Zerto

VERSION 01
JUNI 2017

Industrie 4.0, Digitalisierung und IoT – Fokus: „E-Finance“

Industrie 4.0, Digitalisierung und IoT vor dem Hintergrund der europäischen rechtlichen Rahmenbedingungen - und ihre Konsequenzen für den Einsatz effektiver IT-Systeme im Bereich „E-Finance“

Von Rechtsanwalt und Fachanwalt Für IT-Recht
Dr. Jens Bücking*

* Der Autor ist Rechtsanwalt und Fachanwalt für IT-Recht. Er ist darüber hinaus Gründungspartner der Rechtsanwaltskanzlei e/s/b Rechtsanwälte (http://www.kanzlei.de) sowie zugleich Fachbuchautor im IT-Recht und Lehrbeauftragter an der Hochschule für Technik in Stuttgart und als associate Professor an der E.N.U. in Kerkrade, Niederlande tätig.

Inhalt

1 EINFÜHRUNG UND PROBLEMAUFRISS

Die Schlagworte Internet of Things (IoT) und Industrie 4.0 (I4.0) stehen - vereinfacht dargestellt - für neue, innovative Geschäftsmodelle, die möglich werden durch rasante technische Entwicklungen in den Bereichen Vernetzung von Endgeräten, autonome „Maschinenentscheidungen“ durch Systeme der künstlichen Intelligenz (KI) und Auswertbarkeit großer Datenmengen durch hochleistungsfähige Computersysteme (Big Data/HPC). Für viele der hieraus entstandenen Geschäftsfelder (wie etwa intelligente Produktionsprozesse und robotergesteuerte Analyse- und Beratungsverfahren) sind die auf die analoge Welt zugeschnittenen rechtlichen Rahmenbedingungen nicht ohne Weiteres passend. Neue, dem digitalen Zeitalter gerecht werdende spezifische Gesetze stecken jedoch entweder noch in den Kinderschuhen oder befinden sich womöglich sogar erst im „vorgeburtlichen“ Stadium strategischer Neuausrichtungen in der Politik. Allerdings treibt die EU-Kommission den grenzüberschreitenden Austausch von Waren und Dienstleistungen durch digitale Produktionsprozesse und Dienstleistungen mit hoher Priorität voran. Sie ist im Rahmen der EU-Wachstumsstrategie „Europa 2020“ bestrebt, eine Innovationsunion zu schaffen, die zu einer (weiteren) Defragmentierung und zunehmenden Harmonisierung der digitalen Märkte führen und damit als Motor für die weitere Entfaltung von Industrie 4.0 und IoT wirken soll. Aus diesem Grunde sind die Themen Innovation und Cybersicherheit, da sich gegenseitig bedingend, auf der Agenda der EU-Kommission weit oben angesiedelt.

2 BEGRENZTHEIT DES GELTENDEN RECHTS

Derzeit jedoch besteht noch die Situation, dass beispielsweise um Wesen und Reichweite von Computererklärungen gestritten wird, das Bedürfnis an einem „echten Eigentum“ an Daten (als eine der wichtigsten Ressourcen in der Welt von morgen) und deren globaler Verfügbarkeit nicht befriedigend gelöst werden kann, und dass gerade auch in der Verteilung von Verantwortungsbereichen in der „Smart Production Chain“ durch Gesetzeslücken noch zahlreiche Haftungsfallen versteckt sind, die es zwischen den jeweiligen Geschäftsprozessbeteiligten durch detaillierte Vertragsregelungen zu schließen gilt.

3 MASCHINELLE VERTRÄGE

Mit dem Vertragsrecht beginnen im digitalen Rechtszeitalter aber bereits die Probleme. Es stellt sich die Frage, welchen beteiligten Parteien an einem Geschäftsprozess die in diesem Prozess ausgelösten „Computererklärungen“ jeweils zugerechnet werden. Hier spricht vieles für eine Abgrenzung nach Risikosphären: Ein Vertrag kommt durch zwei übereinstimmende Willenserklärungen - Angebot und Annahme - zustande. Wer die jeweils relevante Erklärung beherrschen konnte, dem wird sie auch (ggfls. haftungsrechtlich) zugerechnet. In Frage kommen hierfür der Programmierer bzw. Hersteller der Software, ferner derjenige, der den Algorithmus nutzt und nach bestimmten Kriterien eine entsprechende Erklärung auslöst (was nach den Geschehnissen der Jahre 2007 ff. für den Börsenhandel und in Folge dessen für die gesamte Weltwirtschaft bereits zu verheerenden Folgen geführt hat), und weitere in den Prozess eingebundene Interakteure. Andererseits müssen schlichte Maschinenerklärungen (als rein technische Übermittlungen) von eigenständig-autonomen Erklärungen (im Sinne der KI) abgegrenzt werden. Absender und Empfänger von Maschinenerklärungen wiederum treffen besondere Sorgfaltspflichten in Bezug auf die Überwachung und Dokumentation der „Erklärungsketten“.

.

4 DIGITALES „EIGENTUM“: DATEN UND DATENGENERIERTE ERZEUGNISSE

In I4.0-Prozessen kann Know-How und geistiges Eigentum (IP) sowohl eingesetzt wie auch erworben werden. Hier stellt sich neben der Frage, wem dieses neue IP gehört insbesondere das Problem, wie sich eingebrachtes IP wirkungsvoll schützen lässt:

4.1 Entstehung und Erwerb von Rechten des geistigen Eigentums (IP) in der IT

Die Schutzrechte des IP (wie der Patent- und Designschutz und das Urheberrecht) knüpfen an das Schöpferprinzip an. Bei der individuellen Produktion auf Kundenwunsch, bei dem die Konzeption und Produktion einem von Kunden initiierten, programmatisch dann aber autonom ablaufenden Prozess folgt, stellt sich die Frage, wem - *gegebenenfalls* - das Schutzrecht an einer solchen Anfertigung zuzuschreiben ist. „*Gegebenenfalls*“ deshalb, weil bei der Vernetzung und Lernfähigkeit von intelligenten Systemen häufig im Ergebnis überhaupt kein Schutzrecht begründet werden kann, da eine eigenpersönlich-geistige Schöpfung stets nur durch eine natürliche Person erbracht werden kann. Computergenerierte Arbeitsergebnisse genießen demgegenüber keine Schutzfähigkeit, wenn sie ohne jedwede menschliche Beteiligung produziert werden. Dies ist etwa der Fall, wenn Computerprogramme neue Computerprogramme schaffen. Ebenso wird es sich bei I4.0-Produkten verhalten, wenn diese kraft ihrer Lernfähigkeit ihre Funktionsweise oder ihr Verhalten autonom (weiter-) entwickeln, mit anderen Produkten oder vernetzten Systemen interagieren und neue Ergebnisse generieren können. Denn wenn das Arbeitsergebnis nicht von einer natürlichen Person eindeutig vorbestimmt ist sondern ergebnisoffen, fehlt es an dem erforderlichen unmittelbaren Zusammenhang zwischen Ergebnis und schöpferischem Schaffensakt („Computer-generated Works“). Werden jedoch Algorithmen lediglich als technische Hilfsmittel eingesetzt, bleibt der schöpferische Prozess maßgeblich von einem natürlichen Urheber beherrscht und planend beeinflusst; in diesem Falle kommt eine Schutzfähigkeit folgerichtig in Betracht („Computer-aided Works“).

Wenn freilich durch arbeitsteilige - und unter Umständen vollständig autonome - Vorgänge im Bereich der Nutzung und Auswertung von Daten Arbeitsergebnisse entstehen, die sich - als Datenerzeugnisse - ihrerseits wirtschaftlich nutzen und verwerten lassen, stellt sich die Frage, wem diese Erzeugnisse (bzw. die etwaigen Rechte hieran) zustehen. Auch hierzu bedarf es vorab fixierter eindeutiger Vertragsregelungen, die - wie zuvor beschrieben - berücksichtigen müssen, dass rein maschinengenerierte Datenerzeugnisse weder dem herkömmlichen Eigentumsbegriff noch den klassischen Schutzrechtskategorien (wie Patent, urheberrechtliches Werk, Design etc.) zuordenbar sind. Es müssen folglich auf dem Vertragswege Bestimmungen zur Zuordnung vorhersehbarer oder zufälliger Nutzungs- und Verwertungsmöglichkeiten getroffen und neue Kategorien von eigentumsähnlichen Rechten geschaffen werden, solange der Gesetzgeber diese Lücken noch nicht geschlossen hat. Auf europäischer Ebene stellen die Regelungen zur Erweiterung des Know-How-Schutzes einen Schritt in diese Richtung dar (dazu unten …).

4.2 Zuordnung des „Dateneigentums“ im Produktivzyklus

Ein „echtes“, d.h. exklusives Eigentumsrecht an Daten gibt es nach vorherrschender Rechtsansicht (noch) nicht, wohl aber eigentumsähnliche Abwehrrechte gegen einen Zugriff auf Daten oder deren Verwendung durch Dritte, die sich insbesondere aus dem Urheberschutz und dem Know-How-Schutz ergeben. Solche Rechte enden aber dort, wo die Daten willentlich die Sphäre des Berechtigten verlassen haben oder aber von Dritten oder maschinell erzeugt wurden. Beim „Dateneigentum“ von maschinenautonom - beispielsweise durch „Smart Cars“ - generierten Daten (wie Mess- bzw. Sensordaten) handelt es sich um ein typisches I4.0-Problem, an dem sich die gelehrten Geister scheiden. In Betracht

kommen sowohl der Betreiber der Maschine als auch der Träger der Entwicklungs- und Vertriebslast, oder eben auch der Provider bestimmter technischer Zusatzeinrichtungen wie beispielsweise Fahrzeug-Apps.

Abermals macht dies eindeutige vertragliche Zuordnungen notwendig. Ohne solche sind nach der herrschenden „Investitionstheorie“ die Daten demjenigen zuzuordnen, der den wirtschaftlich-organisatorischen Aufwand für die Datenerzeugung trägt, den mithin die wesentliche Kostenlast trifft.

Ein weiterer Effekt maschinenautonomer Daten ist freilich, dass die aktuell zur Verfügung stehenden - und auch für die nähere Zukunft erwartbaren - Bandbreiten mit der Entwicklung autonomer Systeme nicht mehr werden Schritt halten können. Daher bedarf es eines sinnvollen Datenmanagements bereits „an der Quelle“ der Datengenerierung. Die Big Data aus den Testreihen werden demnach, um später im Produktiveinsatz (beispielsweise beim Autofahren) direkt verfügbar zu sein und in Steuerungsprozesse eingreifen zu können, zunächst auf Belastbarkeit ausgewertet und erst dann „on board“ als Steuerdaten zum Produktiveinsatz im „Gesamtsystem“ - im Beispiel der „Smart Cars“ bestehend aus Mensch, Maschine und weiteren Steuerungs- und Messeinrichtungen wie Navigation, Kommunikation etc. - gebracht. Die Datenflut durch die Erfassung von Fahrzeugdaten im laufenden Betrieb entfällt.

Auch ohne diese sinnvollen Maßnahmen des Datenmanagements wird der Bedarf an Speicherkapazitäten und IT-Sicherheitslösungen freilich dennoch exponentiell steigen. Dies gilt insbesondere bei vernetzten Einheiten im IoT, die aufgrund ihrer Komplexität eine Vielzahl von Daten erfassen und auswerten müssen wie Roboter, Höchstleistungselektronik und Automotive.

4.3 Kein Schutz des IP ohne Schutz der IT

Die EU hat im Bereich des Schutzes von IP Lücken festgestellt, wenn etwa betriebswichtige Informationen wie Konstruktionspläne, Kundenlisten oder kaufmännisches Wissen plagiiert werden. Solches IP ist grundsätzlich nicht den klassischen Schutzrechten (wie beispielsweise dem Patent- und Designschutz und dem Urheberrecht) zugänglich. Die Strategie der EU ist daher, eine Innovationsunion zu schaffen mit einem verbesserten, einheitlichen Schutz auch von „bloßem“ Know-How. Dieser erweiterte IP-Schutz soll allerdings erst dann eingreifen, wenn „angemessene“ Geheimhaltungsmaßnahmen angewendet (und vertragsrechtlich abgesichert) werden, die objektiv geeignet und den Umständen adäquat sind, um das Geheimnis zu schützen. Ein Blick auf vergleichbare US-Anforderungen zeigt, dass es hierbei unter anderem um physische Zugangsbeschränkungen und deren Absicherung durch effiziente, zeitgemäße IT-Maßnahmen geht. Geprüft wurde insbesondere, ob Firewalls, Sicherheitssoftware und weitere IT-Sicherheitsmechanismen wie Backup und Archivierung und ein „Incident Management“ (inkl. Desaster Recovery / Business Continuity-Plänen etc.) implementiert worden waren. Ohne derlei Maßnahmen zum Geheimhaltungsschutz wäre mithin wichtiges IP - wie insbesondere auch die Produktionsdaten in I4.0-Prozessen - nach aktueller Rechtslage nicht bestimmten Inhabern zugewiesen oder sonst geschützt. Es sind konkrete technische Maßnahmen erforderlich, um einen solchen Schutz zu bewirken.

5 HAFTUNG IN DER „SMART PRODUCTION“ UND „PRODUCT-LIFECYCLE-MANAGEMENT“

In der I4.0-Produktionskette sind erhebliche Gefahren dadurch eröffnet, dass „smart“ oder „customized“ hergestellte Produkte in den Wirtschaftskreislauf gelangen, bei denen es zuvor zu Fehlern im Fertigungsprozess kam, die sich sodann - z.B. als Produktsicherheitsrisiken - in der Produktnutzung fortsetzen.

5.1 Zivilrechtliche (Schadens-) Haftung

Schon die Suche nach dem Haftungsschuldner ist nicht trivial: Es muss entlang der einzelnen Prozessschritte eine Abgrenzung nach Verantwortlichkeitsbereichen vorgenommen werden, was bedingt, dass Gefahrenpotenziale zuvor erkannt und zwischen allen Beteiligten geregelt werden, einschließlich der virulenten Gefahr externer Eingriffe in den Fertigungsprozess durch Cyber-Attacken. Wenn ein Ursachenpfad nicht rückführbar ist auf einen isolierbaren Prozessschritt-Beteiligten, dürfte gelten, dass im Zweifel sämtliche an der Fertigung des Erzeugnisses Beteiligten in

Gesamtschuldnerschaft gegenüber dem Geschädigten haften und sich entsprechend im Wege der Beweislastumkehr entlasten müssen.

Das Haftungspotenzial ist hoch. Softwarefehler, die sich beispielsweise in Computerabstürzen oder Fehlfunktionen äußern, führen häufig zu Sekundärschäden wie Betriebsausfall und entgangenem Gewinn. Aber auch unmittelbare Schäden an Leib, Gesundheit und Eigentum sind denkbar, wenn sich programmatische Fehlfunktionen in Konstruktionsfehlern äußern, die zu Unfällen mit Sach- und Personenschäden führen. Wer hinsichtlich solcher smarter Produkte, auf die kundenseitig hinsichtlich der spezifischen Anforderungen Einfluss genommen werden kann, im Rechtsverkehr als Hersteller auftritt, bleibt trotz der Verlagerung der Fertigungsschritte auf den Kunden zur Verhütung von Produktgefahren verpflichtet.

Die juristische Fachwelt ist sich daher weitgehend dahin einig, dass ein „Produktgedächtnis“ bei I4.0-Prozessen unverzichtbar sein wird, um einerseits das Risiko für die Erzeugerkette beherrschbar zu machen und auf der anderen Seite die Schutzinteressen derjenigen, die mit den Erzeugnissen bestimmungsgemäß in Berührung kommen, abzusichern. Die Mitprotokollierung des gesamten Lebenszyklus eines (auch: Beratungs- oder Finanz-) Produkts - von der Entwicklung über die Fertigung und den Produktiveinsatz bis zur „Stilllegung“ - setzt wiederum HPC und Big Data-Verfahren voraus. Anhand der Datenanalyse kann dann festgestellt werden, ob bestimmte Vorfälle auf einem Produktfehler - und gegebenenfalls abgestuft nach Verantwortungsbereichen rückführbar auf einen Verantwortlichen für einen Zwischenfertigungsprozess - oder auf einem Anwenderfehler beruhen. Umgekehrt können sich Produzent, Hersteller und Vertrieb auf diesem Wege gegebenenfalls entlasten von der - eventuell auch *persönlichen* (vgl. dazu die Strafverfahren der US-Justiz im Abgasskandal) - Produkthaftung.

Es handelt sich hierbei um Sorgfaltspflichten, die dem Bereich der physischen Konstruktion und Fabrikation nachgelagert sind und die - als digitale Form der allgemeinen Produktbeobachtungspflicht - beinhalten, dass die softwaregesteuerten Geräte und Anwendungen gerade auch in der Kombination mit anderen interaktiven Systemen überwacht und auftretende Fehlfunktionen unverzüglich behoben werden bzw. anderenfalls das Produkt - gegebenenfalls durch Fernzugriff - aus dem Produktivbetrieb genommen wird. Im Schadensfall müssen die wesentlichen Vorgänge rekonstruierbar sein. Demzufolge müssen aktive Fehlermeldungen automatisch an den Hersteller rückgemeldet werden.

Ein solches „Product-Lifecycle-Management“ stellt zudem ein geeignetes Instrument dar, Schäden an Leib, Leben und bedeutenden Vermögensgütern von vornherein zu vermeiden. Es zielt auf die Integration sämtlicher Informationen, die im Verlauf des Lebenszyklus eines Produktes anfallen. Hierbei halten die IT-Systeme die relevanten Produktdaten wie Einzelteile, Chargen und Ereignisprotokolle fest; anhand der auf den jeweiligen Tag gespeicherten Informationen ist jedes einzelne Produkt oder jede Charge eindeutig nachvollziehbar, einschließlich der Nachverfolgung von bestimmten besonderen Vorkommnissen mit dem Produkt.

Gerade bei intelligenten Fertigungsprozessen erscheint das „Product-Lifecycle-Management“ mithin alternativlos. Es ermöglicht, Fabrikationsfehler und Bedrohungen der Produktsicherheit durch externe Angriffe auf den Produktionsprozess zu verhindern bzw. produktgenau eingrenzen (und gegebenenfalls den Haftungsentlastungsbeweis erbringen) zu können. Gefordert wird hierbei nicht weniger als ein intensives Monitoring des Produktes im täglichen Einsatz „von der Wiege bis zum Grabe“. IT-Sicherheit und Produktsicherheit sind daher vom Hersteller zu einem einheitlichen Schutzkonzept zu entwickeln (z.B. Branchen wie Industrie, Automotive).

5.2 Fokus „E-Finance“

Auch im Finanzsektor schreitet die Digitalisierung rasant voran. Digitalisierungsprozesse sind den Finanzdienstleistungsaufsichtsbehörden zufolge von den Fachbereichen IT, Risikomanagement, Recht und Innenrevision zu begleiten, im Falle des Outsourcings wird eine eigenständige Abteilung für das Outsourcing-Management empfohlen. Werden unternehmenskritische Prozesse wie ERP, RMS / IKS digitalisiert, neu implementiert oder ausgelagert, ist zudem zwingend das Unternehmensmanagement (Vorstand / Geschäftsführung) in diesen Prozess mit einzubinden.

Dem Datenschutz und der IT-Sicherheit kommt im Finanzwesen besondere Bedeutung zu. Durch die Vernetzung und das Zusammenführen von Big Data können Personenprofile erstellt und Zahlungsgewohnheiten analysiert werden. Die

Europäische Datenschutz-Grundverordnung (EU-DSGV) soll dieser Tendenz, die insbesondere bei „Fintechs“ - Zahlungsdiensteanbietern ohne eigene Banklizenz - zu beobachten ist, Einhalt gebieten.

Der Banken- und Finanzdienstleistungssektor ist in hohem Maße reguliert. So definiert bspw. die E-Geld-Richtlinie der EU elektronisches Geld und regelt den Umgang damit. Die Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSi) schreiben vor, welche Sicherheitsmechanismen implementiert sein müssen, bevor über Websites oder Apps Geldtransaktionen initiiert werden dürfen. Dahinter stehen die europäischen Leitlinien zur Sicherheit von Internetzahlungen (EBA-Leitlinien). Ebenfalls auf europäischer Ebene kommen die Zahlungsdienstrichtlinien PSD II und MiFID II hinzu. MiFID II erweitert die wechselseitigen Informationspflichten von Kunden und Anbietern von Finanzprodukten und Beratungsdienstleistungen, PSD II ordnet unter anderem die Zulassungspflicht von Unternehmen neu, die im Zahlungsverkehr aktiv sind, zwingt Banken ihre Systeme für externe Zahlungsdienstleister zu öffnen und fordert die technische Möglichkeit von Echtzeitzahlungen.

Für Cloud-Lösungen existieren Anforderungskataloge, die Finanzinstitute zu befolgen haben und die weit über die allgemeinen Vorschriften für Industrie und Handel aus dem Bereich IT-Sicherheit hinausgehen. Da aber Cloud auch eine der technologischen Grundlagen ist, um neue Geschäftsmodelle in der Finanzindustrie zu schaffen oder bestehende zu adaptieren sowie Effizienz- und Einsparpotenziale zu nutzen, ist mit noch weiter zunehmender Regulierung, Berichtswesen, Kontrolle und entsprechenden IT-Anforderungen seitens des EU- Gesetzgebers zu rechnen. Auf der anderen Seite werden die Banken damit technologisch in die Lage versetzt, auf das Angebot junger Wettbewerber wie insbesondere Direktbanken und Fintechs adäquat zu reagieren.

Die dazugehörigen IT-Prozesse zur Gewährleistung und Überwachung der Compliance sind naturgemäß besonders anfällig für Cyberattacken. Gerade in diesem Sektor bedarf es daher besonders fortschrittlicher und gehärteter Systeme der IT-Sicherheit. EU-weit existieren entsprechende Mindestanforderungskataloge für das Risikomanagement im Bankenbereich und Sicherheitsanforderungen für die Finanzindustrie als Betreiber sog. „kritischer“ bzw. „essentieller“ Infrastrukturen. Es besteht die Verpflichtung zu einem strengen Berichtswesen und zu einer engen Abstimmung und Kooperation mit den staatlichen Aufsichts- und Datensicherheitsbehörden (vgl. hierzu nochmals ZERTO-Whitepaper „Das neue IT-Sicherheitsgesetz: Erweiterte Rechtspflichten und potenzielle Haftungsfallen des modernen IT-Sicherheitsmanagements“).

Ein Outsourcing ist an strenge Vorgaben geknüpft. Die Angemessenheit des outsourcing-spezifischen Risikomanagements von Banken wird durch die jeweils zuständigen nationalen Behörden geprüft. Die Anforderungen an Risikoanalysen, Notfallkonzepte und Exit-Strategien sind entsprechend hoch. Stets werden bspw. auch die Einhaltung anerkannter Standards und die Eignung ggfls. vorhandener eigener Branchenstandards abgeprüft. Für die IT-Sicherheitsverfahren sind hier insbesondere zu nennen die Standards ISO 2700X (IT-Sicherheitsverfahren, Informationssicherheits-Managementsysteme, IT-Risikomanagement), der Prozessstandard ITIL und der IT-Governance-Standard Cobit als ursprüngliches Werkzeug für IT- Auditoren, das sich jedoch zwischenzeitlich zu einem Werkzeug für die Steuerung der IT aus Unternehmenssicht entwickelt hat und unter anderem auch als Modell zur Sicherstellung der Einhaltung gesetzlicher Anforderungen unter dem Stichwort Compliance eingesetzt wird), und zu guter Letzt selbstverständlich die anerkannten Standards, die aus den Vorgaben nationaler Behörden hervorgegangen sind, wie bspw. die BS- und BSI-Kataloge (BS-Standard 100-1 bis 100-3).

Gerade bei Banking 4.0 wird künftig ein sehr viel höherer Einfluss des Bankkunden auf den Prozess der Geldanlage oder die Inanspruchnahme von Krediten festzustellen sein. Mehr denn je werden die Kunden bestimmen, welches Finanzprodukt sie wie und wann nutzen wollen. Auf die spezifischen Kundenbedürfnisse zugeschnittene Finanzprodukte (autonom, „robo-advised“, „customized“) werden die Regel sein, eine Protokollierung der Beratungs-, Anpassungs- und Entscheidungsprozesse und die tatsächliche Nutzungspraxis des Finanzproduktes sollten auch hier aus Gründen der Rechtssicherheit und Haftungsvermeidung - nach Art eines „Produktgedächtnisses“ aus dem klassischen Produktionssektor verfügbar gehalten werden.

5.3 Strafrechtliche Haftung

Das fahrlässige in Verkehrbringen unsicherer Produkte kann über die geschilderten zivilrechtlichen Haftungsimplikationen zudem strafrechtliche Folgen haben. Dies ist insbesondere der Fall, wenn ein erforderlicher

Produktrückruf trotz erkennbar dringender Gebotenheit nicht vorgenommen wurde. In diesem Falle besteht eine persönliche Strafhaftung sämtlicher Organmitglieder des vertreibenden Unternehmens. Es haften also auch die Geschäftsführer bzw. Vorstände unter dem Gesichtspunkt der sog. „Garantenstellung“ für die Verletzung der Verpflichtung des in Verkehrsbringens eines nicht die Gesundheit gefährdenden Produktes. Eine Sorgfaltspflichtverletzung liegt immer dann vor, wenn trotz konkreten Gefahrenverdachts, etwa bei Häufung von Beschwerden und entsprechenden Rückmeldungen aus dem Handel oder bei Erkenntnissen der Produktbeobachtung die gebotenen Maßnahmen, wie insbesondere der Produktionsstopp und der Rückruf bereits ausgelieferter Produkte, nicht unverzüglich umgesetzt sondern unterlassen werden.

6 BEWEISFÜHRUNG MIT DATEN UND BEWEISSICHERHEIT

Ein großes Problem stellt die Prozessführung im I4.0-Zeitalter dar. Die digitalen Vorgänge sind den Erkenntnismöglichkeiten der beweisbelasteten Partei regelmäßig entzogen. Diese Partei kann sich daher nur auf Indizien und Vermutungen stützen. Im Bereich der Produkthaftung versucht die Rechtsprechung, dieser oftmals als unfair empfundenen Beweisnot über eine Umkehr der Beweislast zu begegnen. Belastende Daten befinden sich zudem in der Regel beim „Dateninhaber“, der als die in Anspruch genommene Partei indessen nicht gehalten ist, dem Gegner das für den gegnerischen Prozesserfolg erforderliche Material zu verschaffen. Auch diese Beweisnot wird zu Recht als unbillig angesehen. Das I4.0-Zeitalter verschärft diese Situation noch. Daher wird im Wege der „sekundären Darlegungslast“, die an die Kenntnisse und Beherrschbarkeit von Vorgängen anknüpft, dem Betreiber auferlegt, bei softwaregesteuerten Vorgängen notwendige interne Beweismittel wie z.B. Fehlerspeicher vorzuhalten. Bei unterbliebener Datenspeicherung kann der sekundär Darlegungsbelastete seiner entsprechenden Verpflichtung nicht genügen und hierdurch den Prozess allein aufgrund von Beweislastgesichtspunkten verlieren. Vor diesem Hintergrund wird der I4.0-Betreiber schon im ureigenen Interesse geeignete Sicherheits- und Vorhaltemechanismen in Bezug auf beweisrelevante Daten verfügbar halten, um sich einen entsprechenden Gegenbeweis zu ermöglichen und sich „exkulpieren“, d.h. von der Haftung entlasten zu können.

Das vorbeschriebene „Product-Lifecycle-Management“ dient mithin nicht zuletzt der Beweissicherheit. Dieser Aspekt hat infolge der Globalisierung der Wirtschaft bereits zunehmend an Bedeutung gewonnen durch die US-amerikanischen „E-Discovery“-Verfahren, mit dem sich auch europäische Konzerne vermehrt konfrontiert sehen. Um auf dieser Grundlage Prozessverluste zu vermeiden, muss gewährleistet sein, dass auf nach den Grundsätzen der Authentizität, Integrität, Vertraulichkeit und Sicherheit gespeicherte - und somit „beweissichere“ - Daten jederzeit zugegriffen werden kann. Allgemein lässt sich international eine Tendenz der Gerichte und Behörden ersehen, die Vorlage von Daten, auch wenn diese bereits vor langer Zeit in großen, gegebenenfalls auch externen und internationalen (Backup-) Speichern abgelegt wurden und entsprechend schwer verfügbar gemacht werden können, für ein laufendes Verfahren in einer beweissicherer Form zu verlangen, wobei diese Verpflichtung besteht unabhängig von gegebenenfalls höherer Gewalt oder etwaigem Fremdverschulden. Dies bedingt den Einsatz zeitgemäßer IT-Systeme, die starke Indizien für Beweissicherheit - und damit letztlich Rechtssicherheit - liefern.

7 GLOBALER DATENSCHUTZ UND CYBERSICHERHEITSKONZEPTE

Von der eingangs beschriebenen Rechtsunsicherheit in besonderem Maße betroffen sind Unternehmen und Organisationen, die große - und teilweise zudem sensible - Datenmengen wie beispielsweise Gesundheits- und Finanzdaten oder geschäftlich geheimhaltungsbedürftige Informationen für maschinenautonome Prozesse binnen kurzer Zeit und gegebenenfalls über Grenzen hinweg durch vernetzte hochpotente IT-Systeme speichern, aufbereiten und analysieren müssen. Diese Organisationen sind zudem Hauptangriffsziel für das „Cybercrime“, in dem international das größte Bedrohungspotenzial für innovative, digitale Geschäftsprozesse gesehen wird:

7.1 Datenschutz

Das internationale Datenschutzrecht mit seinen höchst unterschiedlichen Schutzstandards stellt hier ein erhebliches Hemmnis für das IoT und I4.0-Prozesse dar. Große Hoffung wird daher in die Europäische Datenschutz-

Grundverordnung (EU-DSGV) gesetzt, die zwar einen strengen, dafür aber verlässlichen und EU-weit gültigen Rechtsrahmen bringen wird. Ergänzend kann prinzipiell zwar auch auf zwischenstaatliche Vereinbarungen zum Datenaustausch (wie etwa im Falle der USA mit dem „Privacy Shield"), auf vorformulierte Auftragsdatenverarbeitungsverträge wie die EU-Standardvertragsklauseln oder auf konzernweit verbindliche, jedoch unter Genehmigungsvorbehalt stehenden Datenschutzrichtlinien (Binding Corporate Rules/BCR) zurückgegriffen werden. Die Rechtsprechung hat jedoch gerade in jüngerer Zeit aufgezeigt, dass solche Datenaustauschverträge mit einem erheblichen Risiko belastet sind. Und da auch das rechtliche Schicksal des „Privacy Shield" ungewiss (und bereits Gegenstand eines weiteren Verfahrens vor dem Europäischen Gerichtshof) ist, bedeutet das, dass die Rechtsunsicherheit bis zu einer juristisch belastbaren Nachfolgeregelung fortbesteht. „Privacy Shield" gewährt den Unternehmen de facto lediglich eine Schonfrist. Langfristige Planungen im Rahmen von Wertschöpfungsketten, denen die Verarbeitung von sensiblen Daten zugrunde liegt, erscheinen daher unter Risikogesichtspunkten kaum vertretbar, wenn sie ausschließlich auf die vorhandenen Erlaubnistatbestände für den globalen Datenaustausch gestützt werden.

Die Auswertung und Steuerung von mobilen Systemen erfolgt jedoch durch Datenaustausche in der Regel über Ländergrenzen hinweg. Dies gilt insbesondere bei verteilten Rechenzentren, Grid-Computing und HPC im Bereich Big Data. Big Data und Industrie 4.0-Prozesse müssen daher von vornherein datenschutzrechtlich bis ins Detail durchgeplant werden. Da in diesen Prozessen oft auch Daten mit Personenbezug ihrem ursprünglichen Zweckzusammenhang enthoben, umstrukturiert, kombiniert, analysiert und neuen Nutzungen zugeführt werden, versagen zwangsläufig die - stets nur zweckbezogen erteilten - Einwilligungserklärungen der Betroffenen. Auch hier können allenfalls entsprechende Ausgestaltungen der Vertragsbeziehungen eine Rechtfertigung solcher Datenverarbeitungen gewährleisten.

Oft wird dies jedoch nicht möglich sein. Es muss daher auch nach technischen Lösungen für die datenschutzrechtliche Problematik gesucht werden. So kann beispielsweise eine nach dem Stand der Technik implementierte Verschlüsselung der übermittelten und gespeicherten Daten zu einer (absoluten) Aufhebung jedweder Personenbeziehbarkeit führen, die Rückschlüsse auf eine bestimmte natürliche Person durch technische Rückumwandlungsprozesse oder Matching ausschließt. Erst wenn dies sichergestellt ist, kann von einer echten Anonymisierung ausgegangen werden, die wiederum eine erhebliche Bedeutung für das Geschäftsmodell von Big Data- und I4.0-Prozessen hat. Denn erst dann verlässt der Datenverarbeiter den Anwendungsbereich des Datenschutzrechts.

Dies allerdings erfordert wiederum einen Ausbau der technischen Infrastrukturen in Bezug auf die Verschlüsselung von Anwendungen, Kommunikationsprozessen und Datenbanken. In diesem Kontext beweist sich abermals die Unabdingbarkeit eines effizienten Datenmanagements nach dem Stand der Technik, einschließlich der jederzeitigen Sicherheit und Verfügbarkeit der Daten und deren Wiederherstellbarkeit im Desasterfall, idealerweise auf einen zeitnahen letzten unkompromittierten Wiederherstellungspunkt vor Eintritt des Desasters, um in laufende Produktivprozesse verlustfrei wieder einsteigen zu können (vgl. hierzu schon ZERTO-Whitepaper „Das neue IT-Sicherheitsgesetz: Erweiterte Rechtspflichten und potenzielle Haftungsfallen des modernen IT-Sicherheitsmanagements").

7.2 Cybersicherheit

Das Hauptbedrohungsszenario stellen jedoch nicht Lücken im Gesetz sondern in den unternehmerischen Cybersicherheitskonzepten (und deren technisch-organisatorischer Umsetzung) dar. Da Datenströme über Grenzen hinweg verlaufen und schon aus technischen Gründen (wie Verfügbarkeit, Skalierbarkeit und Bandbreite) auf verschiedene Rechner- und Speicherressourcen verteilt werden müssen, erhöhen sich mit den technischen auch die rechtlichen Anforderungen an die IT-Sicherheit in den Bereichen IoT, „Smart Production", Kollaboration und Big Data-Anwendungen und -Auswertungen. Wenn auch nur auf einem der verteilten Systeme ein Desaster eintritt, kann dies gleichbedeutend sein mit dem vollständigen Ausfall des Fertigungs-, Auswertungs- oder Forschungsvorhabens etc.

Durch die Vernetzung von Systemen und die Automatisierung von Produktionsprozessen erhöhen sich auch die Angriffs- und Bedrohungspotenziale in diesen Bereichen erheblich. Spezifische IT-Sicherheitsregelungen, die entsprechende Schutzvorkehrungen vorschreiben, sind indes in diversen Gesetzeswerken verteilt und betreffen in der Regel nur einzelne, besonders schützenswerte Teilbereiche der Wirtschaft bzw. bestimmte Kategorien von Daten. Staatenübergreifend ist hier exemplarisch die EU-Richtlinie zur Cybersicherheit (NIS-Richtlinie) zu nennen. Es lassen

sich jedoch einige gemeinsame technische und organisatorische Standards wie Verschlüsselung, konfigurationsfehlerfreie Internet- und spezielle Sicherheitssoftware (Firewall, Malware-Scanner, „Intrusion Detection“ und „Data Loss Prevention“), Backup- und „Information Security Management“-Systeme inkl. Maßnahmen zur Angriffsprävention und „Desaster Recovery / Business Continuity“-Management als Stand der Technik herausfiltern. (Auch hier darf wegen weiterer Details verwiesen werden auf das ZERTO-Whitepaper „Das neue IT-Sicherheitsgesetz: Erweiterte Rechtspflichten und potenzielle Haftungsfallen des modernen IT-Sicherheitsmanagements“).

8 FAZIT

Den innovativen Lösungen von global agierenden Unternehmen und deren IT-Systemen, die sich vernetzen um beispielsweise große Datenmengen auszuwerten oder Informationspools und Fertigungs- / Entwicklungsplattformen zu betreiben, stehen spiegelbildlich entsprechende Haftungsrisiken gegenüber, die abzumildern wiederum Aufgabe der Unternehmen selbst ist. Dies bedingt den Einsatz weiterer hoch technisierter Prozesse der automatischen Erfassung und Bewertung von Fehlern und Risiken im Produktions-, Vertriebs- und Produktivprozess.

Auch die anstehenden gesetzlichen Neuerungen (insbesondere auf EU-Ebene), aber auch die beschriebenen Schutzlücken in der derzeit noch analogen Gesetzeswelt, werden die Unternehmen für die ihnen obliegenden Bereiche der sicheren Datenhaltung und Verfügbarkeit in noch weit stärkerem Maße in die Pflicht nehmen als dies bisher schon der Fall war. Die Anforderungen an IT-Ressourcen und die dahinterstehende Sicherheitstechnologien werden dementsprechend erheblich zunehmen. Dies betrifft insbesondere die Gewährleistung eines weitest möglich unterbrechungs- und verlustfreien Betriebs durch ein geeignetes Wiederherstellungs- und Kontinuitätsmanagement:

9 LÖSUNGSANSATZ FÜR DIE DATEN-/ INFORMATIONSSICHERHEIT UND -VERFÜGBARKEIT

Im Bereich Kontinuitätsmanagement ist die klassische synchrone Spiegelung für einen unterbrechungsfreien Betrieb der unternehmenskritischen Systeme und Rechenoperationen zumeist nicht ausreichend. Unter dem Aspekt der Ausfallsicherheit (DR/BC) ist der aktuelle Stand der Technik nicht mehr in der Synchronisation zu sehen, sondern in einer Kombination von redundanten Rechenzentren und einer Softwaretechnologie, die sich Umgebungs- und Applikations-übergreifend sowie speicherneutral den unmittelbar beim Schadensereignis vorliegenden „Letztstand“ des Produktivprozesses „merkt“, ihn repliziert und die betroffenen Systeme im Sekundenbereich wieder produktiv an diesen Letztstand ansetzen lassen kann. Eine solche fortschrittliche Technologie muss sich nicht mehr auf das Wiederanlaufen von Systemen beschränken sondern setzt die Betriebsabläufe unmittelbar fort.

Nachteile der synchronen Spiegelung: Ein Schutz ist nur gegen physikalische Fehler gegeben. Die überwiegende Anzahl von Störungen liegt jedoch im logischen Bereich und ist daher auf beiden Seiten des Spiegels „synchron“ vorhanden. Die Wiederherstellung erfordert dementsprechend den Einsatz kostbarer Zeit bis zur Isolierung und Beseitigung des logischen Fehlers, zum Wiedereinspielen verlorener Daten und Neustart des Produktivsystems. Die Ausfallzeiten liegen üblicherweise im Stunden- wenn nicht Tagebereich. Greifen hier mehrere Sicherheitslösungen ineinander, bringt die Komplexität der Wiederanlaufszenarien zudem einen eigenen Geschäftsprozess mit entsprechendem Administrationsaufwand mit sich, der indes oft an der konsistenten Wiederherstellung der gesamten Unternehmenssteuerungssoftware scheitert.

Der Replikationsansatz sollte daher ganzheitlich sein, unabhängig von Anwendung und umgebender IT-Architektur eine unmittelbare Replikation der Originalbedingungen erlauben und der Zeitversatz sich in engen Grenzen bewegen.

Bei der Lösung „Zerto Virtual Replication (ZVR)“ werden losgelöst von der jeweils eingesetzten Applikation die Vorteile einer asynchronen Spiegelung - wie z.B. die Entfernungsunabhängigkeit - mit der Technik der kontinuierlichen Datensicherung verknüpft. Das Produktivsystem, d.h. die die datenverarbeitende Applikation wird durch die asynchrone Sicherung nicht beeinträchtigt. Durch die permanente Replikation sind RPOs (Recovery Point Objectives) im

Sekundenbereich möglich. Da die Daten bei der Übertragung komprimiert werden, kann die Netzwerkbelastung gering gehalten werden. Der Recovery Point kann für die gesamte Anwendung für jeden Zeitpunkt in Sekundenschritten bis zu 30 Tage rückwirkend wiederhergestellt werden. Durch Virtuelle Protection Groups (VPGs) wird gewährleistet, dass die Applikation - beispielsweise ERP-Systeme wie SAP - ebenso wie die umgebenden bzw. ansetzenden Systeme ganzheitlich und in ihrem produktiven Zusammenspiel genau vom selben Zeitpunkt wiederhergestellt werden können. Auf diese Weise wird eine in sich konsistente und funktionsgerechte Wiederherstellung in Sekundenschritten ohne manuelle Nachkonfigurationen ermöglicht.

Da keine Abhängigkeit von bestimmten Storage-Systemen besteht, können an verschiedenen Lokationen unterschiedliche Systeme eingesetzt werden. Applikation und Daten können zudem in die verschiedenen Cloud-Typen (Private-, Hybrid- und Public) migriert werden, was dem Unternehmen die ganze Bandbreite zur Verfügung stehender Cloud-Lösungen – je nach Anwendung und Produktivbedarf – außerhalb einer bestimmten Cloud-Technologie und Konfiguration eröffnet. Es werden mithin über Rechenzentren hinweg und bis in die jeweilige Cloud-Lösung hinein im Desaster-Fall Wiederherstellungen beliebiger Dateien aus beliebigen Anwendungen möglich mit einem Zeitversatz des Replikationsstandes von nur Sekunden vor dem Desaster - und so ein produktiver Weiterlauf der im Sekundengedächtnis des Systems replizierbaren Daten binnen eines RTOs (Recovery Time Objective) von wenigen Minuten erlaubt. Zudem ist auch ein Desaster Recovery Testing im laufenden Betrieb mit Reporting möglich, was bei anderen Lösungen oft nur sehr aufwändig am Wochenende und nicht im produktiven Betrieb möglich ist. Das Testing mit dem Reporting ist gerade auch bei Audits ein wichtiges Instrument und dokumentiert die Funktionsfähigkeit und Verfügbarkeit der IT.