# Ansprüche auf Herausgabe von Daten in der Insolvenz

*Ansgar Kalle*, Bonn*

*Der Beitrag befasst sich mit der Frage, wie sich Kunden eines insolventen IT-Dienstleisters Zugang zu ihren Daten verschaffen können. Da Unternehmer und Verbraucher ihre Daten zunehmend Dienstleistern anvertrauen, ist davon auszugehen, dass sich Gläubiger und Insolvenzverwalter in Zukunft damit auseinandersetzen müssen, welche Berechtigungen an Daten im Insolvenzfall bestehen. Dieser Beitrag spricht sich u.a. für eine dingliche Berechtigung in Form eines Datenverfügungsrechts aus.*

## A. Tatsächliche Problemstellung

Die deutsche Volkswirtschaft entwickelt sich zurzeit nach Ansicht des Bundeswirtschaftsministeriums insgesamt positiv.[1] Dennoch ereigneten sich 2018 19.302 Unternehmensinsolvenzen.[2] Unternehmer und Verbraucher müssen also stets in Betracht ziehen, dass ihre Vertragspartner in Insolvenz fallen können. Besonders problematisch ist die Insolvenz eines Unternehmens, das eng mit anderen Geschäftspartnern zusammenarbeitet, da dies typischerweise zu komplexen Geschäftsbeziehungen führt, die insolvenzrechtlich abgewickelt werden müssen.

Eine enge Kooperation besteht regelmäßig bei IT-Dienstleistungen. Das Betreiben von IT-Systemen erfordert spezialisiertes Personal und entsprechende Infrastruktur. Beides kann so kostenintensiv sein, dass es sich gerade aus der Sicht von kleineren Unternehmen, Verbrauchern und Behörden anbietet, auf ein eigenes IT-System zu verzichten und stattdessen fremde Dienstleistungen in Anspruch zu nehmen. Als Beispiel sei das Cloud Computing genannt.

Die hiermit verbundene Ersparnis hat jedoch eine Schattenseite: Der Kunde begründet ein starkes Abhängigkeitsverhältnis zum IT-Dienstleister, da er im Regelfall auf den ungestörten Zugriff auf seine Daten angewiesen ist. So wäre etwa eine Anwaltskanzlei, die ihre Akten in einer externen Cloud speichert, kaum arbeitsfähig, wenn sie plötzlich den Zugriff auf die Cloud verlöre. Ähnliche Risiken bestehen etwa für Software-Entwickler und Werbeagenturen. Daten sind also mittlerweile in vielen Branchen ein wesentlicher Bestandteil des Arbeitsalltags.[3] Dementsprechend ist es riskant, sich bei der Datenspeicherung von Dienstleistern abhängig zu machen. Da insbesondere Cloud-Systeme trotz dieses Risikos äußerst populär sind – 2018 nutzten fast drei Viertel aller deutschen Unternehmen Cloud Computing[4] –, muss man sich Klarheit darüber verschaffen, wie der Kunde in der Insolvenz seines IT-Dienstleisters an seine Daten gelangen kann.

Angesichts der wirtschaftlichen Bedeutung von Daten kann der Kunde nicht darauf vertrauen, dass der Insolvenzverwalter diese freiwillig herausgibt – zu attraktiv dürfte es aus dessen Sicht regelmäßig sein, selbst Anspruch auf die Daten zu erheben, um diese für die Masse zu verwerten.[5] Daher benötigt er einen Herausgabeanspruch. Woraus sich ein solcher ergeben könnte, wurde in Rechtsprechung[6] und Literatur[7] bislang selten erörtert.

## B. Rechtliche Problemstellung

Gemäß § 87 InsO können Gläubiger ihre Forderungen gegen den Schuldner ausschließlich nach Maßgabe des Insolvenzrechts verfolgen. An die Stelle der Einzelzwangsvollstreckung tritt nach § 89 Abs. 1 InsO eine Gesamtvollstreckung, bei der gemäß § 1 S. 1 InsO die Interessen einzelner Gläubiger zum Schutz der Gläubigergesamtheit zurückgedrängt werden.[8] Daher genügt es aus Gläubigersicht nicht, eine materiell-rechtliche Berechtigung an Daten zu haben; diese muss auch in der Insolvenz durchsetzbar sein.

Dies trifft gemäß § 47 S. 2 InsO auf Ansprüche zu, die zur Aussonderung berechtigen. Durch Aussonderung kann der Gläubiger geltend machen, dass ein Gegenstand, der vom Insolvenzverwalter als Bestandteil der Ist-Masse in Beschlag genommen worden ist, nicht zur Soll-Masse zählt

---

* Der Autor ist Mitarbeiter am Lehrstuhl von Prof. Dr. Greiner sowie bei der Sozietät Flick Gocke Schaumburg. Der Beitrag beruht auf einer Seminararbeit, die im WS 19/20 bei Prof. Dr. Brinkmann geschrieben wurde.

1 *BMWi,* Jahreswirtschaftsbericht 2019, S. 9.

2 *StBA,* Statistisches Jahrbuch 2019, S. 534.

3 Laut BGHZ 133, 155 (161) sind Daten ein selbständiges vermögenswertes Gut; ähnlich *Berberich*/*Kanschik*, NZI 2017, 1; *Fezer,* ZD 2017, 99; *Zech*, GRUR 2015, 1151 f.

4 *Heidkamp*/*Vogel*/*Pols*, Cloud Monitor 2019, S. 7.

5 Dazu *Blunk*, Zur Verwertbarkeit von Datenbeständen in der Insolvenz, 2006, S. 149 ff.

6 *OLG Düsseldorf* NZI 2012, 887.

7 *Berger,* ZInsO 2013, 569; *Bultmann,* ZInsO 2011, 992; *Jülicher*, ZIP 2015, 2063.

8 *Bork*, Insolvenzrecht, 9. Aufl. 2019, Rn. 1; *Stürner*, in: MüKoInsO, 4. Aufl. 2019, Einleitung Rn. 1.

und deshalb herauszugeben ist.[9] Deshalb ist zu klären, inwiefern Daten ausgesondert werden können. Zu diesem Zweck wird zunächst ermittelt, was genau unter „Daten" zu verstehen ist. Im Anschluss wird unter die entscheidende Voraussetzung des § 47 S. 1 InsO – die Aussonderungsberechtigung – subsumiert.

## I. Definition des Begriffs „Daten"

Ausgangspunkt einer Definition des Begriffs „Daten" könnte das Datenschutzrecht sein. Die DSGVO setzt in Art. 4 Nr. 1 den Begriff des Datums mit dem der Information gleich.[10] Dies entspricht dem Zweck dieser Verordnung, zum Schutz der informationellen Selbstbestimmung möglichst jede personenbezogene Aussage einem strengen Datenschutzregime zu unterstellen.[11] Für andere Rechtsbereiche ist diese Definition jedoch zu weit gefasst: Die Frage nach der rechtsdogmatischen Einordnung von Daten ins materielle Zivilrecht kam dadurch auf, dass der Rechtsverkehr Informationen allmählich als von ihrem Trägermedium verselbstständigte Güter ansah. Diese Entwicklung wurde durch elektronische Medien vorangetrieben, etwa Festplatten und Speicherkarten. Bei diesen können Informationen ohne Substanzbeeinträchtigung von einem Medium auf ein anderes übertragen werden. Dies wird durch eine maschinenlesbare Codierung erreicht. Aus Sicht der DSGVO kommt es auf eine solche Codierung nicht an, da jede personenbezogene Information die informationelle Selbstbestimmung gefährden kann und deshalb datenschutzrechtlich reguliert werden soll. Daher ist das Begriffsverständnis der DSGVO zwar plausibel, jedoch auf einem bestimmten Schutzzweck zugeschnitten. Deshalb lässt es sich nicht auf andere Rechtsgebiete übertragen.[12]
Dass es die Codierung ist, welche die rechtliche Besonderheit von Daten ausmacht, zeigt sich auch im Strafrecht: Gemäß § 202a Abs. 2 StGB gelten nur solche Informationen als Daten, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind. Daher werden Daten im Strafrecht in Anlehnung an die DIN 44300 Nr. 19 von 1972 als maschinenlesbar codierte Informationen definiert.[13]
Folglich ist davon auszugehen, dass der Begriff „Daten" auch im Zivilrecht maschinenlesbar codierte Informationen beschreibt.[14]

## II. Aussonderungsberechtigung

Der Anspruchssteller muss ein dingliches oder persönliches Recht an dem auszusondernden Gegenstand haben, das dazu führt, dass der auszusondernde Gegenstand massefremd ist, er also nicht zur Befriedigung der Gläubigergesamtheit zur Verfügung steht.[15]

### 1. Rechte an Daten

§ 47 S. 1 InsO enthält keine eigenständigen Rechte, sondern ermöglicht lediglich die Durchsetzung von Rechten, die sich aus anderen Rechtsgrundlagen ergeben.[16] Daher ist zu ermitteln, welche Herausgabeansprüche an Daten bestehen können.

#### *a) Eigentum*

Daten sind nicht eigentumsfähig, da ihnen die gemäß § 903 S. 1 BGB notwendige Sachqualität fehlt.[17] Schließlich sind sie nicht verkörpert i. S. v. § 90 BGB.[18]
Möglicherweise sind Daten allerdings dinglich dem Eigentümer des jeweiligen Datenträgers zugeordnet. Eine solche Akzessorietät könnte man damit rechtfertigen, dass Daten auf einem Datenträger gespeichert werden müssen, um nutzbar zu sein. Beide Gegenstände sind also funktional eng miteinander verknüpft. Deshalb gehen Rechtsprechung[19] und Literatur[20] etwa davon aus, dass das Löschen von Daten das Eigentum am Datenträger verletzen kann.
Es bestehen jedoch zwei entscheidende Bedenken dagegen, aus der funktionalen Verknüpfung von Datum und Speichermedium eine akzessorische Rechtsgutszuordnung zu konstruieren:

---

9 *Graf*, Rechtsbehelfe in der Insolvenz, 2018, S. 63-65; *Häsemeyer*, Insolvenzrecht, 4. Aufl. 2007, Rn. 11.01.

10 *Determann*, ZD 2018, 503 (504); *Leeb*/*Liebhaber*, JuS 2018, 534 (535).

11 So insb. EG 10 der DSGVO.

12 So auch *Schulze*, Daten als Kreditsicherungsmittel mit Bestand in der Insolvenz, 2019, S. 4; gegen Gleichsetzung von Datum und Information ebenfalls *Specht*, CR 2016, 288 (290); aA *Determann*, ZD 2018, 503 (504).

13 *OLG Köln* NJW 1992, 125 (127); *Kargl*, in: NK-StGB, 5. Aufl. 2017, § 202a Rn. 4.

14 So auch *Beurskens*, Vom Sacheigentum zum „virtuellen Eigentum"? – Absolute Rechte an „Daten", in: Domej et. al. (Hrsg.), Einheiten des Privatrechts, 2009, 443; *Hoeren*/*Völkel*, Daten als Gegenstand des Rechts, in: Aarnio et al. (Hrsg.), FS Krawietz, 2013, 603; *Markendorf*, ZD 2018, 409 (410); *Schulze*, (Fn. 12), S. 7; *Zech*, Information als Schutzgegenstand, 2012, S. 32; ähnlich *Specht*, CR 2016, 288 (290 f.).

15 *Brinkmann*, in: Uhlenbruck (Hrsg.), InsO, 15. Aufl. 2019, § 47 Rn. 9.

16 *Ganter*, in: MüKoInsO, (Fn. 8), § 47 Rn. 36.

17 *Wilhelm*, Sachenrecht, 5. Aufl. 2017, Rn. 59.

18 *Schulze*, (Fn. 12), S. 37 mwN.

19 *OLG Karlsruhe* NJW 1996, 200 (201); *OLG Oldenburg* ZD 2012, 177.

20 *Spindler*, Der Schutz virtueller Gegenstände, in: Leible/Lehmann/Zech (Hrsg.), Unkörperliche Güter im Zivilrecht, 2011, 261 (277); *Hager*, in: Staudinger (Begr.), BGB, 2017, § 823 Rn. B 60; *Zech*, (Fn. 14), S. 269.

Zum einen widerspräche dies der Verkehrsauffassung.[21] Der Rechtsverkehr betrachtet Daten als eigenständiges, vom Datenträger unabhängiges Gut, deren Wert sich aus ihrem Inhalt ergibt. Der Datenträger ist als bloßer Speicher nahezu beliebig austauschbar. Zudem verknüpfen IT-Dienstleister beispielsweise beim Cloud Computing eine Vielzahl einzelner physischer Speicher zu einem einheitlichen virtuellen.[22] Hinge die Berechtigung an Daten von der Berechtigung am Trägermedium ab, drohten zufällige Zuordnungen, wenn etwa einzelne Datenträger an unterschiedliche Sicherungsnehmer übereignet werden.
Zum anderen widerspräche eine akzessorische Rechtsgutszuordnung dem Willen von IT-Dienstleister und Kunden: Ersterer will keine rechtliche Verantwortung für den Inhalt der Daten übernehmen, letzterer will die Daten nicht an den Dienstleister verlieren.
Daher trifft die dingliche Berechtigung am Datenträger keine Aussage über die rechtliche Zuordnung der auf ihm gespeicherten Daten.[23]

### *b) Immaterialgüterrechte*

Dingliche Rechte an Daten ergeben sich allerdings aus Immaterialgüterrechten. Hierzu zählen zahlreiche spezialgesetzlich geregelte Rechte, etwa Urheber-, Design- und Patentrecht, die jeweils geistige Leistungen schützen.[24] Solche Leistungen können in Form von Daten vorliegen; als Beispiel sei ein auf dem Computer gespeichertes Manuskript eines Romans genannt. Ein weiteres Immaterialgüterrecht ist das durch Rechtsfortbildung anerkannte[25] allgemeine Persönlichkeitsrecht, das u.a. personenbezogene Daten schützt.[26]
Es bestehen jedoch zwei Probleme, die Immaterialgüterrechte als ungeeignet erscheinen lassen, um eine Aussonderung von Daten darauf zu stützen:

#### *aa) Erstes Problem: Beschränkter Schutzbereich*

Zum einen sind die Schutzzwecke der Immaterialgüterrechte jeweils zu eng bestimmt, um Daten in der Insolvenz umfassend schützen zu können.
So schützt etwa das Urheberrecht gemäß § 2 Abs. 2 UrhG lediglich Werke mit persönlicher geistiger Schöpfung. Das setzt eine individuelle Leistung mit einem Mindestmaß an Kreativität voraus.[27] Das oben beispielhaft genannte Romanmanuskript erfüllt diese Voraussetzung typischerweise.[28] Anders verhält es sich jedoch etwa bei einer Sammlung von E-Mail-Adressen zu Werbezwecken, da das bloße Sammeln von Informationen regelmäßig keine persönliche geistige Schöpfung enthält. Zwar kann auch an Datenbanken gemäß § 4 Abs. 2 UrhG ein Urheberrecht bestehen, jedoch schützt dieses nicht die Datenansammlung an sich, sondern deren Systematisierung durch die Datenbank.[29] Schließlich ist diese Ausdruck einer persönlichen geistigen Leistung.[30]
Begehrt also ein Gläubiger unter Berufung auf sein Urheberrecht Herausgabe eines Datenbestands, wäre für jedes Datum einzeln zu prüfen, ob die Anforderungen des § 2 UrhG erfüllt sind. Dabei ist es nicht unwahrscheinlich, dass dies nur auf einen geringen Anteil des Datenbestands zutrifft.[31]
Entsprechendes gilt für andere Immaterialgüterrechte: Das Patent beschränkt sich auf Erfindungen (§ 1 PatG), das Design auf Erscheinungsformen (§ 1 Nr. 1 DesignG); das allgemeine Persönlichkeitsrecht schützt lediglich Daten mit Persönlichkeitsbezug.[32] Das Schutzrecht des Datenbankherstellers aus § 87a UrhG schützt ähnlich wie das Urheberrecht lediglich Datenbanken, nicht aber Daten als solche.[33]
Aus diesem Grund vermitteln die gesetzlich geregelten oder bislang durch Rechtsfortbildung anerkannten Immaterialgüterrechte nur begrenzten Schutz. Je größer ein Datenbestand ist, umso wahrscheinlicher ist es, dass Immaterialgüterrechte lediglich an einem Bruchteil von diesem bestehen.

#### *bb) Zweites Problem: Prozessuale Durchsetzung*

Bei einigen Immaterialgüterrechten besteht zudem eine prozessuale Herausforderung: Der Gläubiger begehrt oft raschen Zugriff auf seine Daten. Diesen kann er nur erzwingen, wenn er ohne großen Aufwand nachweisen kann, dass ihm ein Recht an den Daten zusteht. Diesen Beweis kann er vergleichsweise leicht bei solchen Rechten führen, die erst entstehen, sobald sie nach Prüfung aller materiell-rechtlichen Voraussetzungen in ein öffentliches Register eingetragen werden; so etwa beim Patent.[34]
Problematischer ist die Beweisführung beim Urheberrecht, für das kein Register existiert: Bestreitet der Insolvenzverwalter, dass die Daten durch eine persönliche geistige Schöpfung i. S. v. § 2 Abs. 2 UrhG entstanden sind, müsste das Vorliegen einer solchen im Gerichtsprozess

---

21 So auch *Schulze*, (Fn. 12), S. 39.

22 *Boehm*, ZEuP 2016, 358 (363); *Federrath*, ZUM 2014, 1 (2).

23 So auch *Hoeren*, MMR 2013, 486 (487); *Schulze*, (Fn. 12), S. 44.

24 *Engels*, Patent-, Marken- und Urheberrecht, 10. Aufl. 2018, Rn. 6 ff.

25 BGHZ 24, 72; BGHZ 26, 349 (354); BGHZ 139, 95.

26 *Wandt*, Gesetzliche Schuldverhältnisse, 9. Aufl. 2019, § 16 Rn. 57.

27 *Ensthaler*, Gewerblicher Rechtsschutz und Urheberrecht, 3. Aufl. 2009, S. 2; *Bullinger*, in: Wandtke/Bullinger (Hrsg.), UrhR, 5. Aufl. 2019, § 2 Rn. 21.

28 *Bullinger*, in: Wandtke/Bullinger, (Fn. 27), § 2 Rn. 58.

29 *Berger*, ZInsO 2013, 569 (571); *Determann*, ZD 2018, 503 (505); *Specht*, CR 2016, 288 (293); *Thum*/*Hermes*, in: Wandtke/Bullinger, (Fn. 27), Vor §§ 87a ff. Rn. 31; *Zieger*/*Smirra,* MMR 2013, 418, (420).

30 *Peschel*/*Rockstroh*, MMR 2014, 571 (572); *Zieger*/*Smirra*, MMR 2013, 418 (420).

31 So auch *Jülicher*, ZIP 2015, 2063 (2065).

32 *Wandt*, (Fn. 26), § 16 Rn. 57.

33 *Wiebe*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 4. Aufl. 2019, UrhG § 87a Rn. 1.

34 *Ensthaler*, (Fn. 27), S. 172.

geklärt werden. Hierbei wäre unter höchst unbestimmte Rechtsbegriffe zu subsumieren.[35] Dies erhöht die Gefahr eines langwidrigen Rechtsstreits, der nicht im Interesse des Gläubigers läge.

### *c) Vertragliche Rechte*

Weitere Berechtigungen an Daten können sich aus dem Vertrag zwischen Kunden und IT-Dienstleister ergeben. Schließlich sind diese aufgrund ihrer Privatautonomie frei darin, Berechtigungen an Daten zu vereinbaren. Knüpfen sie an ein gesetzlich typisiertes Vertragsmodell an, können sich solche Rechte zudem aus Gesetz ergeben.
Im Folgenden sollen vertragliche Berechtigungen an Daten anhand zweier praxisrelevanter Fallgestaltungen erörtert werden: Dem Cloud Computing und dem Outsourcing von Datenverarbeitungsaufgaben.

#### *aa) Cloud Computing*

Beim Cloud Computing überlässt der Provider seinem Kunden einen virtuellen Arbeits- und Lagerraum gegen Entgelt. Daher weist es strukturelle Ähnlichkeiten zum Mietvertrag auf.[36] Dies hilft jedoch für die vorliegende Frage nicht weiter, da das Mietrecht kaum Aussagen zu den Rechten des Mieters an den eingebrachten Gegenständen enthält.
Eine solche Aussage muss daher durch vertragliche Gestaltung getroffen werden. Eine derartige Klausel könnte etwa wie folgt lauten: „Der Kunde behält sämtliche Rechte an den Daten, die er in der Cloud speichert. Während der Vertragslaufzeit hat er jederzeit Anspruch auf Zugang zu seinen Daten. Bei Vertragsbeendigung sind ihm die Daten unverzüglich herauszugeben."[37]
In der Praxis sind solche Vereinbarungen bislang allerdings selten. Zwar verwenden insbesondere US-amerikanische Unternehmen, etwa Amazon[38] und Google[39], in ihren AGB sog. Dateneigentumsklauseln, allerdings stellen diese oft nur klar, dass der IT-Dienstleister keine Rechte an den auf seinen Servern gespeicherten Daten erwirbt.
Gegenwärtig verbreitete Vertragswerke lassen also oft klare Zuordnungen von Daten sowie korrespondierende Ansprüche vermissen. Daher stellt sich die Frage, ob entsprechende Rechte durch Vertragsauslegung konstruiert werden können. Wie bereits angesprochen, entspricht es dem Willen eines Cloud-Providers, dass der Kunde als alleiniger Inhaber seiner Daten gilt. Daher dürfte sich aus Verträgen über Cloud Computing im Regelfall zumindest durch ergänzende Vertragsauslegung ergeben, dass der Kunde Inhaber der Daten ist, die er in der Cloud abspeichert.[40] Rechtssicherer ist jedoch eine ausdrückliche Regelung im Vertrag.

#### *bb) Outsourcing von Datenverarbeitungsaufgaben*

In der Praxis ist es ebenfalls verbreitet, externen IT-Dienstleistern Daten zur Erfüllung ausgewählter Aufgaben zu überlassen. Über einen solchen Fall entschied das OLG Düsseldorf 2012. Dort hatte sich eine Werbeagentur verpflichtet, für eine Unternehmensgruppe einen Newsletter zu organisieren. Zu diesem Zweck übermittelte die Gruppe an die Agentur E-Mail-Adressen ihrer Kunden. Eine vertragliche Abrede über die rechtliche Zuordnung dieser Daten bestand nicht. Nach der Insolvenz der Agentur klagte die Unternehmensgruppe gegen den Insolvenzverwalter auf Herausgabe der Daten. Das Gericht gab der Klage statt, da es den Vertrag als entgeltliche Geschäftsbesorgung ansah und in der Folge einen Anspruch aus §§ 675 Abs. 1, 667 Alt. 1 BGB bejahte.[41]
Diese Beurteilung überzeugt im konkreten Fall, da die Agentur durch die Organisation des Newsletters fremde Daten eigenständig nach den Vorgaben der Unternehmensgruppe verwaltete. Dies entspricht dem Typus des § 675 Abs. 1 BGB. Da Datenverarbeitungsaufgaben allerdings auf zahllose Weisen und in zahllosem Umfang ausgelagert werden können, ist es schwer, aus dem Urteil des OLG allgemeingültige Aussagen über Outsourcing-Verträge abzuleiten. Es liegt jedenfalls nahe, im Ausgangspunkt von einem Geschäftsbesorgungsvertrag auszugehen. Im Anschluss ist jedoch zu prüfen, ob der jeweilige Einzelfall eine abweichende Beurteilung gebietet. Trifft dies zu, ist durch Vertragsauslegung zu ermitteln, welche Berechtigungen an den Daten bestehen. Anders als beim Cloud Computing dürfte es weniger eindeutig sein, dass die vom Kunden übermittelten Daten diesem zugeordnet bleiben sollen. Schließlich ist es wahrscheinlich, dass der Dienstleister diese Daten nicht nur nutzt, sondern auch verändert und deshalb Rechte an den Daten erwerben will. Selbst die ergänzende Vertragsauslegung dürfte dann an ihre Grenzen stoßen. Daher besteht in diesen Fällen ein noch stärkeres Bedürfnis nach eindeutiger vertraglicher Regelung.

### *d) Dingliches Datenverfügungsrecht*

Die bisherige Untersuchung hat ergeben, dass Immaterialgüterrechte und Verträge Berechtigungen an Daten vermitteln können. Beides ist jedoch mit Unwägbarkeiten verbunden: Erstere erfassen größere Datenbestände oft nur lückenhaft. Letztere sind nur effektiv, wenn die Parteien das Bedürfnis nach einer Zuordnung von Daten erkennen

35 Dazu im Einzelnen *Bullinger*, in: Wandtke/Bullinger, (Fn. 27), § 2 Rn. 15-25.

36 *Wicker*, MMR 2012, 783 (785); *Böse*/*Rockenbach*, MDR 2018, 70 (71).

37 Angelehnt an *Jülicher*, ZIP 2015, 2063 Fn. 38.

38 *Amazon Web Services*, https://aws.amazon.com/service-terms/, Abruf v. 27.2.2020.

39 *Google*, https://policies.google.com/terms, Abruf v. 27.2.2020.

40 So auch *Bultmann*, ZInsO 2011, 992 (994); *Grützmacher*, ITRB 2004, 260 (261).

41 *OLG Düsseldorf* NZI 2012, 887 f.

und eine solche mit präzisen Klauseln vornehmen.
Größere Rechtssicherheit ließe sich möglicherweise durch die Anerkennung eines dinglichen Datenverfügungsrechts erreichen, das dessen Inhaber mit absoluter Wirkung die umfassende Herrschaftsgewalt über die eigenen Daten zuordnet. Ob ein solches Recht existiert und wie es ausgestaltet sein könnte, wird seit einigen Jahren diskutiert.[42]

### *aa) Begründungsansätze*

Die Befürworter eines solchen Rechts haben zwei Begründungsansätze entwickelt. Einer stützt sich auf eine Analogie zum Sacheigentum,[43] ein anderer betrachtet die Datenverfügungsbefugnis als sonstiges Recht i. S. v. § 823 Abs. 1 BGB[44].
Die Vertreter beider Ansätze stützen sich im Wesentlichen auf zwei Leitüberlegungen:
Zum einen wecke die wirtschaftliche Bedeutung von Daten ein Bedürfnis des Dateninhabers, eine absolute und mit eindeutigem Inhalt ausgestattete Rechtsposition an den eigenen Daten zu haben. Da Daten als Wirtschaftsgüter mittlerweile eine ähnlich zentrale Bedeutung wie Sachen haben, sei es konsequent und ökonomisch sinnvoll, ihnen ein gleichwertiges Schutzniveau zukommen zu lassen.[45] Dies sei auch aus grundrechtlichen Erwägungen heraus geboten: Das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 GG i V. m. Art. 1 Abs. 1 GG schütze in seinen Ausprägungen als Recht auf informationelle Selbstbestimmung und als Recht auf Vertraulichkeit informationstechnischer Systeme Daten.[46] Ursprung und wirtschaftliche Funktion von Daten legen es zudem nahe, diese als Eigentum i. S. v. Art. 14 Abs. 1 S. 1 GG anzusehen.[47]
Zum anderen sei der zivilrechtlichen Schutz von Daten als eigenständiges Rechtsgut eine konsequente Fortsetzung des strafrechtlichen Schutzes: § 303a StGB stellt das Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten – unabhängig von deren Inhalt – unter Strafe.[48] Diese Vorschrift schützt die Verfügungsgewalt über Daten.[49] Im Schrifttum wird diese oft als eigentumsähnlich bezeichnet.[50]

### *bb) Reaktionen des Schrifttums*

Die Konstruktion eines zivilrechtlichen Datenverfügungsrechts wird im Schrifttum überwiegend kritisch gesehen.
Einige Stimmen, darunter die Justizministerkonferenz der Länder, bestreiten bereits das Bedürfnis nach einem solchen Recht, da Daten bereits gegenwärtig adäquat geschützt seien.[51]
Andere halten zwar ein Bedürfnis nach einem stärkeren Schutz von Daten zumindest für möglich, lehnen es jedoch ab, aus der gegenwärtigen Gesetzeslage ein absolutes Recht an Daten herzuleiten. Dies überschreite den Rahmen der Rechtsfortbildung, da die Zivilrechtsordnung bislang keine Anknüpfungspunkte für ein solches Recht enthalte.[52] Hiervon gehe auch das BVerfG aus, das im Volkszählungsurteil ausführte, dass es keine absolute und unbeschränkte Herrschaft über die eigenen Daten gebe.[53]
Ferner wird eingewandt, dass die Eigentumsordnung zu stark an die Körperlichkeit ihres Schutzgegenstands anknüpfe, um sinnvoll auf Daten übertragen werden zu können.[54]
Zudem bestehe die Gefahr, dass ein solches Recht derart abstrakt wäre, dass Rechtsunsicherheit und ein kaum überschaubares Haftungsrisiko drohten.[55]

---

42 *Steinrötter*, MMR 2017, 731 mwN.

43 *Beurskens*, in: Domej et. al, (Fn. 14), 443 (471); *Fezer,* ZGE 2017, 356 (363); *ders*., ZD 2017, 99 (100); *Hoeren*, ZRP 2010, 251 (252); *ders*., MMR 2013, 486 (487 f.); *Hoppen*, CR 2015, 802; *Jülicher*, ZIP 2015, 2063 (2065); angedeutet von *Berger*, ZInsO 2013, 569 (572).

44 *Bartsch*, in: Conrad/Grützmacher (Hrsg.), Recht der Daten und Datenbanken im Unternehmen, 2014, § 22 Rn. 23; *Faustmann*, VUR 2006, 260 (262 f.); *Grützmacher*, CR 2016, 485 (489 f.); *Hoeren*/*Völkel*, in: Aarnio et al., (Fn. 14), 603 (610); *Medicus*/*Lorenz*, Schuldrecht II, 18. Aufl. 2018, § 77 Rn. 2; *Meier*/*Wehlau*, NJW 1998, 1585 (1588 f.); *Wagner*, in: MüKoBGB, 7. Aufl. 2017, § 823 Rn. 294-296; *Schaub*, in: Prütting/Wegen/Weinreich (Hrsg.), BGB, 14. Aufl. 2019, § 823 Rn. 77; *Redeker*, CR 2011, 634 (636); *Schulze*, (Fn. 12), S. 70-76; *Zech*, (Fn. 14), S. 401.

45 *Beurskens*, in: Domej et. al, (Fn. 14), 443 (470 f.); *Fezer,* ZGE 2017, 356 f.; *ders*., ZD 2017, 99 (100); *Hoeren*, MMR 2013, 486 (491); *Jülicher*, ZIP 2015, 2063 (2065); *Wagner*, in: MüKoBGB, (Fn. 44), § 823 Rn. 294.

46 Grundlegend BVerfGE 65, 1 (41 ff.); *Bartsch*, in: Conrad/Grützmacher, (Fn. 44), § 22 Rn. 23; *Meier*/*Wehlau*, NJW 1998, 1585 (1588); *Schaub*, in: Prütting/Wegen/Weinreich (Fn. 44), § 823 Rn. 77.

47 *Faustmann*, VUR 2006, 260 (263); *Schulze*, (Fn. 12), S. 71.

48 BGBl. I, 1986, S. 723 f.

49 *BayObLGSt* 1993, 86 (88 f.); *OLG Nürnberg* ZD 2013, 282 (283); *OLG Naumburg* ZD 2014, 628 (629); *Weidemann*, in: BeckOK StGB, 45. Ed. 02/2020, § 303a Rn. 5; *Fischer*, StGB, 67. Aufl. 2020, § 303a Rn. 4a; *Heger*, in: Lackner/Kühl (Hrsg.), StGB, 29. Aufl. 2018, § 303a Rn. 4; *Hecker*, in: Schönke/Schröder (Hrsg.), StGB, 30. Aufl. 2019, § 303a Rn. 3; *Sondermann*, Computerkriminalität, 1989, S. 35; *Hilgendorf*, in: Satzger/Schluckebier/Widmaier (Hrsg.), StGB, 4. Aufl. 2019, § 303a Rn. 6; *Welp*, IuR 1988, 443 (447 f.).

50 *Weidemann*, in: BeckOK StGB, (Fn. 49), § 303a Rn. 5; *Heger*, in: Lackner/Kühl, (Fn. 49), § 303a Rn. 4; *Hecker*, in: Schönke/Schröder, (Fn. 49), § 303a Rn. 3; *Sondermann*, (Fn. 49), S. 35; *Hilgendorf*, in: Satzger/Schluckebier/Widmaier, (Fn. 49), § 303a Rn. 6.

51 JuMiKo, Arbeitsgruppe „Digitaler Neustart" – Bericht vom 15. Mai 2017, S. 88 f.; *Spickhoff*, Der Schutz von Daten durch das Deliktsrecht, in: Leible/Lehmann/Zech, (Fn. 20), 233 (244); *Peschel*/*Rockstroh*, MMR 2014, 571 (572); *Steinrötter*, MMR 2017, 731 (732); *Hager*, in: Staudinger, (Fn. 20), § 823 Rn. B 192; *Stender-Vorwachs*/*Steege*, NJOZ 2018, 1361 (1366).

52 *Dorner*, CR 2014, 617 (622 f.); *Grützmacher*, CR 2016, 485 (492); *Heymann*, CR 2015, 807 (810); *Czychowski*/*Siesmayer*, in: Kilian/Heussen (Hrsg.), Computerrechts-Handbuch, 34. EL 2018, 20.5 Rn. 26-30; *Markendorf*, ZD 2018, 409 (410); *Ganter*, in: MüKoInsO, (Fn. 8), § 47 Rn. 339q.

53 BVerfGE 65, 1 (42 f.); darauf beziehen sich *Dorner*, CR 2014, 617 (624) und *Härting*, Internetrecht, 6. Aufl. 2017, Rn. 84.

54 *Ensthaler*, NJW 2016, 3473 (3475 f.); *Czychowski*/*Siesmayer*, in: Kilian/Heussen, (Fn. 52), 20.5 Rn. 22; *Redeker*, CR 2011, 634 (638); *Zech*, GRUR 2015, 1151 (1159).

55 *Kerber*, GRUR Int. 2016, 989 (996 f.); *Spickhoff*, in: Leible/Lehmann/Zech, (Fn. 20), 233 (242-244).

Schließlich erschwere ein eigentumsähnliches Recht an Daten die grundrechtlich geschützte Kommunikation in der Gesellschaft und behindere Innovationen.[56]

### *cc) Stellungnahme*

Die wirtschaftliche Bedeutung von Daten weckt ein Bedürfnis nach einer klaren Zuordnung von Daten. Vertragliche Ansprüche und spezialgesetzliche Immaterialgüterrechte vermitteln aus den oben angesprochenen Gründen nur begrenzten Schutz. Eine rechtssicherere und auch zukunftstauglichere Lösung wäre eine dingliche Zuordnung von Daten zu einem Rechtsträger. Mit deren Hilfe könnte u. a. ein Herausgabeanspruch konstruiert werden, der dem Berechtigten den Zugang zu den eigenen Daten sichert. Daher überzeugt es nicht, ein Dateneigentum unter Verweis auf andere Berechtigungen für entbehrlich zu halten. Den Kritikern des Dateneigentums ist zuzugeben, dass Berechtigungen an Daten in Gerichtsprozessen bislang nur selten zu klären waren.[57] Dies scheint dafür zu sprechen, dass es einer solchen Zuordnung nicht bedarf. Jedoch dürfte dieser Umstand lediglich darauf zurückzuführen sein, dass die Bedeutung von Daten als eigenständiges und von einem Datenträger verselbstständigtes Gut des Zivilrechtsverkehrs eine vergleichsweise junge Entwicklung ist. In der Vergangenheit wurden Daten oft nicht als eigenständige Güter wahrgenommen, sondern lediglich als unselbstständige Teile eines Datenträgers. So konnten sich Zivilgerichte bislang oft auf diesen fokussieren und so etwa das Sachmängelgewährleistungsrecht auf Software anwenden.[58] Jüngere Entwicklungen wie das Cloud Computing lassen sich hiermit nicht befriedigend auflösen. Im Strafrecht zeichnete sich bereits früher ab, dass Daten getrennt von ihren Datenträgern zu betrachten sind, weshalb datenspezifische Tatbestände geschaffen wurden. Als der Gesetzgeber 1986 die Grundlagen des heutigen Datenstrafrechts schuf, ging er ausdrücklich davon aus, dass die bisherigen Rechte keinen effektiven Schutz gewährleisteten.[59] Mithin entstand durch die Verselbstständigung von Daten ein Bedürfnis nach deren klarer Zuordnung.

Zweifelhaft ist auch der Einwand, dass ein absolutes Recht an Daten durch unerwünschte Monopolisierung von Informationen Kommunikation und Innovation erschwere: Er vermengt die von den Vertretern des absoluten Rechts bezweckte Zuordnung eines Datums mit der Zuordnung einer Information. Beides ist jedoch voneinander zu trennen:[60] Das Datenverfügungsrecht bezieht sich nicht auf den Inhalt einer Information, sondern ausschließlich auf deren Darstellung durch eine codierte Zeichenfolge. Ein ähnlicher Gedankengang liegt der hM im Strafrecht zugrunde, die Kopien eines Datums nicht deren Inhaber zuordnet, sondern den Kopierenden.[61] Unterscheidet man konsequent Information und deren Abbildung in Datenform, drohen weder eine Beeinträchtigung der Kommunikation noch Rechtsunsicherheit durch ein konturenloses Recht. Dass eine solche Unterscheidung möglich sein muss, zeigt § 303a StGB, der keine Informationen schützt, sondern lediglich deren Darstellung in Datenform.

Für ein Datenverfügungsrecht spricht ferner der Einklang mit strafrechtlichen Wertungen. § 303a StGB zeigt, dass die Rechtsordnung Daten als eigenständiges Rechtsgut anerkennt. Zwar erlaubt der strafrechtliche Schutz eines Guts für sich genommen nicht den Schluss auf einen dinglichen Zuweisungsgehalt, jedoch setzt § 303a StGB tatbestandlich voraus, dass ein gegenüber jedermann wirkendes Datenverfügungsrecht existiert. Damit hat der Gesetzgeber ein Recht an Daten anerkannt, das eine Zuweisungs- und eine Ausschlussfunktion hat. Da § 303a StGB als Schutzgesetz über § 823 Abs. 2 BGB auch im Zivilrecht Geltung entfaltet,[62] ist es nur konsequent, auch dessen Anerkennung eines absoluten Rechts ins Zivilrecht zu übertragen. Das Volkszählungsurteil des Bundesverfassungsgerichts steht dem nicht entgegen: Zwar heißt es dort wörtlich, dass kein absolutes Recht an Daten bestehe,[63] allerdings wurde diese Aussage in einem spezifisch datenschutzrechtlichen Kontext getätigt; die zivilrechtliche Rechtsgutsdogmatik war nicht Gegenstand der Entscheidung. Daher ist zu bezweifeln, dass das Gericht diesbezüglich Stellung beziehen wollte.[64]

Schließlich ist der Einfluss des Art. 14 Abs. 1 S. 1 GG zu berücksichtigen, der alle vermögenswerten Güter schützt, die einer Person rechtlich zugeordnet sind.[65] § 303a StGB geht davon aus, dass Daten durch die Rechtsordnung einem Inhaber zugeordnet werden. Diese Datenverfügungsbefugnis hat einen Vermögenswert. Daher handelt es sich um Eigentum i. S. v. Art. 14 Abs. 1 S. 1 GG. Deshalb ist es geboten, diesen Vermögenswert effektiv zu schützen. Die bislang anerkannten Rechte an Daten bewirken dies nur unzureichend. Ein stärkerer Schutz lässt sich durch die Anerkennung eines absolut wirkenden Datenverfügungsrechts erreichen.

Daher besteht *de lege lata* ein Datenverfügungsrecht. Es handelt sich um ein sonstiges Recht i. S. v. § 823 Abs. 1 BGB, das seinem Inhaber – vorbehaltlich von Schranken wie etwa Datenschutz- und Urheberrecht – ein absolutes dingliches Herrschaftsrecht an den eigenen Daten einräumt. Als eigentumsanalog sollte es nicht bezeichnet wer-

---

56 *Fritzsche*, in: BeckOK BGB, 53. Ed. 02/2020, § 903 Rn. 10; *Determann*, ZD 2018, 503 (504 ff.); *Härting*, (Fn. 53), Rn. 84; *Heun*/*Assion*, CR 2015, 812 (814); *Heymann*, CR 2015, 807 (810); *Spindler*, ZGE 2017, 399 (401); *Wiebe*, ZGE 2017, 394 (396).

57 JuMiKo, (Fn. 51), S. 62.

58 BGHZ 102, 135 (144); *BGH* NJW 2007, 2394 Rn. 15.

59 BT-Drucks 10/5058, S. 34.

60 So auch *Beurskens*, in: Domej et. al, (Fn. 14), 443 (454); *Specht*, CR 2016, 288 (290); *Zech*, (Fn. 14), S. 36-43.

61 *Fischer*, (Fn. 49), § 303a Rn. 6; *Wolff*, in: LK-StGB, 12. Aufl. 2008, § 303a Rn. 16.

62 *OLG Dresden* NJW-RR 2013, 27 (28); *Grützmacher*, ITRB 2004, 282 (283).

63 BVerfGE 65, 1 (42 f.).

64 So auch *Specht*, CR 2016, 288 (293).

65 *Papier*/*Shirvani*, in: Maunz/Dürig (Hrsg.), Grundgesetz Kommentar, 88. EL 8/2019, Art. 14 Rn. 160.

den, da lediglich wenige Vorschriften des Sacheigentums sinnvoll auf Daten angewendet werden können. Eine solche Analogie ist auch nicht erforderlich, da § 823 Abs. 1 BGB und § 1004 BGB, der nach allgemeiner Ansicht[66] analog auf alle absoluten Rechte anzuwenden ist, die von keinem spezialgesetzlichen Abwehranspruch erfasst werden, bereits hinreichenden Schutz vermitteln. Es ist also dem zweiten oben unter aa. beschriebenen Ansatz zu folgen.

### *e) Inhaber des Datenverfügungsrechts*

Nach hM im Strafrecht steht das Datenverfügungsrecht demjenigen zu, der die Daten durch einen sog. Skripturakt erzeugt.[67] Diesem Ansatz folgt auch das zivilrechtliche Schrifttum überwiegend, soweit es das absolute Recht an Daten befürwortet. Es betont, dass – ähnlich wie beim Herstellerbegriff des § 950 BGB[68] – nicht entscheidend sei, wer die Speicherung manuell vornimmt. Maßgeblich sei vielmehr, wer die rechtliche und wirtschaftliche Verantwortung für den Speichervorgang trage.[69]
Dies überzeugt, da der wertende Rückgriff auf das Erzeugen der Daten den notwendigen Spielraum lässt, um aktuelle und künftige technische Entwicklungen sachgerecht beurteilen zu können. Zwar wird dieser Spielraum durch eine begriffliche Unschärfe erkauft, jedoch kann diese Unschärfe bewältigt werden, indem der Skripturakt durch Lehre und Praxis für komplexe Rechtsbeziehungen weiter konkretisiert wird.
Daher erwirbt derjenige das Verfügungsrecht an einem Datum, der dieses eigenverantwortlich auf eigenes Risiko erzeugt, der sog. Skriptor.

## 2. Massefremdheit der Rechte an Daten

Ein Recht ist massefremd, wenn es haftungsrechtlich nicht dem Vermögen des Schuldners zugeordnet ist, weil es nicht für dessen Verbindlichkeiten haftet.[70]

### *a) Spezialgesetzliche Immaterialgüterrechte*

Viele immaterialgüterrechtliche Gesetze enthalten Ansprüche, die nach allgemeiner Ansicht zur Aussonderung berechtigen. Als Beispiele seien die Ansprüche des Urhebers aus §§ 12, 14, 97 Abs. 1, 98 Abs. 2 UrhG genannt.[71]

### *b) Vertragliche Ansprüche*

Bei vertraglichen Ansprüchen ist zu differenzieren: Schuldrechtliche Herausgabeansprüche berechtigen zur Aussonderung, da mit deren Hilfe die gegenwärtige Haftungslage durchgesetzt wird. Anders verhält es sich bei schuldrechtlichen Verschaffungsansprüchen, da diese auf eine Veränderung der gegenwärtigen Haftungslage abzielen.[72]
Wegen der Vielzahl möglicher Vertragsgestaltungen soll die Frage der haftungsrechtlichen Zuordnung im Folgenden exemplarisch anhand der beiden oben besprochenen Vertragsformen, dem Cloud Computing und dem Outsourcing von Datenverarbeitungsaufgaben, analysiert werden.

#### *aa) Cloud Computing*

Beim Cloud Computing sind die Daten haftungsrechtlich dem Kunden zugeordnet, da sich der Provider darauf beschränkt, einen virtuellen Raum bereitzustellen, den dessen Kunde auf eigenes wirtschaftliches Risiko nutzt. Daher hat dieser einen deutlich engeren Bezug zu den Daten als der Cloud-Provider. Problematisch ist allein, dass beim Cloud Computing keiner der gesetzlich typisierten Herausgabeansprüche, etwa §§ 546, 581 Abs. 2, 596 Abs. 1 BGB, einschlägig ist. Daher muss ein entsprechender Anspruch durch Vertrag konstruiert werden.

#### *bb) Outsourcing von Datenverarbeitungsaufgaben*

Überlasst der Kunde seine Daten dem IT-Dienstleister, bleiben diese haftungsrechtlich regelmäßig ihm zugeordnet, da der Dienstleister die Daten lediglich nutzen soll. Dann kann er entweder mithilfe von §§ 675 Abs. 1, 667 Alt. 1 BGB oder mithilfe eines durch die Parteien vereinbarten Anspruchs aussondern.[73] Hat der Dienstleister die Daten selbstständig erzeugt, kommt ein Herausgabeanspruch des Kunden aus §§ 675 Abs. 1, 667 Alt. 2 BGB oder aus Vertrag zumindest dann in Frage, wenn er eine dingliche Berechtigung an den Daten hat.[74] Als eine solche kommt v. a. das Datenverfügungsrecht in Frage, dass dem

---

66 BGHZ 14, 163 (173); *Fritzsche*, in: BeckOK BGB, (Fn. 56), § 1004 Rn. 4; *Volkmann*, in: Spindler/Schuster, (Fn. 33), BGB § 1004 Rn. 1.

67 BayObLG JR 1994, 476, 477; *OLG Nürnberg* ZD 2013, 282 (283); *OLG Naumburg* ZD 2014, 628 (629); *Fischer*, (Fn. 49), § 303a Rn. 4a; *Jüngel*/*Schwan*/*Neumann*, MMR 2005, 820 (821); *Welp*, IuR 1988, 443 (447 f.); bekräftigt durch BT-Drucks. 18/5088, S. 46.

68 BGHZ 112, 243 (249); *Kindl*, in: BeckOK BGB, (Fn. 56), § 950 Rn. 10; *Wilhelm,* (Fn. 17), Rn. 1068.

69 *Beurskens*, in: Domej et. al, (Fn. 14), 443 (459); *Fezer,* ZGE 2017, 356 (360 f.); *ders*., ZD 2017, 99, 100 f.; *Grützmacher*, CR 2016, 485 (491); *Hoeren*, MMR 2013, 486 (487 f.); *Schulze*, (Fn. 12), S. 59-65; *Zech*, (Fn. 14), S. 399; *ders*., CR 2015, 139 (144).

70 *Scholz*, in: HaKoInsO, 7. Aufl. 2019, § 47 Rn. 2; *Häsemeyer*, (Fn. 9), Rn. 1.15, 11.04; *Brinkmann*, in: Uhlenbruck, (Fn. 15), § 47 Rn. 9.

71 *Haneke*, in: BeckOK InsO, 17. Ed. 01/2020, § 47 Rn. 64; *Ganter*, in: MüKoInsO, (Fn. 8), § 47 Rn. 339b.

72 BGHZ 36, 229 (230 f.), *Andres*, in: Nerlich/Römermann, InsO, 39. EL 07/2019, § 47 Rn. 50.

73 Vgl. *OLG Düsseldorf* NZI 2012, 887 (890) mwN.

74 Vgl. *Brinkmann*, in: Uhlenbruck, (Fn. 15), § 47 Rn. 62a.

Kunden zustehen kann, wenn er die Erzeugung der Daten durch den IT-Dienstleister auf eigenes wirtschaftliches Risiko gesteuert hat.

### *c) Datenverfügungsrecht*

Der Inhaber des Datenverfügungsrechts hat einen dinglichen Herausgabeanspruch auf seine Daten. Ähnlich wie beim Eigentumsrecht korrespondiert mit dieser materiellen Berechtigung grundsätzlich die haftungsrechtliche Zuordnung. Es ist also davon auszugehen, dass Daten grundsätzlich haftungsrechtlich ihrem Skriptor zugeordnet sind. Sollte es sich in Zukunft etablieren, Daten als Kreditsicherheiten zu nutzen,[75] dürfte für diesen Fall ähnlich wie beim Eigentum eine differenzierende Beurteilung geboten sein.
Im Grundsatz berechtigt das Datenverfügungsrecht daher zur Aussonderung. Somit kann der Inhaber dieses Rechts über §§ 823 Abs. 1, 249 Abs. 1 BGB und über § 1004 Abs. 1 BGB vom Insolvenzverwalter Herausgabe verlangen. Eine Analogie zu § 985 BGB ist ebenfalls denkbar, jedoch nicht erforderlich, da hierdurch kein über § 1004 BGB hinausgehender Schutz gewährleistet würde.

## 3. Rechtsfolgen der Aussonderung

Der aussonderungsberechtigte Kunde kann vom Insolvenzverwalter verlangen, dass dieser ihm eine Kopie der Daten übermittelt und im Anschluss seine Kopien vernichtet.[76] Die Kosten hierfür trägt die Masse.[77] Da der Gläubiger regelmäßig schnelle Herausgabe will, sollte er die Aussonderung mithilfe einer einstweiligen Verfügung nach § 935 ZPO verfolgen.

## C. Ergebnisse

Der offene Wortlaut des § 47 S. 1 InsO ermöglicht es, Aussonderungsrechte an Daten anzuerkennen. Daher besteht kein Bedürfnis nach einer zusätzlichen datenspezifischen Regelung im Insolvenzrecht, wie sie etwa in Luxemburg mit Art. 567 Abs. 2 Code de commerce existiert.
Die Herausforderung im Umgang mit Daten liegt im materiellen Zivilrecht, das keine Regelungen über die Rechtsverhältnisse an Daten bereithält. Allerdings lässt sich *de lege lata* ein absolutes dingliches Recht am eigenen Datenbestand konstruieren, das seinem Inhaber Herausgabeansprüche vermittelt. Der Gesetzgeber hat dem Rechtsanwender durch die Anerkennung sonstiger absoluter Rechte als Schutzgut hinreichenden Spielraum gelassen, um auch für künftige Entwicklungen einen adäquaten zivilrechtlichen Schutz zu gewährleisten. Dieser wird durch die Anerkennung des absoluten Datenverfügungsrechts gewährleistet.
*De lege ferenda* wäre jedoch eine klarere Regelung der rechtlichen Einordnung von Daten wünschenswert, um das Verhältnis des Datenverfügungsrechts zu anderen absoluten Rechten präziser auszutarieren, als dies durch reine Rechtsfortbildung möglich ist. Angesichts der oft internationalen Tätigkeit von IT-Dienstleistern sollte hierbei zumindest eine EU-weit einheitliche Regelung angestrebt werden.
Da das absolute Recht an Daten jede codierte Information unabhängig von deren Inhalt schützt, kann dessen Inhaber hiermit Daten aller Art aussondern. Zusätzlich können sich Aussonderungsrechte aus Verträgen und aus Immaterialgüterrechten ergeben.

---

75 Dazu *Schulze*, (Fn. 12), S. 85 ff.

76 *Bultmann,* ZInsO 2011, 992 (996) anknüpfend an *BGH* NJW-RR 2004, 1290 f.; *Jülicher*, ZIP 2015, 2063 (2065 f.).

77 *Jülicher*, ZIP 2015, 2063 (2066).