Heinrich C. Mayr, Martin Pinzger (Hrsg.): INFORMATIK 2016,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 1459

Industrie 4.0 – Datenhoheit und Datenschutz

Univers.-Prof. Dr. Dr. Jürgen Ensthaler[1] und Dr. Martin S. Haase[2]

Abstract: Daten werden im Zusammenhang mit vernetzten „intelligenten" Maschinen, mit Gerätschaften, die vom gewerblich tätigen oder privaten Konsumenten benutzt werden und Informationen über Nutzungsart, Funktionsfähigkeit oder Störungen liefern, zu einem Wirtschaftsfaktor werden. Die europäische Kommission ist in ihrer Strategie für einen digitalen Binnenmarkt der Auffassung, dass Daten zum eigenen Produktionsfaktor und Wirtschaftsgut werden.[3] Mit dieser Ansicht verbunden ist dann die Frage nach der „Datenhoheit" – wem gehören die Daten? Darüber hinaus kann die Erhebung und Verarbeitung von Daten, die Aussagen über einen einzelnen Menschen beinhalten, dessen Persönlichkeitsrecht berühren. Soweit Industrie 4.0 zu neuen „Arten" von Datenverarbeitungsprozessen führt, wird der (personenbezogene) Datenschutz vor Herausforderungen gestellt, die im Ansatz bereits teilweise diskutiert wurden und teilweise neu bedacht werden müssen. Außerdem sind in die Anwendung und Auslegung des Datenschutzrechts die neuen technischen Entwicklungen einzubeziehen.

Keywords: Datenhoheit, Datenschutz, personenbezogene Daten, datenschutzrechtliche Zulässigkeit.

1 Berechtigung an Daten – „Datenhoheit"

1.1 Welche Daten sind gemeint?

Unter Daten werden in dem ersten Abschnitt dieses Beitrags Informationen verstanden, die nicht oder nicht ausreichend derart bearbeitet wurden, dass sie den Schutzbereich von Immaterialgüterrechten, wie insbesondere das Patent- oder Urheberrecht erreichen. Umgangssprachlich formuliert handelt es sich bei den Daten um virtuelle Rohmaterialien, die noch keiner oder keiner für einen bislang anerkannten Schutzbereich hinreichenden Bearbeitung unterzogen wurden.

Solche Informationen sind dem immaterialgüterrechtlichen Sprachgebrauch folgend gemeinfrei, d.h., sie können von jedermann benutzt werden. Den Informationen fehlt eine Leistung erfinderischer, origineller und auch leistungsschutzrechtlicher Art, durch die der

[1] TU Berlin, Fakultät VII, Wirtschafts-. Unternehmens- und Technikrecht, Sekr. H- 41, Straße des 17. Juni 135, 10623 Berlin, juergen.ensthaler@tu-berlin.de.
[2] TU Berlin, Fakultät VII, Zivil-, Handels-, Gesellschafts- und Innovationsrecht, Sekr. H- 41, Straße des 17. Juni 135, 10623 Berlin, m.haase@tu-berlin.de.
[3] Commission Staff Working Document, A Digital Single Market Strategy for Europe – Analysis and Evidence, SWD (2015) 100 final, 59; nach einem Bericht in der Zeitschrift FOCUS vom 30.04.2016, S. 106, wurden 90 % der heutigen Daten in den vergangenen zwei Jahren generiert. Weltweit soll danach das Datenvolumen um 50 % pro Jahr steigen.

Schutz derart eingebundener Daten verdient werden kann. Auch das Datenbankrecht des § 87a UrhG, ein Leistungsschutzrecht, wurde bislang für die Schutzgewährung eher abgelehnt. Dies soll im Folgenden näher untersucht werden; der Europäische Gerichtshof (EuGH) hat jedenfalls in mittlerweile zwei Entscheidungen einen Leistungsschutz für erst zu generierende Daten abgelehnt; geschützt werden sollen nur Investitionen in bereits vorhandene Daten.[4] [*Leistner* in De09, S. 427, 438; Ho04, S.34, 35; Ze15, S. 1151, 1157f.]

Um diese Situation geht es aber gerade im Zusammenhang mit den bedeutsamen Daten für den Bereich von Industrie 4.0. Es geht bei der Diskussion um die Datenhoheit darum, dass Unternehmen an ihren Maschinen oder Maschinenteilen Hard- und Softwareelemente anbringen, die beim Nutzer Daten über die Art und Weise der Nutzung sowie über die Funktionalität, die Anfälligkeit und die Abnutzung der Aggregate liefern, die Auskunft über Prozessverträglichkeiten, Nutzungsarten u.ä. generieren und übermitteln. Der Hersteller derartiger Maschinen benötigt die Daten für zahlreiche Zwecke, u.a. zur Optimierung seiner Produkte, zur Erfassung der Kundenwünsche, zur Marktbeobachtung und zur Einschätzung von Gewährleistungs- und Schadensersatzansprüchen.

Die Interessen der kommerziellen oder privaten Nutzer an der Weiterleitung der durch ihre Nutzungen generierten Daten werden recht unterschiedlich sein. Man kann aber unterstellen, dass zumindest die kommerziellen Nutzer bei Kenntnis über die Bedeutung und den wirtschaftlichen Wert der Daten diese Daten nicht ohne Gegenleistung herausgeben bzw. nicht generieren werden.

1.2 Zuordnung über das Vertragsrecht?

Die Frage nach der Nutzungsmöglichkeit und der dafür zu erbringenden Gegenleistung wird künftig wohl zunehmend in Verträgen geregelt werden. Damit ist aber nicht die Frage beantwortet, wem die Daten ursprünglich zugeordnet sind, wem sie gehören. Für die Vertragsgestaltung hat diese Frage zweifache Bedeutung. Es wird nur derjenige eine Gegenleistung erbringen, der etwas erhält, was ihm bislang nicht gehört. Bei den Vertragsregelungen wird es sich zudem regelmäßig um allgemeine Geschäftsbedingungen handeln und für eine Inhaltskontrolle ist die ursprüngliche Zuordnung ein wichtiges Kriterium.

1.3 Berechtigte Interessen an der Zuweisung

Bei der Frage nach der Berechtigung an den Daten gibt es zwei unterschiedliche Interessen zu berücksichtigen. Die Interessen des Unternehmens, das das mit einem Datenerfassungsgerät versehene Produkt liefert und das Unternehmen oder auch die privat nutzende Person, die die Daten durch Nutzung des Produkts generiert, und zwar in der eigenen betrieblichen oder privaten Sphäre.

Beim Herstellerunternehmen wird zu berücksichtigen sein, dass die Datenerhebung durch

[4] EuGH, GRUR 2005, 244 – BHB; EuGH, GRUR 2005, 254 – Fixtures Marketing III.

deren Arbeit vorbereitet wurde. Hinsichtlich des nutzenden Unternehmens bzw. der nutzenden Privatperson wird zu berücksichtigen sein, dass von ihnen die Daten unmittelbar generiert werden.

1.4 Schutzmöglichkeiten de lege lata

1.4.1 Urheberrechtlicher Datenschutz

aa) Die Vorbereitung der Datenerhebung, d.h. die Entwicklung einer Struktur für die Einordnung der Daten, könnte nach dem Datenbankrecht, § 87 a UrhG, geschützt sein. Dieser Schutz bezieht sich aber nicht auf die zu erhebenden und entsprechend einzuordnenden Daten. Deren Schutz ist gerade nicht in den Schutz der Datenbankstruktur einbezogen; der EuGH hat dies gerade auf der Grundlage eines Vorlagebeschlusses des BGH bestätigt.[5] Die europäische Richtlinie 96/9 bestimmt auch ausdrücklich, dass der Schutz nicht auf die Inhalte, die eingebrachten Daten, bezogen ist. Dies ist im Hinblick auf die Begründung des Schutzes selbstverständlich. Es soll durch dieses Leistungsschutzrecht nicht erreicht werden, dass die in eine Sammlung aufgenommenen Elemente selbst einen Schutz erfahren, nur weil sie für die jeweils gegenständliche Sammlung tauglich waren. Selbstverständlich ist auch, dass die einzelnen in der Sammlung befindlichen Elemente nicht ihren evtl. bestehenden Schutz verlieren, nur weil sie Aufnahme gefunden haben.

Mit diesen durch die Richtlinie und den jeweils nationalen Ausführungsgesetzen vorgegebenen Regelungen ist aber für die Bestimmung der genauen Schutzvoraussetzungen noch nicht viel gewonnen.

bb) Damit aus urheberrechtlicher Sicht überhaupt eine Sammlung, eine Datenbank besteht, muss es sich nach Art. 1 Abs. 2 der Richtlinie 96/9/EG um eine Sammlung voneinander unabhängiger Elemente handeln. Dies ist im Hinblick auf die urheberrechtliche Ordnung eine sich selbst erklärende Anforderung. Soweit die einzelnen Elemente nur zusammenhängend einen Sinn ergeben und anders nicht verständlich, nicht irgendwie sinnhaft einzuordnen wären, läge keine Sammlung von Daten vor, sondern ein zusammengehöriges Element, evtl. schon ein Werk oder eben ein schutzloser „Gegenstand".

Der EuGH hat auf der Grundlage eines Vorlagebeschlusses des BGH jüngst entschieden, dass diese Unabhängigkeit großzügig zu bestimmen ist. Es soll nicht allein auf die Zweckbestimmung der Sammlung abgestellt werden, sondern auch auf alle irgendwie möglichen Verwendungsmöglichkeiten. Gibt es danach weitere Verwendungsmöglichkeiten der einzelnen Elemente einer Sammlung, ist deren Unabhängigkeit gegeben. Dem ist zuzustimmen. Käme es für die Feststellung der Unabhängigkeit allein auf die Zweckbestimmung für die konkrete Sammlung an, könnte die Unabhängigkeit nicht mehr nachgewiesen werden; jede Datenbank würde die Schutzfähigkeit verlieren, weil schon keine voneinander unabhängigen Daten aufgenommen wären.[6]

[5] EuGH, GRUR 2015,1187 ff.; BGH, GRUR 2014,1197.
[6] EuGH, GRUR, 2015, 1187 ff.

cc) Damit steht nun aber die Frage an, ob die schutzbegründende Zusammenfassung an sich unabhängiger Elemente in einer Datenbank irgendeine Qualität oder auch nur Besonderheit haben muss, um durch die Zusammenfassung von grundsätzlich ungeschützten und voneinander unabhängigen Elementen einen Leistungsschutz zu erlangen. Richtlinienengeber und Gesetzgeber haben nur geregelt, dass Schutzvoraussetzung die Existenz einer Sammlung sein muss, und diese muss wiederum durch erhebliche Investitionen geschaffen worden sein.

Wesen der Leistungsschutzrechte ist es, die Amortisation gewerblich geschaffener Leistungen zu schützen. Die Verwendung kostengünstiger Übernahmetechniken soll nicht dazu führen, dass der Ersthersteller die Chance auf Amortisation verliert. Von daher betrachtet ist die Aufnahme des Investitionserfordernisses in § 87 a UrhG sicher nicht falsch, der Normzweck wird benannt. Fraglich ist nur, ob dies reicht. Die Frage gewinnt an Bedeutung, wenn in der Literatur nun auch gefolgert wird, dass es keine irgendwie ins Gewicht fallenden Anforderungen an die Systematik der Sammlung, an ihre Ordnungselemente, zu geben braucht; es soll schon genügen, dass die Daten wieder auffindbar sind [*Dreier* in DSS15, §87a Rdnr.7; *Thum/Hermes* in WB14, §87a, Rdnr.21; Ze15, S. 1151, 1157 Fn.51].

Dem ist wohl zuzustimmen, weil es beim Datenbankschutz gerade nicht um den Schutz eines Werkes (im urheberrechtlichen Sinne) geht; insofern ist es richtig, auch einfache Ordnungsstrukturen genügen zu lassen. Dann gewinnt aber die Schutzvoraussetzung „erhebliche Investitionen“ in § 87 a UrhG an Bedeutung. Wenn die semantische Ebene, die jeweilige Ordnungsstruktur, zu vernachlässigen ist, muss sich die Anforderung auf das Sichten und Sammeln beziehen. Es wird dann aber fraglich, wem die Daten bzw. die Sammlung von Daten zuzuordnen sind – dem die Daten generierenden Nutzer oder dem die Erhebung vorbereitenden Unternehmen.

Der EuGH hat vielleicht wegen dieser Schwierigkeit den Schutz auf Investitionen in vorhandene Daten beschränkt. Damit wird dann aber auch die Frage nach dem Schutz erst zu generierender Daten aus dem Datenbankrecht herausgelöst.[7]

1.4.2 Schutz der Daten als Betriebsgeheimnis

Die Daten sind auch nicht als Geschäftsgeheimnis für den Hersteller der Erfassungseinrichtungen geschützt. Der Geheimnisschutz nach § 17 UWG wie auch der Geheimnisschutz nach dem europäischen Richtlinienentwurf hat zur Voraussetzung, dass die entsprechenden Informationen dem Unternehmen zuzuordnen sind. Im Richtlinienentwurf steht, dass der „Inhaber des Geschäftsgeheimnisses“ geschützt wird [Ze15, S. 1151, 1155].[8]

1.4.3 Weitere Leistungsschutzrechte

Leistungsschutzrechte, die Informationen als solche schützen, sind nicht vorhanden. Auch

[7] EuGH, GRUR 2005, 244; EuGH, GRUR 2005, 254.
[8] Art. 2 I lit. C des Richtlinienentwurfs.

das neu ins Urheberrecht eingefügte Schutzrecht für die Presseverleger hat keine Vorbildfunktion, weil die einfachen Daten, also Daten, die nicht irgendwie redaktionell aufgearbeitet wurden, gerade nicht geschützt sind.

Wenn nun davon auszugehen ist, dass weder die Vorbereitung der Datenerhebung Einfluss auf den möglichen Schutzbereich hat, die Daten auch nicht über den Geheimnisschutz geschützt sind, aber auch die Art und Weise der Nutzung insofern ohne Bedeutung sind, wird es schwierig, Zuordnungskriterien zu entwickeln.

1.5 Rechtsdogmatische Anknüpfungspunkte für eine Regelung zum Schutz der Daten

1.5.1 Übernahme sachenrechtlicher Grundsätze

Im Zusammenhang mit dem Schutz der Informationen ist in der Literatur häufig vom „Dateneigentum“ die Rede [Ze15, S. 1151, 1153]. Es bereitet zunächst Schwierigkeiten, die Frage nach einer Berechtigung an Daten bzw. der sog. Datenhoheit vom Sacheigentum abzuleiten.

Die Ableitung ist aufgrund der bürgerlich-rechtlichen Konzeption des Eigentums aus dem 19. Jahrhundert kaum möglich. Das Sacheigentum wurde als eine nahezu allumfassende Berechtigung angesehen (§ 903 BGB).

Dieser Grundsatz ist im Hinblick auf die vielfältigen Nutzungsbeschränkungen zwar ziemlich ausgehöhlt, die Einschränkungen folgen aber weniger aus der Natur der Sache, sondern sind sozial, wettbewerbspolitisch etc. orientiert.

Die Kritik am Immaterialgüterrecht richtet sich dann auch vornehmlich gegen eine zu starke Orientierung am Sacheigentum. So war es über Jahrzehnte üblich, eine Annäherung des Immaterialgüterrechts an das Sacheigentum zu verlangen; das Immaterialgüterrecht sollte nicht mindere Rechte zuteilen, sondern eine möglichst gleiche Qualität haben.[9]

Die Kritik wird in jüngster Zeit zumindest in grundlegenden wissenschaftlichen Veröffentlichungen mehr institutionenökonomisch geführt[Go07, S. 505 ff., 525, 527].[10] Zumindest in der modernen Privatrechtstheorie hat sich mittlerweile die Konzeption eines einheitlichen Eigentums gewandelt, und zwar hin zu einem Verständnis vom Eigentum als „Rechtebündel“. Es wird dahin argumentiert, dass es einen ungeteilten Eigentumsbegriff nicht geben kann, weil der Ausgleich von Individuellem unterschiedliche „Mischverhältnisse“ ergeben muss. Es wird dahin argumentiert, dass, wenn es ein absolutes Eigentumsrecht gäbe, der Gesetzgeber auch nichts mehr zu gestalten bzw. zwischen widerstreitenden Interessen abzuwägen hätte [Go07, S.549; Le02, S.69].

[9] Die wohl einflussreichsten Lehren im deutschsprachigen Raum zum Immaterialgüterrecht (Ulmer, Troller) zielten auf einen möglichst umfassenden, dem Sacheigentum angenäherten Schutz mit nur konkret benannten Sozialschranken als Ausnahmesituationen hin.

[10] Zur Rechtsprechung siehe auch die Handelsvertreterentscheidung des BVerfG aus 1990, BVerfGE 81, 242.

Im Immaterialgüterrecht gibt es seit einiger Zeit eine entsprechende Entwicklung. Galt es noch bis in die achtziger Jahre hinein z.B. im Urheberrecht die Schutzbereiche allein aus der Interpretation des Rechtsbegriffs „geistig persönliche Schöpfung“ zu gewinnen, wird heute der Schutzbereich auch durch eine Abwägung zwischen den Interessen des Berechtigten und dem Freihaltungsinteresse der Allgemeinheit festgelegt.

So hat auch im Hinblick auf das Urheberrecht der BGH die Schranken als nicht mehr eng zu begrenzende Ausnahmen angesehen, sondern als durchaus auslegungsfähige Regelungsbereiche, die das Interesse der Allgemeinheit an Freihaltung auch widerspiegeln sollen. Im Patentrecht zeigt sich diese Rechtsprechung im Zusammenhang mit dem Spannungsverhältnis zwischen patentrechtlichem Schutz und Standardisierung. Man kann durchaus auch der Ansicht sein, dass die wissenschaftliche Diskussion um den patentrechtlichen Schutz der Computersoftware oder um den patentrechtlichen Schutz auf dem Gebiet der Genexpressionen einzig um die Frage nach dem Freihaltungsinteresse kreist, wenn auch die Ansatzpunkte sich unterscheiden.[11]

1.5.2 Übernahme von Regelungen bezüglich des Sacheigentums

Für die anstehende Frage nach einem Schutz für Informationen hat diese Gleichstellung zumindest wesentlicher Grundlagen der beiden Rechtsgebiete dort Bedeutung, wo es um die Übernahme von Regelungsbereichen geht. In Betracht kommt hier § 950 BGB, der die Rechtsfolgen der Bearbeitung eines Rohstoffes bzw. die der Weiterbearbeitung eines Produkts regelt. Der Bearbeiter erwirbt das Eigentum, soweit nicht der Wert der Bearbeitung geringer als der des Stoffes ist. Die Regelung erscheint passend. Bei den gegenständlichen Informationen handelt es sich um „Rohmaterialien“, um unbearbeitete Informationen, Rohinformationen [Ze15, S. 1151 ff.] (mit denen etwas geschieht, die – wenn auch nicht im Sinne von Patent- und Urheberrecht – bearbeitet werden.

Der Normzweck von § 950 BGB ist auf den Leistungsschutz gerichtet und zwar in besonderer Art. Es wird dem Bearbeiter bei entsprechendem Wert der Bearbeitung nicht nur ein schuldrechtlicher Ausgleichsanspruch gegen den Eigentümer der Sache eingeräumt, sondern der bisherige Eigentümer verliert sein Eigentum und erhält seinerseits einen Ausgleichsanspruch zugewiesen. Die Regelung könnte dahin kritisiert werden, dass nur der Wert der Bearbeitung ausgeglichen werden sollte und nicht der Übergang der Verfügungsbefugnis, der Übergang des Eigentums.

Der Grund dafür liegt darin, dass mit einer Bearbeitung die Sache einer neuen bzw. einer bestimmten Zweckbestimmung zugeführt wird. Soweit dies nicht unerlaubterweise geschieht, ist es sachgerecht, nun auch dem Bearbeiter die Verfügungsmöglichkeit über die derart von ihm bearbeitete Sache zuzuordnen. Das ist interessengerecht, soweit man nachvollziehen will – und wohl auch sollte –, dass eine ins Gewicht fallende, für eine Nutzung

[11] Das US-amerikanische Urheberrecht kann dies noch mehr verdeutlichen. Im Unterschied zum Sacheigentum gibt es dort keine konkret benannten Sozialschranken, sondern eine allgemeine „fair-use-Regel“. Einfach gewendet: Wenn die Nutzung nicht die Interessen des Rechtsinhabers berühren, kann genutzt werden.

des Ausgangsstoffes bedeutsame Bearbeitung wohl demjenigen am besten nützt, der entsprechend bearbeitet hat bzw. der Bearbeitung entsprechend nutzen will. Verlangt ist nach § 950 BGB, dass eine neue Sache entsteht.

Die Frage, wer Bearbeiter und wer Lieferant des Ausgangsstoffes ist, lässt sich gut nachvollziehbar bearbeiten. Bearbeiter ist das Unternehmen, das die technischen Vorrichtungen zur Erfassung und Übermittlung der Daten an der jeweiligen Maschine anbringt; der Nutzer, der die Daten generiert, liefert das Rohmaterial. Regelmäßig wird es sich so verhalten, dass die Datengenerierung ohne gesonderten Aufwand erfolgt, und weiterhin wird man regelmäßig dahin urteilen können, dass der Wert der Rohdaten erst durch die vorbereitende Bearbeitung wertvoll wird. Die vorbereitende Bearbeitung schafft erst die semantische Ebene.

1.6 Neues Leistungsschutzrecht

Der rechtlichen Einordnung nach würde es sich bei einem dem Normzweck von § 950 BGB nachgeordneten Recht um ein Leistungsschutzrecht handeln. Belohnt wird nicht die neue technische Idee oder eine geistig persönliche Schöpfung, sondern der mit der Erhebung der Daten erforderliche Aufwand im gewerblichen Bereich. Geschaffen würde auch nicht ein Ausschließlichkeitsrecht an Daten der entsprechenden Art. Jedermann dürfte entsprechende Daten erheben und verwerten; verboten wäre die Entnahme der bzw. einzelner Daten aus der Sammlung. Von einem bereits vorhandenen Leistungsschutzrecht, dem urheberrechtlichen Datenbankrecht, würde sich das neue Leistungsschutzrecht unterscheiden, weil es hier um den Schutz der Daten selbst geht und nicht um den Schutz der Struktur, nach der die Daten geordnet sind. Begrenzt wäre dieses Recht um die Voraussetzung, dass die Informationsgenerierung vom Hersteller der benutzten technischen Einrichtung vorbereitet wurde.

Die durch ein solches Leistungsschutzrecht berührte Interessenkollision zwischen dem Hersteller der Gerätschaften und den die Daten durch Nutzung der Gerätschaften generierenden Personen würde gegen die Nutzer aufgelöst werden; dies wäre rechtspolitisch im Hinblick auf § 950 BGB sehr gut zu begründen. Derjenige, der berechtigterweise die (Roh-) Datenerhebung seinen Verwendungswünschen entsprechend vorbereitet, hat das Sachinteresse an derart eingeordneten Daten und derjenige, der die Rohdaten zur Verfügung stellt, der sie erhebt, erhält für den Verlust einen Wertausgleich.

Das letztlich zu lösende Problem ist dann die Bestimmung des Wertausgleichs. Nicht richtig wäre es, den Wert der Daten danach zu bestimmen, was sie dem Hersteller für seine Planungen von Wert sein könnten; ebenso falsch wäre es, den Wert danach zu bestimmen, welche Gegenleistung auf dem Markt – soweit er besteht – zu erlangen wäre. Solche Berechnungen sind für das Sacheigentum von Bedeutung, wegen der durch die Körperlichkeit gegebenen Exklusivität. Bei den Leistungsschutzrechten wird diese Exklusivität gerade nicht geschaffen. Die Daten könnten von jedermann erhoben werden, jeder könnte sie entsprechend strukturiert erheben. Dies hat dann auch für den gegenständlichen Ausgleichsanspruch Bedeutung. Der Anspruch ist am Aufwand im Zusammenhang mit der

Datenerhebung zu messen und dürfte gering ausfallen, weil die Daten regelmäßig „nebenbei“, bei zweckentsprechender Nutzung der Maschine erhoben werden. Eine sachgerechte Preisfindung wäre über einen Vergleich zu den Kosten für die Speicherung von Datenmengen bei Dritten angezeigt.

2 Der Schutz des Persönlichkeitsrechts durch das Datenschutzrecht

Die beschriebene Zunahme der Erhebung und Verarbeitung von Daten in der Industrie durch vernetzte „intelligente“ Maschinen oder Gerätschaften ist rechtlich über die bereits angesprochenen Rechtsbereiche hinaus unter den Aspekten des Schutzes personenbezogener Daten zu beurteilen. Wie bereits erwähnt, erfolgt die Verarbeitung[12] zunehmend über Hard- und Softwareelemente, die an Maschinen, Maschinenteilen, Gerätschaften oder sonstigen Gegenständen angebracht werden. Häufig können über die Auswertung solcher Daten auch Aussagen über einzelne Menschen abgeleitet werden (z.B. Art und Weise der Nutzung einer Maschine[13]).

Ist eine Zuordnung von Daten [zu den Begriffen „Angabe“, „Datum“ und „Information“, siehe: Ha15, S.116 ff.] zu einer einzelnen natürlichen Person möglich, führt dies i.d.R. zur sachlichen Anwendbarkeit des Datenschutzrechts, wenn durch die Zuordenbarkeit ein Personenbezug entsteht. Die Konsequenz ist, dass die strengen datenschutzrechtlichen Vorschriften zum Schutz personenbezogener Daten eingreifen, und somit die für die Verarbeitung verantwortliche Stelle verpflichtet wird, zahlreiche datenschutzrechtliche Grundsätze und Vorschriften zu beachten.

Das Datenschutzrecht dient – wie die anderen oben bereits erwähnten Rechtsbereiche – ebenfalls dem Ausgleich von unterschiedlichen Interessen. Auf der einen Seite stehen die Interessen der verarbeitenden Stelle(n) an der unbeschränkten Verarbeitung und Nutzung der Daten. Auf der anderen Seite werden durch die Vorschriften und Grundsätze des Datenschutzrechts die Interessen des sog. Betroffenen gewahrt, indem sie das Persönlichkeitsrecht des Betroffenen schützen.[14] Das Datenschutzrecht ermöglicht der betroffenen Person und ggf. der zuständigen Behörde, unzulässige Erhebungs- und Verarbeitungsprozesse rechtlich zu verhindern bzw. zu verbieten.

Im Zusammenhang mit dem Phänomen „Industrie 4.0“ muss hinsichtlich jedes Datenverarbeitungsprozesses geprüft werden, ob und inwieweit das (personenbezogene) Datenschutzrecht anwendbar ist. Darüber hinaus ist festzulegen, welche Stelle für den Verarbeitungsvorgang verantwortlich ist. Soweit keine gesetzlichen Erlaubnisnormen eingreifen, die eine Verarbeitung von personenbezogenen Daten rechtfertigen, ist die verantwortliche

[12] Obwohl das deutsche Datenschutzrecht zwischen der „Erhebung“, „Verarbeitung“ und „Nutzung“ von personenbezogenen Daten differenziert, wird in diesem Beitrag zur Förderung der Übersichtlichkeit nur der Begriff „Verarbeitung“ verwandt.

[13] Konkretes Beispiel: Der Arbeitnehmer A benutzt ein elektronisch kontrolliertes Werkzeug, dessen Betrieb und Nutzung analysiert werden.

[14] Vgl. BVerfGE 65, 1 („Volkszählungsurteil“); § 1 Abs. 1 BDSG.

Stelle auf die Einholung einer wirksamen Einwilligung angewiesen.[15]

2.1 Der sachliche Anwendungsbereich des Datenschutzrechts

EU-weit setzt der sachliche Anwendungsbereich des Datenschutzrechts das Vorliegen personenbezogener Daten voraus.[16] Nach Art. 2 a) EG-Datenschutzrichtlinie[17] sind "personenbezogene Daten" alle Informationen über eine bestimmte oder bestimmbare natürliche Person ("betroffene Person").[18] Die Voraussetzungen des Merkmals „personenbezogene Daten" – insbesondere das Vorliegen von „Informationen", der „Bezug zu einer natürlichen Person" und die „Bestimmbarkeit" – sind hoch umstritten und werden seit Jahren in Rechtsprechung und Literatur umfassend diskutiert [Ha15].

Das Phänomen „Industrie 4.0" stellt zusätzliche, neue Anforderungen an die rechtliche Auslegung der Voraussetzungen des Merkmals „personenbezogene Daten". Durch die neuen Maschinen, die zunehmend mit Sensoren ausgestattet und untereinander vernetzt werden, findet eine massenhafte Generierung und Verarbeitung von Daten statt, die in erster Linie zwar von den Maschinen „stammen" aber vielfach auch Aussagen über einzelne Menschen enthalten.

Das Merkmal „Information" wird in der datenschutzrechtlichen Literatur und Rechtsprechung weit ausgelegt. Hierunter fallen Informationen „unabhängig von der jeweiligen Semantik, Sigmatik, Pragmatik, Darstellungsart, Darstellungsform und Herkunft." [Ha15, S. 453] In dieser Hinsicht werden im Rahmen der „Industrie 4.0" unzählige neue Datenverarbeitungsprozesse entstehen, durch die diese Kriterien erfüllt sind und damit potenzielle Anknüpfungspunkte für das Datenschutzrecht geboten werden.

Personenbezogene Daten liegen allerdings nur dann vor, wenn sich die Informationen (zumindest auch) auf eine natürliche Person beziehen. Vordergründig sind Informationen, die in der Industrie erhoben werden, vielfach Informationen über Gegenstände (z.B. Maschinen). Teilweise beziehen sich die Informationen jedoch nicht nur auf Gegenstände, sondern auch auf deren Nutzer. Auch Informationen, die sich in erster Linie auf einen Gegenstand beziehen, zusätzlich jedoch Aussagen über eine bestimmbare natürliche Person

[15] Anmerkung: Neben dem Schutz personenbezogener Daten durch das Datenschutzrecht bestehen einzelne Gesetzesvorschriften zum Schutz des sog „Know-hows" (Bsp.: § 17 UWG, § 202a ff. StGB), welche vorliegend jedoch nicht näher betrachtet werden.

[16] Vgl. Art. 1 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Amtsblatt Nr. L 281 vom 23/11/1995, S. 0031 ff. (EG-Datenschutzrichtlinie 95/46/EG; ab dem 25.05.2018 wird die EG-Datenschutzrichtlinie 95/46/EG durch die neue Datenschutz-Grundverordnung ersetzt werden).

[17] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Amtsblatt Nr. L 281 vom 23/11/1995, S. 0031 ff..

[18] Eine ähnliche Definition findet sich in Art. 4 Nr. 1 der 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 (Datenschutz-Grundverordnung), Amtsblatt Nr. L 119 vom 04/05/2016, S. 1 ff. (Inkrafttreten: 25.05.2015; Anwendbar ab: 25.05.2018).

enthalten, sind als personenbezogen anzusehen [Ha15, S. 144 f., 174 f.].

Als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind (Art. 2 a) HS 2 EG-Datenschutzrichtlinie 95/46/EG).[19] In Rechtsprechung und Literatur ist nach wie vor umstritten, ob und inwieweit Zusatzwissen – insbesondere dritter Stellen – mit in die Beurteilung der Bestimmbarkeit einbezogen werden [Ha15, S. 290 ff.]. Die angesprochenen vernetzten, „intelligenten" Maschinen verarbeiten über eine Person i.d.R. nicht die „klassischen" personenbezogenen Daten wie Name, Vorname, Anschrift und Geburtsdatum. Vielmehr handelt es sich um Daten, die die Nutzung einer solchen Maschine durch einen Menschen automatisch mit sich bringen. Hierzu zählt z.B. das Arbeitsverhalten (Wie wird eine Maschine durch eine Person genutzt?) oder der Standort (Wo befindet sich die Person, die eine Maschine nutzt?). Häufig können diese Daten nicht direkt einer Person zugeordnet werden. Eine direkte Zuordnung ist auch nicht erforderlich. Denn bei der Frage der Bestimmbarkeit sind zusätzliche Möglichkeiten der verantwortlichen Stelle zu beachten.

Nach dem objektiven Ansatz sind unabhängig von den individuellen Möglichkeiten der verantwortlichen Stelle zusätzlich alle „objektiv" zur Verfügung stehenden Zusatzmöglichkeiten einzubeziehen [Ge13, S.478 ff. (479); Pa08, S.34 ff. (38 f.)]. Nach dem relativen Ansatz kommt es in erster Linie vielmehr auf die individuellen und konkreten Möglichkeiten der jeweils verarbeitenden Stelle an [Ec11, S. 339 (342); GS15, §3, Rdnr.10].[20] Sowohl die streng objektive Ansicht als auch die streng relative Ansicht sind abzulehnen. [AFK06, S. 700 ff. (704)] Nach einer vermittelnden Ansicht sind „dritte Stellen in die Beurteilung mit einzubeziehen (objektives Element), wobei diese Einbeziehung über die Merkmale „unverhältnismäßiger Aufwand" (Art. 2 a) i.V.m. EG 26 S. 2 EG-Datenschutzrichtlinie 95/46/EG) einzuschränken ist." [Ha15, S.320] Nach Erwägungsgrund 26 S. 2 sollten bei der Entscheidung, ob eine Person bestimmbar ist, alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen.

2.2 Verantwortliche Stelle

Im Rahmen der Vernetzung von Gegenständen und Maschinen wird es zunehmend zu einer „Vermischung" von verantwortlichen Stellen kommen. Nach Art. 2 d) EG-Datenschutzrichtlinie 95/46/EG ist der "für die Verarbeitung Verantwortliche" die

[19] Eine ähnliche Definition findet sich in Art. 4 Nr. 1 der 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 (Datenschutz-Grundverordnung), Amtsblatt Nr. L 119 vom 04/05/2016, S. 1 ff..

[20] AG München, Urteil vom 30.09.2008, Az.: 133 C 5677/08, ZUM-RR 2009, 413 ff. (414).

natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.[21] Im Rahmen der „Industrie 4.0" kommt es zu einer Vermischung der Entscheidungsbefugnisse und -möglichkeiten. Über Informationen die mittels Hard- und Softwareelementen erhoben und verwendet werden, die an einer Maschine oder Maschinenteilen angebracht sind, entscheidet häufig sowohl der Hersteller, ggf. der Anbieter als auch der Nutzer.

So überwachen heutzutage beispielsweise Hersteller von Fahrstühlen über verschiedene Sensoren die verschiedenen Abläufe des Fahrstuhlbetriebes. Nichtsdestotrotz findet der Vorgang oft in der Sphäre des Gebäudeeigentümers statt. Nutzer kann schließlich ein Mieter sein, der mit dem Fahrstuhl direkt in seine Wohnung fährt. Darüber hinaus finden Verkettungen von Daten unabhängig von menschlichen Einflüssen automatisch bei den Geräten oder Maschinen untereinander statt. Gerade bei Alltagsgegenständen liegt wiederum die direkte Kontrolle eines vernetzten Produktes (Zahnbürste, Kühlschrank, etc.) in der Regel bei dem Nutzer, der das Produkt häufig als Privatperson nutzt.

Sowohl das deutsche als auch das europäische Datenschutzrecht basieren auf der Vorstellung, dass jeder Erhebungs-, Verarbeitungs- und Nutzungsvorgang einer sog. verantwortlichen Stelle zuzuordnen ist (vgl. §§ 1, Abs. 2, 2, 3 Abs. 7 BDSG; Art. 2 d) S. 1 Datenschutzrichtlinie 95/46/EG). In der deutschen Literatur und Rechtsprechung finden sich verschiedene Konkretisierungen. Teilweise wird in Bezug auf das BDSG vertreten, dass es bezogen auf einen Datenvorgang auch mehrere verantwortliche Stellen geben könne [*Dammann* in Si14, §3, Rdnr.226]. Der Umgang mit personenbezogenen Daten könne auch durch „mehrere natürliche oder juristische Personen (…) in gemeinsamer Verantwortung" erfolgen [*Dammann* in Si14, §3, Rdnr.226]. Dem ist zuzustimmen, da ein Datensatz von mehreren Stellen gleichzeitig erhoben, verarbeitet oder genutzt werden kann (vgl. § 3 Abs. 3 – 5 BDSG) und jede dieser Erhebungen, Verarbeitungen oder Nutzungen eine Verantwortlichkeit begründet.[22]

Der Begriff „verantwortliche Stelle" wurde mit dem BDSG 2001 in das deutsche Datenschutzrecht eingeführt. Ersetzt wurde dadurch das Wort „speichernde Stelle". Nach § 3 Abs. 7 BDSG ist verantwortliche Stelle jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Verantwortlich sei, „wer objektiv über die Daten bestimmen kann, wer die Entscheidungsgewalt über den Zweck und die Mittel der Datenverarbeitung hat".[23] [*Wei-*

[21] Nach Art. 4 Nr. 7 der Datenschutz-Grundverordnung (FN. 12) ist: „Verantwortlicher" die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden".

[22] vgl. § 3 Abs. 7 BDSG; eine ähnliche gemeinsame Verantwortung existiert auch im allgemeinen Zivilrecht z.B. bei der gesamtschuldnerischen Haftung.

[23] Auch die EG-Datenschutzrichtlinie 95/46/EG stellt darauf ab, wer über die Zwecke und Mittel der

chert in Dä14, §3 Rdnr. 54] Für die Begründung einer datenschutzrechtlichen Verantwortung i.S.d. BDSG würde ausreichen, „dass die Verarbeitungstätigkeit im eigenen Tätigkeits- und Haftungsbereich stattfindet und die Möglichkeit besteht, in tatsächlicher Hinsicht auf den Verarbeitungsvorgang einzuwirken." [*Buchner* in TG13, §3, Rdnr.52] Bei der Abgrenzung komme es in erster Linie auf eine „juristische" und nicht auf eine „funktionale" Betrachtung an [*Weichert* in Dä14, §3 Rdnr. 54].

Die Verfügungs- und Entscheidungsgewalt sind geeignete Anknüpfungspunkte für die Festlegung der verantwortlichen Stelle, denn diese sind unmittelbar ausschlaggebend für die Missbrauchsgefahr und das Gefährdungspotenzial im Hinblick auf das informationelle Selbstbestimmungsrecht. Auch die reine Einwirkungsmöglichkeit kann ausreichen, denn nach § 3 Abs. 4 Nr. 3 b) BDSG ist Übermitteln auch das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft. Durch eine solche Übermittlung kann also eine weitere Verantwortlichkeit entstehen. Dieser Vorgang führt i.d.R. jedoch nicht dazu, dass die ursprüngliche Stelle die Verantwortung verliert. In erster Linie müssen die objektiven und tatsächlichen Umstände herangezogen werden.[24]

Die datenschutzrechtliche Verantwortlichkeit setzt weder den „Besitz der Daten" noch die „physische Herrschaft über den Verarbeitungsprozess" voraus [*Dammann* in Si14, §3, Rdnr. 225]. Das bedeutet, dass das Eigentum an der oder die Verantwortung für die Datenverarbeitungsanlage und die Verantwortung für die Datenerhebung, -verarbeitung oder -nutzung auseinanderfallen können [*Dammann* in Si14, §3, Rdnr. 224]. Dies ergibt sich aus den Regelungen zur Auftragsdatenverarbeitung (vgl. § 11 BDSG). Auch kommt es nicht auf die „Belegenheit der Datenverarbeitungsanlage" an. [*Weichert* in Dä14, Rdnr. 56]

In den vergangenen Jahren wurde die datenschutzrechtliche Verantwortung in der Bundesrepublik Deutschland unter anderem im Zusammenhang mit der Nutzung sozialer Netzwerke und dem Anbieten von Suchmaschinen diskutiert. Biete ein soziales Netzwerk seinen Nutzern die Möglichkeit, eine sog. „Fanpage" einzurichten, läge die datenschutzrechtliche Verantwortung bei dem Anbieter des sozialen Netzwerks, wenn dieser über das Netzwerk unmittelbar die IP-Adresse erhalte und Cookies anlege.[25] Die datenschutzrechtliche Verantwortlichkeit sei untrennbar mit der Datenerhebung und -verarbeitung verbunden.[26] Außerdem komme es darauf an, wer die Entscheidung über die Erhebungen und Verarbeitungen treffe und welche Zwecke verfolgt würden.[27] Auch sei relevant, wer die „Mittel zur Erreichung des Zweckes" sowie „Art und Weise" der Zielerreichung festlege.[28]

Verarbeitung entscheidet (vgl. Art. 2 d) S. 1).

[24] Allerdings kann über einen Willen zur Einrichtung einer Auftragsdatenverarbeitung nach § 11 BDSG die Verantwortlichkeit auch subjektiv beeinflusst werden. Schließlich müssen in diesem Fall mit Schaffung einer entsprechenden („juristischen") Vereinbarung wiederum tatsächliche Umstände geschaffen werden.

[25] OVG für das Land Schleswig-Holstein, Urteil vom 04.09.2014, Az.: 4 LB 20/13, juris, Rdnr. 77.

[26] OVG für das Land Schleswig-Holstein, Urteil vom 04.09.2014, Az.: 4 LB 20/13, juris, Rdnr. 78.

[27] OVG für das Land Schleswig-Holstein, Urteil vom 04.09.2014, Az.: 4 LB 20/13, juris, Rdnr. 78.

[28] OVG für das Land Schleswig-Holstein, Urteil vom 04.09.2014, Az.: 4 LB 20/13, juris, Rdnr. 79.

Dieser Bewertung stehe auch nicht entgegen, dass derjenige, der die „Fanpage“ eingerichtet hat (sog. „Fanpage-Betreiber“), ein eigenes Interesse an der Datenverarbeitung haben könnte und von dieser (mit)profitiert.[29] Diese Kriterien lassen sich auf typische Vorgänge im Rahmen der Industrie 4.0 übertragen. Pauschal gesagt, können stets auch die Personen und Stellen in die Verantwortung genommen werden, die bildlich gesprochen im Hintergrund stehen.

2.3 Einwilligung

Innerhalb der Europäischen Union müssen verantwortliche Stellen jede Erhebung und Verarbeitung von personenbezogenen Daten rechtfertigen (vgl. Art. 6 ff. EG-Datenschutzrichtlinie 95/46/EG, Art. 5 ff. Datenschutz-Grundverordnung, § 4 Abs. 1 BDSG). Soweit keine Erlaubnisnorm vorliegt, ist eine Einwilligung des Betroffenen erforderlich. Die datenschutzrechtliche Einwilligung ist basierend auf dem informationellen Selbstbestimmungsrecht an besondere Voraussetzungen gebunden (Bestimmtheit, Informiertheit, Freiwilligkeit, i.d.R. Schriftform, vgl. Art. 2 h) EG-Datenschutzrichtlinie 95/46/EG, Art. 7 Datenschutz-Grundverordnung, § 4a BDSG). Die Informationspflicht stellt dort eine rechtliche Herausforderung dar, wo die Informationsverarbeitung auf komplexen oder geheimhaltungsbedürftigen technischen Vorgängen basiert. Die Schriftform könnte insbesondere im Widerspruch zur steigenden Automatisierung stehen. Die Auslegung dieser Voraussetzungen hat die gesellschaftliche und technische Entwicklung in den Blick zu nehmen.

Literaturverzeichnis

[AFK06] Arning, Marian; Forgó, Nikolaus; Krügel, Tina: Datenschutzrechtliche Aspekte der Forschung mit genetischen Daten, Datenschutz und Datensicherheit (DuD) 2006, S. 700 – 705.

[Dä14] Däubler, Wolfgang; Klebe,Thomas; Wedde, Peter; Weichert, Thilo: Bundesdatenschutzgesetz – Kompaktkommentar zum BDSG, 4. Auflage, Bund Verlag, Frankfurt am Main, 2014.

[DSS15] Dreier, Thomas; Schulze, Gernot; Specht, Louisa: Urheberrechtsgesetz, 5. Auflage, C.H.BECK, München, 2015.

[De09] Derclaye, Estelle: Research Handbook on the Future of EU Copyright, Edward Elgar, Cheltenham, 2009.

[Ec11] Eckhardt, Jens: IP-Adresse als personenbezogenes Datum – neues Öl ins Feuer, Personenbezug im Datenschutzrecht, Computer und Recht (CR) 2011, S. 339 – 344.

[Ge13] Gerlach, Carsten: Personenbezug von IP-Adressen, Computer und Recht (CR) 2013, S. 478 – 484.

[29] OVG für das Land Schleswig-Holstein, Urteil vom 04.09.2014, Az.: 4 LB 20/13, juris, Rdnr. 78.

[Go07] Godt, Christine: Eigentum an Information: Patentschutz und allgemeine Eigentumstheorie am Beispiel genetischer Information, Mohr Siebeck, München, 2007.

[GS15] Gola, Peter; Schomerus, Rudolf: BDSG Bundesdatenschutzgesetz Kommentar, 12. Auflage, C.H.BECK, München, 2015.

[Ha15] Haase, Martin Sebastian, Datenschutzrechtliche Fragen des Personenbezugs, Mohr Siebeck, Tübingen, 2015.

[Ho04] Hoeren, Thomas: Anmerkung zu EuGH Urteil vom 09.11.2004 – C- 203/02 (Datenbankschutz) MultiMedia und Recht (MMR) 2005, Heft 1, 34 – 36.

[Le02] Lepsius, Oliver: Besitz und Sachherrschaft im öffentlichen Recht, Mohr Siebeck, Tübingen, 2002.

[Pa08] Pahlen-Brandt, Ingrid: Datenschutzrecht braucht scharfe Instrumente, Datenschutz und Datensicherheit (DuD) 2008, S. 34 - 40.

[Si14] Simitis, Spiros: Bundesdatenschutzgesetz – Kommentar, 8. Auflage, Nomos, Baden-Baden, 2014.

[TG13] Taeger/Gabel, Kommentar zum BDSG und den Datenschutzvorschriften des TKG und TMG, 2. Auflage, Fachmedien Recht und Wirtschaft, Frankfurt a.M., 2013.

[WB14] Wandtke, Artur-Axel; Bullinger, Winfried; Praxiskommentar zum Urheberrecht, 4. Auflage, C.H.BECK, München, 2014.

[Ze15] Zech, Herbert: “Industrie 4.0” – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, Gewerblicher Rechtsschutz und Urheberrecht (GRUR) 2015, Heft 12, 1151 - 1160.