Recht an Daten in der Smart Factory

Rechtsanwalt Dr. Thomas Thalhofer, Noerr LLP, München

Hauptvoraussetzung für die „intelligente Fabrik", die als ein Ergebnis der laufenden vierten industriellen Revolution durch die „Industrie 4.0" zu erwarten ist, ist die Verarbeitung großer Mengen an Daten von vernetzten und teilweise autonom handelnden Maschinen im „Internet of Things" (IoT). Daten stellen im Zeitalter der Digitalisierung ein zentrales und auch sehr wertvolles Wirtschaftsgut dar. Man denke nur an die Möglichkeit der Auswertung von Sensordaten für Produktentwicklung oder die Analyse von Kundenwünschen. Mangels eines kodifizierten „Datenrechts" und einer folglich recht diffusen Rechtslage ist umstritten, ob überhaupt ein Recht an Daten existiert, und wenn ja, wie dieses ausgestaltet ist. Wem die begehrten maschinengenerierten Daten gehören und welchen Beteiligten an der Wertschöpfungskette welche Rechte zur Nutzung zustehen, ist aber eine der wichtigsten zu klärenden Rechtsfragen im Bereich der „Industrie 4.0" dar. Daher beschäftigt sich der Beitrag mit verschiedenen Lösungsansätzen, auch auf europarechtlicher Ebene.

I. Ausgangslage

Die aufgrund der Entwicklung der Industrie 4.0 entstehende „Smart Factory" zeichnet sich wesentlich durch die Verarbeitung von großen Mengen an Daten und deren Verarbeitung von vernetzten und teilweise autonom agierenden Maschinen aus, welche sich wiederum dieser Daten bedienen. Durch Auswertung dieser Daten werden Maschinen in der Lage sein, bestimmte Handlungen determiniert auszuführen, zum Beispiel Bestellungen bei Lieferanten bei sich abzeichnendem Rohstoffbedarf der Fabrik.

Aber nicht nur in der Smart Factory fallen maschinengenerierte Daten an. Am Beispiel Auto wird deutlich, dass diverse Daten im Auto selbst erhoben werden, wie die Motortemperatur, Geschwindigkeit, Auto-Betriebswerte, aber auch vom Kunden generierte Daten wie zB Nutzung der Entertainmentsysteme oder Wegstrecken im Navi. Wem diese maschinengenerierten Daten „gehören", wer sie nutzen und verwerten darf, stellt eine der wichtigsten zu klärenden Rechtsfragen im Bereich der „Industrie 4.0" dar. Da Hersteller, Softwareentwickler und Nutzer meist auseinanderfallen und auch Nutzungsrechte Dritter in Betracht kommen, ist diese Frage auf Basis der aktuellen Rechtslage *de lege lata* nicht einfach zu beantworten.

Bisher ist lediglich die Zuweisung für personenbezogene Daten durch das Bundesdatenschutzgesetz (BDSG) und die ab Mai 2018 geltende Europäische Datenschutzgrundverordnung (DS-GVO) aus rechtlicher Sicht gelöst. Bei personenbezogenen Daten handelt es sich gem. § 3 BDSG um *„Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person"*, wie zB Anschrift, Geschlecht, Standort eines Mobilgeräts und gerade nicht maschinenbezogene Daten. Die Verfügungsbefugnis für diese Daten steht dem Betroffenen (Datensubjekt) zu, auf den sich das jeweilige Datum bezieht.

Anders verhält sich dies bei maschinengenerierten Daten, die keinen Personenbezug aufweisen. Hier fehlt es an einer expliziten gesetzlichen Regelung, die alle diese Daten erfasst. Mit dem Internet der Dinge und der vernetzten Produktion, zum Beispiel durch umfangreichen Einsatz von Sensorik und Machine-to-Machine Communication (M2M), wird diese Art der Daten aber einen ungeheuren Mengenzuwachs erfahren – und steigenden wirtschaftlichen Wert.

II. Arten rechtlicher Zuweisung

1. Übersicht

Das Gesetz sieht verschiedene Arten rechtlicher Zuweisung vor. Die umfassendste Regelung stellen Eigentumsrechte dar, die gleichzeitig Abwehr- und Zuweisungsgehalt umfassen. Unterschieden wird hierbei zwischen Sacheigentum und geistigem Eigentum an Immaterialgütern. Schon heute existiert eine Reihe von Regelungen, die zwar keinen umfassenden Schutz für alle Arten von Daten gewähren, jedoch unter gewissen Voraussetzungen oder in bestimmten Situationen auf Daten zur Anwendung kommen.

2. „Dateneigentum"

Es liegt nahe, zuerst über eine Eigentümerstellung in Bezug auf Daten unter Anwendung von § 903 BGB nachzudenken. Daten haben indes keine körperliche Form und können somit nicht Gegenstand eines Eigentumsrechts nach § 903 BGB sein, da das BGB Eigentum nur an Sachen, also an körperlichen Gegenständen nach § 90 BGB anerkennt. Eine direkte Anwendung von § 903 BGB scheidet damit aus.

Denkbar wäre daher, das „Eigentum" an Daten durch eine analoge Anwendung des § 903 BGB auf Grundlage einer strafrechtlichen Norm wie die der §§ 202 a f., 303 a StGB herzuleiten (Hoeren MMR 2013, 486). Zuordnungskriterien für das „Dateneigentum", also die Verfügungsbefugnis über die Daten könnten das Sacheigentum an dem Datenträger oder der „Skripturakt", also der Prozess des Erschaffens des jeweiligen Datums sein. Rechtsdogmatisch müsste dafür jedoch zunächst eine vergleichbare Interessenlage bestehen. Hiergegen spricht, dass aufgrund der mangelnden Körperlichkeit von Daten (im Gegensatz zu körperlichen Sachen) keine klare Begrenzung des Schutzumfangs besteht (Ehlen/Brandt CR 2016, 571). Eine weiterhin für die Analogie erforderliche planwidrige Regelungslücke im Gesetz lehnen die meisten IT-Rechtler mit der Begründung ab, dass bereits ein ausreichendes Schutzsystem aus ua Datenschutz und Urheberrecht existiere (Peschel/Rockstroh MMR 2014, 571 [572]). Zwar bestün-

de nach § 903 BGB ein Eigentumsrecht an dem physischen Medium, auf welchem die Daten gespeichert sind, wie zum Beispiel an einer Festplatte, aber nicht an den eigentlichen Daten (OLG Oldenburg BeckRS 2011, 28832). Ein reflexartiger Schutz über das Eigentum an dem jeweiligen Datenträger wäre nicht sinnvoll, zumal der Eigentümer der Festplatte dann automatisch das Recht an allen sich darauf befindlichen Daten hätte. Dies erscheint nicht als ein sachgerechtes Ergebnis, was am Bespiel eines Cloud Computing Anbieters für Hosting plastisch wird. Hier ist von Seiten des Cloud-Kunden sicher nicht gewollt, dass die Daten in der Cloud dem Cloud-Anbieter allein durch das Hochladen gehören sollen. Der Cloud-Anbieter ist aber ohne Zweifel der Eigentümer der Infrastruktur. Zu dem gleichen Ergebnis kommt man, wenn man eine Eigentumszuweisung über § 947 BGB durch Verbindung der Daten mit dem körperlichen Medium, dem Datenträger, prüft.

3. Recht an Daten als „sonstiges Recht" im Sinne des § 823 I BGB

Bisher konnte sich auch der Ansatz, ein Recht an Daten als „sonstiges Recht" nach § 823 I BGB zu qualifizieren, nicht durchsetzen. Umstritten ist jedoch auch bei den Befürwortern, wie weit ein entsprechender Schutz nach § 823 I BGB reichen würde. Teilweise wird hierbei auf das einzelne Datum abgestellt, manchmal aber auch auf den in den Daten verkörperten Wert. Es wird außerdem diskutiert, ob es sich bei § 823 I BGB um eine positive Nutzungsbefugnis handelt oder lediglich um ein negatives Abwehrrecht (Verbietungsrecht) (Zdanowiecki in Noerr: Rechtliche Herausforderungen der Digitalisierung/Industrie 4.0, November 2015, abzurufen unter: http://bdi.eu/media/themenfelder/digitalisierung/downloads/20151117_Digitalisierte_Wirtschaft_Industrie_40_Gutachten_der_Noerr_LLP.pdf, S.21).

4. § 823 II BGB iVm § 303 a StGB als Schutzgesetz

Ein weiterer Ansatz könnte sich aus § 823 II BGB iVm § 303 a StGB ergeben. Dieser schützt jedoch nur gegen das Ändern der Daten, nicht gegen das Lesen und liefert somit auch keinen Schutz vor dem Zugriff Dritter im Sinne eines Ausschließlichkeitsrechts.

5. Zwischenergebnis

Nach alledem existiert nach herrschender Ansicht für Daten kein allgemeines Recht mit absoluter Wirkung gegenüber dem gesamten Rechtsverkehr. Allerdings erkennt die Rechtsprechung durchaus an, dass Zuordnungskriterien für Daten existieren. So hatte etwa das OLG Naumburg entschieden, dass es durchaus Kriterien gibt, unter denen Rechte an Daten für eine bestimmte Person gegeben sein können (BeckRS 2014, 19058). Das OLG entschied, dass die Daten aus einer Radarfalle der Polizeidienststelle gehören, welcher der Polizist, der die Daten durch den so genannten „Skripturakt" erzeugt hatte, angehört. Skripturakt ist dabei der Schaffensprozess, durch den das betreffende Datum erzeugt wurde. Nach der Auffassung des Gerichts sollen virtuelle Güter, abhängig von ihrem technischen Herstellungsprozess, einer bestimmten Person zugeordnet werden.

III. Sondervorschriften für bestimmte Datenkategorien

1. §§ 87 a, 87 b UrhG

Besondere Vorschriften, wie zB UWG und UrhG, bieten für gewisse Kategorien von Daten bestimmte Abwehrrechte gegen einen Zugriff auf Daten und/oder deren Verwendung. Zunächst sind hier §§ 87 a, 87 b UrhG als leistungsrechtliche Schutznormen zugunsten eines Datenbankherstellers zu nennen. Der Schutz des § 87 a UrhG ist allerdings, wie nachfolgend zu zeigen sein wird, stark lückenhaft. Zum einen ist eine Datenbank im Sinne des UrhG nur eine solche, deren *„Beschaffung, Überprüfung oder Darstellung eine nach Art oder Umfang wesentliche Investition erfordert"* (instruktiv zur Auslegung der Tatbestandsmerkmale Dreier in Dreier/Schulze, UrhG, § 87 a, 5. Aufl. 2015, Rn. 11 ff.). Eine wesentliche Investition ist dann gegeben, wenn bei objektiver Betrachtung keine ganz unbedeutenden, von jedermann leicht zu erbringenden Aufwendungen erforderlich waren, um die Datenbank zu erstellen (BGH GRUR 2011, 724 – Zweite Zahnarztmeinung II = GRUR-Prax 2011, 299 [Lüft]). Kleine und einfache Datenbanken unterfallen damit per se schon nicht dem Leistungsschutzrecht der §§ 87 a, 87 b UrhG.

Ferner verlangt § 87 a UrhG als Voraussetzung für eine Subsumption unter den Datenbankbegriff „eine Sammlung von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet" sind. Kein Schutz besteht mangels systematischer oder methodischer Anordnung der einzelnen Elemente hingegen für bloße „Datenhaufen", d. h. für die noch nicht besonders geordnete Ansammlung der sog. Rohdaten (OLG Köln MMR 2007, 443). Damit scheidet ein wesentlicher Teil von Big Data, nämlich die häufig noch unstrukturierten Datensammlungen, die sich im Besitz von Unternehmen befinden, aus dem Datenbankschutz vollständig aus.

Schließlich schützen §§ 87 a, 87 b die Datenbank nur als Gesamtheit und nicht das einzelne Datum, und hinsichtlich der Gesamtheit nur die Nutzung wesentlicher Teile. Die Nutzung unwesentlicher Datenbankteile steht hingegen grundsätzlich jedermann frei (Dreier in: Dreier/Schulze, 5. Aufl. 2015, UrhG § 87 b Rn. 9), auch wenn dies wiederholt geschieht. Einen Schutz einzelner Daten gewährleistet §§ 87 a, 87 b UrhG.

Darüber hinaus könnte man noch an die Anwendung des Datenbankurheberrechts nach § 4 II UrhG denken. Dieses verlangt jedoch einen urheberrechtlichen Schutz gemäß § 2 II UrhG eine „persönliche geistige Schöpfung" verlangt, die bei rein maschinell erzeugten Daten in aller Regel nicht vorliegen wird.

Auch das UrhG liefert damit keine allgemeine Grundlage für ein Dateneigentum.

2. § 17, 18 UWG

Das Gesetz gegen den unlauteren Wettbewerb (UWG) enthält in seinen §§ 17, 18 Abwehrrechte in Bezug auf Betriebs- und Geschäftsgeheimnisse. Die engen Voraussetzungen für die Anwendung des § 17 UWG sind der Zusammenhang mit einem Geschäftsbetrieb, fehlende

Offenkundigkeit, Geheimhaltungsinteresse und Geheimhaltungswille, folglich die Zuordnung zum Unternehmensinhaber als (ggf. Mit-)„Eigentümer“ oder zumindest als „Inhaber“ einer Lizenz oder einer Nutzungsberechtigung (Köhler: Köhler/Bornkamm, 35. Aufl. 2017, UWG § 17 Rn. 1-13).

Weitere Einschränkungen liegen darin, dass nicht sämtliche Arten und Personen von den Beschränkungen der Datenverwendung erfasst sind. Vielmehr haben die in Rede stehenden Tatbestände sehr spezifische Voraussetzungen. Nach § 17 I UWG kann nur ein bei dem Unternehmer Beschäftigter (nicht Mitarbeiter eines anderen Unternehmens), Täter eines Geheimnisverrats sein. In § 17 II UWG, dem Betriebsspionagetatbestand, ist unbefugtes Verschaffen oder Sichern der Daten durch den Täter erforderlich. Problematisch ist häufig auch die Abgrenzung hinsichtlich des Kriteriums „unbefugt“, beispielsweise wenn zwei Unternehmen zusammenarbeiten und dabei voneinander Daten erheben.

Der Straftatbestand des § 18 UWG stellt zwar auf das unbefugte Verwerten von Unterlagen ab. Er ist jedoch auf *„anvertraute[n] Vorlagen oder Vorschriften technischer Art“* beschränkt, was die relevanten Datenkategorien in der Smart Factory, nämlich maschinenerzeugte Daten, in der Regel nicht erfassen wird.

Aufgrund des engen Anwendungsbereichs können somit auch die Regelungen der §§ 17, 18 UWG nicht als allgemeine Grundlage für ein Dateneigentum dienen.

IV. Ergebnis de lege lata und Empfehlung

Ein Dateneigentum im Rechtssinne existiert nach derzeitiger Rechtslage folglich nicht. Es ist deswegen für Unternehmen empfehlenswert, die Zuweisung von Rechten an Daten durch eindeutige Vertragsregelungen zwischen den an der Datenerzeugung, -verarbeitung und -nutzung Beteiligten zu gewährleisten. Dieser Schutz wird zwar nur zwischen den Vertragsparteien wirksam, leistet lediglich Hilfe bei der Zuordnung in deren Verhältnis und führt nicht zu einer abschließenden Klärung der Frage, wem die Daten eigentlich „gehören“. Dennoch sind vertragliche Regelungen zur Vermeidung von Streit zwischen den an der Smart Factory beteiligten Unternehmen sehr bedeutsam, und es ist den Firmen zu empfehlen, mit Blick auf Maschinendaten eine vertragliche Strategie zu entwickeln, zum Beispiel in Allgemeinen Geschäftsbedingungen (AGB).

Man wird nicht leugnen können, dass vertragliche Regelungen aufgrund der Relativität der Schuldverhältnisse gegenüber einem echten „Dateneigentum“ nur einen „Workaround“ darstellen, auch nicht zuletzt weil sie wiederum rechtlichen Beschränkungen unterliegen, wie zum Beispiel dem AGB- und Kartellrecht (Grützmacher CR 2016, 485 [486]). In Kombination mit den vertraglichen Regelungen kann daher auch die faktische Zugangssicherung zu den Daten ein wesentlicher Aspekt sein. In der Praxis lässt sich ein Ausschluss Dritter von der Datennutzung auch dadurch erreichen, dass einfach praktisch wenig Dritte Zugang zu den Daten haben, und sich ihnen dadurch eben gerade keine Nutzungsmöglichkeit eröffnet.

V. Ausblick

Bisher werden in keinem europäischen Land nicht verkörperte Daten unter den von Eigentumsrechten erfassten körperlichen Gegenstand subsumiert (Boehm ZEuP 2016, 358 [380 ff.]. Die EU-Kommission hat in ihrer „Strategie für einen digitalen Binnenmarkt in Europa“ aus Mai 2015 eine europäische Initiative zum „freien Datenfluss“ vorgestellt, die sich ua mit den Fragen des Eigentums an Daten, ihrer Nutzbarkeit und des Zugangs zu den Daten in bestimmten Situationen befasst, zB wenn Daten von Maschinen und im Zusammenwirken zwischen Maschinen erzeugt werden. Am 3.10.2016 hat die EU-Kommission die Folgenabschätzung in der Anfangsphase der Initiative für freien Datenfluss veröffentlicht, welche die nächsten möglichen Schritte der EU-Kommission zusammenfasst. Diese betont, dass die EU-Kommission das Konzept des Eigentums an Daten weiter erforschen will. Am 10.1.2017 hat die EU-Kommission die Mitteilung „Building an European Data Economy“ präsentiert. Dort wird schwerpunktmäßig auf den ungehinderten Datenfluss in der EU, die Frage nach Zugang und Übertragung von Rohdaten, insbesondere von Software oder Maschinen, die Haftung bei „Internet of things“, sowie autonomen System und Portabilität von nicht-personenbezogenen Daten abgestellt. Die Kommission unterbreitet eine mögliche, allerdings vage formulierte Regelung für das Thema „ownership“/Eigentum an Daten, indem ein Leistungsschutzrecht für nicht personenbezogene Daten eingeführt werden könnte, und zwar in Form eines dinglichen Rechts oder eines subjektiven Abwehrrechts. Ein subjektives Abwehrrecht wäre dem Know-how-Schutz ähnlich, würde allerdings über den Inhalt der RL 2016/943/EU hinausgehen.

Auch in Deutschland wird die Frage, ob es der Einführung eines neuen Datenrechtes bedarf, im Nachgang zu den Initiativen auf europäischer Ebene nun nicht nur von IT-Rechtlern, sondern auch von Politikern intensiv diskutiert. Klar positioniert hat sich hier Bundesverkehrsminister Dobrindt, dessen Ministerium im „Strategiepapier Digitale Souveränität“ vom 27.3.2017 das Postulat *„Wir brauchen ein Datengesetz in Deutschland“* aufstellt (http://www.bmvi.de/SharedDocs/DE/Artikel/DG/daten-gesetz.html).

Gesetzgeberischen Handlungsbedarf sieht offenbar auch Bundeskanzlerin Merkel, die anlässlich der CeBit in einem Video-Podcast für eine einheitliche Regelung hinsichtlich des Eigentums an Daten in der EU aussprach (https://www.bundesregierung.de/Content/DE/Pressemitteilungen/BPA/2017/03/2017-03-18-podcast.html). Unter den IT-Rechtlern ist indes durchaus umstritten, ob eine gesetzliche Regelung nötig oder überhaupt sinnvoll ist (dagegen etwa Gützmacher CR 2016, 485 [495], der lediglich für die Berücksichtigung des § 69 e UrhG im Kontext des Dateneigentums sowie für einen Schutz von Datenformaten auf europäischer Ebene plädiert).

Ob also ein Eigentum an Daten geschaffen wird, ob die Bestimmung der Nutzungsrechte an Daten weiterhin vertraglich erfolgen soll oder ob der Gesetzgeber eine gänzlich andere Lösung wählt, ist eine brisante rechtspolitische Frage, deren Antwort wir mit Spannung erwarten dürfen. ■