

Specht-Riemenschneider • Werry • Werry (Hrsg.)

Datenrecht in der Digitalisierung

Leseprobe, mehr zum Buch unter [ESV.info/978-3-503-18782-9](https://www.esv.info/978-3-503-18782-9)

Datenrecht in der Digitalisierung

Herausgegeben von

Prof. Dr. Louisa Specht-Riemenschneider

Inhaberin des Lehrstuhls für Bürgerliches Recht, Informations- und Datenrecht an der Rheinischen-Friedrich-Wilhelms-Universität Bonn sowie Direktorin des Instituts für Handelsrecht, Leiterin der Forschungsstelle für Rechtsfragen neuer Technologien sowie Datenrecht (ForTech),

Nikola Werry LL.M. (UK), Rechtsanwältin,
KPMG Law Rechtsanwaltsgesellschaft, Frankfurt a.M.

und

Susanne Werry LL.M. (UK), Rechtsanwältin,
Clifford Chance Deutschland LLP, Frankfurt a.M.

mit Beiträgen von

Dr. Simon Apel, Dr. jur. Malte Beyer-Katzenberger, Margarita Bidler, Linda Bienemann, Dr. Micha Brechtel, Prof. Dr. Lothar Determann, Dr. Tobias Dienlin, Prof. Dr. Martin Ebers, Jochen Eimer, Jörn Erbguth, Victoria Fast, Lava Gaff, Anne Britta Haas, Anton Haberl, Anka Hakert, Dr. Anke Hofmann, Michael Intveen, Prof. Dr. Wolfgang Kerber, Dr. Karsten Krupna, Prof. Dr. Franz Lehner, Dr. Dimitrios Linardatos, Sebastian Louven, Marina Lutz, Dr. Jan Henrik Pesek, Dipl.-Jur. Alisa Rank-Haedler, Charlotte Röttgen, Dr. Gunnar Sachs, Dr. Bernd Schmidt, Dr. Daniel Schnurr, Kay Schröder, Prof. Dr. Jan H. Schumann, Prof. Dr. Louisa Specht-Riemenschneider, Tobias Steudner, Lorenz Volbers, Nikola Werry, Susanne Werry, Prof. Dr. Thomas Widjaja, Dr. Michael Wohlfarth, Prof. Dr. Ling Yu

Leseprobe, mehr zum Buch unter [ESV.info/978-3-503-18782-9](https://www.esv.info/978-3-503-18782-9)

ERICH SCHMIDT VERLAG

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Weitere Informationen zu diesem Titel finden Sie im Internet unter

ESV.info/978-3-503-18782-9

Gedrucktes Werk: ISBN 978-3-503-18782-9

eBook: ISBN 978-3-503-18783-6

Alle Rechte vorbehalten

© Erich Schmidt Verlag GmbH & Co. KG, Berlin 2020

www.ESV.info

Dieses Papier erfüllt die Frankfurter Forderungen der Deutschen Nationalbibliothek und der Gesellschaft für das Buch bezüglich der Alterungsbeständigkeit und entspricht sowohl den strengen Bestimmungen der US Norm Ansi/Niso Z 39.48-1992 als auch der ISO Norm 9706.

Gesetzt aus der Stempel Garamond, 9/11 Punkt

Satz: multitext, Berlin

Druck und Bindung: Kösel, Altusried-Krugzell

Vorwort

Datenrecht – Ein Definitionsversuch

Der rechtliche Umgang mit Daten ist eine der zentralen Herausforderungen, vor der Wissenschaft und Praxis heute stehen. Daten sind dabei als unkörperliche Gegenstände nicht unmittelbar eigentumsfähig i.S.d. § 903 BGB, unterliegen aber zahlreichen anderen rechtlichen Regelungen. So können sie beispielsweise Gegenstand des Geheimnisschutzes sein oder auch deliktsrechtlichen und strafrechtlichen Schutz genießen. Das Datenschutzrecht unterstellt personenbezogene Daten dem Verbotsprinzip und gestattet ihre Verarbeitung allein bei Vorliegen einer Einwilligung oder eines anderen gesetzlichen Erlaubnistatbestands. Auch kartellrechtliche Fragen gewinnen nicht erst seit dem – gegenwärtig außer Vollzug gesetzten – Beschluss des Bundeskartellamtes¹, Facebook umfassende Beschränkungen bei der Verarbeitung von Nutzerdaten aufzuerlegen, an Bedeutung.

Das „Datenrecht“ kann insofern – ebenso wie das Internetrecht und das Medienrecht – als Querschnittsmaterie beschrieben werden, dessen einendes Element das Regelungsobjekt Daten ist. Erfasst sind dabei sowohl personenbezogene als auch nicht-personenbezogene Daten. Wie kein anderes Rechtsgebiet adressiert das Datenrecht aber nicht nur Regelungsaspekte *de lege lata*, sondern fragt vor allem nach den Regulierungsoptionen des Regulierungsobjektes Daten *de lege ferenda*. Es befindet sich damit in einer steten Entwicklung und versucht, mit den technischen und gesellschaftlichen Entwicklungen angemessen Schritt zu halten. Tatsächlich ist es aber häufig so, dass das Recht diesen Entwicklungen erst mit einem Abstand nachfolgt, was nicht selten mit einem erheblichen Maß an Rechtsunsicherheit einhergeht.

Daten zeichnen sich dabei dadurch aus, dass sie aufgrund ihrer Unkörperlichkeit ubiquitär verfügbar sind und eine Vervielfältigung und Weitergabe weltweit binnen Sekunden mit äußerst geringem Kostenaufwand möglich ist. Gleichzeitig kann ihre wirtschaftliche Bedeutung nicht hoch genug geschätzt werden. Dies wirft unter anderem die Frage auf, ob der derzeitige rechtliche Regelungsrahmen, der noch immer häufig an das körperliche Trägermedium anknüpft, noch angemessen ist, denn für ihre wirtschaftliche Relevanz, ihre Verwertung und Weitergabe ist dieses körperliche Trägermedium längst nicht mehr ausschlaggebend.

¹ Vgl. https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2019/07_02_2019_Facebook.html (24. 03. 2019).

Bei der Ausgestaltung eines Regelungsrahmens für den Umgang mit Daten sind aber nicht nur rechtliche Aspekte zu berücksichtigen. Die Ausgestaltung von Rechtspositionen an unkörperlichen Gütern bedarf stets der Rechtfertigung. Da hierfür auch und gerade ökonomische Erwägungen in Betracht kommen, ist zwingend auch eine Auseinandersetzung mit ökonomischen Gesichtspunkten gefordert. Dieses Handbuch greift daher auch ökonomische Erwägungen auf, wo sie sinnvoll und erforderlich sind.

Denkt man an die datenschutzrechtlichen Herausforderungen unserer Zeit, so sind diese im Umgang mit Daten auch und gerade durch das Phänomen der Informationsüberlastung des Betroffenen gekennzeichnet. Auch dieses Problem kann nicht allein aus juristischer Perspektive gelöst werden, sondern fordert eine interdisziplinäre Betrachtung: In diese müssen bildwissenschaftliche Erkenntnisse (Standardisierung von Informationen durch Symbole) ebenso einbezogen werden, wie Erwägungen aus Verhaltensforschung und Psychologie zur Erörterung des sogenannten Privacy Paradox. Dieses beschäftigt sich mit der Frage, ob eine Asymmetrie zwischen theoretischer Sorge um den sorgsamsten Umgang mit personenbezogenen Daten und tatsächlichem Verhalten existiert und wie dieser Asymmetrie ggf. begegnet werden kann.

All diese – z.T. interdisziplinär zu betrachtenden – Problembereiche haben wir mit den übrigen komplexen und – z.T. rechtsvergleichend zu betrachtenden – rechtlichen Fragestellungen im Umgang mit Daten zusammengeführt, um den Versuch einer ersten Grenzziehung des sich noch im Entstehen befindlichen „Datenrechts“ zu unternehmen. Dabei treten täglich neue Fragen auf und wohl kein Rechtsgebiet unterliegt einer solchen Aktualitätsanpassung, wie das Datenrecht. Es ist daher ein Akt der Unmöglichkeit, bei Drucklegung dieses Handbuchs tatsächlich sämtliche tagesaktuellen Fragen umfangreich aufgearbeitet zu haben, ohne dass die wissenschaftliche Tiefe dabei in Mitleidenschaft gezogen würde. Wir haben uns daher dafür entschieden, einige Fragen für eine zweite Auflage aufzusparen, so etwa den Umgang mit Daten im Prozess. Auch die explizite Adressierung von Zugangsansprüchen zu Daten außerhalb des Kartellrechts z. B. gegen den Staat oder im Sinne des Vorschlags eines „Daten-für-alle-Gesetzes“ bleibt einer Neuauflage vorbehalten.

Für die Erstauflage haben wir stattdessen die uns – v. a. in der privat- und datenschutzrechtlichen Diskussion – am relevantesten erscheinenden Bereiche des Datenrechts durch mit der Materie in Praxis und Wissenschaft betraute Kollegen und Kolleginnen aufarbeiten lassen und uns dabei den folgenden Bereichen gewidmet:

Dr. Malte Beyer-Katzenberger erläutert einleitend die politische Relevanz verschiedener Facetten des Datenrechts. Das Datenschutzrecht – und dabei insbesondere die Datenschutzgrundverordnung – spielt in seiner Anwendbarkeit eine erhebliche Rolle für das Datenrecht. *Dr. Karsten Krupna* und *Dr. Bernd Schmidt* skizzieren daher zunächst die Grundzüge des europäischen Datenschutzrechts und geben einen Überblick über die wichtigsten Aspekte (§ 2.1). Gefolgt wird der

Überblick von Beiträgen, die sich vertieft mit verschiedenen Bereichen des Datenschutzes auseinandersetzen. *Nikola* und *Susanne Werry* stellen die europäische Rechtslage betreffend den internationalen Datentransfer dar, gehen auf Herausforderungen verschiedener Instrumente ein und stellen Lösungsansätze vor (§ 2.2). Zwei in der aktuellen Wirtschaft sehr relevanten Bereichen für Datenschutzfragen widmen sich *Lava Gaff* mit dem Thema Datenschutz bei Virtual und Augmented Reality (§ 2.3) und *Marina Lutz* mit dem Thema Datenschutz im Online-Marketing (§ 2.4), in dem sowohl auf das Zusammenspiel zwischen Datenschutz und unlauterem Wettbewerb, wie auch die ePrivacy-Verordnung eingegangen wird. *Michael Intveen* greift das Thema ePrivacy-Verordnung auf und beleuchtet diese aus dem Blickwinkel ihrer Auswirkungen auf den für die Digitalisierung ebenfalls sehr relevanten Bereich der automatisierten Fahrzeugsysteme und des vernetzten Fahrens (§ 2.5).

In enger Verbindung mit dem Datenschutzrecht steht das Privacy Paradox, das als Phänomen allerdings der interdisziplinären Betrachtung bedarf. *Prof. Dr. Thomas Widjaja* und *Prof. Dr. Jan Schumann* widmen sich gemeinsam mit *Margarita Bidler* sowie *Tobias Steudner* daher zunächst aus wirtschaftswissenschaftlicher Perspektive den Kundenwahrnehmungen und dem Kundenverhalten beim Bezahlen von digitalen Dienstleistungen mit personenbezogenen Daten (§ 3.1), bevor *Dr. Tobias Dienlin* das Privacy Paradox aus psychologischer Perspektive erörtert (§ 3.2). Kann eine Asymmetrie zwischen theoretischer Sorge um den Umgang mit personenbezogenen Daten und dem tatsächlichen Verhalten der Betroffenen, in dem nicht selten eine massenhafte Hingabe von Daten zu beobachten ist, tatsächlich festgestellt werden, ließe sich dieser Asymmetrie möglicherweise jedenfalls in einem gewissen Umfang durch eine Verbesserung der Informationsvermittlung entgegenwirken. Wie eine solche Informationsvermittlung durch Visualisierung verbessert werden kann, untersuchen *Prof. Dr. Louisa Specht-Riemenschneider* und *Linda Bienemann* aus rechtlicher Sicht (§ 3.3) sowie *Kai Schröder*, der die Potentiale der Informationsvisualisierung im Datenschutz aus kommunikationswissenschaftlicher Perspektive diskutiert (§ 3.4).

Einen weiteren wesentlichen Bereich des Datenrechts stellen potentielle Vermögensrechte an Daten dar. *Prof. Dr. Wolfgang Kerber* erläutert hier einleitend Dateneigentum, Datenzugangsrechte und Datengovernance aus ökonomischer Perspektive (§ 4.1), bevor *Charlotte Röttgen* Rechtspositionen an Daten *de lege lata* und *de lege ferenda* im europäischen Rechtsraum diskutiert (§ 4.2). Auch andernorts wird die Frage von Rechten an Daten gestellt, am relevantesten sind dabei wohl die Erwägungen aus den USA und China. *Apl. Prof. Dr. Lothar Determann* (§ 4.3) und *Prof. Dr. Ling Yu* (§ 4.4) erläutern die Rechtslage in diesen Staaten.

Neben vermögensrechtlichen Rechtspositionen an Daten spielt auch der vertragsrechtliche Umgang mit Daten eine erhebliche Rolle und dies v. a. deshalb, weil Daten mittlerweile ein nicht unerheblicher ökonomischer Wert zugesprochen wird. Im Vorfeld der Erörterungen zur Typisierung von Verträgen, in denen Daten den Leistungsgegenstand darstellen (*Alisa Rank-Haedler*, § 5.2) sowie der Frage, ob Daten eine Gegenleistung im Vertrag darstellen können (*Dr. Dimitrios*

Linardatos, § 5.3), beschäftigt sich *Prof. Dr. Franz Lehner* daher mit der Preis- und Wertermittlung von Daten und Informationen (§ 5.1). *Dr. Simon Apel* und *Dr. Anke Hofmann* erörtern sodann Daten in der Unternehmenstransaktion (§ 5.4), bevor *Anne Britta Haas* den vertragsrechtlichen Teil des Handbuchs mit der Darstellung des Outsourcings und insbesondere der Herausforderungen des Cloud Computings schließt (§ 5.5).

§ 6 widmet sich dem Phänomen der Kryptowährungen. *Jörn Erbguth* diskutiert hier Bitcoin, E-Geld und virtuelle Währungen, bevor *Anka Hakert* die Besteuerung dieser Kryptowährungen in den Blick nimmt (§ 6.2).

Ein wesentliches Thema für den Bereich des Datenrechts ist auch die Ausübung von Marktmacht durch Daten, die in § 7 aus ökonomischer (*Dr. Daniel Schnurr*, *Viktoria Fast* und *Dr. Michael Wohlfahrt*, § 7.1) und juristischer Perspektive (*Sebastian Louven*, § 7.2) eruiert wird.

§ 8 beleuchtet sodann digitale Geschäftsmodelle – Datenbasierte Chancen und Risiken für Unternehmen (*Lorenz Volbers* und *Anton Haberl*), bevor in § 9 die Haftung für fehlerhafte Daten aufgearbeitet wird. Besonders relevant scheint dabei die Haftung für fehlerhafte Gesundheitsdaten (*Jochen Eimer* und *Dr. Jan Henrik Pesek*, § 9.1), die Haftung für fehlerhafte Daten beim autonomen Fahren (*Prof. Dr. Martin Ebers*, § 9.2) sowie die Haftung für fehlerhafte Daten in der Industrie 4.0 (*Dr. Gunnar Sachs*, § 9.3). Hier könnten weitere zahlreiche haftungsrelevante Bereiche erörtert werden, beispielsweise die Haftung für fehlerhafte Daten in Suchmaschinenergebnisseiten und Suchmaschinenergänzungsvorschlägen. Die erste Konturierung eines Datenrechts verlangt aber nach einer Schwerpunktsetzung auch im Verhältnis zu den übrigen Kapiteln. Den Abschluss des Werks bildet eine Erörterung von *Dr. Simon Apel* und *Dr. Micha Brechtel* zur Zwangsvollstreckung in Datenbestände (§ 10).

Wir bedanken uns herzlich bei den Autoren für die gute Zusammenarbeit. Ein besonderer Dank gilt auch Frau *Rebecca Rohmer* vom Lehrstuhl für Bürgerliches Recht, Informations- und Datenrecht der Rheinischen Friedrich-Wilhelms-Universität Bonn, die die teils mit erheblichem Aufwand verbundene redaktionelle Betreuung des Handbuchs vollständig übernommen hat und deren Genauigkeit, Fleiß und Einsatz nicht genug gelobt werden können.

Bonn/Frankfurt am Main, im April 2019

Louisa Specht-Riemenschneider
Nikola Werry
Susanne Werry

Inhaltsübersicht

| | |
|--|-----|
| Vorwort: Datenrecht – Ein Definitionsversuch <i>(Prof. Dr. Specht-Riemenschneider; Nikola Werry LL.M.; Susanne Werry LL.M.)</i> | 5 |
| Inhaltsverzeichnis | 11 |
| § 1 Neuartige Rechtsfragen in Bezug auf Daten in Zeiten des Internets der Dinge, von Big Data und Künstlicher Intelligenz? – Anmerkungen aus rechtspolitischer Perspektive <i>(Dr. Malte Beyer-Katzenberger)</i> | 37 |
| § 2 Datenschutzrecht | 61 |
| § 2.1 Überblick zum europäischen Datenschutzrecht <i>(Dr. Karsten Krupna; Dr. Bernd Schmidt, LL.M.)</i> | 63 |
| § 2.2 Internationaler Transfer personenbezogener Daten <i>(Nikola Werry LL.M.; Susanne Werry LL.M.)</i> | 93 |
| § 2.3 Datenschutz bei Virtual und Augmented Reality <i>(Lava Gaff)</i> | 153 |
| § 2.4 Datenschutz im Onlinemarketing <i>(Marina Lutz)</i> | 203 |
| § 2.5 Auswirkungen der ePrivacy-Verordnung im Automobilsektor <i>(Michael Intveen)</i> | 251 |
| § 3 Privacy Paradox | 283 |
| § 3.1 Kundenwahrnehmungen und Kundenverhalten beim Bezahlen von digitalen Dienstleistungen mit personenbezogenen Daten <i>(Margarita Bidler, M.Sc.; Tobias Steudner, M.Sc.; Prof. Dr. Jan H. Schumann; Prof. Dr. Thomas Widjaja)</i> | 285 |
| § 3.2 Das Privacy Paradox aus psychologischer Perspektive <i>(Dipl.-Psych. Dr. Tobias Dienlin)</i> | 305 |
| § 3.3 Informationsvermittlung durch standardisierte Bildsymbole <i>(Prof. Dr. Specht-Riemenschneider; Linda Bienemann)</i> | 324 |
| § 3.4 Potentiale der Informationsvisualisierung im Datenschutz – eine kommunikationswissenschaftliche Betrachtung <i>(Kay Schröder)</i> | 345 |
| § 4 Vermögensrechte an Daten | 361 |
| § 4.1 Dateneigentum, Datenzugangsrechte und Datengovernance aus ökonomischer Perspektive <i>(Prof. Dr. Wolfgang Kerber)</i> | 363 |
| § 4.2 Rechtspositionen an Daten: Die Rechtslage im europäischen Rechtsraum <i>(Charlotte Röttgen)</i> | 371 |

| | |
|--|-----|
| § 4.3 Rechtspositionen an Daten: Die Rechtslage in den USA (Prof. Dr. Lothar Determann) | 408 |
| § 4.4 Rechtspositionen an Daten: Die Rechtslage in China (Prof. Dr. Ling Yu)..... | 440 |
| § 5 Vertragsrechtliche Implikationen | 469 |
| § 5.1 Preis- und Wertermittlung für Daten und Informationen (Prof. Dr. Franz Lehner) | 471 |
| § 5.2 Daten als Leistungsgegenstand: Vertragsrechtliche Typisierung (Alisa Rank-Haedler)..... | 489 |
| § 5.3 Daten als Gegenleistung im Vertrag mit Blick auf die Richtlinie über digitale Inhalte (Dr. Dimitrios Linardatos) | 506 |
| § 5.4 Datenbestände in der Unternehmens-Transaktion (M&A) (Dr. Simon Apel; Dr. Anke Hofmann) | 560 |
| § 5.5 Daten-Outsourcing (Anne Britta Haas, LL. M.) | 589 |
| § 6 Kryptowährungen | 641 |
| § 6.1 Bitcoin/E-Geld/Virtuelle Währungen (Jörn Erbguth) | 643 |
| § 6.2 Die Besteuerung von Kryptowährungen (Anka Hakert, LL.M.) ... | 693 |
| § 7 Marktmacht durch Daten | 743 |
| § 7.1 Marktmacht durch Daten: Eine Analyse aus ökonomischer Perspektive (Victoria Fast, M.Sc.; Dr. Daniel Schnurr; Dr. Michael Wohlfarth)..... | 745 |
| § 7.2 Marktmacht durch Daten: Eine Analyse aus rechtswissenschaftlicher Perspektive (Sebastian Lowven)..... | 779 |
| § 8 Digitale Geschäftsmodelle – Datenbasierte Chancen und Risiken für Unternehmen (Anton Haberl; Lorenz Volbers) | 821 |
| § 9 Haftung für fehlerhafte Daten | 843 |
| § 9.1 Haftung für fehlerhafte Gesundheitsdaten (Jochen Eimer, LL.M.; Dr. Jan Henrik Pesek)..... | 845 |
| § 9.2 Haftung für fehlerhafte Daten beim autonomen Fahren (Prof. Dr. Martin Ebers) | 874 |
| § 9.3 Haftung für fehlerhafte Daten – Industrie 4.0 (Dr. Gunnar Sachs) . | 915 |
| § 10 Datenbestände in Zwangsvollstreckung und Insolvenz (Dr. Simon Apel; Dr. Micha Brechtel) | 941 |
| Herausgeberinnen | 983 |
| Stichwortverzeichnis | 985 |

Inhaltsverzeichnis

| | |
|---|-----------|
| Vorwort: Datenrecht – Ein Definitionsversuch | 5 |
| Inhaltsübersicht | 9 |
| § 1 Neuartige Rechtsfragen in Bezug auf Daten in Zeiten des Internets der Dinge, von Big Data und Künstlicher Intelligenz? – Anmerkungen aus rechtspolitischer Perspektive | 37 |
| A. Die Datenwirtschaft in Zeiten des Internets der Dinge, von Big Data und Künstlicher Intelligenz..... | 40 |
| B. Was ist der rechtliche Befund aus gemein-europäischer Sicht? | 41 |
| C. Rechtspolitischer Handlungsbedarf für IoT-Daten? | 42 |
| I. Welche Aspekte sind in der Diskussion zu berücksichtigen? Welche Daten und welche Aspekte genießen bereits Schutz? | 42 |
| II. Zwischenergebnis: Welche rechtspolitischen Ziele sollten verfolgt werden?..... | 46 |
| III. Welcher Wert wird bei der Datenerzeugung geschöpft? | 47 |
| IV. Ist der Handlungsbedarf sektorbezogen oder sektorübergreifend? | 48 |
| D. Rechtliche Antworten | 49 |
| E. Evidenzbasierte Politikgestaltung | 51 |
| F. Was folgt? | 53 |
| § 2 Datenschutzrecht | 61 |
| § 2.1 Überblick zum europäischen Datenschutzrecht | 63 |
| A. Begriff und Regelungsumfeld | 66 |
| B. Anwendungsbereich des europäischen und mitgliedstaatlichen Datenschutzrechts | 68 |
| I. Die Verarbeitung personenbezogener Daten (sachlicher Anwendungsbereich) | 68 |
| II. Ausnahmen vom Anwendungsbereich der DS-GVO..... | 69 |
| III. Der räumliche Anwendungsbereich | 71 |
| C. Grundsatz der Rechenschaftspflicht und Datenschutzorganisation | 73 |
| D. Rechtfertigungstatbestände | 75 |
| E. Recht auf Datenübertragbarkeit | 78 |
| F. Privacy by Design und Privacy by Default | 81 |

| | | |
|--------------|---|-----------|
| I. | Die Sicherstellung der Einhaltung von Art. 25 DS-GVO durch den Verantwortlichen und Maßnahmen zur Risikominimierung gegenüber dem Hersteller | 81 |
| II. | Die Sicherstellung der Einhaltung von Art. 25 DS-GVO durch den Verantwortlichen und Maßnahmen zur Risikominimierung gegenüber dem Auftragsverarbeiter | 84 |
| G. | Meldung von Datenschutzverletzungen | 84 |
| I. | Meldung an die Aufsichtsbehörde | 85 |
| II. | Meldung innerhalb von 72 Stunden nach Kenntnis | 85 |
| III. | Maßnahmenplan bei Datenschutzverletzung | 87 |
| IV. | Verpflichtung der Beschäftigten | 88 |
| H. | Auftragsverarbeitung und internationaler Datentransfer | 89 |
| I. | Auftragsverarbeitung nach der DS-GVO | 89 |
| II. | Internationaler Datentransfer | 91 |
| § 2.2 | Internationaler Transfer personenbezogener Daten | 93 |
| A. | Einleitung | 94 |
| B. | Grundsätze des Datentransfers | 95 |
| I. | Innerhalb Deutschlands/EU/EWR. | 95 |
| II. | Außerhalb der EU/dem EWR. | 96 |
| C. | Internationaler Datentransfer (im Einzelnen) | 97 |
| I. | Artikel 45 DS-GVO – Datentransfer aufgrund eines Angemessenheitsbeschlusses | 97 |
| 1. | Grundsätze | 97 |
| 2. | Gegenwärtig bestehende Angemessenheitsbeschlüsse | 99 |
| 3. | Folgen und Auswirkungen auf bestehende Angemessenheitsbeschlüsse | 99 |
| 4. | Überprüfung von Angemessenheitsbeschlüssen. | 100 |
| 5. | Privacy Shield (als Sonderfall des Angemessenheitsbeschlusses) | 100 |
| a) | Einleitung und Hintergrund. | 100 |
| b) | Entwicklung | 101 |
| aa) | Safe Harbor-Abkommen | 101 |
| bb) | Safe Harbor-Urteil. | 101 |
| cc) | Privacy Shield. | 102 |
| c) | Kritik | 103 |
| d) | Alternativen und Ausblick | 105 |
| II. | Artikel 46 DS-GVO. | 105 |
| 1. | Einleitung und Hintergrund. | 105 |
| 2. | Behördenvereinbarungen. | 109 |
| 3. | Verbindliche interne Datenschutzvorschriften – Artikel 47 DS-GVO. | 110 |
| a) | Einleitung und Hintergrund. | 110 |
| b) | Adressatenkreis | 114 |

| | | |
|-----------|--|------------|
| c) | Inhaltliche Anforderungen | 116 |
| aa) | Interne rechtliche Verbindlichkeit | 116 |
| bb) | Vermittlung durchsetzbarer Rechte | 118 |
| cc) | Inhaltliche Mindestanforderungen | 120 |
| d) | Verfahren zur Genehmigung | 122 |
| e) | Fortgeltung bestehender BCR | 125 |
| 4. | Standarddatenschutzklauseln, die von der Kommission erlassen werden | 126 |
| a) | Einleitung und Hintergrund | 126 |
| b) | Existierende Standarddatenschutzklauseln | 127 |
| c) | Standarddatenschutzklauseln zwischen Verantwortlichen..... | 127 |
| d) | Standarddatenschutzklauseln für Auftragsverarbeiter . | 129 |
| 5. | Standarddatenschutzklauseln von einer Aufsichtsbehörde | 130 |
| 6. | Genehmigte Verhaltensregeln gemäß Artikel 40..... | 131 |
| a) | Grundsätze | 131 |
| b) | Entstehungsprozess | 132 |
| c) | Genehmigte Verhaltensregeln | 132 |
| d) | Für allgemein gültig erklärte Verhaltensregeln | 132 |
| e) | Überwachungsstellen | 133 |
| f) | Rechtswirkung | 133 |
| g) | Ausblick..... | 134 |
| h) | Praxiserfahrung..... | 135 |
| 7. | Genehmigter Zertifizierungsmechanismus..... | 136 |
| a) | Einleitung..... | 136 |
| b) | Verfahren | 136 |
| c) | Vorgehen | 136 |
| d) | Kleine und mittlere Unternehmen | 137 |
| e) | Fazit | 138 |
| 8. | Artikel 46 Abs. 3 – Genehmigungsbedürftige Garantien.. | 139 |
| III. | Artikel 49 | 140 |
| 1. | Artikel 49 Abs. 1 UAbs. 1 lit. a) | 141 |
| 2. | Artikel 49 Abs. 1 UAbs. 1 lit. b) | 142 |
| 3. | Artikel 49 Abs. 1 UAbs. 1 lit. c) | 143 |
| 4. | Artikel 49 Abs. 1 UAbs. 1 lit. d)..... | 144 |
| 5. | Artikel 49 Abs. 1 UAbs. 1 lit. e) | 144 |
| 6. | Artikel 49 Abs. 1 UAbs. 1 lit. f) | 146 |
| 7. | Artikel 49 Abs. 1 UAbs. 1 lit. g) | 146 |
| 8. | Artikel 49 Abs. 1 UAbs. 2, Abs. 6 | 147 |
| 9. | Artikel 49 Abs. 3 | 149 |
| 10. | Artikel 49 Abs. 5..... | 149 |
| D. | Brexit-Problematik: Welche Lösungen kann es geben? | 150 |
| E. | Fazit | 151 |

| | |
|---|-----|
| § 2.3 Datenschutz bei Virtual und Augmented Reality | 153 |
| A. Einführung: AR und VR | 155 |
| I. Gang der Untersuchung | 156 |
| II. Technische Grundlagen und Funktionen..... | 156 |
| 1. Technische Grundlagen | 156 |
| 2. Datenschutzrechtlich relevante Funktionen | 157 |
| a) VR-Funktionen | 157 |
| b) AR-Funktionen | 159 |
| B. AR und VR aus datenschutzrechtlicher Perspektive | 159 |
| I. Vorrang der Verordnung über Privatsphäre und elektronische Kommunikation („ePrivacy-Verordnung (E)“) | 159 |
| II. Anwendbarkeit des Datenschutzrechts | 160 |
| 1. Sachlich | 160 |
| 2. Räumlich | 161 |
| III. Tracking des Nutzers | 161 |
| 1. Körper-, Kopf- und Eye-Tracking für VR | 162 |
| a) „Interaktionsdaten“ des Nutzers als Gesundheitsdaten, Art. 9 Abs. 1 DS-GVO | 162 |
| b) Eye-Trackingdaten als biometrische Daten, Art. 9 Abs. 1 DS-GVO | 165 |
| c) Rechtmäßigkeit des Körper-, Kopf- und Eye-Trackings..... | 166 |
| aa) Anforderungen an die Einwilligung | 166 |
| bb) Anforderungen an die Einwilligung eines Kindes.... | 169 |
| cc) Vereinbarkeit mit Datenschutzgrundsätzen | 170 |
| 2. Tracking durch AR-Anwendungen | 172 |
| a) Verarbeitung von Standortdaten (Positions-Tracking) | 172 |
| b) Verarbeitung von Nutzerdaten für AR..... | 173 |
| c) Rechtmäßigkeit der Verarbeitung von Nutzerdaten für AR..... | 173 |
| 3. Zusammenfassung..... | 176 |
| IV. Nutzung von Smartcams für AR und VR..... | 176 |
| 1. Anwendungsvorrang des KUG | 177 |
| 2. Rechtmäßigkeit der Umgebungserfassung durch Videostream für AR und VR? | 180 |
| a) Verarbeitung von Nutzerdaten und personenbezogenen Daten Dritter | 180 |
| b) Verarbeitung sensibler Daten, Art. 9 Abs. 1 DS-GVO | 181 |
| c) Nur bedingte Rechtmäßigkeit | 182 |
| 3. Umgebungserfassung für AR als „Videoüberwachung öffentlich zugänglicher Räume“, § 4 BDSG? | 185 |
| 4. Rechtmäßigkeit der dreidimensionalen Erfassung des physischen Raums für eine „AR-Cloud“ | 187 |
| a) Verarbeitung personenbezogener Daten..... | 188 |
| b) Rechtmäßigkeit einer AR-Cloud?..... | 189 |

| | |
|---|------------|
| 5. Zusammenfassung | 191 |
| V. Rechtmäßigkeit des AR-Einsatzes im Arbeitsumfeld | 192 |
| 1. Verarbeitung von Beschäftigtendaten durch AR-Nutzung | 193 |
| 2. Rechtmäßigkeit nach § 26 Abs. 1 BDSG | 193 |
| 3. Einwilligung des Arbeitnehmers | 194 |
| 4. Zusammenfassung | 196 |
| VI. Data Protection by Design und Data Protection by Default: Pflichten von AR- und VR-Anbietern, Art. 25 DS-GVO | 196 |
| 1. Data Protection by Design | 196 |
| 2. Data Protection by Default | 199 |
| VII. Erforderlichkeit einer Datenschutz-Folgenabschätzung für AR- und VR-Anwendungen, Art. 35 DS-GVO | 199 |
| C. Zusammenfassung und Ausblick | 200 |
| § 2.4 Datenschutz im Onlinemarketing | 203 |
| A. Übersicht | 204 |
| I. Einführung | 204 |
| II. Arten und Werkzeuge des Onlinemarketings | 206 |
| 1. Cookies, Digital Fingerprinting und Werbe-IDs | 207 |
| 2. Targeting | 208 |
| a) Tracking | 209 |
| b) Profiling und Online-Behavioral-Advertising | 209 |
| c) Cross-Media-Marketing (Cross-Device-Tracking) | 210 |
| d) Re-Marketing | 211 |
| 3. Social Media-Marketing | 211 |
| 4. E-Mail-Werbung | 212 |
| B. Rechtsgrundlagen | 212 |
| I. DS-GVO | 212 |
| II. BDSG | 214 |
| III. TMG und TKG | 215 |
| IV. ePrivacy-Verordnung | 216 |
| 1. Allgemeines | 216 |
| 2. Verordnungsentwurf der Kommission | 217 |
| 3. Wesentliche Inhalte des Entwurfs nach dem LIBE-Ausschuss | 219 |
| C. Einzelprobleme | 220 |
| I. Verbot mit Erlaubnisvorbehalt – die Erlaubnistatbestände der DS-GVO | 220 |
| 1. Berechtigte Interessen, Art. 6 Abs. 1 S. 1 lit. f) | 220 |
| 2. Vertragserfüllung | 222 |
| 3. Einwilligung | 222 |
| a) Widerruflichkeit | 223 |
| b) Formerfordernisse | 224 |
| c) Abgabe in Kenntnis der Sachlage und für den konkreten Fall | 224 |
| d) Alteinwilligungen | 227 |

| | |
|--|-----|
| e) Elektronische Form der Einwilligung | 229 |
| f) Freiwilligkeit und Koppelungsverbot | 230 |
| II. Gestattung einzelner Marketingmaßnahmen | 232 |
| 1. Tracking mittels Cookies, Fingerprints, Werbe-IDs | 232 |
| a) Bisherige Rechtslage | 232 |
| b) Rechtslage nach der DS-GVO – Interimslösung | 233 |
| c) Ausblick ePrivacy-Verordnung | 235 |
| 2. Analytics | 237 |
| 3. Profiling | 238 |
| 4. Cross-Media-Marketing (Cross-Device-Tracking) | 240 |
| 5. Social Media-Marketing | 241 |
| a) Social Plugins | 241 |
| b) Verantwortlichkeit von Social Media-Seitenbetreibern | 242 |
| 6. E-Mail-Werbung | 244 |
| a) UWG | 245 |
| b) Datenschutzrecht | 247 |
| III. Betroffenenrechte | 249 |
| 1. Auskunft (Art. 15 DS-GVO) | 249 |
| 2. Berichtigung (Art. 16 DS-GVO) | 249 |
| 3. Löschung (Art. 17 DS-GVO) | 249 |
| 4. Einschränkung der Verarbeitung (Art. 18, 19 DS-GVO) | 250 |
| 5. Datenübertragbarkeit (Art. 20 DS-GVO) | 250 |
| 6. Widerspruch (Art. 21 DS-GVO) | 250 |
| § 2.5 Auswirkungen der ePrivacy-Verordnung | |
| im Automobilssektor | 251 |
| A. Einführung | 251 |
| B. Kernpunkte der neuen ePrivacy-Verordnung | 253 |
| I. Tragende Erwägungsgründe | 253 |
| II. Wesentliche Bestimmungen der neuen ePrivacy-Verordnung | 263 |
| III. Problempunkte in der neuen ePrivacy-Verordnung | 268 |
| C. Auswirkungen der neuen ePrivacy-Verordnung auf den | |
| Bereich vernetztes Fahren („Connected Cars“) | 270 |
| I. Automatisierte Fahrzeugsysteme und vernetztes Fahren | 270 |
| II. Technische Anwendungen im Bereich Connected Cars | 273 |
| III. Elektronische Kommunikation im Bereich Connected Cars | |
| und Verarbeitung der insoweit erhobenen Daten | 276 |
| D. Fazit | 280 |
| § 3 Privacy Paradox | 283 |
| § 3.1 Kundenwahrnehmungen und Kundenverhalten beim Bezahlen | |
| von digitalen Dienstleistungen mit personenbezogenen Daten .. | 285 |
| A. Einleitung | 288 |
| B. Privacy Calculus Theorie | 290 |
| I. Nutzenwahrnehmung | 291 |

| | |
|---|-----|
| II. Risikowahrnehmung | 291 |
| C. Einflussfaktoren auf die Kundenwahrnehmung der Datenpreisgabe. | 292 |
| I. Individuelle Faktoren | 292 |
| 1. Generelle Privatsphärebedenken | 292 |
| 2. Sozio-demografische Faktoren | 293 |
| 3. Persönlichkeitsmerkmale | 293 |
| 4. Individuelle Neigungen | 294 |
| 5. Individuelle Erfahrungen | 295 |
| 6. Kulturelle Faktoren..... | 295 |
| II. Service- und unternehmensspezifische Faktoren | 296 |
| 1. Sensibilität der Daten | 296 |
| 2. Relevanz der Daten..... | 297 |
| 3. Kontrolle | 297 |
| 4. Vertrauen | 298 |
| III. Schutzmöglichkeiten | 299 |
| 1. Individueller Selbstschutz | 300 |
| 2. Stellvertreterkontrolle..... | 301 |
| D. Affektive Prozesse bei der Kundenwahrnehmung | 302 |
| E. Zusammenfassung und Handlungsempfehlungen | 303 |
| § 3.2 Das Privacy Paradox aus psychologischer Perspektive | 305 |
| A. Einleitung | 307 |
| B. Was ist Privatheit?. | 308 |
| C. Wie lässt sich Verhalten erklären? | 310 |
| D. Wie lässt sich Verhalten im Internet verstehen? | 312 |
| I. Personenbezogene Faktoren..... | 312 |
| II. Umweltbezogene Faktoren..... | 313 |
| E. Das Privacy Paradox | 314 |
| I. Historie | 314 |
| II. Analyse | 316 |
| F. Diskussion | 319 |
| I. Bewertung..... | 319 |
| II. Gesellschaftliche Implikationen | 321 |
| G. Fazit | 323 |
| § 3.3 Informationsvermittlung durch standardisierte Bildsymbole | 324 |
| A. Einleitung | 325 |
| B. Gang der Untersuchung | 328 |
| C. Scheitern der textbasierten datenschutzrechtlichen Einwilligung | 329 |
| D. Konzepte effizienter Informationsvermittlung | 331 |
| E. Vorteile visueller Informationsvermittlung | 334 |
| F. Informationspflichten der Datenschutzerklärung | 335 |

| | | |
|--------------|--|-----|
| I. | Informationspflichten nach der DS-GVO | 336 |
| II. | Informationspflichten nach BDSG-neu und TMG | 337 |
| III. | Entfall von Informationspflichten. | 338 |
| IV. | Zur Visualisierung geeignete Informationen | 338 |
| G. | Erforderlichkeit eines Schichtenmodells. | 339 |
| I. | Ausgestaltung. | 339 |
| II. | Rechtliche Zulässigkeit des Schichtenmodells. | 341 |
| H. | Vorteile der Verwendung des Schichtenmodells. | 342 |
| I. | Fazit. | 343 |
| § 3.4 | Potentiale der Informationsvisualisierung im Datenschutz – eine kommunikationswissenschaftliche Betrachtung | 345 |
| A. | Einleitung | 345 |
| B. | Vergleichbare Ansätze im Datenschutz | 349 |
| I. | Die Entwicklung einer Bildsprache für Datenverarbeitungsvorgänge | 350 |
| II. | Creative Commons-Ansatz im Datenschutz. | 351 |
| C. | Informationsvisualisierung durch Icons | 353 |
| § 4 | Vermögensrechte an Daten | 361 |
| § 4.1 | Dateneigentum, Datenzugangsrechte und Datengovernance aus ökonomischer Perspektive | 363 |
| A. | Einleitung | 363 |
| B. | Zur Diskussion über ein Ausschließlichkeitsrecht an Daten. .. | 364 |
| C. | Zur Diskussion über Zugangsrechte an Daten und optimale Governance-Lösungen für Daten | 367 |
| § 4.2 | Rechtspositionen an Daten: | |
| | Die Rechtslage im europäischen Rechtsraum | 371 |
| A. | Einleitung. | 373 |
| B. | Rechtspositionen an Daten im Rechtsraum der Europäischen Union. | 375 |
| I. | Schutz von Daten über den Eigentumsschutz am Trägermedium | 375 |
| II. | Urheberrechtlicher Schutz von Datenbanken und Datenbankwerken | 376 |
| 1. | Ausschließliches Recht an Daten bei Datenbankwerken . | 377 |
| a) | Inhalt und Struktur des Datenbankwerks | 377 |
| b) | Unabhängige Zugänglichkeit | 377 |
| c) | Schutz von Daten in Form eines Datenbankwerks. ... | 378 |
| 2. | Sui generis-Leistungsschutzrecht von Datenbanken | 378 |
| 3. | Fazit | 380 |
| III. | Schutz von Geschäftsgeheimnissen. | 380 |
| 1. | Geheimnisschutz = Schutz von Informationen | 381 |

| | |
|--|-----|
| 2. Daten als Geschäftsgeheimnisse | 382 |
| 3. Möglichkeit einer Datenzuordnung | 383 |
| IV. Schutz von Daten über das Datenschutzrecht..... | 383 |
| 1. Datenschutz und Schutz von Daten..... | 384 |
| 2. Inhaltliche Ausgestaltung des Datenschutzrechts..... | 384 |
| a) Das Recht auf Datenübertragbarkeit nach der DS-GVO | 385 |
| b) Das Recht auf Datenübertragbarkeit nach französischem Beispiel | 386 |
| 3. Fazit | 386 |
| V. Zusammenfassung | 387 |
| C. Wie werden Daten vertragsrechtlich behandelt? | 388 |
| I. Status Quo in der Praxis..... | 388 |
| II. Richtlinienvorschlag über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte..... | 390 |
| D. Wie werden Daten eines Unternehmens in der Insolvenz behandelt? | 392 |
| I. Daten des Insolvenzschuldners | 393 |
| 1. Zuordnungsanforderungen für die Massebefangenheit ... | 393 |
| 2. Sonderfall: Datenschutzrechtliche Position eines Dritten . | 394 |
| II. Insolvenz des Cloud-Anbieters und Daten Dritter..... | 395 |
| III. Vorreiterrolle Luxemburg..... | 396 |
| IV. Zusammenfassung | 397 |
| E. Entwicklungen/Bestrebungen der Europäischen Union/ auf Unionsebene | 397 |
| I. Mitteilung „Aufbau einer Europäischen Datenwirtschaft“ .. | 398 |
| 1. Zugang zu Daten..... | 398 |
| 2. Interoperabilität von Daten | 399 |
| 3. Data Producer’s Right | 400 |
| II. Zusammenfassung | 401 |
| F. Ansätze der Wissenschaft, Daten zuzuordnen | 401 |
| I. Herleitung eines Dateneigentums aus § 303a StGB..... | 402 |
| II. Recht am eigenen Datenbestand | 404 |
| III. Zuordnung über das Datenschutzrecht | 405 |
| IV. Zusammenfassung | 405 |
| G. Zusammenfassung und Ausblick | 406 |
| § 4.3 Rechtspositionen an Daten: Die Rechtslage in den USA | 408 |
| A. Einführung | 410 |
| B. Daten und Informationen | 411 |
| C. Eigentumsrechte an Informationen an sich und in Werken, Datenbanken, Gegenständen und Immobilien | 413 |
| I. Eigentum im amerikanischen Recht | 413 |
| II. Immobilieneigentum (Real Property) | 417 |
| III. Eigentum an beweglichen Sachen (Personal Property) | 418 |

| | |
|--|-----|
| IV. Schutz von Geschäftsgeheimnissen (Trade Secret Law) | 419 |
| V. Patente | 420 |
| VI. Markenrecht (trademark law) | 421 |
| VII. Urheberrecht (copyright law) | 422 |
| VIII. State law on misappropriation – Schutz vor missbräuchlicher Verwendung. | 425 |
| IX. Data Privacy – Schutz der Privatsphäre | 426 |
| X. Zusammenfassung. | 428 |
| D. Rechte und Beschränkungen des Zugriffs auf Informationen | 429 |
| I. Beschränkungen zum Schutz der Privatsphäre (data privacy law) | 429 |
| II. Computer Interference Laws | 429 |
| III. Umwelt- und Wettbewerbsrecht. | 429 |
| IV. Verträge | 430 |
| V. Konkursrecht. | 431 |
| E. Interessen an Daten | 431 |
| I. Fahrzeugeigentümer | 431 |
| II. Fahrer und Passagiere | 432 |
| III. Andere Verkehrsteilnehmer | 433 |
| IV. Hersteller | 433 |
| V. Zusatzdienstanbieter. | 435 |
| VI. Autohändler und -lieferanten | 435 |
| VII. Versicherungsgesellschaften | 436 |
| VIII. Strafverfolgung und Regierungsbehörden. | 436 |
| F. Sollte ein neues Eigentumsrecht an Daten geschaffen werden? | 437 |
| I. Kreativität und technologischer Fortschritt | 437 |
| II. Kontraindikation zum Schutz der Privatsphäre | 439 |
| G. Zusammenfassung | 439 |
| § 4.4 Rechtspositionen an Daten: Die Rechtslage in China | 440 |
| A. Einleitung. | 442 |
| B. Rechtspositionen an Daten in China | 443 |
| I. Schutz von Geschäftsgeheimnissen. | 443 |
| 1. Definition des Geschäftsgeheimnisses | 443 |
| a) Nicht öffentlich | 444 |
| b) Geschäftlicher Wert | 445 |
| c) Geheimhaltung. | 446 |
| 2. Tatbestand des § 9 cUWG | 447 |
| 3. Rechtsfolgen | 448 |
| a) Zivilrechtliche Rechtsfolgen | 448 |
| b) Verwaltungsrechtliche Rechtsfolgen | 449 |
| c) Strafrechtliche Rechtsfolgen | 450 |
| II. Schutz von Datenbanken und Datenbankwerken | 451 |
| 1. Urheberrechtlicher Schutz von Datenbankwerken | 451 |
| a) Schutzvoraussetzungen | 451 |

| | |
|--|------------|
| b) Schutz von Daten in Form eines Datenbankwerks ... | 452 |
| c) Rechtsinhalte und Schrankenregelungen | 453 |
| 2. Wettbewerbsrechtlicher Schutz von Datenbanken | 453 |
| III. Schutz von Daten über das Datenschutzrecht | 454 |
| 1. Definition der „Personenbezogenen Information“ | 457 |
| 2. Inhaltliche Ausgestaltung | 457 |
| 3. Rechtsfolgen | 458 |
| IV. Strafrechtlicher Schutz von personenbezogenen Daten | 459 |
| C. Wie werden Daten vertragsrechtlich behandelt? | 461 |
| D. Wie werden Daten eines Unternehmens in der Insolvenz behandelt? | 463 |
| E. Ansätze und Entwicklung | 464 |
| I. Dateneigentum | 464 |
| II. Data Controller: Recht am eigenen Datenbestand | 465 |
| III. Datenrecht sui generis | 466 |
| F. Zusammenfassung und Ausblick | 467 |
| § 5 Vertragsrechtliche Implikationen | 469 |
| § 5.1 Preis- und Wertermittlung für Daten und Informationen | 471 |
| A. Bedeutungszunahme von Daten und Notwendigkeit der Wertermittlung | 472 |
| B. Begriffsverständnis und Zusammenhang von Daten und Informationen | 474 |
| C. Wie kann man Daten messen? | 476 |
| D. Herausforderungen in Verbindung mit der monetären Bewertung von Daten | 478 |
| E. Der Preis von personenbezogenen Daten | 481 |
| F. Methoden zur Ermittlung des Datenwerts | 483 |
| G. Fazit | 487 |
| § 5.2 Daten als Leistungsgegenstand: Vertragsrechtliche Typisierung .. | 489 |
| A. Abgrenzung Daten als Gegenleistung und Daten als Leistungsgegenstand | 490 |
| B. Vorfragen | 491 |
| I. Personenbezug der Daten | 491 |
| II. Rechtlicher Rahmen | 492 |
| 1. Datenschutzrechtlicher Rahmen | 492 |
| 2. Strafrechtlicher Rahmen | 493 |
| 3. Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union sowie die geplante Richtlinie zu Verträgen über digitale Inhalte | 494 |
| III. Konsequenzen bei Verstößen gegen den rechtlichen Rahmen | 494 |
| 1. Mögliche Nichtigkeit nach § 134 BGB | 494 |

| | |
|--|------------|
| 2. Datenschutzaufsicht, Verbandsklagerecht bzw. Sanktionen im Datenschutzrecht | 495 |
| C. Denkbare Vertragsinhalte | 495 |
| D. Bisherige Einordnung durch die Rechtsprechung | 496 |
| E. Vertragstypologische Einordnung | 497 |
| I. Kaufvertrag | 498 |
| 1. Sachkauf (§§ 433 ff. BGB) | 498 |
| 2. Rechtskauf bzw. Kauf eines sonstigen Gegenstandes (§ 453 BGB) | 498 |
| II. Werklieferungsvertrag § 650 BGB | 500 |
| III. Werkvertrag (§ 631 BGB) | 501 |
| IV. Mietvertrag (§ 535 BGB) | 501 |
| V. Pacht (§ 581 BGB) | 502 |
| VI. Dienstvertrag (§ 611 BGB) | 503 |
| F. „Steuerungsmöglichkeiten“ im Vertrag | 504 |
| § 5.3 Daten als Gegenleistung im Vertrag mit Blick auf die Richtlinie über digitale Inhalte | 506 |
| A. Einführung | 509 |
| B. Vorschlag einer Richtlinie über digitale Inhalte (DIRL) | 512 |
| I. Hintergrund, Ziele und Entwicklung | 512 |
| II. Verhältnis der DIRL zu anderen Rechtsakten | 513 |
| 1. Datenschutzrechtliche Regelungen | 513 |
| 2. Vertragsrechtliche Regelungen | 513 |
| III. Partieller Vollharmonisierungsansatz der DIRL | 514 |
| C. Inhalt und Anwendungsbereich der DIRL | 515 |
| I. Personeller Anwendungsbereich | 515 |
| II. Sachlicher Anwendungsbereich | 516 |
| 1. Verträge über die Bereitstellung von digitalen Inhalten .. | 516 |
| 2. Ausgenommene Verträge | 517 |
| 3. Daten als Gegenleistung | 518 |
| a) Gemäß Art. 3 Abs. 1 DIRL gegenleistungsfähige Daten | 519 |
| b) Einwilligung oder Daten als Leistungsgegenstand? .. | 520 |
| aa) Meinungsstand | 520 |
| bb) Stellungnahme und eigener Ansatz | 522 |
| (1) Grundsatz der informierten Einwilligung | 523 |
| (2) Unternehmenspraxis und ökonomische Erwägungen . | 525 |
| (3) Missachtung der Anbieterinteressen | 525 |
| (4) Autonome Erfüllung durch den Schuldner wird unmöglich | 527 |
| (5) Eigener Ansatz: Einwilligung als Wirksamkeitsvoraussetzung | 528 |
| cc) Auswirkungen des Art. 6 Abs. 1 lit. b) DS-GVO | 529 |
| dd) Freiwilligkeit und Wirksamkeit der Einwilligung | 530 |

| | |
|---|-----|
| (1) Freiwillige Einwilligung und Koppelungsverbot | 531 |
| (2) Daten als Gegenleistung und Koppelungsverbot | 531 |
| (3) Folgen eines Verstoßes gegen das Koppelungsverbot. . | 533 |
| ee) Widerruflichkeit der Einwilligung | 534 |
| c) Synallagmatische Verknüpfung von Leistung und Gegenleistung? | 539 |
| aa) Auswirkungen. | 541 |
| bb) Daten zur Erfüllung vertraglicher und gesetzlicher Pflichten | 542 |
| (1) Personenbezogene Daten zur Erfüllung vertraglicher Pflichten | 542 |
| (2) Personenbezogene Daten zur Erfüllung rechtlicher Pflichten | 544 |
| (3) Sonstige Daten. | 544 |
| cc) Rechtsfolge bei unberechtigter Kommerzialisierung der von Art. 3 Abs. 1 UAbs. 2 DURL erfassten Daten | 545 |
| dd) Passive Datenpreisgabe | 546 |
| d) Entgeltcharakter der Daten als Gegenleistung | 548 |
| e) Einheiten von Kryptowährungen als Gegenleistung .. | 550 |
| 4. Schuldrechtliches oder dingliches Rechtsgeschäft? | 551 |
| D. Leistungspflichten und Rechtsbehelfe bei Leistungsstörungen | 554 |
| I. Leistungszeit | 554 |
| II. Leistungsinhalt | 555 |
| III. Vertragsbeendigung | 557 |
| § 5.4 Datenbestände in der Unternehmens-Transaktion (M&A) | 560 |
| A. Einführung | 561 |
| I. Grundlagen: Formen des Unternehmenskaufs. | 563 |
| 1. Asset-Deal | 563 |
| 2. Share-Deal | 563 |
| II. Strukturierung/Vorbereitung der Transaktion durch Due Diligence und Geheimhaltungsvereinbarung/NDA | 564 |
| III. Bedeutung der Rechtswahl. | 565 |
| 1. Vertragsstatut | 565 |
| 2. Territorialitätsprinzip | 566 |
| IV. Kategorisierung der datenrechtlichen Bezugsobjekte | 567 |
| 1. Sondergesetzlich geschützte Daten | 567 |
| a) Urheberrecht und verwandte Schutzrechte. | 567 |
| b) Geschäfts- und Betriebsgeheimnisse, Know-how | 567 |
| c) Personenbezogene Daten. | 570 |
| 2. Vertraglich geschützte Daten. | 571 |
| B. Daten im Asset-Deal | 572 |
| I. Sondergesetzlich geschützte Daten | 572 |
| 1. Urheberrecht und verwandte Schutzrechte | 572 |
| 2. Geschäfts- und Betriebsgeheimnisse, Know-how. | 574 |
| a) Konkretisierung des Know-hows. | 575 |

| | |
|---|-----|
| b) Verkäuferpflichten im Zusammenhang mit der Überlassung des Know-hows. | 576 |
| c) Absicherungsklauseln | 576 |
| 3. Personenbezogene Daten. | 577 |
| a) Offenlegung anonymisierter und pseudonymisierter Daten im Rahmen eines Asset-Deals | 578 |
| b) Insbesondere: Datenschutzrechtliche Beurteilung der Due Diligence | 579 |
| c) Übertragung von Mitarbeiterdaten | 580 |
| d) Erwerb von Kundendaten. | 582 |
| aa) Kundendaten aus bestehenden Vertragsverhältnissen . | 582 |
| bb) Isolierte Übertragung von Kundendaten | 584 |
| II. Vertraglich geschützte Daten. | 586 |
| C. Daten im Share-Deal | 586 |
| I. Sondergesetzlich geschützte Daten. | 586 |
| 1. Urheberrecht und verwandte Schutzrechte | 586 |
| 2. Geschäfts- und Betriebsgeheimnisse, Know-how | 587 |
| 3. Personenbezogene Daten | 587 |
| II. Vertraglich geschützte Daten. | 588 |
| § 5.5 Daten-Outsourcing | 589 |
| A. Outsourcing im Allgemeinen | 590 |
| I. Begriff des Outsourcings | 590 |
| II. Klassifizierung des Outsourcings als Auftragsverarbeitung oder sonstige Übermittlung. | 591 |
| III. Outsourcing im Konzern. | 593 |
| B. Cloud Computing | 594 |
| I. Definition des Cloud Computing und Virtualisierung | 594 |
| II. Beteiligte beim Cloud Computing | 596 |
| III. Cloud Modelle | 597 |
| IV. Cloud-Service Modelle. | 598 |
| V. Empfehlungen von Aufsichtsbehörden vor Inkrafttreten der DS-GVO | 599 |
| VI. Überblick über die datenschutzrechtlichen Herausforderungen beim Cloud Computing | 600 |
| VII. Anwendbares Recht | 602 |
| VIII. Übermittlung an einen Dritten oder Auftragsverarbeitung | 604 |
| IX. Ausgewählte cloud-spezifische Herausforderungen bei einer Auftragsverarbeitung | 607 |
| 1. Dokumentation der Weisung und Weisungsgebundenheit | 607 |
| 2. Offenlegung und schriftliche Fixierung der Subunternehmer | 608 |
| 3. Unterstützungspflichten des Auftragsverarbeiters. | 611 |
| a) Anfragen von Betroffenen | 611 |
| b) Datenschutz-Folgenabschätzung und Meldepflichten. | 613 |
| c) Vergütung der Unterstützungsleistung | 614 |

| | |
|---|------------|
| 4. Datenlöschung | 614 |
| 5. Prüf- und Auskunftsrechte des Verantwortlichen | 615 |
| 6. Einschaltung von Auftragsverarbeitern oder Unterauftragsverarbeitern außerhalb der EU/EEA | 616 |
| 7. Haftung des Auftragsverarbeiters | 618 |
| C. Daten- und IT-Sicherheit | 618 |
| I. Allgemeines | 618 |
| 1. Beurteilung der technischen Situation und Entscheidung über die erforderlichen technischen und organisatorischen Maßnahmen | 619 |
| 2. Konkrete Maßnahmen zur IT-Sicherheit | 620 |
| II. Herausforderungen der Datensicherheit im Bereich Cloud Computing | 620 |
| III. IT-Sicherheit und Zertifizierungen | 623 |
| 1. Allgemeines | 623 |
| 2. Genehmigte Verhaltensregeln und genehmigte Zertifizierungsverfahren unter der DS-GVO | 625 |
| a) Genehmigte Verhaltensregeln | 625 |
| b) Genehmigte Zertifizierungsverfahren | 626 |
| IV. Besonderheiten für „kritische Infrastrukturen“: Das BSIG | 626 |
| D. Verarbeitung besonderer Kategorien personenbezogener Daten | 627 |
| E. Herausgabeverlangen ausländischer Behörden und Gerichte | 628 |
| I. Extraterritoriale Zugriffsansprüche | 629 |
| II. Regelungen der DS-GVO zur Datenübermittlung und Offenlegung | 630 |
| III. Dilemma der in Anspruch genommenen Unternehmen | 631 |
| IV. Europäisches oder nationales Modell als Lösung? | 631 |
| F. Industrie- und sektorspezifische Herausforderungen bei der Weitergabe von Daten im Rahmen von Outsourcing und Cloud Computing | 632 |
| I. Strafbarkeit der Weitergabe von Daten durch Berufsgeheimnisträger | 632 |
| II. Outsourcing im Bank- und Finanzsektor | 634 |
| III. Outsourcing in der Healthcare-Industrie | 638 |
| § 6 Kryptowährungen | 641 |
| § 6.1 Bitcoin/E-Geld/Virtuelle Währungen | 643 |
| A. Daten als Zahlungsinstrumente mit ggf. weiteren Funktionen | 644 |
| I. Begriffsklärungen | 644 |
| II. Dimensionen | 645 |
| B. Funktionsweise | 645 |
| I. Autonomie des Systems | 645 |
| II. Forderungscharakter | 646 |

| | |
|--|-----|
| III. Weitere Funktionalitäten | 646 |
| IV. Token-Design | 647 |
| C. Technische Realisierung | 647 |
| I. Technologische Grundlagen | 647 |
| 1. Kryptographische Hashfunktionen | 647 |
| 2. Kryptographische Signatur | 648 |
| II. Ablage auf einem Server | 650 |
| III. Ablage auf einer Blockchain | 651 |
| 1. Bitcoin und die Bitcoin-Blockchain | 651 |
| a) Grundprinzipien | 651 |
| b) Bitcoin-Adressen | 652 |
| c) Bitcoin-Transaktionen | 653 |
| d) Bitcoin-Blöcke | 654 |
| e) Mining (Proof-of-Work) | 655 |
| f) Bitcoin-Wallets | 656 |
| g) Bitcoin-Exchanges | 659 |
| h) Privatheit der Transaktionen | 659 |
| 2. Weiterentwicklungen | 660 |
| a) Payment Channels und Lightning Networks | 660 |
| b) Anonyme Transaktionen | 662 |
| c) Smart Contracts | 664 |
| d) Gerichteter azyklischer Graph (DAG)/Hashgraph .. | 665 |
| e) Andere Consens-Mechanismen | 667 |
| f) Consortium Blockchains | 668 |
| 3. Probleme und Grenzen der Blockchains | 669 |
| a) Energieverbrauch des Proof-of-Work Mining | 669 |
| b) Skalierbarkeit und Transaktionsgebühren | 670 |
| c) Blockchain-Governance | 671 |
| IV. Ablage auf einem Speichermedium des Inhabers | 673 |
| 1. Geldkarte | 673 |
| 2. Payment Channels und nicht publizierte signierte Transaktionen | 674 |
| D. Juristische Einordnung | 674 |
| I. Bitcoins | 674 |
| 1. Rechtsnatur im Zivilrecht | 674 |
| 2. Token-Economy/Sachenrecht | 675 |
| 3. Vertrags- und Leistungsstörung | 676 |
| 4. Zwangsvollstreckung | 676 |
| 5. Strafrechtliche Vermögensabschöpfung | 677 |
| a) Einziehbare Objekte | 677 |
| b) Grund der Einziehung | 678 |
| c) Non-conviction-based confiscation | 678 |
| d) Beschlagnahmung | 679 |
| 6. Regulierung | 679 |
| a) Aktuelle Regulierung | 679 |

| | |
|--|------------|
| b) Weitere Entwicklung der Regulierung | 680 |
| c) Internationale Regulierung | 681 |
| 7. Datenschutz | 682 |
| a) Personenbezogene Daten | 682 |
| b) Haushaltsausnahme | 683 |
| c) Datenschutzrechtlich Verantwortlicher | 683 |
| d) Auftragsverarbeiter | 684 |
| e) Rechtfertigung | 684 |
| f) Weitere Anwendungen | 685 |
| 8. Haftung für illegale Inhalte | 686 |
| II. E-Geld | 687 |
| 1. Wann handelt es sich um E-Geld? | 687 |
| 2. Erlaubnisvorbehalt | 690 |
| III. Verschieden Tokenarten – Klassifikation für Initial Coin Offerings (ICOs) | 690 |
| 1. Kryptowährungen – Zahlungs-Token | 690 |
| 2. Utility Token – Nutzungs-Token | 690 |
| 3. Security/Asset Token – Anlage-Token | 691 |
| E. Ausblick | 692 |
| § 6.2 Die Besteuerung von Kryptowährungen | 693 |
| A. Einleitung | 693 |
| B. Kryptowährungen im deutschen Steuerrecht | 696 |
| I. Ertragsteuer | 696 |
| 1. Einordnung als immaterielles Wirtschaftsgut | 696 |
| 2. Einkunftsart | 698 |
| a) Überblick | 698 |
| b) Abgrenzung der privaten von der gewerblichen Tätigkeit | 699 |
| 3. Gewerbliche Einkünfte | 703 |
| a) Bilanzierende Unternehmen | 703 |
| aa) Bilanzierungsfähigkeit von Kryptowährungen | 703 |
| bb) Aktivierung und ertragsteuerliche Folgen | 704 |
| (1) An- und Verkauf von Kryptowährungen gegen Euro .. | 704 |
| (2) An- und Verkauf von Kryptowährungen im Tausch gegen andere Wirtschaftsgüter | 704 |
| (3) Selbst geschaffene Kryptowährungen | 705 |
| b) Sonstige Unternehmer, § 4 Abs. 3 EStG | 707 |
| c) Besteuerung von ICOs | 707 |
| 4. Nicht gewerbliche Einkünfte | 708 |
| a) Einkünfte aus dem Verkauf und Tausch von Kryptowährungen | 709 |
| aa) Einkünfte aus Kapitalvermögen gem. § 20 EStG? | 709 |
| (1) Überblick | 709 |
| (2) Keine Einkünfte aus Kapitalvermögen durch Veräußerung von Kryptowährungen | 710 |

| | |
|--|------------|
| bb) Einkünfte aus privaten Veräußerungsgeschäften gem. § 23 EStG. | 711 |
| (1) Anschaffung | 711 |
| (2) Veräußerung | 712 |
| (3) Haltefrist | 712 |
| (4) Fristberechnung | 714 |
| (5) Ermittlung des Veräußerungsgewinns | 717 |
| (6) Zeitpunkt der Besteuerung | 722 |
| b) Sonstige Einnahmen im Zusammenhang mit Kryptowährungen | 723 |
| aa) Hard Forks | 723 |
| bb) Airdrops | 724 |
| cc) Mining | 726 |
| II. Umsatzsteuer | 728 |
| 1. Der Einsatz von Kryptowährungen als Entgelt | 728 |
| 2. Mining von Kryptowährungen | 732 |
| C. Grenzüberschreitende Aktivitäten von Unternehmen mit Sitz in Deutschland | 733 |
| I. Einsatz von Kryptowährungen als Zahlungsmittel | 733 |
| II. Mining-Aktivitäten | 734 |
| D. Sonstige Kryptoassets und die Forderung nach einer Datensteuer | 735 |
| I. Sonstige Kryptoassets | 736 |
| 1. Security und Equity Token | 736 |
| 2. Utility Token | 737 |
| 3. Forwards und Futures | 740 |
| 4. Sonstige virtuelle Wirtschaftsgüter | 740 |
| II. Die Forderung nach einer Besteuerung von Daten (Digitalsteuer) | 741 |
| § 7 Marktmacht durch Daten | 743 |
| § 7.1 Marktmacht durch Daten: | |
| Eine Analyse aus ökonomischer Perspektive | 745 |
| A. Einführung | 748 |
| B. Wettbewerbsvorteile durch Daten | 750 |
| I. Datensammlung und Profilbildung mittels Trackingtechnologien | 751 |
| II. Datengetriebene Qualitätsverbesserung und Personalisierung | 753 |
| III. Zielgerichtete Werbung | 756 |
| IV. Preisdiskriminierung | 760 |
| C. Marktmacht durch Daten | 762 |
| I. Zugang zu Daten | 762 |
| II. Netzwerkeffekte und mehrseitige Märkte | 764 |
| III. Wechselkosten | 766 |

| | |
|--|------------|
| IV. Skalen-, Verbund- und Feedbackeffekte..... | 768 |
| V. Zugangsgewährung und Datenaustausch | 770 |
| VI. Diskriminierung, vertikale Integration und Marktmacht- übertragung..... | 771 |
| 1. Diskriminierung von Drittanbietern in Plattformmärkten | 772 |
| 2. Marktmachtübertragung..... | 772 |
| D. Maßnahmen zur Abschwächung von Datenmacht | 774 |
| I. Erhöhung der Transparenz..... | 774 |
| II. Recht auf Datenübertragbarkeit..... | 775 |
| III. Zugangsverpflichtung zu Datenpools | 776 |
| E. Schlussbemerkungen | 777 |
| § 7.2 Marktmacht durch Daten: | |
| Eine Analyse aus rechtswissenschaftlicher Perspektive | 779 |
| A. Einleitung und kartellrechtliche Hintergründe | 781 |
| I. Verbot des Missbrauchs einer marktbeherrschenden Stellung | 783 |
| II. Fusionskontrolle | 784 |
| III. Verbot wettbewerbsbeschränkender Kooperationen..... | 784 |
| B. Daten und Marktmacht | 786 |
| I. Marktbestimmung bei datenbezogenen Geschäftsmodellen.. | 786 |
| 1. Defizite herkömmlicher Bestimmungsmöglichkeiten bei Plattformen | 786 |
| 2. Kartellrechtliche Erfassung von Plattformen..... | 788 |
| 3. Unentgeltliche Leistungen und „Bezahlung mit Daten“ .. | 789 |
| 4. Unterschiedliche Kategorien von Daten | 790 |
| II. Datenmacht und Marktmacht | 791 |
| 1. Marktanteilsbezogene Bewertung der Marktstellung.... | 791 |
| 2. Marktbeherrschung bei Plattformen..... | 792 |
| a) Netzwerkeffekte | 792 |
| b) Multi-Homing..... | 793 |
| c) Skalierung und Größenvorteile..... | 795 |
| d) Zugang zu Daten | 796 |
| e) Innovation | 798 |
| 3. Relative oder überlegene Marktmacht | 801 |
| III. Marktmachtmissbrauch | 803 |
| 1. Verhältnis des Missbrauchsverbots zu anderen objektiven Rechtsmaterien | 803 |
| 2. Essential Facilities Doctrine und Geschäftsverweigerung . | 804 |
| 3. Behinderungsmisbrauch und Lock-in..... | 806 |
| 4. Diskriminierungsmisbrauch | 807 |
| 5. Ausbeutungsmisbrauch..... | 808 |
| C. Zugangsbedingungen zu Daten | 811 |
| I. Informationsaustausch..... | 812 |
| 1. Outsourcing und Lieferantenplattformen | 813 |
| 2. Daten-Kooperationen..... | 815 |

| | |
|--|------------|
| 3. Blockchain..... | 816 |
| II. Standardisierung und Normierung..... | 817 |
| III. Schnittstelleninformationen..... | 819 |
| § 8 Digitale Geschäftsmodelle – Datenbasierte Chancen und Risiken für Unternehmen..... | 821 |
| A. Der unternehmerische Zielkonflikt..... | 823 |
| B. „Data is the new oil“..... | 829 |
| I. Daten als Basis digitaler Geschäftsmodelle..... | 830 |
| II. Datengetriebene Geschäftsmodelle..... | 830 |
| 1. Datenstrategie..... | 833 |
| 2. Data Governance und Datenmanagement..... | 834 |
| C. DS-GVO – Der Schutz des Kunden..... | 836 |
| D. Herausforderungen digitaler Geschäftsmodelle im Spannungsfeld Innovation vs. Sicherheit..... | 838 |
| E. Fazit: Datengetriebene Vision und Verantwortung..... | 840 |
| § 9 Haftung für fehlerhafte Daten..... | 843 |
| § 9.1 Haftung für fehlerhafte Gesundheitsdaten..... | 845 |
| A. Digitalisierung im Gesundheitswesen..... | 846 |
| I. Hintergrund..... | 846 |
| II. Aktuelle Entwicklungen..... | 847 |
| 1. Medizin 4.0..... | 847 |
| 2. Telemedizin..... | 847 |
| 3. Mobile Health..... | 849 |
| III. Rechtliche Einordnung digitaler Gesundheitsprodukte und -anwendungen..... | 850 |
| 1. Hintergrund..... | 850 |
| 2. Produktklassifizierung durch Zweckbestimmung und Wirkweise..... | 851 |
| 3. Software als Medizinprodukt..... | 851 |
| 4. Grenzen subjektiver Zweckbestimmung..... | 852 |
| 5. Exkurs: Software als Arzneimittel..... | 853 |
| IV. Marktteilnehmer im Bereich digitaler Gesundheitsprodukte und -anwendungen..... | 853 |
| B. Fehlerhafte Gesundheitsdaten..... | 854 |
| I. Definition der Gesundheitsdaten..... | 854 |
| II. Ebenen der Fehlerhaftigkeit..... | 854 |
| C. Haftung für fehlerhafte Gesundheitsdaten..... | 855 |
| I. Haftung für Medizinprodukte..... | 856 |
| 1. Haftung vor Marktreife..... | 856 |
| a) § 823 Abs. 2 BGB..... | 856 |
| b) ProdHaftG..... | 857 |
| aa) Anwendbarkeit des ProdHaftG..... | 857 |

| | |
|---|------------|
| bb) Berücksichtigung des § 1 Abs. 2 Nr. 5 ProdHaftG | 859 |
| c) Ergebnis | 859 |
| d) Exkurs: Probandenversicherung | 859 |
| 2. Haftung nach Marktreife | 860 |
| a) § 823 Abs. 1 BGB | 860 |
| aa) Umfang der Verkehrssicherungspflichten | 860 |
| (1) Konstruktions-, Fabrikations- und Instruktionspflichten | 861 |
| (2) Produktbeobachtungspflichten | 861 |
| (3) Reaktionspflichten | 862 |
| bb) Konkretisierung der Verkehrssicherungspflichten bei Medizinprodukten | 862 |
| (1) Produktbeobachtungspflichten nach § 3 MPSV | 863 |
| (2) Reaktionspflichten nach § 14 MPSV | 863 |
| b) § 823 Abs. 2 BGB | 864 |
| aa) Verletzung von Schutzgesetzen | 864 |
| bb) § 4 MPG als Schutzgesetz | 865 |
| cc) Exkurs: IT-Sicherheitsgesetze als Schutzgesetze | 865 |
| c) ProdHaftG | 865 |
| aa) Fehlerhafte Produkte | 866 |
| bb) Produkthersteller | 866 |
| cc) Software als Produkt | 866 |
| dd) Beweislastumkehr nach EuGH | 867 |
| d) Ergebnis | 868 |
| II. Haftung für sonstige Produkte | 869 |
| III. Exkurs: Haftungsbeschränkungen | 870 |
| 1. Gesetzliche Haftungsbeschränkungen | 870 |
| 2. Vertragliche Haftungsbeschränkungen | 871 |
| a) AGB | 871 |
| b) Einbeziehung gegenüber dem tatsächlichen Nutzer | 871 |
| c) Inhaltliche Grenzen von AGB | 872 |
| d) Ergebnis | 872 |
| D. Schluss/Ausblick | 872 |
| § 9.2 Haftung für fehlerhafte Daten beim autonomen Fahren | 874 |
| A. Einleitung | 877 |
| I. Daten als „Antrieb“ autonomer Fahrzeuge | 877 |
| II. Präzisierung der Fragestellung | 878 |
| III. Gang der Darstellung | 879 |
| IV. Disclaimer | 879 |
| B. Autonomes Fahren: Rechtsbeziehungen im Internet der Dinge | 880 |
| I. Das digitale Ökosystem autonomer Fahrzeuge | 880 |
| 1. In-Car-Technologien | 881 |
| 2. Backend-Prozesse | 882 |
| 3. V2V- und V2I-Kommunikation | 883 |
| II. Potentielle Fehlerquellen und Schädiger | 884 |

| | |
|---|-----|
| C. Schadensersatzansprüche gegen den Nutzer des Fahrzeugs .. | 885 |
| I. Haftung für vermutetes Verschulden (§ 18 Abs. 1 S. 1 StVG) | 885 |
| II. Verschuldenshaftung (§ 823 Abs. 1 BGB) | 886 |
| D. Schadensersatzansprüche gegen den Fahrzeughalter | 887 |
| I. Gefährdungshaftung (§ 7 Abs. 1 StVG) | 887 |
| II. Abschaffung der Gefährdungshaftung de lege ferenda? | 888 |
| E. Schadensersatzansprüche gegen den Fahrzeugverkäufer | 889 |
| I. Sachmängelhaftung | 889 |
| II. Haftung für mangelhafte Backend-Daten | 890 |
| F. Schadensersatzansprüche gegen den Fahrzeughersteller | 891 |
| I. Haftungsszenarien | 891 |
| II. Haftungsgrundlagen | 892 |
| 1. Überblick | 892 |
| 2. Unterschiede zwischen der Produkt- und Produzentenhaftung | 892 |
| III. Produkt- und Produzentenhaftung für fehlerhafte Daten? | 893 |
| 1. ProdHaftG | 894 |
| 2. Deliktische Produzentenhaftung (§ 823 Abs. 1 BGB) | 895 |
| IV. Haftungssubjekte | 896 |
| 1. Endhersteller | 896 |
| 2. Zulieferer, insb. Software- und Datenlieferanten | 896 |
| 3. Weitere Haftungssubjekte | 897 |
| V. Fabrikationsfehler | 897 |
| VI. Konstruktionsfehler | 898 |
| 1. Fehlerhafte Software als Konstruktionsfehler | 898 |
| 2. Technische Standards | 898 |
| 3. Sicherheitserwartungen an die fahrzeugeigene Software. | 899 |
| 4. Sicherheitserwartungen an selbstlernende Software | 900 |
| 5. Grenzen der Herstellerhaftung: Stand von Wissenschaft und Technik | 902 |
| VII. Instruktionsfehler | 903 |
| VIII. Produktbeobachtungs- und Rückrufpflichten | 904 |
| 1. Produktbeobachtungspflichten | 904 |
| 2. Produktrückrufpflicht und Pflicht zum kostenlosen Software-Update | 905 |
| IX. Beweislastverteilung, insb. bei Konstruktionsfehlern | 906 |
| 1. Beweisprobleme | 906 |
| 2. Event Data Recorder | 907 |
| 3. Zwischenergebnis | 908 |
| G. Schadensersatzansprüche gegen IT-Dienstleister, insb. Backend-Betreiber | 908 |
| I. Haftungsbegrenzungen nach dem TMG | 909 |
| 1. Abgestufte Haftung nach dem TMG | 909 |
| 2. Haftung von Backend-Betreibern | 909 |
| II. Vertragliche Gewährleistungshaftung | 910 |

| | |
|--|-----|
| III. Deliktische Ansprüche aus § 823 Abs. 1 BGB..... | 911 |
| H. Ausblick | 912 |
| § 9.3 Haftung für fehlerhafte Daten – Industrie 4.0 | 915 |
| A. Industrie 4.0 | 916 |
| I. Ziele | 917 |
| II. Wesentliche Herausforderungen | 918 |
| B. Haftungsrisiken | 920 |
| I. Vertragliche Gewährleistung..... | 920 |
| 1. Schuldrechtliche Besonderheiten..... | 921 |
| 2. Datenfehler..... | 922 |
| 3. Verschuldensunabhängige Gewährleistungsrechte | 922 |
| 4. Anspruch auf Schadenersatz oder Ersatz vergeblicher Aufwendungen | 923 |
| a) Vertretenmüssen | 923 |
| b) Haftungsfolgen | 924 |
| II. Außervertragliche Haftung..... | 925 |
| 1. Verschuldensabhängige Deliktshaftung | 925 |
| a) Sach- oder Personenschäden | 926 |
| b) Schäden an Datenbeständen | 927 |
| aa) Eigentum an Daten..... | 927 |
| bb) Daten als „sonstiges Recht“ i. S. v. § 823 Abs. 1 BGB . | 928 |
| 2. Produkthaftung | 929 |
| a) Anwendungsbereich..... | 929 |
| b) Herstellereigenschaft | 930 |
| c) Produktfehler | 930 |
| C. Haftungslücken in der Industrie 4.0 | 932 |
| I. Unvermeidbare Fehler..... | 933 |
| II. Maschinenhaftung? | 933 |
| III. Mögliche Lösungsansätze | 935 |
| D. Maßnahmen zur Risikoreduzierung | 936 |
| I. Vertragliche Gestaltungsmöglichkeiten..... | 936 |
| II. Digital Governance | 937 |
| E. Fazit | 939 |
| § 10 Datenbestände in Zwangsvollstreckung und Insolvenz..... | 941 |
| A. Einführung | 944 |
| I. Grundlagen zum Zwangsvollstreckungsrecht | 946 |
| 1. Allgemeines | 946 |
| 2. Problem: Offenbarung der Daten im Zwangsvollstreckungsverfahren..... | 948 |
| a) Aus Gläubigersperspektive | 948 |
| b) Aus Schuldnersperspektive | 950 |

| | | |
|-----------|---|-----|
| 3. | Vollstreckung in einzelne Gegenstandskategorien | 951 |
| a) | Körperliche Gegenstände (Datenträger) | 951 |
| b) | Unkörperliche Gegenstände | 952 |
| aa) | Ausgangspunkt | 952 |
| bb) | Insbesondere: Vertragliche Nutzungsrechte | 952 |
| II. | Grundlagen zum Insolvenzrecht | 953 |
| 1. | Übergang der Verwaltungs- und Verfügungsbefugnis | 953 |
| 2. | Insolvenzmasse | 954 |
| 3. | Verträge in der Insolvenz | 955 |
| III. | Rechtliche Kategorisierung der datenrechtlichen Bezugsobjekte | 956 |
| 1. | Sondergesetzlich geschützte Daten | 957 |
| a) | Urheberrecht und verwandte Schutzrechte | 957 |
| aa) | Datenbankwerk, §§ 2 Abs. 2, 4 Abs. 2 S. 1 UrhG | 957 |
| bb) | Datenbankherstellerrecht, §§ 87a UrhG | 958 |
| cc) | Weitere Anknüpfungspunkte im UrhG | 959 |
| b) | Geschäftsgeheimnisse, Know-how | 959 |
| c) | Personenbezogene Daten | 961 |
| d) | Allgemeines Persönlichkeitsrecht (Kommerzielle Elemente) | 961 |
| e) | Vertraglich geschützte Daten | 962 |
| f) | Sonstige Daten | 963 |
| 2. | Datenträger | 963 |
| B. | Daten in der Zwangsvollstreckung | 963 |
| I. | Allgemeines | 963 |
| II. | Sondergesetzlich geschützte Daten | 964 |
| 1. | Urheberrecht und verwandte Schutzrechte | 964 |
| 2. | Geschäfts- und Betriebsgeheimnisse, Know-how | 966 |
| 3. | Personenbezogene Daten | 966 |
| 4. | Allgemeines Persönlichkeitsrecht (Kommerzielle Elemente) | 968 |
| 5. | Vertraglich geschützte Daten | 969 |
| C. | Daten in der Insolvenz | 970 |
| I. | Massezugehörigkeit von Daten | 970 |
| II. | Aussonderung von Daten in der Insolvenz | 971 |
| 1. | Urheberrecht, Leistungsschutzrechte und verwandte Schutzrechte | 971 |
| 2. | Personenbezogene Daten | 972 |
| 3. | Allgemeines Persönlichkeitsrecht (Kommerzielle Elemente) | 972 |
| 4. | Vertraglich und insb. auftragsrechtlich geschützte Daten | 972 |
| III. | Vertragsgestaltung | 973 |
| 1. | Anwendbares Recht und internationale Zuständigkeit | 973 |
| 2. | Insolvenzrechtliche Schranken vertraglicher Gestaltung | 974 |

| | |
|--|------------|
| 3. Sicherung des Datenzugriffs | 975 |
| 4. Sicherung von Nutzungsrechten | 976 |
| IV. Datenschutz in der Insolvenz | 978 |
| 1. Meinungsstand unter Geltung des BDSG a.F. | 979 |
| 2. Rechtslage seit Geltung der DS-GVO | 980 |
| a) Datenschutzrechtliche Verantwortlichkeit des Insolvenzverwalters | 980 |
| b) Datenschutzrechtliche Verantwortlichkeit des vorläufigen Insolvenzverwalters | 981 |
| Herausgeberinnen | 983 |
| Stichwortverzeichnis | 985 |

§ 6.1

Bitcoin/E-Geld/Virtuelle Währungen

Jörn Erbguth*

Literatur: *Arnone/Laurens/Segalotto/Sommer*, Central Bank Autonomy: Lessons from Global Trends, 56 IMF Staff Papers, 263–296 (2009); *Auffenberg*, Bitcoins als Rechnungseinheiten – Eine kritische Auseinandersetzung mit der aktuellen Verwaltungspraxis der BaFin, NVwZ 2015, 1184–1187; *Bausch/Heetkamp*, Wie kommt der „Kuckuck“ auf den Bitcoin? Dispute Resolution 2018, 7–10; *Beaucamp/Henningsen/Florian*, Strafbarkeit durch Speicherung der Bitcoin-Blockchain? Ein Lösungsversuch aus technischer und rechtlicher Sicht, MMR 2018, 501–507; *Blum/Feldman/Micali*, Non-Interactive Zero-Knowledge and Its Applications, in: Proceedings of the twentieth annual ACM symposium on Theory of computing (STOC '88), 1988, 103–112; *Boehm/Pesch*, Bitcoins: Rechtliche Herausforderungen einer virtuellen Währung – Eine erste juristische Einordnung, MMR 2014, 75–79; *Dietsch*, Umsatzsteuerliche Einordnung von Initial Coin Offerings, MwStR 2018, 546–551; *Erbguth/Fasching*, Wer ist Verantwortlicher einer Bitcoin-Transaktion? Anwendbarkeit der DS-GVO auf die Bitcoin-Blockchain, ZD 2017, 560–565; *Goger*, Bitcoins im Strafverfahren – Virtuelle Währung und reale Strafverfolgung, MMR 2016, 431–434; *Greier*, Möglichkeiten strafprozessualer Sicherung von Bitcoins gemäß §§ 111b ff. StPO, wistra 2016, 249–257; *Erman* (Hrsg.) BGB, 15. Aufl. 2017, Köln: Verlag Dr. Otto Schmidt; *Halpin/Piekarska*, Introduction to Security and Privacy on the Blockchain, IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), IEEE Press, 1–3 (2017); *Heckelmann*, Zulässigkeit und Handhabung von Smart Contracts, NJW 2018, 504–510; *Heine*, Bitcoins und Botnetze – Strafbarkeit und Vermögensabschöpfung bei illegalem Bitcoin-Mining, NSTz 2016, 441–504; *Hoffmann/Johannes*, DS-GVO: Anleitung zur autonomen Auslegung des Personenbezugs – Begriffsklärung der entscheidenden Frage des sachlichen Anwendungsbereichs, ZD 2017, 221–226; *Joecks/Miebach* (Hrsg.), Münchener Kommentar zum StGB, 3. Aufl. 2017, München: C. H. Beck; *Kaulartz*, Die Blockchain-Technologie, CR 2016, 474–480; *Kaulartz*, Rechtliche Grenzen bei der Gestaltung von Smart Contracts, DSRITB 2016, 1023–1037; *Kilian/Heussen* (Hrsg.), Computerrechts-Handbuch, 33. Aufl. 2017, München: C. H. Beck; *Korte*, Vermögensabschöpfung reloaded, wistra 2018, 1–12; *Koshy/Koshy/McDaniel*, An Analysis of Anonymity in Bitcoin Using P2P Network Traffic, in: Christin/Safavi-Naini (Hrsg.), Financial Cryptography and Data Security 18th International Conference, FC 2014, Revised Selected Papers, 2014, Springer: Berlin, Heidelberg, S. 469–485; *Krüger/Lampert*, Augen auf bei der Token-Wahl – privatrechtliche und steuerliche Herausforderungen im Rahmen eines Initial Coin Offering, BB 2018, 1154–1160; *Kütük/Sorge*, Bitcoin im deutschen Vollstreckungsrecht – Von der „Tulpenmanie“ zur „Bitcoinmanie“, MMR 2014, 643–646; *Matzutt/Hiller/Henze/Ziegeldorf/Müllmann/Hohlfeld/Wehrle*, A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin, in: Proceedings of the 22nd

* Jörn Erbguth ist Diplom-Jurist und Diplom-Informatiker, berät zu Blockchain und Datenschutz, promoviert aktuell an der Uni Genf sowie ist Lehrbeauftragter an verschiedenen Schweizer Universitäten.

Der Verfasser möchte sich für das wertvolle Feedback bedanken, welches er insbesondere von Rechtsanwältin Katrin Kirchert erhalten hat.

International Conference on Financial Cryptography and Data Security, 2018, Springer: Berlin, Heidelberg; *Oelschlägel/Scholz* (Hrsg.), Rechtshandbuch Online-Shop, 2. Aufl. 2017, Köln: Verlag Dr. Otto Schmidt; *Peters*, Sabotage von Blockchains durch Einschleusung strafrechtsrelevanter Inhalte?, in: Taeger (Hrsg.), Rechtsfragen digitaler Transformationen – Gestaltung digitaler Veränderungsprozesse durch Recht, Tagungsband DSRI-Herbstakademie 2018, Edewecht: OIWR, S. 381–395; *Rückert*, Vermögensabschöpfung und Sicherstellung bei Bitcoins – Neue juristische Herausforderungen durch die ungeklärte Rechtsnatur von virtuellen Währungseinheiten, MMR 2016, 295–300; *Saive*, Haftungsprivilegierung von Blockchain-Dienstleistern gem. §§ 7 ff. TMG – Blockchain-Teilnehmer: Homo homini hostis oder Host Provider? CR 2018, 186–193; *Schilling/Hübner*, „Non-conviction-based confiscation“ – Ein Fremdkörper im neuen Recht der strafrechtlichen Vermögensabschöpfung?, StV 2018, 49–57; *Schimansky/Bunte/Lwowski* (Hrsg.), Bankrechts-Handbuch, 5. Aufl. 2017, München: C. H. Beck; *Meyer zu Schwabedissen* (Hrsg.), Die Erlaubnis zum Betreiben des E-Geld Geschäfts, 2015, Köln: RWS Verlag Kommunikationsforum GmbH; *Simmchen*, Blockchain (R)Evolution, MMR 2017, 162–165; *Spindler/Bille*, Rechtsprobleme von Bitcoins als virtuelle Währung, WM 2014, 1357–1369; *Kale/Dhamdhere*, Survey Paper on Different Type of Hashing Algorithm, International Journal of Advance Scientific Research and Engineering Trends, Vol. 3, Issue 2, February 2018; *Schwintowski/Klausmann/Kadgien*, Das Verhältnis von Blockchain-Governance und Gesellschaftsrecht, NJOZ 2018, 1401; Möri, Blockchain und Datenschutz, Jusletter IT 23.05.2019 – http://jusletter-it.weblaw.ch/issues/2019/23-Mai-2019/blockchain-und-daten_cbe632b9ad.html (09.08.2019); Finck, Blockchain and the General Data Protection Regulation, Panel for the Future of Science and Technology (STOA), European Parliament, PE 634.445, 24.07.2019, – [https://www.europarl.europa.eu/stoa/en/document/EPRS_STU\(2019\)634445](https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2019)634445) (09.08.2019); EU-Blockchain Observatory: Blockchain and the GDPR v. 16. 10. 2018 – https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf (09.08.2019).

A. Daten als Zahlungsinstrumente mit ggf. weiteren Funktionen

I. Begriffsklärungen

- 1 Für Bitcoin und andere Kryptowährungen sind die Begriffe **virtuelle Währungen**, **Kryptowährungen** und **autonome** bzw. **dezentrale Kryptowährungen** gebräuchlich. Virtuelle Währung ist der Wortgebrauch der Zentralbanken und Finanzmarktregulierer. Das Adjektiv virtuell soll dabei ausdrücken, dass es sich nicht um offizielle Währungen, sondern um digitale Ersatzwährungen handelt.¹ Technisch dagegen beschreibt der Begriff Kryptowährung Bitcoin & Co besser. Diese Währung basiert vor allem auf Kryptografie. Um Kryptowährungen **ohne zentrale Steuerung** von **zentral gesteuerten** Kryptowährungen zu unterscheiden, werden erstere auch autonome oder dezentrale Kryptowährungen genannt.

Bei Bitcoins spricht man von **Coins**. Diese Begrifflichkeit wurde auch von späteren Kryptowährungen übernommen. Bei **Ethereum** können die Coins weitere, frei programmierbare Funktionalitäten erhalten. Zur Differenzierung werden die Coins dort **Tokens** genannt. Inzwischen ist Tokens der Überbegriff und Coins bezeichnet Tokens, bei denen die Hauptfunktion die Zahlungsfunktion ist. Im

¹ BaFin, Virtual Currencies (Virtuelle Währungen) – https://www.bafin.de/DE/Verbraucher/Finanzwissen/Fintech/VirtuelleWaehrungen/virtuelle_waehrungen_artikel.html (09.08.2019).

Entwurf des Gesetzes zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie wird auch übergreifend von **Kryptowerten** gesprochen.

II. Dimensionen

Wer ein elektronisches System konstruieren möchte, welches Tokens verwaltet, ² muss drei Fragenbereiche klären:

- Wie soll das System *funktionieren*? Dabei muss etwa geklärt werden, wie z.B. die Zahlungseinheiten entstehen, nach welchen Regeln sie übertragen und gehandelt werden können, wer die Tokens akzeptieren soll, ob es weitere Funktionen gibt, die an die Tokens geknüpft werden und welche Art von Kontroll- und Eingriffsmöglichkeit bestehen sollen.
- Wie soll das System *technisch realisiert* werden? Eine Buchführung über Tokens kann klassisch auf einem zentralen Server erfolgen. Unsere Bankkonten werden so geführt. Natürlich gibt es dabei auch Backup- und Spiegelserver. Diese sind jedoch meistens hierarchisch organisiert und werden von zentralen Akteuren kontrolliert. Blockchains dagegen ermöglichen die dezentral-parallele Kontenführung auf einer Vielzahl von Systemen, um das Risiko von Manipulationen durch einzelne Akteure auszuschließen. Entscheidende Fragen sind dabei, wie (und ob) sich die Teilnehmer identifizieren müssen, wie die Synchronisation erfolgt, wie Konflikte gelöst werden und wie ggf. gewünschte Beschränkungen und Zusatzfunktionen realisiert werden?
- Schließlich bedarf es einer *juristischen Betrachtung* der Rechtsnatur der Tokens und des regulatorischen Umfeldes. Handelt es sich um eine Art Gutschein, e-Geld, eine virtuelle Währung oder eine andere Art von Finanzinstrument? Wird der Herausgeber oder Händler dadurch zum Zahlungsinstitut, e-Geld-Institut, Kreditinstitut oder Finanzdienstleistungsinstitut und muss er die entsprechenden Genehmigungen einholen und Regulierungen beachten?

Die drei Fragenbereiche hängen eng zusammen. Wer neue Tokens gestalten will, muss daher in einem iterativen Prozess ein passendes funktionales Modell finden, welches technisch mit tragbarem Aufwand realisiert werden kann und juristisch zu akzeptablen Regulierungen und Genehmigungspflichten führt.

B. Funktionsweise

Ein elektronisches System zur Verwaltung von Tokens kann sehr unterschiedlich ³ ausgestaltet sein und sehr unterschiedlichen Zwecken dienen. Daher sind zunächst eine Vielzahl von Fragen zu klären:

I. Autonomie des Systems

Bei konventionellen Währungen – auch Fiat-Währungen genannt – stärkt die **Autonomie der Zentralbank** die Währung.² Je geringer der Einfluss der Politik ⁴

² *Agone/Laurens/Segalotto/Sommer*, Central Bank Autonomy: Lessons from Global Trends, IMF Staff Papers, June 2009, S. 263–296.

ist, desto größer ist das Vertrauen in die Währung. Dieses Prinzip gilt auch für Kryptowährungen. Daher ist es eine entscheidende Frage, wie viel Kontrolle der Herausgeber der Tokens behält, welche Eigenschaften vorab unveränderlich festgeschrieben werden und ob er den Inhabern der Zahlungseinheiten volle Verfügungsfreiheit gewährt: Können die Inhaber die Zahlungseinheiten autonom an Dritte transferieren, oder hat der Herausgeber die Möglichkeit, die Transfers zu blockieren? Kann jeder Außenstehende ein Konto eröffnen und Tokens von einem Inhaber erwerben, oder muss ein zentraler Akteur z.B. aus Compliance-Gründen zunächst einer Kontoeröffnung zustimmen? Kann der Herausgeber neue Tokens nach Belieben erstellen oder ist die Menge der Zahlungseinheiten und die Erstellung weiterer Tokens zu Beginn unveränderbar vorgegeben?

II. Forderungscharakter

- 5 Ein System mit hoher Autonomie kann vom Herausgeber nachträglich nur sehr eingeschränkt kontrolliert oder manipuliert werden. Dadurch können die Tokens einen Wert erhalten, selbst wenn sie **keine Forderungen gegenüber dem Herausgeber** oder **Dritten** darstellen. Gut passt dazu auch, wenn die Tokens als Gutscheine für Leistungen auf der Blockchain aber nicht gegen den Herausgeber dienen. Bei Ethereum kann so z.B. die Ausführung von Programmen auf der Blockchain mit den Ether-Tokens „bezahlt“ werden.

Behält der Herausgeber dagegen ein großes Maß an Kontrolle, so hängt der Wert der Tokens davon ab, dass diese mit entsprechenden Forderungen hinterlegt sind. Der Herausgeber kann dazu Waren oder Dienstleistungen für die Tokens versprechen. Bei einigen Kryptowährungen garantiert der Herausgeber auch direkt einen Betrag in einer Fiat-Währung. Dadurch sind diese Kryptowährungen an diese Fiat-Währung gekoppelt und werden auch als **Stable Coins** bezeichnet.³ Eine weitere Variante stellt die geplante Kryptowährung **libra** dar, bei der der Wert nicht an eine einzelne Währung, sondern an einen Währungskorb bzw. Korb von Assets gekoppelt werden soll.⁴

III. Weitere Funktionalitäten

- 6 Neben einfachen Forderungen können an die Tokens auch weitere Funktionalitäten gebunden werden. So lassen sich z. B. Stimmrechte realisieren, die elektronisch ausgeübt werden. Die Tokens können auch eine automatische Verzinsung erfahren. Wenn Tokens als Bonuspunkte vergeben werden, können diese an Bedingungen oder Fristen gekoppelt werden. Die Tokens können in Computerspielen als Währung zum Kauf virtueller Waren oder zum Freischalten von Spiel-funktionen verwendet werden und dabei komplexen Regeln unterliegen. Die funktionale Gestaltung der Tokens lässt sich frei programmieren, woraus sich praktisch endlose Gestaltungsmöglichkeiten ergeben.

³ Z. B.: tether – <https://tether.to> (09.08.2019).

⁴ *Catalani/Graty/Hou/Parasouraman/Wernerfelt*, Die Libra-Reserve – https://libra.org/de-DE/wp-content/uploads/sites/14/2019/06/TheLibraReserve_de_DE.pdf (07.08.2019).

IV. Token-Design

Bei der Entwicklung von Software-Systemen hilft die Beschreibung des Lebenszyklus und der typischen Anwendungsfälle⁵ (Use-Cases) um einen Eindruck von dem gewünschten System zu erhalten. Der Lebenszyklus beginnt mit dem Erstellen der ersten Tokens in einem **Token Generating Event (TGE)** oder dem kombinierten Erstellen und Verkaufen der Tokens in einem **Initial Coin Offering (ICO)** sowie ggf. der weiteren Generierung von Tokens beim Mining. Die Charakterisierung wird fortgesetzt mit der Beschreibung der Verwendung, der Funktionalität und wenn gewünscht der Kontrolle bzw. Governance der Tokens und Transaktionen. Schließlich kann man die Tokens entweder für die Ewigkeit generieren oder auch Situationen beschreiben, in denen Tokens eingezogen werden. Dieses Token-Design hat technische und juristische Implikationen. In einem iterativen agilen Prozess wird ein Design erstellt und gründlich getestet. Einmal in den Echtbetrieb gestartet, sollten die Regeln dagegen technisch vor Veränderungen geschützt sein, denn der technische Schutz vor Manipulationen ist ein wesentlicher Faktor für das Vertrauen der Token-Inhaber und damit für die Werthaltigkeit der Tokens. Umgekehrt ist es aber auch sinnvoll, einen gegen Missbrauch besonders geschützten Weg zur Korrektur von Bugs (Programmfehlern) oder sonstigen Anpassung von Regeln einzubauen (vgl. Blockchain-Governance, Rn. 56 ff.).

C. Technische Realisierung

Die technische Realisierung erfolgt durch Programmierung. Daher gibt es hier keinen Numerus Clausus von Alternativen, sondern ein breites Spektrum an Realisierungsmöglichkeiten. Diese lassen sich grob nach dem Ort der Speicherung einteilen. Werden die Zahlungseinheiten auf einem Server des Herausgebers gespeichert? Liegen die Zahlungseinheiten auf einer Blockchain, die auf vielen Rechnern parallel vorhanden ist? Oder werden die Zahlungseinheiten auf Systemen der Inhaber gespeichert, wie z.B. auf einer Geldkarte?

Ohne die Kryptografie mit den Konzepten der kryptographischen Hashfunktion und der digitalen Signatur wären viele dieser Systeme nicht realisierbar. Daher folgt zunächst eine Einführung in diese technologischen Grundlagen:

I. Technologische Grundlagen

1. Kryptographische Hashfunktionen

Eine zentrale Rolle bei der Distributed Ledger Technologie sind kryptographische Hash-Funktionen. **Hashfunktionen**⁶ sind eine Art digitaler Fingerabdruck. Für jedes digitale Objekt – ob wenige Zeichen oder mehrere Terabyte an Daten –

⁵ Rouse, Definition use case, Search Software Quality – <http://searchsoftwarequality.techtarget.com/definition/use-case> (09.08.2019).

⁶ Hashfunktion, Wikipedia – <https://de.wikipedia.org/wiki/Hashfunktion> (09.08.2019).

kann ein digitaler Fingerabdruck berechnet werden. Der Fingerabdruck – auch **Hashwert** genannt – hat immer die gleiche Zeichenlänge – z.B. 256 Bit – d.h. 43 Zeichen in der üblichen Base64-Schreibweise. Wie bei einer Quersumme ändert sich der Fingerabdruck mit jeder kleinsten Änderung des digitalen Objektes. Kryptographische Hashfunktionen⁷ zeichnen sich zusätzlich dadurch aus, dass sie Einwegfunktionen⁸ sind, d.h., dass sie nicht einfach umgekehrt werden können. Das bedeutet, dass aus dem Hashwert kein passendes Objekt errechnet werden kann. Vielmehr kann ein solches nur durch Ausprobieren gefunden werden und das auch nur theoretisch, denn dieses Ausprobieren ist beim fachgerechten Hashing so langwierig, dass es als praktisch unmöglich gilt, ein passendes Objekt zu einem Hashwert zu finden. Mit Hilfe des kryptographischen Hashwertes eines digitalen Objekts kann daher sowohl bewiesen werden, dass das Objekt nicht verändert wurde, als auch, dass es bei der Berechnung des kryptographischen Hashwertes bereits existierte. Im Folgenden sind mit Hashfunktionen und Hashwerte gemeint. Einige frühere Hashfunktionen⁹ gelten inzwischen als unsicher. Das liegt daran an, dass in diesen Hashfunktionen Schwachstellen gefunden wurden. Bei Bitcoin wird der Hashingalgorithmus SHA-256 verwendet, der bislang als sicher gilt. Zwar lassen sich auch bei unsicheren Hashingalgorithmen aus einem Hashwert keine komplexen gehashten Objekte rekonstruieren. Aber die Beweisfunktion und Sicherheit der sie verwendenden Blockchain wäre beeinträchtigt. Eine bereits bekannte neue Gefahr sind Quantencomputer. Diese rechnen nicht per se schneller, sondern anders und können Einwegfunktionen daher teilweise umkehren. Bereits heute lässt sich abschätzen, welche Algorithmen beeinträchtigt sein werden, wo Anpassungsbedarf besteht und welche Alternativen vorhanden sind.¹⁰

2. Kryptographische Signatur

- 10 Auf jeder Blockchain muss geprüft werden, ob eine Transaktion tatsächlich von dem Berechtigten stammt. In der Regel erfolgt dies durch eine **kryptographische Signatur** der Transaktion mit einem privaten Schlüssel. Die kryptographische Signatur beruht auf einem **asymmetrischen Kryptosystem**,¹¹ wie es auch für die

⁷ Kryptographische Hashfunktion, Wikipedia – https://de.wikipedia.org/wiki/Kryptographische_Hashfunktion (09.08.2019).

⁸ Einwegfunktion, Wikipedia – <https://de.wikipedia.org/wiki/Einwegfunktion> (09.08.2019).

⁹ Die Hashfunktionen md5 und SHA-1 gelten inzwischen als unsicher. Das bedeutet, dass es Hashwerte gibt, zu denen mehrere passende Objekte gefunden werden können. Vgl. Kale/Dhamdhare, Survey Paper on Different Type of Hashing Algorithm, International Journal of Advance Scientific Research and Engineering Trends, Vol. 3, Issue 2, February 2018, S. 14 – http://www.ijasret.com/VolumeArticles/FullTextPDF/189_4.Survey_Paper_on_Different_Type_of_Hashing_Algorithm.pdf (07.08.2019).

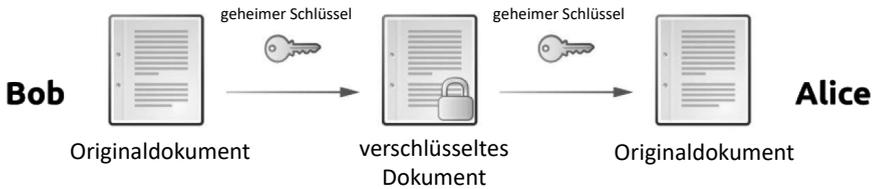
¹⁰ Chen et al., Report on Post-Quantum Cryptography, NISTIR 8105, S. 2 <https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf> (08.08.2019).

¹¹ Asymmetrisches Kryptosystem, Wikipedia – https://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem (09.08.2019).

asymmetrische Verschlüsselung – auch **Public Key Encryption** genannt – verwendet wird.

Bei einer **symmetrischen Verschlüsselung** (Abbildung 1 oben) wird für die Verschlüsselung und die Entschlüsselung der gleiche Schlüssel verwendet. Diese Verschlüsselung hat jedoch den Nachteil, dass der Schlüssel vorab abhörerischer übertragen werden muss. Zudem muss für jede Kommunikationsbeziehung ein eigener Schlüssel übertragen werden. Eine Alternative zur symmetrischen Verschlüsselung ist daher die **asymmetrische Verschlüsselung** (Abb. 1 unten). 11

Symmetrische Verschlüsselung



Asymmetrische Verschlüsselung

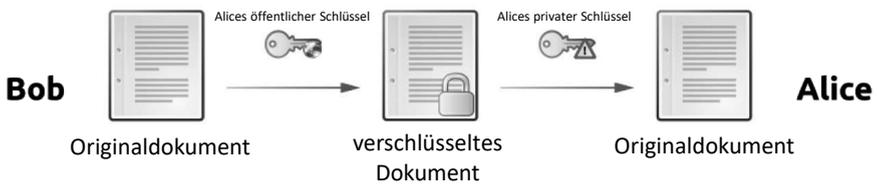


Abb. 1: Symmetrische Verschlüsselung und asymmetrische Verschlüsselung¹²

Hierbei gibt es einen öffentlichen **Schlüssel**, den jeder kennen darf und einen **privaten Schlüssel**, den nur der Empfänger kennt. Die Verschlüsselung ist dann so gestaltet, dass die Entschlüsselung einer mit dem öffentlichen Schlüssel verschlüsselten Nachricht nur mit dem privaten Schlüssel möglich ist. Die Verschlüsselung mit dem öffentlichen Schlüssel ist genauso wie die kryptographische Hashfunktion eine Einwegfunktion. Das bedeutet, dass mit dem öffentlichen Schlüssel aus der verschlüsselten Nachricht die ursprüngliche Nachricht nicht wiederhergestellt werden kann. Für die asymmetrische Verschlüsselung kann daher der öffentliche Schlüssel frei verteilt werden. Dabei muss allerdings verifiziert werden, dass beim Verteilen des öffentlichen Schlüssels dieser nicht ausgetauscht wird, da sonst ein Man-in-the-Middle die Nachrichten abfangen, entschlüsseln und dann mit dem richtigen Schlüssel unbemerkt an den eigentlichen Adressaten weiterleiten könnte.

¹² Adoption der Grafiken von Fleshgrinder (<https://commons.wikimedia.org/wiki/User:Fleshgrinder>)

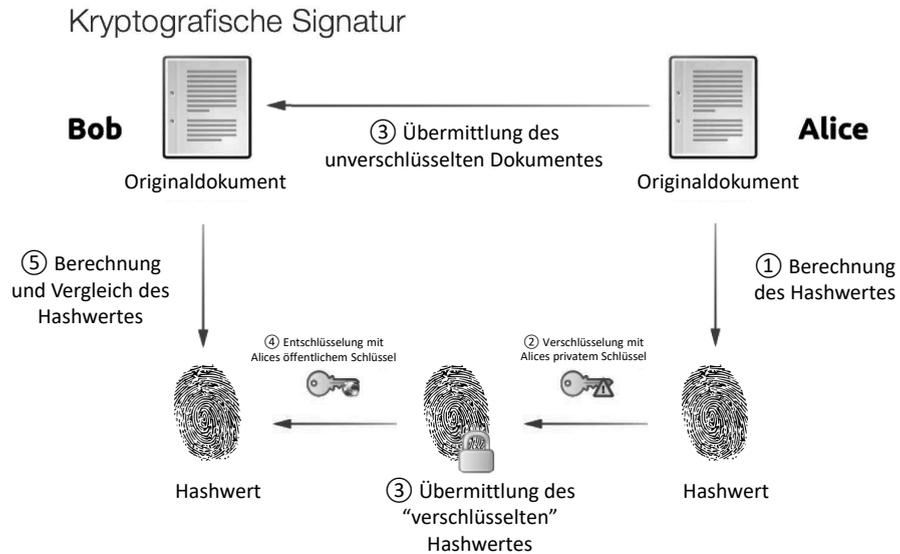


Abb. 2: Kryptographische Signatur

- 12 Die kryptographische Signatur (Abb. 2) verwendet ebenso öffentliche und private Schlüssel, tauscht aber die Verschlüsselungsfunktion aus. Neben der eigentlich versendeten Nachricht, wird ein Hashwert der Nachricht mit dem privaten Schlüssel „verschlüsselt“ und zusätzlich zur Nachricht versendet. Lässt sich der „verschlüsselte“ Hashwert vom Empfänger mit dem öffentlichen Schlüssel des Absenders entschlüsseln und passt dann zur Nachricht, so ist belegt, dass die Nachricht mit dem privaten Schlüssel des Absenders signiert wurde. Im Folgenden sind, wenn von Signaturen bzw. signieren gesprochen wird, kryptographische Signaturen gemeint.

II. Ablage auf einem Server

- 13 Die einfachste Form der Implementierung eines Systems zur Verwaltung von Tokens, ist die Ablage auf einem zentralen Server. Banken verwalten auf diese Art und Weise Girokonten, Fluggesellschaften die gesammelten Flugmeilen und Telefongesellschaften die Prepaid-Zahlungen. Der Betrieb eines Servers wird abgesichert durch redundante, parallel dazu laufende Spiegelserver. Zudem werden regelmäßig Backups angefertigt. Die Bank, der Herausgeber der Tokens oder der jeweilige Systemadministrator haben stets die Kontrolle über diese Systeme und können im Prinzip Einträge verändern. Dies ist das klassische Bankmodell, bei dem die Inhaber der Zahlungseinheiten dem Herausgeber vertrauen müssen. Dieses Vertrauen wird aber in der Regel ergänzt durch einen Berichtigungsanspruch, den die Inhaber gegenüber dem Herausgeber auch rechtlich durchsetzen können.

▼ Rechte an Daten werden in der Digitalisierung zunehmend relevant. Dabei geht es aber nicht nur um spezifische Fragen des Datenschutzrechts für neue Medien, sondern auch und gerade um Vermögensrechte an Daten, vertragsrechtliche Vorgaben für die Weitergabe und Nutzung von Daten, kartellrechtliche Fragen sowie die Zwangsvollstreckung in Datenbestände.

Das Handbuch gibt eine erste Definition des neuen Rechtsgebietes „Datenrecht“ und adressiert die hier auftretenden Fragestellungen. Dabei wagt es einen Blick über den juristischen Tellerrand hinaus auch in andere Disziplinen.

Leseprobe, mehr zum Buch unter ESV.info/978-3-503-18782-9



www.ESV.info