Specht-Riemenschneider • Werry • Werry (Hrsg.)

Datenrecht in der Digitalisierung

ESV ERICH SCHMIDT VERLAG

ESV ERICH SCHMIDT VERLAG

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

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

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 Bundeskartellamtes[1], 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 Rechtgebiet 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 einigem 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 sorgsamen 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 Datenschutzechtes 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 anderenorts 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 zahleiche 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

Inhaltsverzeichnis

§ 9.3

Haftung für fehlerhafte Daten – Industrie 4.0

*Dr. Gunnar Sachs**

Literatur: *Bartsch*, Daten als Rechtsgut nach § 823 Abs. 1 BGB, in: Conrad/Grützmacher (Hrsg.), Recht der Daten und Datenbanken in Unternehmen, 2014, Köln: Verlag Dr. Otto Schmidt, S. 297–302; *Borges*, Haftung für selbstfahrende Autos – Warum eine Kausalhaftung für selbstfahrende Autos gesetzlich geregelt werden sollte, CR 2016, 272–280; *Bräutigam/Klindt*, Industrie 4.0, das Internet der Dinge und das Recht, NJW 2015, 1137–1142; *Cornelius*, Vertragsabschluss durch autonome elektronische Agenten, MMR 2002, 353–358; *Deutsch*, Das neue System der Gefährdungshaftungen: Gefährdungshaftung, erweiterte Gefährdungshaftung und Kausal-Vermutungshaftung, NJW 1992, 73–77; *Hoeren*, Dateneigentum – Versuch einer Anwendung von § 303a StGB im Zivilrecht, MMR 2013, 486–491; *Horner/Kaulartz*, Verschiebung des Sorgfaltsmaßstabs bei Herstellung und Nutzung autonomer Systeme, CR 2016, 7–14; *Jänich*, Rechtsprobleme des autonomen Fahrens, NVZ 2015, 313–318; *Palandt* (Begr.), Bürgerliches Gesetzbuch, 78. Aufl. 2019, München: C. H. Beck; *Redeker*, Information als eigenständiges Rechtsgut – Zur Rechtsnatur der Information und dem daraus resultierenden Schutz, CR 2011, 634–639; *Redeker* (Hrsg.), IT-Recht, 6. Aufl. 2017, München: C. H. Beck; *Reichwald/Pfisterer*, Autonomie und Intelligenz im Internet der Dinge – Möglichkeiten und Grenzen autonomer Handlungen, CR 2016, 208–212; *Säcker/Riexecker/Oetker/Limperg,* Münchner Kommentar zum Bürgerlichen Gesetzbuch, Band 1, 8. Aufl. 2018, München: C. H. Beck; *Säcker/Riexecker/Oetker/Limperg,* Münchner Kommentar zum Bürgerlichen Gesetzbuch, Band 3, 7. Aufl. 2016, München: C. H. Beck; *Säcker/Riexecker/Oetker/Limperg,* Münchner Kommentar zum Bürgerlichen Gesetzbuch, Band 6, 7. Aufl. 2017, Münchener: C. H. Beck; *Schäfer/Ott*, Lehrbuch der ökonomischen Analyse des Rechts, 5. Aufl. 2012, Berlin: Springer; *Schroeter*, Untersuchungspflicht und Vertretenmüssen des Händlers bei der Lieferung sachmangelhafter Ware, JZ 2010, 495–499; *Soergel* (Hrsg.), Kommentar zum Bürgerlichen Gesetzbuch, Band 2, 13. Aufl. 1999, Stuttgart: Kohlhammer; *Spindler*, Roboter, Automaten, künstliche Intelligenz, selbst-steuernde-KfZ: Braucht das Recht neue Haftungskategorien? – Eine kritische Analyse möglicher Haftungsgrundlagen für autonome Steuerungen, CR 2015, 766–776; *Staudinger* (Hrsg.), Kommentar zum Bürgerlichen Gesetzbuch, Berlin: Sellier/de Gruyter; *Weller*, Die Verantwortlichkeit des Händlers für Herstellerfehler, NJW 2012, 2312–2317; *Zech*, Daten als Wirtschaftsgut – Überlegungen zu einem „Recht des Datenerzeugers" – Gibt es für Anwenderdaten ein eigenes Vermögensrecht bzw. ein übertragbares Ausschließlichkeitsrecht? CR 2015, 137–146; *Zech*, Information als Schutzgegenstand, 2012, Tübingen: Mohr Siebeck.

* Dr. Gunnar Sachs, Maître en droit (Paris) ist Rechtsanwalt, Fachanwalt für Gewerblichen Rechtsschutz und Partner im Düsseldorfer Büro der weltweit vertretenen Anwaltssozietät Clifford Chance.

1 Um im digitalen Wettbewerb bestehen zu können, investieren Unternehmen immer häufiger in die Entwicklung neuer digitaler Produkte sowie in die Ablösung vormals analoger Produkte durch digitalisierte Abläufe und Strukturen. Da viele Marktteilnehmer nicht oder allenfalls nur unzureichend über das für die Einführung solcher neuen Produkte und Prozesse erforderliche Personal und Knowhow verfügen, werden digitale Expertise und Entwicklungen samt aller damit verbundenen Risiken häufig von außen zugekauft oder ganze Projekte an externe Anbieter vergeben. Im Wettlauf um die digitale Marktführerschaft in den einzelnen Wirtschaftsbereichen richten viele Unternehmen ihren Fokus dabei ausschließlich auf technische Neuentwicklungen und lassen außer Acht, dass ihre digitalen Angebote zugleich eine Vielzahl neuer Risiken und Verantwortungen mit sich bringen, deren Nichtbeachtung nicht allein die jeweils neuen Produkte und Prozesse, sondern sie selbst im Bestand gefährden kann.

2 Obschon der Digitalisierungstrend bereits seit geraumer Zeit das Wirtschaftsleben bestimmt, fehlt vielen Unternehmen der Blick für das große Ganze. Digitalisierungsstrategien werden oftmals nicht zentral gesteuert, geschweige denn die damit jeweils verbundenen wirtschaftlichen und rechtlichen Anforderungen unternehmensübergreifend in sinnvollen Prozessen abgebildet. Vielfach wissen nicht einmal alle mit Digitalisierungsfragen befassten Unternehmensbereiche voneinander. Dadurch werden nicht nur Chancen vergeben, sondern vor allem auch Risiken begründet. Manche Unternehmen verpassen so den Schutz digitaler Neuentwicklungen, öffnen Flanken für Cyber-Angriffe und Daten-Lecks, vernachlässigen das digitale Vertragsmanagement, versäumen die Beweissicherung in digitalen Prozessen, riskieren einen rechtwidrigen Umgang mit Daten und setzen sich dadurch erheblichen Haftungsrisiken aus.

3 Die Digitalisierung wird in der Industrie noch erheblich deutlichere Spuren hinterlassen als die Compliance- und Datenschutz-Entwicklungen in den letzten Jahren. Doch statt aus den Schwierigkeiten zu lernen, mit denen alle Unternehmen bei der Implementierung neuer Compliance- und datenschutzrechtlicher Prozesse zu kämpfen hatten und haben, ist bei der Umsetzung des Digitalisierungstrends ein ähnliches Chaos zu beobachten wie in den ersten Jahren der Compliance- und Datenschutzbewegungen. Erschwerend kommt hinzu, dass die mit der Digitalisierung typischerweise verbundenen Themenschwerpunkte – anders als im Compliance- und Datenschutzbereich – im Unternehmen häufig dezentralisiert von zahlreichen verschiedenen Funktionsträgern betreut werden.

A. Industrie 4.0

4 „Industrie 4.0" ist ein Begriff, der auf die Forschungsunion der Bundesregierung und ein gleichnamiges Projekt aus deren Hightech-Strategie aus dem Jahr 2006 zurückgeht. Danach soll die industrielle Produktion in Deutschland mit moderner Informations- und Kommunikationstechnik verzahnt werden. Technische Grundlage hierfür sollen intelligente und digital vernetzte, internetgestützte Systeme sein, die eine weitgehend selbstorganisierte Produktion und den direkten

Datenaustausch zwecks Kommunikation und Kooperation zwischen Menschen, Maschinen, Anlagen, Logistik und Produkten ermöglichen.

I. Ziele

5 Das zentrale Ziel der digitalen Transformation hin zur Industrie 4.0 besteht in der internetgestützten Vernetzung aller Marktteilnehmer sowie deren Produkte und Dienstleistungen über das sogenannte „Internet der Dinge" (*Internet of Things*, „IoT"). Das IoT bezeichnet ein Netzwerk verschiedenster physischer Objekte, die mittels eingebetteter Elektronik über das Internet miteinander verknüpft sind und untereinander kommunizieren. Dabei werden physische Abläufe und Dienstleistungen mit der digitalen Welt verbunden. Ein Beispiel sind etwa digitalisierte Warenwirtschaftssysteme, die sich weitgehend selbst verwalten und Wareneinund -ausgänge IT-gestützt steuern.

6 Wesentliche Voraussetzung für die digitale Transformation der Industrie ist damit ein möglichst schnelles und für große Datenvolumina ausgelegtes Internet. Auch wenn die deutsche Bundesregierung die Digitalisierung mit ihrer Werbekampagne „Industrie 4.0" vollmundig zur vierten industriellen Revolution erklärt hat, bleibt Deutschland beim Internetausbau im internationalen Vergleich weit zurück. Trotz der inzwischen weithin bekannten Marketinginitiative „Industrie 4.0" beläuft sich der Anteil der Glasfaserkabel bei den bis heute in Deutschland verlegten Breitbandverbindungen auf gerade einmal 3,2 Prozent.[1]

7 Auch die Europäische Union hat die digitale Transformation längst mit in ihre politische Agenda aufgenommen und arbeitet am Ausbau eines Digitalen Binnenmarktes (*Digital Single Market*, „DSM"). Der Digitale Binnenmarkt beschreibt einen Wirtschaftsraum zwischen den Mitgliedstaaten der Europäischen Union, welcher die Wettbewerbsfähigkeit der europäischen Wirtschaft im Digitalbereich stärken soll. Um dies zu erreichen, sollen europaweit ein besserer Zugang zu digitalen Waren und Dienstleistungen, bessere Rahmenbedingungen für digitale Netze und eine stärkere Digitalisierung der Wirtschaft geschaffen werden. Ein Bereich, in dem diese Entwicklungen bereits weiter vorangeschritten sind und der insoweit zumindest in Teilen als Vorbild dienen kann, ist der Energiesektor. Hier wird in Europa nicht nur die flächendeckende Einführung digitaler und mit dem Internet verbundener Energiezähler, sogenannter „Smart Meter", vorangetrieben. Vielmehr soll europaweit ein „Smart Grid", ein intelligentes Stromnetz, implementiert werden, welches Stromerzeuger, Speicher, elektrische Verbraucher und Netzbetriebsmitteln in Energieübertragungs- und -verteilungsnetzen der Elektrizitätsversorgung kommunikativ vernetzt und steuert, um so alle miteinander verbundenen Bestandteile noch besser zu überwachen und die Energieversorgung auf Basis eines effizienten und zuverlässigen Systembetriebs zu optimieren.

[1] https://de.statista.com/infografik/3553/anteil-von-glasfaseranschluessen-in-ausgewaehlten-laendern/ (26. 07. 2019).

II. Wesentliche Herausforderungen

8 Die Entwicklung und Markteinführung digitaler Angebote wirft eine Vielzahl rechtlicher und regulatorischer Fragen auf. Nachfolgend soll lediglich ein Überblick über einige wesentliche Herausforderungen gegeben werden.

9 Schwierigkeiten bereitet häufig bereits die rechtliche Einordnung neuer digitaler Produkte. Dies gilt insbesondere in regulierten Industrien wie etwa dem Gesundheitsbereich. So können beispielsweise für Gesundheitszwecke bestimmte digitale Therapiemodelle als Medizinprodukte einzuordnen sein und damit strengen gesundheitsrechtlichen Anforderungen unterfallen. Wie in der einschlägigen Gesetzesbegründung klargestellt wird, ist etwa Software ein Medizinprodukt, wenn sie spezifisch vom Hersteller für einen der in der europarechtlich harmonisierten Definition für Medizinprodukte genannten medizinischen Zwecke bestimmt ist. Dagegen ist Software für allgemeine Zwecke (wie z. B. reine Textverarbeitungsprogramme, Tabellenkalkulationen, Betriebssysteme *etc.*) kein Medizinprodukt, auch wenn sie im Zusammenhang mit der Gesundheitspflege genutzt wird. Die Frage, ob und ggf. wie ein bestimmtes digitales Therapiemodell als Medizinprodukt zu qualifizieren ist, hängt nach dem derzeit (noch) geltenden nationalen Recht daher etwa von folgenden Überlegungen ab: Ist das Produkt nach der Zweckbestimmung des Herstellers zur Erkennung, Verhütung, Überwachung, Behandlung oder Linderung von Krankheiten, zur Erkennung, Überwachung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen, zur Untersuchung, Ersetzung oder Veränderung des anatomischen Aufbaus oder eines physiologischen Vorgangs oder zur Empfängnisregelung zu dienen bestimmt? Wird seine bestimmungsgemäße Hauptwirkung nicht durch pharmakologisch oder immunologisch wirkende Mittel oder Metabolismus am oder im menschlichen Körper erreicht, sondern ihre Wirkungsweise allenfalls durch solche Mittel unterstützt? Und wird das digitale Produkt separat oder aber verbunden mit einem Medizinprodukt für dessen einwandfreies Funktionieren verwendet? Handelt es sich bei einem digitalen Therapiemodell mit medizinischer Zweckbestimmung tatsächlich um ein Medizinprodukt, darf es in Europa nicht ohne entsprechende CE-Zertifizierung in Verkehr gebracht werden.

10 Viele digitale Angebote sehen zudem die Verarbeitung personenbezogener Daten sowie eine anschließende Datenübermittlung an Dritte vor. Auf diese Vorgänge finden die strengen Vorschriften der unmittelbar in allen europäischen Mitgliedstaaten geltenden Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (sog. „Datenschutz-Grundverordnung", **„DS-GVO"**) Anwendung. Gesteigerte Anforderungen gelten dabei für besonders schutzwürdige personenbezogene Daten wie etwa Gesundheits-, genetische und biometrische Daten. Bei Gesundheitsdaten handelt es sich um personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person einschließlich der Erbringung von Gesundheitsdienstleistungen beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen (Art. 4 Nr. 15

DS-GVO). Genetische Daten sind demgegenüber personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden (Art. 4 Nr. 13 DS-GVO). Biometrische Daten schließlich meint mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten (Art. 4 Nr. 14 DS-GVO).[2]

11 Die digitale Transformation hin zur Industrie 4.0 geht regelmäßig mit der Erhebung, Speicherung und Verarbeitung großer Datenbestände, sogenannter „Big Data", in unterschiedlichen Formen, Größen und Geschwindigkeiten einher. Der Begriff „Big Data" meint polystrukturierte Daten, welche gesammelt, aufbereitet und mit modernen analytischen Verfahren systematisch ausgewertet werden. Ihre Erhebung, Speicherung und Verarbeitung kann neben den bereits genannten datenschutzrechtlichen Herausforderungen auch zu Datenmonopolen und den damit verbundenen kartellrechtlichen Risiken führen. Zugleich erlegt sie den jeweils Verantwortlichen die Verpflichtung auf, für die Sicherheit der jeweiligen Datenbestände und der zu deren Erhebung, Speicherung und Verarbeitung genutzten IT-Systeme zu sorgen (sog. „Cyber Security"). „Cyber Security" befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der klassischen IT-Sicherheit wird dabei auf den gesamten „Cyber"-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und Informationen mit ein.

12 Da Anbieter digitaler Produkte für deren Entwicklung und Pflege sowie für damit verbundene Datenauswertungen häufig auch immer wieder auf dieselben Dritten zurückgreifen, begründen sie dadurch zugleich die Gefahr scheinselbständiger Beschäftigung oder illegaler Arbeitnehmerüberlassung samt aller damit verbundenen rechtlichen und finanziellen Risiken – wie etwa der Fiktion unbefristeter Arbeitsverhältnisse mit den betroffenen Dritten, Nachzahlungen an Sozialversicherungsbeiträgen, Steuerberichtigungen, Bußgelder und Strafen. Zugleich ergeben sich insoweit regelmäßig Probleme bei der Abgrenzung und dem Schutz von Knowhow sowie bei Fragen der Produkthaftung für die jeweiligen digitalen Angebote. Dies gilt umso mehr, als viele digitale Produkte auf sogenannter „Künstlicher Intelligenz" beruhen und damit die Einspeisung von Drittwissen erfordern. In diesem Zusammenhang stellt sich regelmäßig die Frage nach dem „Eigentum" und sonstigen Vermögensrechten an Knowhow und Daten. Dabei sind Daten eigentumsrechtlich weitgehend unreguliert.[3] Handelt es sich um personenbezogene Daten, unterliegt jeder Umgang mit ihnen freilich dem Daten-

[2] Vgl. auch § 2.1.
[3] Vgl. auch § 4.1 ff.

schutzrecht. Bereichsspezifische Regelungen wie der Geschäftsgeheimnisschutz oder der Datenbankschutz können sowohl für personenbezogene Daten als auch für nicht personenbezogene Daten zur Anwendung gelangen. V.a. bedarf es passender Vertragsgestaltungen. Und auch die Sicherung von Daten und IT-Systemen wird mit der digitalen Transformation an Bedeutung gewinnen. In diesem Zusammenhang wird unter anderem das am 29. 06. 2017 verkündete Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (sog. "NIS-Richtlinie") zu beachten sein.

B. Haftungsrisiken

13 Die Folgen fehlerhafter Daten können in der Industrie 4.0 vor dem einleitend dargelegten Hintergrund vielfältig sein. Bei der Begründung eines vertraglichen oder der Entstehung eines außervertraglichen Haftungsanspruchs ergeben sich in der Praxis häufig Schwierigkeiten hinsichtlich der Schadenskausalität, der Zurechnung sowie des Vertretenmüssens. Dabei ist gerade in vernetzten Liefer- und Wertschöpfungsketten aufgrund der inhärenten Komplexität kaum überschaubar, wie sich ein einzelner Datenfehler und die darauf beruhende Schadensfolge auswirken können. Dies gilt umso mehr, als selbst bei nachträglichen Analysen Datenfehler und darauf beruhende Schadensfolgen häufig nicht mehr im Detail reproduzierbar sind. Diese Umstände können die Darlegung und den Beweis haftungsbegründender Tatsachen erheblich erschweren.

I. Vertragliche Gewährleistung

14 Datenfehler können grundsätzlich auf zwei Ebenen, nämlich bei der Datenerzeugung sowie bei der Datennutzung, entstehen (vgl. zur vertraglichen Typisierung Kapitel 5.2). Daten werden dabei typischerweise auf Grundlage von Kaufverträgen veräußert oder auf Nachfrage programmiert oder verarbeitet. Die insoweit maßgebliche vertragliche Gewährleistung sieht sowohl verschuldensunabhängige Mängelrechte (Nacherfüllung, Minderung, Rücktritt) als auch verschuldensabhängige Ersatzansprüche (Schadensersatz, Ersatz vergeblicher Aufwendungen) vor, die ein Vertretenmüssen im konkreten Fall voraussetzen. Datenkäufer oder -besteller haben nach § 433 Abs. 1 S. 2 BGB oder § 633 Abs. 1 BGB Anspruch auf einen sach- und rechtsmangelfreien Kaufgegenstand oder ein sach- und rechtsmangelfreies Werk. Daneben kann auf Daten, die lediglich auf Zeit überlassen werden (etwa im Bereich des „Cloud Computing“), auch das mietrechtliche Gewährleistungsrecht Anwendung finden.[4] Voraussetzung aller vertraglichen Gewährleistungsrechte ist das Vorliegen eines Schuldverhältnisses.

[4] Grundsätzlich hierzu: BGH, Urt. v. 15. 11. 2006 – XII ZR 120/04.

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.

9 783503 187829 € (D) 134,–

www.ESV.info