken, wäre es denkbar, einen allgemeinen und damit umfassenden rechtlichen Schutz der faktischen Zuordnung von Sachdaten durch Einführung eines Besitzes an Sachdaten vorzusehen.

Das Institut des Besitzes ist bei der Suche nach einer möglichen Lösung aus verschiedenen Gründen naheliegend: Zum einen ist der Ausgangspunkt der Regelung des Besitzesrechts das Bestehen von Besitz, also von tatsächlicher Gewalt an einer Sache[250], was der faktischen Kontrolle über Daten entspricht.[251] Zum andern sieht das Besitzesrecht vergleichsweise einfache Mittel vor, um die tatsächliche Herrschaft bei Verlust wieder zu erlangen und sich gegen die Störung des Besitzes zu wehren. So ist beim Besitzesschutz (Art. 926 ff. ZGB) vorgesehen, dass zur Rückgabe einer Sache verpflichtet ist, wer diese Sache einem anderen durch verbotene Eigenmacht entzogen hat (Art. 927 Abs. 1 ZGB). Bei Störungen des Besitzes durch verbotene Eigenmacht kann der Besitzer ausserdem die Beseitigung der Störung und die Unterlassung

243 Siehe dazu Blockchain Taskforce, Positionspapier zur rechtlichen Einordnung von ICO's, Bern/Zug, April 2018, abrufbar unter <https://blockchainfederation.ch/downloads/>.
244 Bundesrat, Blockchain-Bericht, 47 ff.
245 Bundesrat, Bericht Elektronische Register, 27 ff.
246 Bundesrat, Botschaft Elektronische Register, BBl 2020 276 ff. Aus dem Schrifttum dazu Kuhn/Stengel/Meisser/Weber, Jusletter IT 23. Mai 2019, Rz. 6 ff.; Kramer/Oser/Meier, Jusletter 6. Mai 2019, Rz. 26 ff. und Rz. 60.
247 Zum Stand der Revision siehe vorn D.I.2.e).
248 Siehe dazu Oberson, AJP 2017, 232 ff., zu ähnlichen Fragen im Zusammenhang mit der Besteuerung von Robotern.
249 Ebenso Kohler, sic! 2020, 412.
250 BK-ZGB, Stark/Lindemann, Vor Art. 926–629 N 6; BSK-ZGB II, Ernst, Vor Art. 926–929 N 5; differenzierend Hrubesch-Millauer/Graham-Siegenthaler/Roberto, Rn. 02.03, für die die «tatsächliche Gewalt einer Person über eine Sache» «Besitz im materiellen Sinne» darstellt.
251 Siehe dazu Eckert, SJZ 2016, 265, nach welchem die tatsächliche Gewalt innehat, «wer den Zugriff auf die zu beurteilenden, auf einem spezifischen Datenträger gespeicherten digitalen Daten auch tatsächlich steuern kann».

weiterer Störungen verlangen (Art. 928 ZGB). Als verbotene Eigenmacht gilt dabei jede Störung des Besitzes, die nicht durch Einwilligung des Besitzers oder durch Gesetzesnorm gedeckt ist[252]. Der Begriff ist damit äusserst weit und erfasst auch Konstellationen, bei denen eine deliktische Haftung nicht besteht, namentlich mangels Verschuldens[253]. Im Besitzesrechtsschutz (Art. 930 ff. ZGB) ist zudem vorgesehen, dass der Besitzer, dem eine bewegliche Sache gestohlen wird oder verloren geht oder sonst wider seinen Willen abhanden kommt, die Sache während fünf Jahren jedem Empfänger abfordern kann (Art. 934 Abs. 1 ZGB). Die Herausgabeansprüche beruhen auf dem Gedanken, dass die tatsächliche Herrschaft wieder hergestellt werden soll, wenn sie gegen den Willen des Besitzers verloren gegangen ist.

Dieser Ansatz lässt sich möglicherweise auch auf die tatsächliche Herrschaft an Sachdaten übertragen. Ob sich damit allerdings die heute erkennbaren und allfällige künftige Probleme überzeugend lösen liessen und sich nicht neue Folgeprobleme ergeben würden, erscheint zweifelhaft, wie eine summarische Prüfung aus theoretischer und praktischer Perspektive zeigt:

Aus *theoretischer Sicht*[254] könnten zugunsten der Einführung eines Datenbesitzes ähnliche Argumente ins Feld geführt werden wie beim Dateneigentum, etwa dass Daten einen Wert haben, der zu schützen sei oder ein Datenbesitz die Autonomie der Bürger stärken würde[255]. Allerdings ist zu bedenken, dass viele dieser Argumente bei Sachdaten erst gar nicht greifen, weil sie auf die Bedürfnisse oder Wünsche der betroffenen Personen ausgerichtet sind, wie etwa bei der Stärkung der Autonomie oder der Forderung nach einer Partizipation am Wert von (Personen-)Daten[256]. Zudem greifen beim Datenbesitz dieselben Gegenargumente wie beim Dateneigentum. Das gilt namentlich auch für das gewichtigste theoretische Argument, nach welchem die Einführung eines Datenbesitzes ein Mittel zur Korrektur von Marktversagen sein könnte[257]. Denn wie im Zusammenhang mit dem Dateneigentum bereits ausgeführt wurde[258], liegt kein Marktversagen vor und es braucht namentlich keine besonderen Anreize für die Schaffung von Sachdaten, die regelmässig als Nebenprodukte anderer Tätigkeiten anfallen[259]. Die Einführung eines Datenbesitzes würde auch nicht zur Senkung von Transaktionskosten beitragen. Da die faktische Herrschaft über Daten schon heute die Ausgangslage bei Vertragsverhandlungen bestimmt und ein Datenbesitz gerade an dieser Herrschaft anknüpfen würde, könnte ein Datenbesitz auch nicht zu einer einfacheren und Transaktionen fördernden Zuordnung von Sachdaten führen. Zwar könnte es ein Datenbesitz vereinfachen, Sachdaten im Rahmen von Vertragsverhandlungen herauszugeben, weil ein Rechtsanspruch auf Rückgabe bestehen würde. Solche Ansprüche lassen sich aber ohne weiteres vertraglich vereinbaren. Vor allem aber ist die Übergabe von Daten im Rahmen von Vertragsverhandlungen meist gar nicht erforderlich[260]. Die Einführung eines Datenbesitzes lässt sich damit aus theoretischer Perspektive nicht rechtfertigen.

Aus einer *praktischen Perspektive* könnte sich ein Bedarf nach einem Datenbesitz ergeben, wenn sich konkrete Probleme mit den bestehenden Rechtsregeln nicht überzeugend lösen liessen und die Lücken (nur) durch die Einführung eines Datenbesitzes geschlossen werden könnten. Dies wäre der Fall, wenn das Schaffen spezifischer Regeln für den Datenbesitz im Vergleich zur aktuellen Rechtslage einen zusätzlichen Schutz der tatsächlichen Herrschaft an Daten vermitteln könnte, weil die Störung oder Entziehung der Herrschaft über die Daten weder vom Geheimnisschutz des UWG erfasst ist noch die Voraussetzungen eines Straftatbestands erfüllt, sodass weder die wettbewerbsrechtlichen noch die deliktsrechtlichen Beseitigungs-, Unterlassungs- und Restitutionsansprüchen greifen würden[261]. Da der Besitzesschutz unabhängig von Verschulden und Widerrechtlichkeit

252 Hrubesch-Millauer/Graham-Siegenthaler/Roberto, Rn. 02.95; siehe dazu auch: BK-ZGB, Stark/Lindemann, Vor Art. 926–929 N 21, 41; BSK-ZGB II, Ernst, Vor Art. 926–929 N 9, 18.
253 Hrubesch-Millauer/Graham-Siegenthaler/Roberto, Rn. 02.95; BK-ZGB, Stark/Lindemann, Vor Art. 926–929 N 39.
254 Die wenigen bisherigen Ausführungen der Lehre zum Datenbesitz (Hoeren, Jusletter 11. Mai 2020, *passim*; ders., MMR 2019, *passim*; Michl, NJW 2019, *passim*) behandeln die theoretischen Grundlagen eines solchen Rechtsinstituts nicht.
255 Siehe dazu vorn, D.I.1.
256 Siehe dazu vorn, D.I.1 .
257 Siehe dazu vorn, D.I.1.b).
258 Siehe dazu vorn, D.I.1.b)(ii).
259 Siehe dazu vorn, D.I.1.b)(ii) und D.I.1.a).
260 Siehe dazu vorn, D.I.1.b)(iii).
261 Siehe dazu vorn, C.III.3., C.III.4 und C.III.5.

greift und nicht nur bestimmte Wettbewerbshandlungen erfasst, könnte sich die datenbesitzende Person diesfalls auf Art. 927 und Art. 928 ZGB berufen, um entzogene Daten zurückzuverlangen oder die Unterlassung von Störungen ihres Datenbesitzes zu erwirken. Überdies wäre bei Eingriffen in den Datenbesitz die Widerrechtlichkeit im Sinn von Art. 41 OR ohne weiteres gegeben[262], was die Begründung deliktsrechtlicher Ansprüche inkl. eines allfälligen Schadenersatzanspruchs vereinfachen würde.

In der Praxis dürften die Fälle indessen selten sein, in denen die Anwendung des Besitzesrechts die datenbesitzende Person tatsächlich vor Schutzlücken bewahren würde und es auch sachlich angezeigt wäre, das Besitzesrecht anzuwenden. Anders als beim Dateneigentum[263] werden in der Lehre denn auch kaum praktische Probleme angeführt, die sich durch die Einführung eines Datenbesitzes sachgerecht lösen liessen. Genannt wird das Beispiel des Eigentümers eines autonom fahrenden und laufend Daten erfassenden Fahrzeugs, der die Zugriffsmöglichkeit des Fahrzeugherstellers auf die Daten unterbricht. Aus einer wertenden Perspektive sei der Hersteller hier als Datenbesitzer zu betrachten und dieser könne wegen der Störung seines Datenbesitzes gegen den Eigentümer des Fahrzeugs vorgehen[264]. Selbst wenn es mit Blick auf die getätigten Investitionen und die Weiterentwicklung des Fahrzeugsystems nachvollziehbar sein mag, dass der Fahrzeughersteller auf die Daten zugreifen können sollte, ist die Einführung eines Datenbesitzes hier jedenfalls keineswegs erforderlich, um den Zugriff rechtlich zu gewährleisten. Vielmehr kann sich der Hersteller (kauf-)vertraglich den Zugriff ausbedingen und mit tatsächlichen Massnahmen absichern. Ein Bedarf nach einem Datenbesitz ist damit nicht ersichtlich. Hinzu kommt, dass es sich bei den hier in Frage stehenden Daten regelmassig um Personendaten handeln wird, weshalb das Beispiel kaum zur Begründung des hier interessierenden Besitzes an Sachdaten dienen kann.

Darüber hinaus liesse sich der Bedarf nach einem Datenbesitz anhand sämtlicher praktischer Probleme im Einzelnen prüfen, die im Zusammenhang mit dem Dateneigentum näher untersucht worden sind. Da beim Datenbesitz analoge Überlegungen greifen, kann im Wesentlichen auf die entsprechenden Ausführungen verwiesen werden[265]. Namentlich erscheint auch hier fraglich, ob die mit dem geltenden Recht nicht (sinnvoll) geregelten Konstellationen beim Datenverlust[266] und beim *Web-Scraping*[267] die Einführung eines Datenbesitzes zu rechtfertigen vermögen. Auch bei der Datenportabilität und im Erbgang sind punktuelle Eingriffe in die geltende Rechtsordnung, wie sie vereinzelt bereits diskutiert wurden, angemessener als die Einführung eines allgemeinen Datenbesitzes. Bei Daten im Konkurs ist ausserdem zu bedenken, dass der blosse Besitz nicht zur Aussonderung berechtigen würde[268]; vor allem aber erscheint das heutige Problem mit den neuen Bestimmungen des SchKG bald als gelöst[269].

Zusammenfassend lässt sich festhalten, dass das geltende Recht ohne Datenbesitz keineswegs vor grundlegenden und allgemeinen Problemen, sondern höchstens vor vereinzelten punktuellen Herausforderungen steht. Die Einführung eines Besitzes an Sachdaten erscheint deshalb nicht angezeigt. Stattdessen sollten die praktischen Probleme mit spezifischen Regeln gelöst werden, die den ausgewiesenen Bedürfnissen im konkreten Fall angemessen Rechnung tragen. An dieser Einschätzung ändert nichts, dass die negativen Folgen der Einführung eines Datenbesitzes im Vergleich zum Dateneigentum deutlich geringer ausfallen würden, weil der Besitz eine ungleich schwächere Rechtsposition vermittelt als das Eigentum und ihm in der Rechtsordnung auch keine vergleichbar transversale Bedeutung zukommt[270]. Dennoch könnte auch ein Datenbesitz als neues Rechtsinstitut zu Problemen führen, die derzeit kaum vorhersehbar sind. Die Einführung eines Besitzes an Sachdaten ist deshalb abzulehnen.

262 Nach herrschender Lehre gilt der Besitz als absolut geschütztes Rechtsgut, weshalb dessen Verletzung die Widerrechtlichkeit im Sinn von Art. 41 OR begründet, siehe dazu BSK-OR I, Kessler, Art. 41 N 33; Rey/Wildhaber, Rz. 839.
263 Siehe dazu vorn, D.I.
264 Hoeren, Jusletter 11. Mai 2020, Rz. 39 ff.
265 Siehe dazu vorn, D.I.2.
266 Gemeint ist hier die Konstellation, in der eine Person einen Datenverlust erfährt, da sie den betreffenden Datenträger verliert; siehe dazu vorn, D.I.2.c).
267 Gemeint ist hier das Web-Scraping als solches, d.h. das Vorgehen, bei dem Daten mit technischen Mitteln gezielt von einer Webseite extrahiert werden; siehe dazu vorn, D.I.2.f).
268 Siehe dazu BSK-SchKG, Russenberger, Art. 242 N 15; KUKO-SchKG, Bürgi, Art. 242 N 1.
269 Siehe dazu vorn, D.I.2.d).
270 Siehe dazu vorn, D.I.

III. *Sui-generis*-Recht an Datenbanken

Das *sui-generis*-Recht an Datenbanken ist in erster Linie ein Resultat der Industriepolitik und der Rechtsharmonisierung der damaligen EG[271]. Aus heutiger Sicht fällt auf, dass bei Erlass der Datenbanken-RL Mitte der 90er-Jahre keine vertiefte Auseinandersetzung mit den theoretischen oder praktischen Gründen für die Einführung eines solchen Rechtsinstituts erfolgt ist. Die Einsicht, dass Schutzrechte nicht leichtfertig geschaffen werden sollten und stets einer Rechtfertigung bedürfen, hat sich erst später durchgesetzt.

Als mögliche Rechtfertigung für die Schaffung eines spezifischen Schutzrechts für Datenbanken steht aus *theoretischer Perspektive*, wie beim Dateneigentum, die Beseitigung eines Marktversagens im Vordergrund[272]. Für die *Produktion von Datenbanken* stellt sich die Frage, ob ein spezifischer Rechtsschutz erforderlich ist, weil Wettbewerber ohne diesen Schutz die Leistung des Datenbankherstellers übernehmen könnten und damit hinreichende Anreize für die Produktion von Datenbanken fehlen würden. In Erwägungsgrund 7 der Datenbanken-RL wird dieser Gedanke denn auch angeschnitten, indem darauf hingewiesen wird, die Kosten der Übernahme betrügen nur einen Bruchteil der Kosten, die zur Entwicklung der Datenbank notwendig seien. Dies allein vermag die Schaffung eines spezifischen Schutzrechts für Datenbanken aber nicht zu rechtfertigen. Denn Datenbanken sind (wie Daten) zwar ihrer Natur nach öffentliche Güter[273], aber anders als urheberrechtlich geschützte Werke der Literatur und Kunst oder patentierte Lehren zum technischen Handeln sind die Inhalte einer Datenbank praktisch nie öffentlich zugänglich. Der Zugriff Dritter lässt sich damit in aller Regel wirkungsvoll mit tatsächlichen Massnahmen verhindern und durch den Geheimnisschutz (Art. 6 UWG und Art. 162 StGB) rechtlich absichern. Die Einführung eines spezifischen Rechts an Datenbanken wäre deshalb nur erforderlich, wenn die Gewährung von Cybersicherheit, ein gutes Zugangsmanagement und die sorgfältige Verwaltung von Berechtigungen nicht ausreichen würden, um die Übernahme der Inhalte von Datenbanken und deren Verwertung durch Dritte zu verhindern. Dies scheint allerdings nicht der Fall zu sein. Vielmehr hat die EU-Kommission schon in der ersten Evaluation der Datenbanken-RL im Jahr 2005 eingeräumt, dass *keine positiven Auswirkungen des neu geschaffenen Schutzes erkennbar* seien[274]. An dieser Feststellung hat sich seither nichts geändert[275]. Gestützt auf die tatsächliche Herrschaft über Datenbanken sind *Transaktionen über ganze Datenbanken* oder Teile davon ohne weiteres möglich. Wie bei Transaktionen an Daten reichen die Mittel des Vertragsrechts hierfür allerdings ohne weiteres aus[276]. Und wie dort ist auch hier nicht erkennbar, dass Transaktionen wegen des fehlenden Rechtsschutzes unterbleiben würden. Aus einer theoretischen Perspektive besteht damit kein Anlass, einen dem europäischen *sui-generis*-Recht vergleichbaren Rechtsschutz für Datenbanken zu schaffen.

Aus einer *praktischen Perspektive* könnte sich, wie beim Dateneigentum[277], ein Bedarf nach einem spezifischen Schutzrecht für Datenbanken ergeben, wenn konkrete Probleme bestehen würden, die sich mit den bestehenden Rechtsregeln nicht überzeugend lösen liessen. Anders als bei einem allfälligen Dateneigentum oder einem Datenbesitz sind solche Probleme allerdings kaum ersichtlich. Vielmehr betreffen die meisten der für Dateneigentum und Datenbesitz untersuchten praktischen Probleme zwar eine Mehrzahl von Daten, aber nicht ganze Datenbanken im Sinn des *sui-generis*-Rechts[278]. Soweit Datenbanken betroffen sind, kann für mögliche Lösungsansätze auf die Ausführungen zu Dateneigentum und Datenbesitz verwiesen werden, die nicht nur für eine begrenzte Menge von Daten, sondern auch für ganze Datenbanken gelten[279]. Spezifische praktische Probleme, die nur oder zumindest ganz besonders bei Datenbanken auftreten, sind nicht ersichtlich.

271 Siehe dazu vorn, C.II.4.
272 Siehe dazu vorn, D.I.1.b)
273 Thouvenin/Weber/Früh, Datenpolitik, 9.
274 Europäische Kommission, Evaluation, 25; siehe dazu auch Kur, GRUR Int. 2006, 726; Köklü, 307.
275 Europäische Kommission, Study legal protection of databases, ii.
276 Siehe dazu vorn, D.I.1.b)(iii).
277 Siehe dazu vorn, D.I.
278 Siehe dazu vorn, C.II.4.
279 Siehe dazu vorn, D.I und D.II.

Damit lässt sich festhalten, dass die Einführung eines spezifischen Schutzrechts für Datenbanken in der Schweiz (auch heute) nicht sinnvoll wäre[280]. Die Erfahrung der EU hat vielmehr gezeigt, dass ein solches Schutzrecht keine erkennbaren positiven Effekte zu erzielen vermag. Die negativen Effekte würden sich zwar wohl in Grenzen halten, zumal der Anwendungsbereich eines solchen Schutzrechts begrenzt wäre und ihm auch keine dem Eigentum vergleichbare transversale Bedeutung in der Rechtsordnung zukommen würde. Das weitgehende Fehlen negativer Effekte allein kann allerdings nicht als Argument für die Einführung eines neuen Schutzrechts angeführt werden.

Ein Schutzbedarf bestünde folglich nur, wenn keine Datenbanken mehr geschaffen würden, weil deren Inhaber davon ausgehen müssten, die Leistung würde so rasch und umfassend von Dritten übernommen, dass eine Amortisation unmöglich wäre. Die Übernahme und Verwertung der Inhalte von Datenbanken wird allerdings meist schon dadurch verhindert, dass diese durch angemessene faktische Massnahmen gegen den Zugriff Dritter geschützt werden. In diesen Konstellationen – und auch bei öffentlich zugänglichen Datenbanken – greift (bei angemessener Auslegung und Anwendung) zudem der Schutz von Art. 5 lit. c UWG.

IV. Fazit

Die vorstehende Analyse hat gezeigt, dass aus heutiger Sicht mit Bezug auf Sachdaten weder aus einer theoretischen noch aus einer praktischen Perspektive ein Bedarf nach der Einführung eines Dateneigentums, eines Datenbesitzes oder eines Schutzrechts für Datenbanken besteht.

Aus theoretischer Perspektive lässt sich festhalten, dass die heutigen Märkte für die Produktion, die Nutzung und den Handel mit Sachdaten auch (und vielleicht: gerade) ohne Eigentumsrechte an Daten grundsätzlich funktionieren. Namentlich erscheint es nicht erforderlich, dass die Rechtsordnung weitere Anreize für das Sammeln und Analysieren von Sachdaten setzt[281]. Ein Eigentum an Sachdaten dürfte zudem weder die Transaktionskosten senken und dadurch den Handel mit Daten fördern[282] noch die Allokation von Kosten und Nutzen verbessern[283]. Dasselbe gilt für das Schaffen von Datenbesitz und die Einführung eines spezifischen Schutzrechts an Datenbanken.

Aus praktischer Perspektive erscheint ein Eigentum an Sachdaten zwar als Möglichkeit, gewisse Probleme zu lösen, die sich mit den geltenden Rechtsregeln nur teilweise lösen lassen. Die Rechtsordnung steht aber derzeit nicht vor grundlegenden Problemen, die nur mit der Einführung eines Eigentums an Sachdaten gelöst werden könnten. Vielmehr sind einige spezifische Probleme erkennbar, die sich mit spezifischen Anpassungen einiger konkreter Rechtsnormen bewältigen lassen, etwa im Schuldbetreibungs- und Konkursrecht[284], im Erbrecht[285] oder bei der Übertragung von Wertrechten auf der *Blockchain*[286]. Auch aus einer praktischen Perspektive ist deshalb von der Einführung eines Eigentums an Sachdaten abzusehen. Dasselbe gilt auch für das Schaffen von Datenbesitz und die Einführung eines spezifischen Schutzrechts an Datenbanken.

Offen bleibt einstweilen, ob sich ein Schutz *öffentlich zugänglich gemachter Sachdaten* rechtfertigen könnte, um Anreize für eine intensivere Datennutzung *(data sharing)* zu schaffen. Dies ist bisher noch nicht hinreichend erforscht.

280 Zu entsprechenden Forderungen in der URG-Revision von 2007 siehe Botschaft URG 2007, BBl 2006 3407; SHK-URG, Auf der Maur, Art. 33 N 10; kritisch zum *sui-generis* Recht auch Weber, 590. Argumente für ein solches Recht finden sich hingegen bei BSK-UWG, Arpagaus, Art. 5 N 38; Gilliéron, Medialex 2010, 71 ff., 75 sowie Adler, Medialex 1997, 65 f.
281 Siehe dazu vorn, D.I.1.b)(ii).
282 Siehe dazu vorn, D.I.1.b)(iii).
283 Siehe dazu vorn, D.I.1.a).
284 Siehe dazu vorn, D.I.2.d).
285 Siehe dazu vorn, D.I.2.d).
286 Siehe dazu vorn, D.I.2.g).

E. Erkenntnisse

Die vorliegende Studie hat zu den folgenden Erkenntnissen geführt:

1. Der *Begriff der Sachdaten* ist – im Gegensatz zum Begriff der Personendaten – nicht gesetzlich definiert. Sein Gehalt bestimmt sich durch Umkehrschluss: Sachdaten sind alle Daten, die nicht als Personendaten zu qualifizieren sind. Da vom jeweiligen Kontext abhängt, ob Daten als Personendaten zu qualifizieren sind (relativer Begriff), lässt sich der Gegenstand der Untersuchung dieser Studie nicht *ex ante* auf bestimmte Konstellationen eingrenzen. Vielmehr lässt sich nur *ex post* bestimmen, ob Daten in einer konkreten Konstellation als Sachdaten zu qualifizieren sind.

2. Die *Nutzung von Sachdaten* ist frei. Wer also über Sachdaten verfügt oder auf diese zugreifen kann, darf diese auch verwenden. Einschränkungen ergeben sich nur aus allfälligen Rechten Dritter, bspw. Immaterialgüterrechten.

3. Das Schweizer Recht kennt *kein Eigentum an Sachdaten*. Es enthält aber verschiedene Normen, die den Inhabern von Sachdaten unter bestimmten Voraussetzungen eine Rechtsposition vermitteln, die einem Eigentum an Sachdaten nahekommt. Dabei ist zwischen einer absolut-rechtlichen Zuordnung und einem rechtlichen Schutz der faktischen Zuordnung zu unterscheiden. Beide Ansätze können einen Anspruch auf Unterlassung der Nutzung und auf Herausgabe der Sachdaten sowie auf Schadenersatz vermitteln; diese Ansprüche wirken gegenüber jedermann *(erga omnes)*:

   - Eine *absolut-rechtliche Zuordnung* vermitteln die *Immaterialgüterrechte*, insbesondere das Urheberrecht, das Patentrecht und die urheberrechtlichen Leistungsschutzrechte. Diese Schutzinstrumente beziehen sich zwar auf Informationen als immaterielle Güter (semantische Ebene), sie erfassen aber auch die Repräsentation dieser Informationen in Form von Daten (syntaktische Ebene).

   - Einen *rechtlichen Schutz der faktischen Zuordnung* vermitteln insbesondere das UWG und das Strafrecht. Im Vordergrund stehen dabei der Schutz von Geschäftsgeheimnissen (Art. 6 UWG und Art. 162 StGB) und der Schutz gegen die unmittelbare Übernahme marktreifer Arbeitsergebnisse durch technische Reproduktionsverfahren (Art. 5 lit. c UWG). Voraussetzung für die Anwendung von Art. 5 lit. c UWG ist allerdings, dass Sachdaten und entsprechende Datenbanken (richtigerweise) als marktreife Arbeitsergebnisse verstanden werden.

4. Eigentumsähnliche Rechtspositionen an Sachdaten lassen sich auch durch *vertragliche Vereinbarungen* schaffen. Diese wirken aber immer nur unter den Vertragsparteien *(inter partes)*.

5. Die *Einführung eines neuen Rechtsinstruments* für die Zuordnung von Sachdaten – insbesondere ein Dateneigentum, ein Datenbesitz oder ein spezifisches Schutzrecht für Datenbanken – wäre nur angezeigt, wenn dies nicht nur aus theoretischer, sondern auch aus praktischer Perspektive erforderlich wäre. Beides ist nicht der Fall.

   - Aus *theoretischer Perspektive* ist entscheidend, dass in den Märkten für Sachdaten *kein Marktversagen* vorliegt, weder bei der «Produktion» von Sachdaten und entsprechenden Datenbanken noch bei Transaktionen mit solchen Daten.

   - Aus *praktischer Perspektive* ist massgeblich, dass im Kontext von Sachdaten zwar gewisse praktische Probleme bestehen. Diese sind aber nicht derart allgemein oder umfassend, dass sie sich nur mit einem neuen Rechtsinstrument zur Zuordnung von Sachdaten lösen liessen. Die konkreten Probleme sind vielmehr durch spezifische Anpassungen der Rechtslage zu lösen, etwa im Erbrecht oder im Schuldbetreibungs- und Konkursrecht. Diesen Weg hat der Gesetzgeber bereits eingeschlagen und einzelne Anpassungen vorgenommen.

Damit besteht *kein Anlass für die Schaffung eines neuen Rechtsinstruments* für die Zuordnung von Sachdaten. Das gilt für den Datenbesitz und ein spezifisches Schutzrecht für Datenbanken – und ganz besonders für ein Dateneigentum.

6. Neben dem fehlenden Bedarf sprechen zwei weitere Gründe gegen die Einführung eines Eigentums an Sachdaten:

   - Zum einen würde sich ein Eigentum an Sachdaten wegen der transversalen Bedeutung des Eigentums in der Rechtsordnung auf eine Vielzahl anderer Normen auswirken und ein solches Recht könnte neue praktische Probleme hervorrufen, die heute noch gar nicht erkennbar sind. Es besteht deshalb die Gefahr, dass ein *Eigentum an Sachdaten mehr Probleme schaffen als lösen würde*.

   - Zum andern erscheint die Schaffung eines Eigentums (nur) an Sachdaten schon deshalb ausgeschlossen, weil der Gegenstand eines solchen Eigentums nicht *ex ante* bestimmt werden kann. Ob Daten als Sachdaten zu qualifizieren sind, hängt vom jeweiligen Kontext ab, ein und dasselbe Datum kann deshalb in einer Konstellation als Sach- und in einer anderen als Personendatum zu qualifizieren sein. Ein Eigentum an Sachdaten würde damit, je nach Kontext, bestehen, fehlen, begründet werden oder wieder entfallen. An einem derart *fluiden Gegenstand können nicht sinnvoll Eigentumsrechte* begründet werden.

7. Die Analyse der Schutzinstrumente im geltenden Recht hat gezeigt, dass dem Geheimnisschutz (Art. 6 UWG und Art. 162 StGB) für die Zuordnung von Sachdaten zentrale Bedeutung zukommt. Bei *öffentlich zugänglichen Sachdaten* greift dieser Schutzmechanismus aber nicht. Hier könnte deshalb ein Schutzbedarf bestehen. Ob dieser allerdings ausgewiesen ist, erscheint fraglich, zumal kaum einzusehen ist, weshalb die Rechtsordnung Mittel zur Kontrolle der Nutzung von Sachdaten zur Verfügung stellen sollte, wenn diese Daten von deren Inhaber selbst öffentlich zugänglich gemacht worden sind. Anderes mag gelten, wenn Dritte Sachdaten gegen den Willen des Inhabers öffentlich zugänglich gemacht haben. Diese Konstellation dürfte allerdings äusserst selten sein; sie vermag deshalb kaum einen Bedarf zur Einführung eines Eigentums an Sachdaten zu begründen. Wenn ein Schutzbedarf dennoch bejaht werden sollte und man (zugleich) *Anreize für das öffentliche Zugänglichmachen von Sachdaten setzen* möchte, wäre es allerdings denkbar, dass die Rechtsordnung – ähnlich wie im Patentrecht, aber unter Verzicht auf eine Prüfung und Registrierung – einen Schutz von Sachdaten dann (aber nur dann) gewährt, wenn diese öffentlich zugänglich gemacht werden.

F. Verzeichnis
Literatur

Abegg-Vaterlaus Lukas, Von 3D Druckern und Blockchain Tokens – Digitale Sachverhalte im Recht, in: Maute/Mackenrodt (Hrsg.), GRUR Junge Wissenschaft, Recht als Infrastruktur für Innovation, Baden-Baden 2019, 319

Adler Tibère, Bases de données, sites Internet, «produits intellectuels»: quelle protection?, Medialex 1997, 65 f.

Amstutz Marc, Dateneigentum, Funktion und Form, AcP 2018, 438–551

Amstutz Marc/Roberto Vito/Trüeb Hans Rudolf (Hrsg.), Handkommentar zum Schweizerischen Privatrecht, Wirtschaftsrechtliche Nebenerlasse: FusG, UWG, PauRG und KKG, 3. Aufl., Zürich 2016 (zit. CHK–UWG, Bearbeiterin)

Arnet Ruth, in: Breitschmid/Jungo (vgl. dort), Art. 641–645 ZGB

Arnet Ruth/Eitel Paul, in: Breitschmid/Jungo (vgl. dort), Art. 919–941 ZGB

Arpagaus Reto, in: Hilty/Arpagaus (vgl. dort), Art. 5 UWG

Arpagaus Reto/Frick Markus R., in: Hilty/Arpagaus (vgl. dort), Art. 5 UWG

Arrow Kenneth J., Economic Welfare and the Allocation of Resources for Invention, in: Universities-National Bureau Committee for Economic Research, Committee on Economic Growth of the Social Science Research Council National Bureau of Economic Research (Hrsg.), The Rate and Direction of Inventive Activity: Economic and Social Factors, Princeton 1962, 609–626

Auf der Maur Rolf, in: Müller/Oertli (vgl. dort), Art. 33 URG

Barrelet Denis/Egloff Willi, Das Neue Urheberrecht, Kommentar zum Bundesgesetz über das Urheberrecht und verwandte Schutzrechte, 4. Aufl., Bern 2020 (zit. Barrelet/Egloff, Bearbeiterin)

Baudenbacher Carl (Hrsg.), Lauterkeitsrecht, Kommentar zum Gesetz gegen den unlauteren Wettbewerb (UWG), Basel/Genf/München 2001 (zit. Baudenbacher, Bearbeiterin)

Baudenbacher Carl, in: Baudenbacher (vgl. dort), Art. 5

Baudenbacher Carl/Glöckner Jochen, in: Baudenbacher (vgl. dort), Art. 6

Bauer Hannes/Fuhr Alfred/Heynike François/Schönhagen Leonie, Risikofeststellung Dateneigentum, in: Stiftung Datenschutz (Hrsg.), Dateneigentum und Datenhandel, Berlin 2019, 15–28

Belser Eva Maria/Epiney Astrid/Waldmann Bernhard, Datenschutzrecht, Bern 2011

Benhamou Yaniv/Tran Laurent, Circulation des biens numériques: de la commercialisation à la portabilité des données, sic! 2016, 571–591

Berberich Matthias/Golla Sebastian, Zur Konstruktion eines «Dateneigentums» – Herleitung, Schutzrichtung, Abgrenzung, PinG 2016, 165–176

Berger Mathis, Die Immaterialgüterrechte sind abschliessend aufgezählt (numerus clausus), in: Kurer/Ritscher/Sangiorgio/Aschmann (Hrsg.), Binsenwahrheiten des Immaterialgüterrechts, Festschrift für Lucas David zum 60. Geburtstag, Zürich 1996, 3–8

Blechta Gabor-Paul, in: Maurer-Lambrou/Blechta (vgl. dort), Art. 2 und 3 DSG

Brauchbar Birkhäuser Simone, in: Jung/Spitz (vgl. dort), Art. 5 UWG

Bräutigam Peter/Klindt Thomas, Digitalisierte Wirtschaft/Industrie 4.0, Gutachten im Auftrag der BDI zur rechtlichen Situation, zum Handlungsbedarf und zu ersten Lösungsansätzen, November 2015, <http://bdi.eu/media/themenfelder/digitalisierung/downloads/20151117_Digitalisierte_Wirtschaft_Industrie_40_Gutachten_der_Noerr_LLP.pdf>

Brehm Roland, Berner Kommentar, Die Entstehung durch unerlaubte Handlungen, Art. 41–61 OR, 4. Aufl., Bern 2013 (zit. BK–OR, Bearbeiterin)

Breitschmid Peter/Jungo Alexandra (Hrsg.), Handkommentar zum Schweizerischen Privatrecht, Sachenrecht, Art. 641–977 ZGB, 3. Aufl., Zürich 2016 (zit. CHK–ZGB, Bearbeiterin)

Briner Robert G., Big Data und Sachenrecht, Jusletter IT 21. Mai 2015

Büchler Andrea/Jakob Dominique (Hrsg.), Kurzkommentar, Schweizerisches Zivilgesetzbuch, Basel 2018 (zit. KUKO–ZGB, Bearbeiterin)

Buchner Benedikt, Is there a Right to One's Own Personal Data?, ZGE 2017, 416–419

Budzikiewicz Christine, Digitaler Nachlass, AcP 2018, 558–593

Bühler Gregor, Verlust von Daten, Jusletter IT Flash 11. Dezember 2017

Bull Hans Peter, Wieviel sind „meine Daten" wert?, CR 2018, 425–432

von Büren Roland/David Lucas (Hrsg.), Schweizerisches Immaterialgüter- und Wettbewerbsrecht, SIWR I/1 Grundlagen, 2. Aufl., Basel 2002, (zit. SIWR I/1, BearbeiterIn)

von Büren Roland/David Lucas (Hrsg.), Schweizerisches Immaterialgüter- und Wettbewerbsrecht, SIWR II/1, 3. Aufl., Basel 2014, (zit. SIWR II/1, BearbeiterIn)

Bürgi Urs, in: Hunkeler (vgl. dort), Art. 242 SchKG

Cheneval Francis, Property rights of personal data and the financing of pensions, CRISPP 2018, 1–23

Cherpillod Ivan, in: Müller/Oertli (vgl. dort) Art. 4 URG

Cherpillod Ivan, in: De Werra/Gilliéron (vgl. dort), Art. 10 LDA

Chrobak Lennart, Digital Estate «Revisited», Jusletter IT Flash 11. Dezember 2017

Cohen Guy, Reflection on 'data ownership', in: The British Academy/The Royal Society/techUK (Hrsg.), Data ownership, rights and controls: Reaching a common understanding, Discussion at a British Academy, Royal Society and techUK seminar on 3 October 2018, Grossbritannien, 26–27

David Lucas, Ist der Numerus clausus der Immaterialgüterrechte noch zeitgemäss?, AJP 1995, 1403–1410

Denga Michael, Gemengelage privaten Datenrechts, NJW 2018, 1371–1376

Dessemontet François, in: von Büren/Lucas (vgl. dort), Einführung: Immaterialgüterrecht und Privatrecht, 1–24

Determann Lothar, Gegen Eigentumsrechte an Daten, ZD 2018, 503–508

Determann Lothar, Kein Eigentum an Daten, MMR 2018, 277–278

Determann Lothar, No One Owns Data, Hastings L. J. 2018, 1–44

De Werra Jacques/Gilliéron Philippe (Hrsg.), Commentaire Romand, Propriété intellectuelle, Basel 2013 (zit. CR-LDA, BearbeiterIn)

De Werra Jacques, Création d'un accès non-volontaire aux données non-personnelles par un mécanisme général de licences obligatoires ou de licences FRAND, Rapport pour l'Institut Fédéral de la Propriété Intellectuelle, Genf 2020

Domej Tania/Schmidt Céline P., in: Büchler/Jakob (vgl. dort), Art. 641

Donatsch Andreas (Hrsg.) StGB-Kommentar, Schweizerisches Strafgesetzbuch mit V-StGB-MStG und JStG, 20. Aufl., Zürich 2018, (zit. Donatsch, BearbeiterIn)

Dorner Michael, Know-how-Schutz im Umbruch, Köln 2013

Dorner Michael, Big Data und «Dateneigentum», Grundfragen des modernen Daten- und Informationshandels, CR 2014, 617–628

Drexl Josef/Hilty Reto M./Desaunettes Luc/Greiner Franziska/Kim Daria/Richter Heiko/Surblyté Gintaré/Wiedemann Klaus, Data Ownership and Access to Data, Position Statement of the Max Planck Institute for Innovation and Competition, Research Paper No. 16–10, 16. August 2016

Druey Jean Nicolas, Information als Gegenstand des Rechts, Zürich 1995

Eckert Martin, Digitale Daten als Wirtschaftsgut: digitale Daten als Sache, SJZ 2016, 245–249

Eckert Martin, Digitale Daten als Wirtschaftsgut: Besitz und Eigentum an digitalen Daten, SJZ 2016, 265–274

Egloff, Willi, in: Barrelet/Egloff (vgl. dort), Art. 4, 10, 33 und 38 URG

Eigenmann Antoine/Fanti Sébastien, Successions, Données Personnelles, Numériques et Renseignements, SJ 2017 II, 193–226

Elteste Ulrike, Screen Scraping, CR 2015, 447–451

Ernst Wolfgang, in: Geiser/Wolf (vgl. dort), Art. 919–941 ZGB

Esken Saskia, Dateneigentum und Datenhandel, in: Stiftung Datenschutz (Hrsg.), Dateneigentum und Datenhandel, Berlin 2019, 73–83

Fahrländer Lukas, in: Heizmann/Loacker (vgl. dort), Vor Art. 5 UWG, Art. 5 lit. a und b UWG

Fairfield Joshua A.T., Virtual Property, Boston Univ. L. Rev. 2005, 1047–1102

Ferrari Hofer Lorenza/Vasella David, in: Amstutz/Roberto/Trüeb (vgl dort), Art. 6 UWG

Fezer Karl-Heinz, Dateneigentum der Bürger, ZD 2017, 99–105

Fezer Karl-Heinz, Repräsentatives Dateneigentum, ein zivilgesellschaftliches Bürgerrecht, Studie im Auftrag der Konrad-Adenauer-Stiftung e.V. zum Thema „Einführung eines besonderen Rechts an Daten", Sankt Augustin 2018

Fiolka Gerhard, in: Niggli/Wiprächtiger (vgl. dort), Art. 147 StGB

Flückiger Alexandre, L'autodétermination en matière de données personnelles: un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété?, AJP 2013, 837–864

Flume Johannes W., in: Hau/Posek (vgl. dort), § 249 Art und Umfang des Schadensersatzes

Frick Markus R., in: Hilty/Arpagaus (vgl. dort), Art. 46 UWG

Fröhlich-Bleuler Gianni, Eigentum an Daten?, Jusletter 6. März 2017

Früh Alfred, Datenzuordnung und Datenzugang. Eine Übersicht über Stand und Entwicklungspotenziale zweier komplementärer Aspekte der Datenpolitik, digma 2019, 172–177

Fuchs Nicolas, Die Besitzesschutzklagen nach Art. 927 ff. ZGB, Zürich/St. Gallen

Gaster Jens, Teil 7.6, Sui-generis-Recht der Datenbankrichtlinie in: Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, 51. EL, Februar 2020

Geiser Thomas/Wolf Stephan (Hrsg.), Zivilgesetzbuch II, Art. 457–977, Art. 1–61 SchlT ZGB, 6. Aufl., Basel 2019 (zit. BSK–ZGB II, Bearbeiterin)

Gerschwiler, Stefan, in: Passadelis/Rosenthal/Thür (vgl. dort), § 3, Prinzipien der Datenbearbeitung durch Privatpersonen und Behörden

Gilliéron Philippe, Google Actualités: faux problème ou vrai danger pour les éditeurs de presse?, Medialex 2010, 71 ff.

Golliez André, Zugang zu Sachdaten im privaten Sektor als Open und Shared Data, Bericht im Auftrag des Eidgenössischen Instituts für Geistiges Eigentum IGE, 2020

Haab Robert/Simonius August/Scherrer Werner/Zobl Dieter (Hrsg.), Zürcher Kommentar, Kommentar zum Schweizerischen Zivilgesetzbuch, Band IV: Das Sachenrecht, Erste Abteilung, Das Eigentum, Art. 641 bis 729, 2. Aufl., Zürich 1977 (zit. ZK–ZGB, Haab)

Hagen Wolfgang, Facebook & Google entflechten? Warum digitale Medien-Monopole eine Gefahr für Demokratien sind – Essay, Medienpolitik, APuZ 2018, 29–34

Hau Wolfgang/Poseck Roman (Hrsg.), Beck'scher Online-Kommentar BGB, 54. Edition, München 2020 (zit. Hau/Poseck, Bearbeiterin)

Heiss Helmut, in: Heizmann/Loacker (vgl. dort), Art. 8 UWG

Heizmann Reto/Loacker Leander D. (Hrsg.), UWG Bundesgesetz gegen den unlauteren Wettbewerb, Kommentar, Zürich 2018 (zit. Heizmann/Loacker, Bearbeiterin)

Heller Michael A., The Tragedy of the Anticommons: Property in the Transition from Marx to Markets, Harv. L. Rev. 1998, 621–688

Hess-Odoni Urs, Die Herrschaftsrechte an Daten, Jusletter 17. Mai 2004

Heymann Thomas, Rechte an Daten, Warum Daten keiner eigentumsrechtlichen Logik folgen, CR 2016, 650–657

Hildebrandt Mireille, Properties, property and appropriateness of information, in: Hildebrandt/van der Berg (Hrsg.), Information, Freedom and Property, Abingdon 2016, 34–53

Hilty Reto M., Die Leistungsschutzrechte im schweizerischen Urheberrechtsgesetz, UFITA 1994, 85–140

Hilty Reto M., Lizenzvertragsrecht, Bern 2001 (zit. Lizenzvertragsrecht)

Hilty Reto M., «Leistungsschutz» – made in Switzerland? Klärung eines Missverständnisses und Überlegungen zum allgemeinen Schutz von Investitionen, in: Ahrens/Bornkamm/Kunz-Hallstein (Hrsg.), Festschrift für Eike Ullmann, Saarbrücken 2006 (zit. Leistungsschutz)

Hilty Reto M., Urheberrecht, Bern 2011 (zit. Urheberrecht)

Hilty Reto M./Arpagaus Reto (Hrsg.), Basler Kommentar, Bundesgesetz gegen den unlauteren Wettbewerb (UWG), Basel 2013 (zit. BSK–UWG, BearbeiterIn)

Hoeren Thomas, Dateneigentum, Versuch einer Anwendung von § 303a StGB im Zivilrecht, MMR 2013, 486–491

Hoeren Thomas, Big data and the ownership in data: recent developments in Europe, EIPR 2014, 751–754

Hoeren Thomas, Sieben Beobachtungen und eine Katastrophe, sic! 2014, 212–217

Hoeren Thomas, Datenbesitz statt Dateneigentum, MMR 2019, 5–8

Hoeren Thomas, Datenbesitz statt Dateneigentum?, Jusletter 11. Mai 2020

Horn Nikolai/Reinhardt Marc, Arbeitsgruppe Innovativer Staat, Denkimpuls Innovativer Staat: Datenhoheit – Gerechtigkeitsfrage in einer Digitalen Gesellschaft, Initiative D21, 8. Oktober 2018

Hornung Gerrit/Goeble Thilo, Data ownership im vernetzten Automobil, CR 2015, 265–273

Hrubesch-Millauer Stephanie/Graham-Siegenthaler Barbara/Roberto Vito, Sachenrecht, 5. Aufl., Bern 2017

Hugenholtz Bernt, Data Property in the System of Intellectual Property Law: Welcome Guest or Misfit?, in: Schulze/Staudenmayer/ Lohsse (Hrsg.), Trading Data in the Digital Economy: Legal Concepts and Tools, Münster Colloquia on EU Law and the Digital Economy III, Baden-Baden 2017, 75–99 (zit. System of Intellectual Property Law)

Hugenholtz Bernt, Against ‚data property', in: Ullrich/Drahos/Ghidini (Hrsg.), Kritika: Essays on Intellectual Property, Cheltenham/Northampton 2018, 48–71 (zit. Against ‚data property')

Hunkeler Daniel (Hrsg.), Kurzkommentar SchKG, Schuldbetreibungs- und Konkursgesetz, 2. Auflage, Basel 2014 (zit. KUKO–SchKG, BearbeiterIn)

Hürlimann Daniel/Zech Herbert, Rechte an Daten, sui generis 2016, 89–95

Isenring Stefan, in: Donatsch (vgl. dort), Art. 320 StGB

Janeček Václav, Ownership of personal data in the Internet of Things, CLSR 2018, 1039–1052

Jarchow Thomas/Estermann Beat, BAKOM, Big Data: Chancen, Risiken und Handlungsbedarf des Bundes, Ergebnisse einer Studie im Auftrag des Bundesamts für Kommunikation, 26. Oktober 2015

Jecklin Barbara, Leistungsschutz im UWG, Bern 2003

Jentzsch Nicola, Dateneigentum – Eine gute Idee für die Datenökonomie?, Stiftung Neue Verantwortung, Berlin 2018

Jenny Andreas, Die Nachahmungsfreiheit, Zürich 1997

Jung Peter/Spitz Philippe (Hrsg.), Bundesgesetz gegen den unlauteren Wettbewerb (UWG), 2. Aufl., Bern 2016 (zit. SHK-UWG, BearbeiterIn)

Kaiser Barbara, Werbeblocker – grünes Licht für ein rotes Tuch, in: Thouvenin/Weber (Hrsg.), Werbung – Online, Zürich 2017, 161–194

Kerber Wolfgang, Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection, GRUR Int. 2016, 639–647

Kerber Wolfgang, A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis, GRUR Int. 2016, 989–998

Kerber Wolfgang, Governance of Data: Exclusive Property vs. Access, IIC 2016, 759–762

Kessler Martin, in: Widmer Lüchinger/Oser (vgl. dort), Art. 41, Art. 43 OR

Kilian Wolfgang, Personal Data: The Impact of Emerging Trends, CRi 2012, 169–175

Köklü Kaya, Sui generis Schutz von Datenbanken, in: Hilty/Jaeger (Hrsg.), Europäisches Immaterialgüterrecht, Funktionen und Perspektiven, Berlin 2018, 306–310

Kramer Stefan/Oser David/Meier Urs, Tokenisierung von Finanzinstrumenten de lege ferenda, Unter besonderer Berücksichtigung von nicht kotierten Aktien, Jusletter 6. Mai 2019

Kren Kostkiewicz Jolanta/Wolf Stephan/Amstutz Marc/Fankhauser Roland (Hrsg.), ZGB Kommentar, Schweizerisches Zivilgesetzbuch, 3. Aufl., Zürich 2016 (zit. Kren Kostkiewicz et al., BearbeiterIn)

Kreutz Oliver, Der Webseitennutzungsvertrag – Fiktion oder unbekanntes Rechtsgeschäft?, ZUM 2018, 162–168

Kübler Philip, Rechtsschutz von Datenbanken (EU-USA-Schweiz), Zürich 1999, 269 ff.

Kühling Jürgen/Sackmann Florian, Rechte an Daten, Regulierungsbedarf aus Sicht des Verbraucherschutzes?, Rechtsgutachten im Auftrag des Verbraucherzentrale Bundesverbandes, 20. November 2018

Kuhn Hans/Stengel Cornelia/Meisser Luzius/Weber Rolf H., Wertrechte als Rechtsrahmen für die Token-Wirtschaft, Jusletter IT 23. Mai 2019

Landreau Isabelle/Peliks Gérard/Binctin Nicolas/Pez-Pérard Virginie, My data are mine, report, GenerationLibre, Paris 2018

Laudon Kenneth C., Markets and Privacy, Communications of the ACM 1996 No. 9, 92–104

Laux Christian, Das Recht auf Datenportabilität, digma 2019, 166–170

Lessig Lawrence, The Future of Ideas, New York 2001

Locke John, Zweite Abhandlung über die Regierung, Kommentar von Ludwig Siep, Frankfurt am Main 2007

Luckey Jan, in: Prütting/Wegen/Weinreich (Hrsg.), BGB Kommentar, 14. Aufl. Köln 2019

Mabillard Ramon, in: Jung/Spitz (vgl. dort), Art. 6 UWG

Marbach Eugen/Ducrey Patrik/Wild Gregor, Immaterialgüter- und Wettbewerbsrecht, 4. Aufl., Bern 2017

Martenet Vincent/Pichonnaz Pascal (Hrsg.), Commentaire Romand, Loi contre la concurrence déloyale, Basel 2017 (CR–LCD, BearbeiterIn)

Marx Gary T., Genies: bottled and unbottled, in: Hildebrandt/van der Berg (Hrsg.), Information, Freedom and Property, Abingdon 2016, 9–33

Mauerhofer Marc André, Die Rechtsstellung des Lizenznehmers im Verletzungsprozess, Zürich/St. Gallen 2010

Maurer-Lambrou Urs/Blechta Gabor-Paul (Hrsg.), Datenschutzgesetz/Öffentlichkeitsgesetz, 3. Aufl., Basel 2014 (zit. BSK-DSG, BearbeiterIn)

Meyerdierks Per, Sind IP-Adressen personenbezogene Daten?, MMR 2009, 8–13

Michl Fabian, «Datenbesitz» – ein grundrechtliches Schutzgut?, NJW 2019, 2729–2733

Moore Adam/Himma Ken, "Intellectual Property", in: Zalta (Hrsg.), The Stanford Encyclopedia of Philosophy (Winter 2018 Edition), <https://plato.stanford.edu/archives/win2018/entries/intellectual-property>, zuletzt besucht am 10. Juli 2019

Mosimann Peter, in: von Büren/Lucas (vgl. dort), Verwandte Schutzrechte, 229–412

Müller Barbara K./Oertli Reinhard (Hrsg.), Urheberrechtsgesetz (URG), 2. Aufl., Bern 2012 (zit. SHK–URG, BearbeiterIn)

Naumer Hans-Jörg, Dateneigentum statt Datenkapitalismus, in: Stiftung Datenschutz (Hrsg.), Dateneigentum und Datenhandel, Berlin 2019, 233–239

Neuenschwander Peter K./Oeschger Simon, Daten im Konkurs, Jusletter IT Flash 11. Dezember 2017

Niggli Marcel Alexander/Hagenstein Nadine, in: Niggli/Wiprächtiger (vgl. dort), Art. 162 StGB

Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), Strafrecht I + II, Strafgesetzbuch, Jugendstrafgesetz, Basler Kommentar, 4. Aufl., Basel 2018 (zit. BSK–StGB, BearbeiterIn)

Nussbaumer Arnaud, in: Martenet/Pichonnaz (vgl. dort), Art. 5 LCD

Oberholzer Niklaus, in: Niggli/Wiprächtiger (vgl. dort), Art. 320 StGB

Oberson Xavier, Taxer les robots? L'émergence d'une capacité contributive électronique, AJP 2017, 232–239

Passadelis Nicolas/Rosenthal David/Thür Hanspeter (Hrsg.), Datenschutzrecht, Beraten in Privatwirtschaft und öffentlicher Verwaltung, Basel 2015 (zit. Passadelis/Rosenthal/Thür, BearbeiterIn)

Paal Boris P./Hennemann Moritz, Big Data im Recht – Wettbewerbs- und daten(schutz)rechtliche Herausforderungen, NJW 2017, 1697–1701

Pedrazzini Federico A./Pedrazzini Mario M., Unlauterer Wettbewerb UWG, 2. Aufl., Bern 2001

Pfortmüller Herbert, in: Müller/Oertli (vgl. dort), Art. 10 URG

Pichonnaz Pascal in: Pichonnaz/Foëx/Piotet (vgl. dort), Art. 919 CC

Pichonnaz Pascal/Foëx Bénédict/Piotet Denis (Hrsg.), Commentaire Romand, Code civil II, art. 457–977 CC, art. 161 Tit. fin. CC, Basel 2016 (zit. CR-CC II, BearbeiterIn)

Picht Peter Georg, Vom materiellen Wert des Immateriellen, Jus Privatum, Beiträge zum Privatrecht, Band 230, Tübingen 2018

Podszun, Rupprecht, Wandlungen des Schutzgegenstands, in: Dreier/Hilty (Hrsg.), Vom Magnettonband zu Social Media, Festschrift 50 Jahre Urheberrechtsgesetz (UrhG), 2015, 361–378

Pombriant Denis, Data, Information and Knowledge – Transformation of data is key, CRi 2013, 97–102

Portmann Wolfgang, Wesen und System der subjektiven Privatrechte, Zürich 1995

Probst Thomas, Die unbestimmte «Bestimmbarkeit» der von Daten betroffenen Personen im Datenschutzrecht, AJP 2013, 1423–1436

Probst Thomas, in: Jung/Spitz (vgl. dort), Art. 8 UWG

Prütting Hanns/Wegen Gerhard/Weinreich Gerd (Hrsg.), BGB Kommentar, 14. Aufl., Köln 2019 (zit. Prütting/Wegen/Weinreich, BearbeiterIn)

Purtova Nadezhda, The illusion of personal data as no one's property, LIT 2015, 83–111

Purtova Nadezhda, The law of everything. Broad concept of personal data and future of EU data protection law, LIT 2018, 40–81

Rey Heinz/Wildhaber Isabelle, Ausservertragliches Haftpflichtrecht, 5. Aufl., Zürich 2018

Richter Heiko, The Power Paradigm in Private Law, Towards a Holistic Regulation of Personal Data, in: Bakhoum/Conde Gallego/Mackenrodt/Surblytė-Namavičienė (Hrsg.), Personal Data in Competition, Consumer Protection and Intellectual Property Law, Towards a Holistic Approach?, Berlin 2018, 527–577

Richter Heiko/Hilty Reto M., Die Hydra des Dateneigentums – eine methodische Betrachtung, in: Stiftung Datenschutz (Hrsg.), Dateneigentum und Datenhandel, Berlin 2019, 241–259

Ritter Jeffrey/Mayer Anna, Regulating Data as Property: A New Construct for Moving Forward, Duke L. & Tech. Rev. 2018, 220—277

Rosenthal David, in: Rosenthal/Jöhri (vgl. dort), Art. 15 DSG

Rosenthal David/Jöhri Yvonne (Hrsg.), Handkommentar zum Datenschutzgesetz, Zürich 2008 (zit. HK–DSG, Bearbeiterin)

Russenberger Marc, in: Staehelin/Bauer (vgl. dort), Art. 242 SchKG

Säcker Franz Jürgen/Rixecker Roland/Oetker Hartmut/Limperg Bettina (Hrsg.), Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 6, Schuldrecht – Besonderer Teil IV §§ 705–853, Partnerschaftsgesellschaftsgesetz, Produkthaftungsgesetz, 7. Aufl., München 2017 (zit. Säcker et al., Bearbeiterin)

Samuelson Pamela, Privacy As Intellectual Property?, Stanford L. Rev. 2000, 1125–1173

Sattler Andreas, From Personality to Property?, in: Bakhoum/Conde Gallego/Mackenrodt/Surblytė-Namavičienė (Hrsg.), Personal Data in Competition, Consumer Protection and Intellectual Property Law, Towards a Holistic Approach?, Berlin 2018, 27–54

Schiele Felix/Laux Fritz/Connolly Thomas M., Applying a Layered Model for Knowledge Transfer to Business Process Modelling (BPM), IJAIS 2014, 156–166

Schlinkert Hans-Jürgen, Industrie 4.0 – wie das Recht Schritt hält, ZRP 2017, 222–225

Schmid Alain/Schmidt Kirsten Johanna/Zech Herbert, Rechte an Daten – zum Stand der Diskussion, sic! 2018, 627–639

Schmid Jörg/Hürlimann-Kaup Bettina, Sachenrecht, 5. Aufl., Zürich 2017

Schmid Niklaus, Computer- sowie Check- und Kreditkarten-Kriminalität, Ein Kommentar zu den neuen Straftatbeständen des schweizerischen Strafgesetzbuches, Zürich 1994

Schmidt Kirsten Johanna, Datenschutz und Big Data – Ein Spannungsverhältnis, in: Maute/Mackenrodt (Hrsg.), Recht als Infrastruktur für Innovation, GRUR Junge Wissenschaft, München 2018, 265–284

Schmidt Kirsten Johanna, Datenmärkte ohne «Dateneigentum», Wie der Handel mit Personendaten durch Anpassungen des Datenschutzrechts gefördert werden könnte, digma 2019, 178–182

Schwartmann Rolf/Hentsch Christian-Henner, Parallelen aus dem Urheberrecht für ein neues Patentverwertungsrecht, PinG 2016, 117–126

Schwarz Jörg, Geheimnisschutz- und Spionagestrafrecht, in: Ackermann/Heine (Hrsg.), Wirtschaftsstrafrecht der Schweiz, Hand- und Studienbuch, Bern 2013

Schweitzer Heike/Peitz Martin, Ein neuer europäischer Ordnungsrahmen für Datenmärkte?, NJW 2018, 275–280

Sendrowski Heiko, Zum Schutzrecht «sui generis» an Datenbanken, GRUR 2005, 369–377

Specht Louisa, Ausschliesslichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen, CR 2016, 288–296

Specht Louisa, Property Rights Concerning Personal Data, ZGE 2017, 411–415

Specht Louisa/Rohmer Rebeca, Zur Rolle des informationellen Selbstbestimmungsrechts bei der Ausgestaltung eines möglichen Ausschliesslichkeitsrechts an Daten, PinG 2016, 127–132

Spindler Gerald, Data and Property Rights, ZGE 2017, 399–405

Sprecher Franziska, Datenschutz und Big Data im Allgemeinen und im Gesundheitsrecht im Besonderen, ZBJV 2018, 482–519

Staehelin Daniel/Bauer Thomas (Hrsg.), Bundesgesetz über Schuldbetreibung und Konkurs I (Art. 1158 SchKG) + II (Art. 159352 SchKG) inkl. Ergänzungsband, 2. Aufl., Basel 2016, (zit. BSK–SchKG, Bearbeiterin)

Stark Emil W./Lindenmann Barbara (Hrsg.), Berner Kommentar, Schweizerisches Zivilgesetzbuch, Der Besitz, Art. 919–941 ZGB, 4. Aufl., Bern 2016, (zit. BK-ZGB, Bearbeiterin)

Stauber Demian, Web Scraping, Jusletter IT Flash 11. Dezember 2017

Steinauer Paul-Henri, Les droit réels, Tome I, 6. Aufl., Bern 2019

Stender-Vorwachs Jutta/Steege Hans, Wem gehören meine Daten?, NJOZ 2018, 1361–1367

Stürner Rolf (Hrsg.), Jauernig Bürgerliches Gesetzbuch, Kommentar, 17. Aufl., München 2018 (zit. Stürner, Bearbeiterin)

Succi Sauro/Coveney Peter V., Big Data: the End of the Scientific Method?, Philos. Trans. Royal Soc. A 2019/377, 1–15

Swire Peter P./Litan Robert E., None of your business: world of data flows, electronic commerce, and the European Privacy Directive, Washington D.C. 1998

Teichmann Arndt, in: Stürner (vgl. dort), BGB § 249

Thouvenin Florent, Funktionale Systematisierung von Wettbewerbsrecht (UWG) und Immaterialgüterrechten, Köln 2007 (zit. Systematisierung)

Thouvenin, Florent, in: Hilty/Arpagaus (vgl. dort), Art. 8 UWG

Thouvenin Florent, Forschung im Spannungsfeld, von Big Data und Datenschutzrecht: eine Problemskizze, in: Boehme-Nessler/Rehbinder (Hrsg.), Big Data: Ende des Datenschutzes?, Gedächtnisschrift für Martin Usteri, Bern 2017, 27–53 (zit. Forschung)

Thouvenin Florent, Wem gehören meine Daten?, SJZ 2017, 21–32

Thouvenin Florent, Art. 5 lit. c UWG – reloaded, sic! 2018, 595–614

Thouvenin Florent/Früh Alfred/Lombard Alexandre, Eigentum an Sachdaten: Eine Standortbestimmung, SZW 2017, 25–34

Thouvenin Florent/Weber Rolf H./Früh Alfred, Data Ownership: Taking stock and mapping the issues, in: Dehmer/Emmert-Streib (Hrsg.), Frontiers in Data Science, Boca Raton 2018, 111–145 (zit. Data Ownership)

Thouvenin Florent/Weber Rolf H./Früh Alfred, Elemente einer Datenpolitik, Zürich 2019 (zit. Datenpolitik)

Tissot Nathalie, La protection des bases de données accessibles par les réseaux informatiques, Medialex, 4/1996, 194–202

Trebeck Joachim/Schulte-Wissermann Lisa, Die Geheimnisschutzrichtlinie und deren Anwendbarkeit, Auswirkungen auf Compliance und Whistleblowing im deutschen Arbeitsrecht, NZA 2018, 1175–1180

Tuor Peter/Schnyder Bernhard/Schmid Jörg/Jungo Alexandra, Das Schweizerische Zivilgesetzbuch, 14. Aufl., Zürich 2015

Ullrich Hanns, Lizenzkartellrecht auf dem Weg zur Mitte, GRUR Int. 1996, 555–568

Ursic Helena, The Failure of Control Rights in the Big Data Era: Does a Holistic Approach Offer a solution?, in: Bakhoum/Conde Gallego/Mackenrodt/Surblytė-Namavičienė (Hrsg.), Personal Data in Competition, Consumer Protection and Intellectual Property Law, Towards a Holistic Approach?, Berlin 2018, 55–83

Wagner Gerhard, in: Säcker et al. (vgl. dort), BGB § 823

Wandtke Artur-Axel, Ökonomischer Wert von persönlichen Daten, MMR 2017, 6–12

Weber, Rolf H., Dritte Spuren zwischen absoluten und relativen Rechten?, in: Honsell et. al., Aktuelle Aspekte des Schuld- und Sachenrechts, Festschrift für Heinz Rey, Zürich 2003, 583–595

Weber Rolf H./Chrobak Lennart, Rechtsinterdisziplinarität in der digitalen Datenwelt, Jusletter 4. April 2016

Weber Rolf H./Chrobak Lennart, in: Heizmann/Loacker (vgl. dort) Art. 5 lit. c UWG

Weber Rolf H./Iacangelo Salvatore, Rechtsfragen bei der Übertragung von Token, Jusletter IT Flash 24. Mai 2018

Weber Rolf H./Laux Christian/Oertly Dominic, Datenpolitik als Rechtsthema, Zürich 2016

Weber Rolf H./Thouvenin Florent, Gutachten zur Möglichkeit der Einführung eines Datenportabilitätsrechts im schweizerischen Recht und zur Rechtslage bei Personal Information Management Systems (PIMS), Zürich 22. Dezember 2017

Weber Rolf H./Thouvenin Florent, Dateneigentum und Datenzugangsrechte– Bausteine der Informationsgesellschaft?, ZSR 2018 I, 43–74

Weissenberger Philippe, in: Niggli/Wiprächtiger (vgl. dort), Art. 143 und 143bis StGB

Widmer Lüchinger Corinne/Oser David (Hrsg.), Basler Kommentar, Obligationenrecht I, Art. 1–529 OR, 7. Aufl., Basel 2020 (zit. BSK–OR I, BearbeiterIn)

Wiebe Andreas, Protection of industrial data – a new property right for the digital economy?, GRUR Int. 2016, 877–884

Wiebe Andreas, Schutz von Maschinendaten durch das sui-generis-Schutzrecht für Datenbanken, GRUR 2017, 338–345

Wiebe Andreas/Schur Nico, Ein Recht an industriellen Daten im verfassungsrechtlichen Spannungsverhältnis zwischen Eigentumsschutz, Wettbewerbs- und Informationsfreiheit, ZUM 2017, 461–473

Witte Andreas, in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Aufl., München 2019, § 6, Der Rechtsschutz von Datenbanken

Wolf Stephan, in: Kren Kostkiewicz et al. (vgl. dort), Art. 641–645 ZGB

Wolf Stephan/Wiegand Wolfgang, in: Geiser/Wolf (vgl. dort), Vor Art. 641 ff. und Art. 641 ZGB

Żdanowiecki Konrad, Recht an Daten, in: Bräutigam/Klindt (Hrsg.), Digitalisierte Wirtschaft/Industrie 4.0, November 2015, 19–29

Zech Herbert, Information als Schutzgegenstand, Tübingen 2012

Zech Herbert, „Industrie 4.0" – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, 1151–1160

Zech Herbert, Daten als Wirtschaftsgut – Überlegung zu einem „Recht des Datenerzeugers", CR 2015, 137–146

Zech Herbert, Information as Property, JIPITEC 2015, 192–197

Zogg Samuel, Bitcoin als Rechtsobjekt – eine zivilrechtliche Einordnung, recht 2019, 95–120

F. Verzeichnis
Materialien

Blockchain Taskforce, Positionspapier zur rechtlichen Einordnung von ICO's, Bern/Zug, April 2018, abrufbar unter <https://blockchainfederation.ch/downloads/>

Bundesrat, Botschaft zu einem Bundesgesetz gegen den unlauteren Wettbewerb vom 18. Mai 1983, BBl 1983 II 1009 (zit. Botschaft UWG)

Bundesrat, Botschaft zum Bundesgesetz über den Datenschutz vom 23. März 2017, BBl 1988 II 413 (zit. Botschaft DSG 1988)

Bundesrat, Botschaft zum Bundesbeschluss über die Genehmigung von zwei Abkommen der Weltorganisation für geistiges Eigentum und zur Änderung des Urheberrechtsgesetzes vom 10. März 2006, BBl 2006 3389 (zit. Botschaft URG 2007)

Bundesrat, Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941 (zit. Botschaft DSG 2017)

Bundesrat, Rechtliche Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz, Bern 14. Dezember 2018 (zit. Blockchain-Bericht)

Bundesrat, Botschaft zur Änderung des Schweizerischen Zivilgesetzbuches (Erbrecht) vom 29. August 2018, BBl 2018 5813 (zit. Botschaft Erbrecht)

Bundesrat, Botschaft zum Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register vom 27. November 2019, BBl 2020 233 ff. (zit.: Botschaft Elektronische Register)

Bundesrat, Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register, Erläuternder Bericht zur Vernehmlassungsvorlage, Bern 22. März 2019 (zit. Bericht Elektronische Register)

Economiesuisse, Eine Datenpolitik des Vertrauens für Fortschritt und Innovation, Dossierpolitik #03/18, Zürich 12. März 2018 (zit. Economiesuisse)

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation/Bundesamt für Kommunikation, Eckwerte für eine Datenpolitik in der Schweiz, Medienrohstoff, Bern 9. April 2018 (zit. UVEK/BAKOM)

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK, Bericht zu den Empfehlungen der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit: Kenntnisnahme und weiteres Vorgehen, Bern 15. Oktober 2019 (zit. UVEK, Datenbearbeitung und Datensicherheit)

Eidgenössisches Finanzdepartement, Bericht der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit, Bern 17. August 2018 (zit. EFD, Datenbearbeitung und Datensicherheit)

Ethics Advisory Group, Report 2018, 25. Januar 2018, abrufbar unter <https://edps.europa.eu/data-protection/our-work/publications/ethical-framework/ethics-advisory-group-report-2018_en>

Europäische Kommission, 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, Brüssel 10. Januar 2017 (zit. Aufbau einer Europäischen Datenwirtschaft)

Europäische Kommission, DG Internal Market and Services Working Paper, First evaluation of Directive 96/9/EC on the legal protection of databases vom 12. Dezember 2005 (zit. Evaluation)

Europäische Kommission, Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases, SMART 2017/0084, 2018 (zit. Study legal protection of databases)

Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit, Bericht vom 17. August 2018, abrufbar unter <https://www.newsd.admin.ch/newsd/message/attachments/53591.pdf>

Impressum

© 2020
Universität Zürich

Herausgeberin:
Universität Zürich

Center for Information Technology,
Society, and Law (ITSL)
Universität Zürich
Rämistrasse 74|38
8001 Zürich

Universität Zürich[UZH]

CENTER FOR INFORMATION TECHNOLOGY SOCIETY AND LAW — ITSL

Center for Information Technology, Society, and Law (ITSL)

Zuordnung von Sachdaten

Eigentum, Besitz und Nutzung bei nicht-personenbezogenen Daten