sensspielraum hinsichtlich des Umfangs zu implementierender IT-Sicherheitsmassnahmen zu, während das „Ob“ zumeist nicht dem „Business Judgment“ unterliegen dürfte.

1.3 Vertragsrechtliche Nebenpflichten

Selbst wenn Unternehmen Vertragsbeziehungen eingehen, deren jeweiliger Gegenstand keinen direkten Bezug zu IT-Sicherheit aufweist, können die Parteien im Rahmen der Erfüllung ihrer vertraglichen Nebenpflichten dazu gezwungen sein, IT-Sicherheitsmassnahmen vorzuhalten. Die Verpflichtung zur Rücksichtnahme auf die Rechte, Rechtsgüter und Interessen der anderen Vertragspartei kann die Einhaltung einschlägiger gesetzlicher IT-Sicherheitspflichten auch zu einer vertraglichen Pflicht machen, „da den Vertragspartnern durch Zwischenfälle materielle oder immaterielle Schäden entstehen können“ (Voigt, 2018, S. 42). Vertragliche Nebenpflichten zur IT-Sicherheit sind umso bedeutsamer, je abhängiger eine Vertragspartei von den Leistungen und der Wirksamkeit dieser IT-Sicherheit des anderen Vertragspartners ist. Die entsprechenden risikobasierten Massnahmen sind jeweils für den konkreten Einzelfall zu bestimmen (Voigt, 2018, S. 42).

1.4 IT-Sicherheit „by design“

Aufgrund der Vernetzung von Zuliefererkomponenten, Herstellerprodukten sowie unternehmensinternen IT-Systemen werden die vernetzten Objekte selbst zu Quellen für IT-Sicherheitsrisiken (Rockstroh & Kunkel, 2017, S. 77). Von vernetzten Produkten ausgehende Sicherheitsrisiken bedrohen nicht nur Vermögenssphären, in welchen sich betreffenden Produkte letztendlich befinden, sondern alle hiermit sphärenübergreifenden vernetzten Systeme gleichermassen (Bundesamt für Sicherheit in der Informationstechnik, 2013, S. 10; Schlinkert, 2017, S. 222). Daher liegt auch die Vorhaltung produktbezogener IT-Sicherheitsmassnahmen im Interesse aller Wertschöpfungsakteure und Verbraucher.

Hersteller bzw. Verkäufer von IT-Produkten haften für IT-Schwachstellen zunächst regelmässig nach dem allgemeinen kaufrechtlichen Gewährleistungsrecht (Rockstroh & Kunkel, 2017, S. 77). Ein Produkt ist aus kaufrechtlicher Sicht frei von Sachmängeln, wenn es die zwischen den Vertragsparteien vereinbarte Beschaffenheit aufweist oder sich nicht für die gewöhnliche Verwendung eignet.[5] Aus diesem Grund sollten Hersteller und Verkäufer vernetzter Produkte die IT-sicherheitsrelevanten Eigenschaften möglichst umfassend und präzise beschreiben (Rockstroh & Kunkel, 2017, S. 77). Aus delikts-[6] und produkthaftungsrechtlicher Sicht können sich Herstellerpflichten u. a. aus technischen Standards wie IEC 62443 sowie aus den berechtigten Erwartungen der Kunden an die IT-Sicherheit des jeweiligen Produkts ergeben. Es ist dabei stets zu berücksichtigen, dass Software nicht fehlerfrei programmiert werden kann, sich die Bedrohungslagen immer schneller verändern und dass das erforderliche Mass an IT-Sicherheit nur durch Zusammenwirken aller Beteiligten erreicht werden kann (Rockstroh & Kunkel, 2017, S. 77).

[5] für Deutschland: § 434 BGB; für Österreich: § 922 ABGB; für die Schweiz: Art. 197 OR
[6] insbesondere Produzentenhaftung in Deutschland

Cyber-Physische Systeme

Der Begriff des Cyber-Physischen Systems (CPS) beschreibt ein Phänomen der digitalen Vernetzung und Automatisierung. Ein CPS besteht aus einer Vielzahl von Endgeräten, die in ein einheitliches, oft unternehmensübergreifendes Netzwerk integriert sind, in welchem sie miteinander kommunizieren und angesteuert werden können (Bundesministerium für Bildung und Forschung, 2015, S. 6). Ein typisches CPS ist beispielsweise eine digital integrierte, industrielle Wertschöpfungskette, deren Bestelloberflächen, Industrieroboter, Smart-Lager, Logistikroboter und sogar Endprodukte allesamt miteinander Daten austauschen und zentral angesteuert werden können. Wichtiges Merkmal eines CPS ist seine Fähigkeit, koordiniert und ohne menschliches Zutun auf Veränderungen in seiner Umwelt zu reagieren (Bruch, 2015, S. 87). So kann das beschriebene System bei einem Auftragseingang selbstständig Produktionsprozesse anstossen, die notwendigen Bauteile bestellen und Lagerraum freiräumen.

In der Praxis bieten diese Systeme potenziell beachtliche Effizienzvorteile. Sie verursachen aber technische Herausforderungen bei ihrer Implementierung und werfen eine Reihe von Rechtsfragen auf. Da sich diese Fragen vor allem mit der Haftung für eventuelle Fehler des Systems befassen, sind sie nicht nur für Nutzer von CPS relevant, sondern auch für deren Kunden und Geschäftspartner.

1. Vertragsrechtliche Implementierung eines CPS

Die Komplexität eines CPS spiegelt sich in den für eine Implementierung notwendigen vertraglichen Strukturen wider. Im Mittelpunkt steht das Verhältnis zwischen dem Betreiber und dem Hersteller bzw. Provider der CPS-Endgeräte. Da der Provider, neben der reinen Überlassung der Endgeräte, regelmässig auch eine Reihe von internetbasierten Diensten rund um deren Steuerung und Vernetzung erbringt, lässt sich das Betreiber-Provider-Verhältnis meist nur als typengemischter Vertrag zusammenfassen. Dieser kann wiederum, nach den Umständen des Einzelfalls, kauf-, miet-, dienst-, oder werkvertragliche Elemente enthalten (Heuer-James, Chibanguza & Stücker, 2018, S. 2823; Horner & Kaulartz, 2016, S. 24). Wird die Konnektivität der Endgeräte nicht durch die IT-Infrastruktur des Betreibers gewährleistet, so ist es regelmässig notwendig, hierzu zusätzlich einen Mobilfunkanbieter einzuschalten, welcher im Rahmen eines Dienstvertrages Datenvolumen zur Verfügung stellt (Langer, 2016, S. 29).

2. Zurechnung von Systemverhalten

Die Frage der Zurechnung des Verhaltens eines CPS zu einer Vertragspartei ist von grosser Bedeutung für die Praxis, jedoch rechtlich noch in weiten Teilen unklar. Grund hierfür ist die vermeintliche Autonomie eines CPS. Dieses besitzt freilich keinen eigenen Handlungswillen, vielmehr reagiert es auf Basis von Verknüpfungen und Algorithmen auf seine Umwelt. Dieser Entscheidungsfindungsprozess wird durch eine Vielzahl von Faktoren beeinflusst – hierzu zählen insbesondere die zur Steuerung verwendete Software,

die Struktur der Vernetzung sowie die konkret von den verschiedenen Endgeräten erhobenen und eingespeisten Daten (Horner & Kaulartz, 2016, S. 24). Von besonderer Bedeutung ist dabei, dass an einem CPS beteiligte Parteien möglicherweise einen massgeblichen Einfluss auf das Verhalten von nicht in ihrem Besitz stehenden Endgeräten ausüben können (Pieper, 2016, S. 189). Durch die Komplexität des CPS wird die Nachvollziehbarkeit von Systemverhaltensweisen eingeschränkt. Die Schaffung des Rechtskonstrukts einer elektronischen Person zur Bewältigung dieses Problems ist nach herrschender Meinung aus systematischen und praktischen Gründen nicht überzeugend (Kluge & Müller, 2017, S. 31; Heuer-James, Chibanguza, & Stücker, 2018, S. 2818). Mangels einer universellen Lösung gilt es an dieser Stelle stattdessen, bestimmte Zurechnungstatbestände individuell zu untersuchen.

Im Falle eines Vertragsabschlusses durch ein autonomes System hat grundsätzlich der Betreiber des CPS für die Erfüllung dieses Vertrags einzustehen. Freilich mag nicht immer gewiss sein, ob eine Willenserklärung des Systems auch den Willen des Betreibers widerspiegelt, jedoch ist es erst der Betreiber, der durch Einsatz eines CPS ein solches Risiko schafft (ausführlicher hierzu: Heuer-James, Chibanguza & Stücker, 2018, S. 2822; Groß, 2018, S. 5). Zum Schutze der Rechtssicherheit im Geschäftsverkehr sollte dieser daher auch Verantwortung für die Erfüllung der vertraglichen Leistungspflichten tragen.

Verursacht ein CPS eine vertragliche Pflichtverletzung, z. B. eine Fehllieferung, so hat dessen Betreiber diese nicht von vornherein als sein eigenes Verschulden zu vertreten. Das CPS ist nicht als Erfüllungsgehilfe des Betreibers zu behandeln (Heuer-James, Chibanguza, & Stücker, 2018, S. 2829), vielmehr muss sich Letzterer nur seine eigene Einflussnahme auf das System zurechnen lassen. Dies ermöglicht eine Exkulpation im Rahmen der schuldrechtlichen Beweislastumkehr, sofern sich in der Praxis festzustellen lässt, welche Faktoren und Inputs für das Fehlverhalten des Systems massgeblich waren, welche nicht dem Betreiber zuzurechnen waren (Horner & Kaulartz, 2016, S. 24).

Handelt ein CPS schliesslich deliktisch, so bietet sich eine Haftungszurechnung über die Annahme von Verkehrssicherungspflichten an (Rempe, 2016, S. 18). Der Betreiber des CPS handelt demnach kausal deliktisch, wenn er es unterlässt, nach dem Herbeiführen einer Gefahrenlage durch Implementierung eines autonomen Systems, die notwendigen Massnahmen zum Schutze des Verkehrs zu treffen. Bei der Bestimmung des Verschuldens ist dann auf die subjektive Vorhersehbarkeit der Schädigung abzustellen (Rempe, 2016, S. 19). Jedoch ist auch dieser Ansatz in der Anwendung problematisch. Zum einen bedarf er einer klaren Risikoverteilung, d. h. einer Festlegung, welcher CPS-Teilnehmer für welchen Aspekt der übergeordneten „Gefahrenlage“ verantwortlich ist. Zum anderen besteht bislang kein fester Massstab für den Umfang der zur Verkehrssicherung notwendigen Massnahmen (Heuer-James, Chibanguza & Stücker, 2018, S. 2830).

3. Regulatorische Fragen

Die Konnektivität von CPS-Endgeräten wird in der Praxis regelmässig mithilfe von Mobilfunknetzen gewährleistet. In einem solchen Fall liegt in der Bereitstellung dieser Konnektivität ein Telekommunikationsdienst (TK-Dienst) im Sinne des Telekommunikationsgesetzes vor (Grünwald & Nüßing, 2015, S. 381). Erbringer dieses TK-Dienstes sind entweder der Mobilfunkanbieter selbst oder möglicherweise der Provider, sofern dieser Konnektivität von einem „Primäranbieter“ bezieht und dann an seine Nutzer weiterverkauft (Sassenberg & Kiparski, 2017, S. 18). TK-Dienste unterliegen einigen gesetzlichen Sonderregelungen, insbesondere bestimmten Kundenschutzvorschriften, dem Fernmeldegeheimnis, dem Kommunikationsdatenschutz sowie einer Haftungsbeschränkung bei fahrlässig verursachten Vermögensschäden (Grünwald & Nüßing, 2015, S. 381).

Ein CPS erhebt und verarbeitet regelmässig Daten, sowohl mit als auch ohne Personenbezug. Bei deren Implementierung und Nutzung ist daher stets die Gewährleistung des personen- wie auch unternehmensbezogenen Datenschutzes zu beachten, wie er im Kapitel „Daten mit Personenbezug“ dargestellt wird.

Cloud-Computing und digitale Plattformen

Die Durchdringung von Wirtschaft und Gesellschaft durch Informations- und Kommunikationstechnologie ist ein zentrales Kennzeichen der heutigen Zeit. Disruptive Innovationen und Geschäftsmodelle mit einer zunehmenden Serviceorientierung zwingen die meisten Branchen zur *Digitalisierung* (Hahn, 2016, S. 595). Lösungsansätze im Zuge dieser digitalen Transformation bieten digitale Plattformen, deren infrastruktureller Kern das Cloud-Computing ist. Im Folgenden werden daher zunächst die Formen des Cloud-Computing und seine typischen Rechtsfragen und dann das Themenfeld der digitalen Plattformen dargestellt.

1. Cloud-Computing

Unter Cloud-Computing wird ein Geschäftsmodell im Informationstechnologie-Sektor verstanden, bei dem der Cloud-Anbieter dem Cloud-Nutzer IT-Leistungen wie Speicherplatz und Anwendungsprogramme über das Internet zur Verfügung stellt (Böhm, Leimeister, Riedl, & Krcmar, 2009, S. 8). Diese IT-Leistungen werden in der sogenannten Cloud bereitgehalten, einem Verbund aus mehreren Servern, der vom Cloud-Nutzer „wie ein grosser Computer verwendet werden kann“ (Lehmann & Giedke, 2013, S. 609). Cloud-Computing kann anhand der drei Leistungsarten Software as a Service (SaaS), Platform as a Service (PaaS) und Infrastructure as a Service (IaaS) unterschieden werden. SaaS-Angebote erlauben den Zugriff auf Anwendungsprogramme, die auf der Infrastruktur des Cloud-Anbieters installiert sind. PaaS-Angebote ermöglichen dem Cloud-Nutzer den Zugriff auf Programmier- und Entwicklungsumgebungen zur Entwicklung und zum Betrieb von Software. Bei IaaS-Angeboten stellt der Cloud-Anbieter seiner Kundschaft eine virtualisierte Rechenzentrumsinfrastruktur (z. B. Server, Storage, Netzwerk) über das Internet zur Verfügung. Erhebungen von Eurostat und der Hochschule für Wirtschaft Zürich zeigen, dass die Nutzung von Cloud-Computing in Unternehmen zunimmt, mithin also immer mehr Unternehmen ihren Betrieb von E-Mail-, Office- oder Kommu-