Rechtliche Aspekte automatisierter Systeme

Rechtskonforme Gestaltung unserer Zukunft

Dirk Heckmann · Alexander Schmid

Der folgende Beitrag beschäftigt sich mit den Chancen und Gefahren, die sich bei der Verwendung automatisierter Systeme ergeben, zeigt auf, welche Rechtsvorschriften zur Gewährleistung von Funktions- und Informationssicherheit derzeit existieren und erläutert, wie automatisierte Systeme datenschutzkonform gestaltet werden können.

Chancen und Gefahren automatisierter Systeme

In hohem Maße automatisierte Systeme wie etwa automatisierte Industrie- und Dienstleistungsroboter, automatisierte Kfz oder automatisierte Drohnen werden bereits in naher Zukunft eine Vielzahl an Lebensbereichen des Menschen einnehmen und insofern die bislang primären Einsatzgebiete – zuvorderst in der Industrie – verlassen. Zu denken ist dabei nicht nur an die Paketzustellung mittels automatisierter Transportdrohnen. Auch in den Bereichen Gesundheits- und Pflegewesen, zur Beratung in Geschäften oder zur Unterstützung im Haushalt werden sich endlose Einsatzmöglichkeiten für automatisierte und artifiziell intelligente Systeme ergeben.

Den Chancen, die sich aus der Verwendung dieser neuen Technologien ergeben, stehen jedoch auch nicht unbedeutende Bedenken gegenüber. Gerade bei intelligenten und automatisierten Systemen können Funktionsstörungen in der Soft- oder Hardware, unbefugte Zugriffe von außen oder aber eine inadäquate Programmierung zahlreiche Personen- oder Sachgefährdungen auslösen, etwa dann, wenn ein automatisiertes System nicht mehr kontrollierbar ist und mit einer Person oder Sache kollidiert. Die hierbei bestehenden konkreten Gefährdungsszenarien unterscheiden sich naturgemäß je nach Art und Weise, Einsatzzweck und -ort sowie nach der konkreten technischen Ausgestaltung des Systems. Die Gewährleistung von Funktionssicherheit, von Informationssicherheit sowie einer adäquaten und maschinenethischen Programmierung muss aus diesen Gründen im Mittelpunkt der künftigen technischen Entwicklung automatisierter Systeme stehen.

Ein automatisiertes System ist dabei von der Erhebung, Verarbeitung und Nutzung zahlreicher Sensorinformationen abhängig, zu denen häufig auch personenbezogene oder -beziehbare Daten gehören und insofern vom Recht auf informationelle Selbstbestimmung (anerkannt vom BVerfG im Jahre 1983 und hergeleitet aus Art. 2 Abs. 1, Art. 1 Abs. 1 GG) geschützt werden. Dabei steht die Gewährleistung von Funktionssicherheit des automatisierten Systems in einer Wechselwirkung zum Datenschutz: Je mehr Daten erhoben und verarbeitet werden, desto genauer ist das digitale Raumabbild und -verständnis des automatisierten Systems und desto besser kann dieses seine Umwelt und die darin befindlichen Personen und Sachen schützen. Dennoch darf das Ziel, die Funktionssicherheit eines automatisierten Systems bestmöglich zu gewährleisten, nicht zu einer Aushöhlung des Datenschutzrechts führen. Vielmehr sind beide Seiten in einen schonenden Ausgleich zu bringen und demnach beiden

DOI 10.1007/s00287-017-1042-5

Dirk Heckmann · Alexander Schmid
Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht, Universität Passau
Gottfried-Schäffer-Str. 20, 94032 Passau
E-Mail: heckmann@mein-jura.de, mail@schmid-recht.de

Zusammenfassung
Automatisierte Systeme werden unser Leben nachhaltig verändern. So werden wir unsere bestellte Ware per automatisierter Transportdrohne erhalten, unsere Autos werden intelligent und selbstfahrend sein und unser Zuhause wird umfassend „smartifiziert". Diese technischen Neuerungen und Chancen stehen jedoch in einem Spannungsverhältnis zu den sich hierbei ergebenden Risiken, die mitunter aus der Verletzung von Personen, der Beschädigung von Sachen oder dem Verlust über unsere Datenhoheit bestehen. Die technische Ausgestaltung automatisierter Systeme bedarf daher bereits heute rechtlicher Rahmenbedingungen, die diesen Gefährdungen einerseits effektiv entgegenwirken, andererseits aber die technische Innovationskraft nicht unnötig ausbremsen.

bestmöglich Geltung zu verschaffen. Forschungsbedarf besteht zukünftig daher in der Klärung der Frage, wie die IT-Sicherheit (Funktionssicherheit und Informationssicherheit) automatisierter Systeme bestmöglich gesteigert und gewährleistet werden kann, ohne zugleich das Datenschutzrecht zu vernachlässigen.

Diesen Grundsatzfragen sollen sich die folgenden Ausführungen widmen.

IT-Sicherheit automatisierter Systeme

Der deutsche Begriff der „IT-Sicherheit" ist nicht klar umgrenzt und definiert. Während stellenweise hierunter lediglich der Schutz der IT vor böswilligen Angriffen von außerhalb verstanden wird, ist die IT-Sicherheit richtigerweise weiter auszulegen. IT-Sicherheit umfasst insofern einerseits den Schutz der auf einem IT-System gespeicherten und verarbeiteten Informationen vor einer unberechtigten Einsicht (Vertraulichkeit), Manipulation (Integrität) oder Löschung (Datenverfügbarkeit) (sog. Informationssicherheit als Teilgebiet der IT-Sicherheit). Andererseits umfasst die IT-Sicherheit aber auch die Sicherstellung, dass ein IT-System so funktioniert, wie dies von seinen Entwicklern im Rahmen der Systemausgestaltung vorgegeben wurde und insofern keine unzulässigen Systemzustände annimmt (sog. Funktionssicherheit als weiteres Teilgebiet der IT-Sicherheit). Im Rahmen der Funktionssicherheit kommt es insofern darauf an, dass die realisierte Ist-Funktionalität des Systems auch der vorgegebenen Soll-Funktionalität entspricht [3].

Gewährleistung von Informationssicherheit (Security)

In Deutschland existiert bislang kein einheitliches und zentrales Informationssicherheitsrecht, sodass hierbei eine Vielzahl an Normen und Standards zu beachten sind, die je nach Art und Weise, Einsatzzweck und -ort sowie abhängig von der konkreten technischen Ausgestaltung des automatisierten Systems variieren. Diese Rechtsunsicherheit konnte auch das sog. IT-Sicherheitsgesetz (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme v. 17.7.2015) nur stellenweise beseitigen, als dieses schwerpunktmäßig nur für die Betreiber sog. kritischer Infrastrukturen einschlägig ist und daher ebenfalls ein Spezialgesetz darstellt. Zudem wurde durch das IT-Sicherheitsgesetz, anders als der Name vermuten lässt, kein neues einheitliches Gesetz geschaffen, sondern lediglich bereits bestehende nationale Regelungen abgeändert (sog. Artikelgesetz).

Derzeit kann als zentrale Informationssicherheitsnorm daher nur auf § 9 Bundesdatenschutzgesetz (BDSG) zurückgegriffen werden, der jedoch lediglich pauschal und systemunabhängig bestimmt, dass öffentliche und nichtöffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die *erforderlichen technischen und organisatorischen Maßnahmen* zu treffen haben, um die Ausführungen des BDSG sowie die IT-Sicherheitszielsetzungen gem. der Anlage zum BDSG zu erfüllen. Zu der Frage, welche konkreten Maßnahmen zur Umsetzung dieser Verpflichtung zu erfüllen sind, trifft das Gesetz jedoch keine weitere Aussage, was aus Gründen der Systemunabhängigkeit und daher der breiten Anwendbarkeit der Normen aber auch zweckgerecht ist. Dieser Mangel an konkreten Handlungsempfehlungen wird auch mit Blick in die vom Gesetz genannte Anlage zu § 9 BDSG nicht beseitigt. Denn so finden sich in der Anlage zu § 9 BDSG zwar acht IT-Sicherheitszielsetzungen (Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, Trennung von zweckgebundenen Datenverarbeitungsvorgängen). Auch hierbei wird der Anwender aber konkrete

Abstract
Automated systems will change our lives sustainably. In this way, we will receive our ordered goods by automated transportation drones, our cars will be intelligent and driverless and our home will become "smartified". These technical innovations and chances do, however, go hand in hand with new risks, which mostly consist in the violation of persons, the damage of things or the loss of data integrity. The development of automated systems therefore requires a legal framework, which on the one hand effectively counteracts these risks, but on the other hand does not slow down those technical innovations unnecessarily.

Handlungsempfehlungen vergeblich suchen. Zur Konkretisierung dieser allgemeinen Bestimmungen ist daher auf die zahlreichen und unterschiedlichsten IT-Sicherheitsstandards zurückzugreifen, deren Umsetzung (mangels eigener Rechtswirkung) grundsätzlich zwar freiwillig ist, die zur Erfüllung der verbindlichen Regelungen des BDSG aber herangezogen werden können. Allen voran ist hierbei der sog. IT-Grundschutzkatalog des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu nennen, der aufgrund seines modularen Aufbaus eine präzise Modellierung des zum Einsatz kommenden IT-Systems ermöglicht. Je nach Art und Weise, dem Einsatzzweck und -ort sowie von der konkreten Systemausgestaltung können im Einzelfall aber auch weitere, ganz spezielle Standards und Normen beachtlich sein.

Diese Systematik der pauschalen gesetzlichen Forderungen unter Konkretisierung durch IT-Sicherheitsstandards wird auch nach Inkrafttreten der Europäischen Datenschutzgrundverordnung (EU-DSGVO) im Jahr 2018 beibehalten werden. Denn auch die EU-DSGVO enthält in Art. 5 Abs. 1 lit. f EU-DSGVO lediglich den Grundsatz, dass die Sicherheit („Integrität und Vertraulichkeit") personenbezogener Daten hinreichend gewährleistet werden muss. Ähnlich pauschal wird dies dann erneut durch Art. 32 EU-DSGVO wiederholt.

Gewährleistung von Funktionssicherheit (Safety)

Es versteht sich von selbst, dass auch die Anforderungen zur Gewährleistung von Funktionssicherheit je nach betroffenem System variieren. So ergeben sich bei dem Einsatz einer automatisierten Drohne etwa andere Gefahrenquellen als bei einem automatisierten Pflegeroboter zum Einsatz im Gesundheitswesen oder bei einem automatisierten Rasenmäherroboter. Bei dem Einsatz einer automatisierten Drohne ist etwa sicherzustellen, dass keine Personen oder fremde Sachen durch Absturz oder Kollision verletzt werden. Die Gefährdungen, die von einer Drohne ausgehen, können dabei sowohl unmittelbarer (etwa wenn eine Person oder eine Sache direkt von einer Drohne getroffen oder aufgrund der rotierenden Propeller verletzt wird), als auch mittelbarer (etwa wenn eine Drohne auf eine Autobahn abstürzt und hierbei zwar kein Kfz direkt trifft, als Folge aber einen Unfall auslöst) Natur sein. Dagegen wäre bei dem Einsatz eines automatisierten Pflegeroboters im Gesundheitswesen etwa sicherzustellen, dass dieser die auszuführenden Pflegehandlungen fachgerecht durchführt und den Patienten nicht verletzt.

Ebenso unterschiedlich wie die denkbaren Gefahrenquellen, die von automatisierten Systemen ausgehen, sind auch die in Deutschland zu beachtenden Rechtsnormen hinsichtlich der Gewährleistung von Funktionssicherheit. Als zentrale Norm kann hierbei zwar das Produktsicherheitsgesetz (ProdSG) mit seinen bislang vierzehn Produktsicherheitsverordnungen (ProdSV) angeführt werden. Weiterhin existieren aber auch eine Reihe an spezialisierten DIN-, ISO-, EN- und IEC-Normen.

Gewährleistung von IT-Sicherheit durch Produktbeobachtungspflichten?

Es stellt eine enorme Herausforderung für die Entwickler und Programmierer automatisierter Systeme dar, dem automatisierten System für jede erdenkliche Situation eine adäquate Reaktion vorzugeben. Denn durch die umfassende Steuerungsübernahme durch das automatisierte System wird dieses in der Praxis auch auf Situationen treffen, die in der Entwicklungsphase nicht kalkulierbar und nicht vorhersehbar waren. So muss eine automatisierte Transportdrohne etwa auf eine Vielzahl an Ereignissen adäquat reagieren können, die neben Wind- und Wetterveränderungen auch aus auf Kollisionskurs befindlichen anderen Luftfahrzeugen bestehen können. Vor allem dann, wenn ein automatisiertes System auch auf menschliche Fahrer oder Piloten und daher auch auf teilweise irrationales

Verhalten reagieren muss, wird deutlich, dass eine abschließende Systementwicklung „am Reißbrett" nur bedingt möglich ist.

Im Rahmen des etablierten Softwareentwicklungsmodells in der Informatik, das zuvorderst aus den Stufen „designtime" und „runtime" besteht, wird zukünftig daher verstärkt auf eine kontinuierliche Produktverbesserung im Rahmen der „runtime" zu bestehen sein. Hierbei werden zukünftig auch sog. Produktbeobachtungsmechanismen zum Einsatz kommen, die ein automatisiertes System auch im Praxiseinsatz permanent auf Hardware- oder Softwarefehler, aber auch auf inadäquates Systemverhalten hin überwachen. Wird von diesen Mechanismen ein fehlerhaftes oder unerwünschtes Systemverhalten identifiziert, ist dieses mitsamt der relevanten Protokolldateien umgehend an den Entwickler zu melden, der dann auch außerhalb seiner geplanten Aktualisierungsintervalle unverzüglich entsprechende Patches bereitzustellen hat.

Da der Einsatz solcher Produktbeobachtungsmechanismen seinerseits auf der Erhebung, Verarbeitung und Nutzung von Systemdaten beruht und hierbei auch personenbezogene Begleitdaten involviert sein können, sind auch diese Mechanismen stets datenschutzkonform auszugestalten und insofern eine Balance zwischen einer effektiven Produktbeobachtung und der Gewährleistung des Datenschutzrechts zu finden.

Datenschutzkonformität automatisierter Systeme

Neben dem Schutz der Funktionssicherheit und der Informationssicherheit ist auch sicherzustellen, dass ein automatisiertes System nur im Rahmen der geltenden Datenschutzrechte personenbezogene oder -beziehbare Daten erhebt, verarbeitet oder nutzt. Die datenschutzrechtlichen Anforderungen an ein automatisiertes System sollen daher im Folgenden, auch anhand von zwei Praxisbeispielen, erläutert werden.

Datenschutzrechtliche Relevanz automatisierter Systeme

Automatisierte Systeme ersetzen bislang durch Menschen durchgeführte Eingaben und Steuerungen. Diese Kontrollübernahme ist von der Erhebung, Verarbeitung und Nutzung zahlreicher Sensordaten abhängig. Gerade bei dem Einsatz von intelligenten Kamerasystemen oder sonstigen optisch-elektronischen Einrichtungen werden hierbei auch zahlreiche personenbezogene Daten absichtlich oder als Begleitdaten erhoben, verarbeitet oder genutzt, etwa wenn eine Person den Sensorerfassungsbereich des Systems betritt oder umgekehrt aber das System in den räumlichen Aufenthaltsbereich einer Person eindringt. Dieser Datenumgang mit personenbezogenen Daten steht in Deutschland unter einem sog. Verbot mit Erlaubnisvorbehalt, wie im weiteren Verlauf noch gezeigt werden wird, und ist daher nur zulässig, wenn das geltende Datenschutzrecht dies erlaubt.

Rechtsquellen des Datenschutzrechts

Föderalismusbedingt existieren in Deutschland sowohl sechzehn Landesdatenschutzgesetze (LDSG) (etwa das BayDSG für das Bundesland Bayern) als auch ein zentrales Bundesdatenschutzgesetz (BDSG). Zudem ist der Datenschutz auch Gegenstand mehrerer spezialgesetzlicher Regelungen, etwa im Telemediengesetz (TMG) für die Betreiber von Telemedien (meist Betreiber von Webseiten im Internet), im Telekommunikationsgesetz (TKG) für die Betreiber von Telekommunikationsnetzen oder im Sozialgesetzbuch (SGB) für die Verarbeitung von Sozialdaten (etwa durch Krankenkassen).

Als Abgrenzung zwischen den Landesdatenschutzgesetzen und dem Bundesdatenschutzgesetz ist ausschlaggebend, welche datenschutzrechtlich verantwortliche Stelle die personenbezogenen oder -beziehbaren Daten erhebt, verarbeitet oder nutzt. Ist dies eine öffentliche Stelle des Bundes oder aber eine nichtöffentliche Stelle (etwa ein Unternehmen aus der Wirtschaft), so sind die Vorgaben des Bundesdatenschutzgesetzes ausschlaggebend. Für die öffentlichen Stellen eines Bundeslandes kommt hingegen das jeweilige Landesdatenschutzgesetz zum Einsatz.

Ab ihrem Inkrafttreten im Jahr 2018 wird die Europäische Datenschutzgrundverordnung (EU-DSGVO) die nationalen Datenschutzgesetze überwiegend ersetzen (dabei handelt es sich um einen sog. Anwendungsvorrang: Die EU-DSGVO überlagert in ihrem Anwendungsbereich das nationale Datenschutzrecht, das dann nur dort anwendbar bleibt, wo die EU-DSGVO gerade nicht anwendbar ist, vgl. hierzu Art. 2 f. EU-DSGVO).

Ein auf die Anforderungen von automatisierten Systemen spezialisiertes Datenschutzrecht existiert nicht. Hierbei ist insofern auf die allgemeinen Da-

tenschutzvorschriften des BDSG, der LDSG, der EU-DSGVO oder einer spezialgesetzlichen Regelung zurückzugreifen. Im Vordergrund der folgenden Ausführungen sollen die derzeit für die deutsche Wirtschaft geltenden Bestimmungen des BDSG stehen.

Verbot mit Erlaubnisvorbehalt

§ 4 Abs. 1 BDSG formuliert das sog. Verbot mit Erlaubnisvorbehalt. Demnach ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder aber eine Einwilligung des Betroffenen vorliegt. Insofern bedarf jede datenschutzrechtlich relevante Handlung entweder eines gesetzlichen Rechtfertigungstatbestandes oder aber einer vorherigen Zustimmung.

Datenschutzrechtliche Einwilligung. Hinsichtlich der Einwilligung des Betroffenen ist zu beachten, dass diese stets freiwillig zu erfolgen hat [5]. Umstritten ist daher etwa, ob auch im Rahmen eines Arbeits- und Beschäftigungsverhältnisses eine Einwilligung des Arbeitnehmers in datenschutzrechtliche Eingriffe durch den Arbeitgeber legitim sein kann, da im Rahmen eines Beschäftigungsverhältnisses stets ein Über-/Unterordnungsverhältnis vorliegen wird und daher fraglich ist, ob der Arbeitnehmer hierbei noch „freiwillig" entscheiden kann. Im Ergebnis wird dies stets nur im konkreten Einzelfall zu bestimmen und davon abhängig sein, welche Daten in welchem Umfang betroffen sind und für welchen Zweck diese erhoben werden.

Zudem kann eine Einwilligung nur dann rechtswirksam abgegeben werden, wenn diese auch auf einer informierten Entscheidung des Betroffenen basiert, dieser also in Kenntnis der vollständigen Sachlage einwilligt [5]. Insbesondere ist der Einwilligende daher über die Art, den Umfang und den Nutzungszweck der erhobenen, verarbeiteten oder genutzten Daten in verständlicher Weise zu unterrichten.

Datenschutzrechtliche Erlaubnistatbestände des BDSG. Als datenschutzrechtliche Erlaubnistatbestände kommen für nichtöffentliche Stellen im Rahmen des BDSG die §§ 28 ff. BDSG in Betracht, soweit keine spezialgesetzlichen Erlaubnistatbestände aus anderen Rechtsvorschriften ersichtlich sind. Hierbei ist zuvorderst § 28 BDSG zu nennen, der als allgemeiner Erlaubnistatbestand die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten für bestimmte Zwecke erlaubt.

Für die Zwecke eines Beschäftigungsverhältnisses, also immer dann, wenn personenbezogene Daten für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder für dessen Durchführung oder Beendigung erhoben, verarbeitet oder genutzt werden sollen, ist weiterhin § 32 BDSG zu beachten, der dann dem allgemeineren § 28 BDSG vorgeht.

Werden öffentlich zugängliche Räume mittels optisch-elektronischer Einrichtungen erfasst, kann weiterhin aber auch § 6b BDSG zu beachten sein, der dann wiederum den allgemeineren § 28 und § 32 BDSG vorgeht. Im Rahmen automatisierter Systeme muss eine Anwendung des § 6b BDSG etwa dann diskutiert werden, wenn diese Systeme zur Orientierung im Raum und zum Schutz der sich im Raum befindlichen Personen und Sachen optisch-elektronische Einrichtungen wie etwa Kamerasysteme einsetzen [6]. Für die Anwendung des § 6b BDSG ist jedoch zu beachten, dass hierbei ein „Beobachten" und damit eine längerdauernde Observation vorausgesetzt wird. Das nur kurzzeitige und punktuelle optische Erfassen eines Raumabschnitts fällt demnach nicht unter § 6b BDSG [2], sondern dann weiterhin unter § 28 BDSG. Ob eine solche „Beobachtung" im Sinne der Vorschrift vorliegt, kann erneut nur anhand des konkret verwendeten automatisierten Systems im Einzelfall bestimmt werden.

Da § 4 Abs. 1 BDSG auch „andere Rechtsvorschriften" als statthaft erachtet, können in einem Arbeitsverhältnis etwa auch Betriebsvereinbarungen oder Tarifverträge datenschutzrechtliche Bestimmungen enthalten.

Prinzip der Datenvermeidung und der Datensparsamkeit

Dem deutschen Datenschutzrecht sind die Prinzipien der Datenvermeidung und der Datensparsamkeit immanent. Dies kommt dadurch zum Ausdruck, dass die verschiedenen gesetzlichen Erlaubnistatbestände stets das Kriterium der „Erforderlichkeit" der jeweiligen Datenerhebung, -verarbeitung oder -nutzung fordern, diese also nicht weiter gehen darf, als dies für den konkreten Zweck unumgänglich ist. Die Prinzipien der Datenvermeidung und Datensparsamkeit haben

aber auch explizit Eingang in den Wortlaut des § 3a BDSG gefunden, als hierbei bestimmt wird, dass „die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen […] an dem Ziel auszurichten [sind], so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert".

Für die Ausgestaltung eines automatisierten Systems bedeutet dies, dass bereits von Anfang an im Rahmen der technischen Systemgestaltung der Datenschutz bedacht und integriert werden muss („Privacy by Design"). Die Sensorik eines automatisierten Systems etwa, die für die Lagebestimmung im Raum, für die Erkennung von Hindernissen und für den Schutz der in der Nähe befindlichen Personen oder Sachen zuständig ist, muss insofern so gestaltet werden, dass hierbei nicht unbedacht jede erdenkliche Umgebungsinformation erhoben, verarbeitet oder gespeichert wird. Vielmehr sind die für den Systemablauf notwendigen Informationen präzise und zielgenau zu erheben sowie unwichtige Daten unverzüglich auszufiltern.

Dies kann in einem ersten Schritt etwa dadurch erfolgen, dass der Sensorerfassungsbereich des Systems auf ein notwendiges Minimum beschränkt wird. So bedarf ein stationärer Roboter, der mit seinen Greifarmen nur im Umkreis von zwei Metern hantieren kann, keiner Sensorwerte von in einem weit größeren Umkreis liegenden Bereich des Raumes.

Doch auch innerhalb eines notwendigen Erfassungsradius unterliegt eine Datenerhebung, -verarbeitung und -nutzung engen Grenzen. Benötigt das automatisierte System zur ordnungsgemäßen Operation beispielsweise keinen Personenbezug der erhobenen Daten (bspw. da hierbei die Information ausreicht, dass sich *eine* Person im Erfassungsbereich befindet, aber irrelevant ist, *welche* Person dies ist), so sind die erhobenen Daten unverzüglich zu anonymisieren. Da das BDSG nur bei personenbezogenen oder -beziehbaren Daten Anwendung findet, der Personenbezug eines Datums nach einer stattgefundenen Anonymisierung aber eliminiert wird, ist die weitere Verarbeitung von anonymisierten Daten datenschutzrechtlich unproblematisch.

Neben der Beschränkung des Sensorerfassungsbereichs und der unverzüglichen Anonymisierung der personenbezogenen Daten fordern die Prinzipien der Datenvermeidung und Datensparsamkeit als dritte Stufe weiterhin, dass die dennoch auf dem System verbleibenden personenbezogenen Daten, die gerade nicht ausgefiltert oder anonymisiert werden können (etwa wenn der Personenbezug für die weitere Systemausführung von Relevanz ist), unverzüglich dann gelöscht oder gesperrt werden, wenn diese Daten nicht mehr benötigt werden, sich also der Erhebungszweck erledigt hat.

Anwendungsbeispiele des datenschutzkonformen Einsatzes von automatisierten Systemen

Ebenso wie die zur Gewährleistung von Funktionssicherheit und Informationssicherheit relevanten Maßnahmen stets nur für den konkreten Einzelfall anhand des spezifisch einzusetzenden automatisierten Systems bestimmt werden können, kann auch die datenschutzrechtliche Perspektive nicht für alle automatisierten Systeme pauschalisiert werden. Die Datenschutzkonformität eines automatisierten Systems ist insofern unter anderem abhängig von der konkreten Systemausgestaltung (welche Daten werden zu welchem Zweck für welche Zeitdauer in welchem Umfang erhoben) und dem Einsatzzweck und –ort des Systems (welche persönlichkeitsrechtliche Intensität haben die Daten). Im Folgenden sollen daher zwei konkrete Einsatzszenarien von automatisierten Systemen datenschutzrechtlich besprochen werden. Dabei wird das derzeit noch geltende BDSG zugrunde gelegt.

Beispiel 1: Automatisierte Transportdrohne zur Lieferung von Warensendungen an den Endkunden. Bereits zahlreiche Logistikunternehmen und Warenhäuser planen zukünftig, eilige Warensendungen auch per automatisierter Transportdrohne an den Endkunden zu liefern. Laut einer aktuellen Studie der Bitkom wäre hierzu auch jeder dritte Verbraucher bereits bereit. Jeder fünfte Befragte würde sich zu diesem Zweck gar eine spezielle Paketbox einrichten [1].

Nicht verwunderlich ist daher, dass auch der DHL-Konzern bereits mehrere Drohnenmodelle erfolgreich getestet hat. Hierzu wurden zunächst

Medikamente testweise vom deutschen Festland auf die Nordseeinsel Juist geflogen. In einem anschließenden Projekt wurden sodann Pakete von der Talstation bei Reit im Winkl zu einer Bergalm transportiert. Insbesondere in ebensolchen Einsatzszenarien, also dann, wenn unwegsames Gelände oder Wasser überbrückt werden soll, zeigen sich die Vorteile des Transports per Drohne.

Doch auch der gewöhnliche Verbraucher soll zukünftig per Drohne beliefert werden. So plant das Online-Warenhaus Amazon, Bestellungen mittels seines „Amazon Prime Air"-Dienstes künftig innerhalb von 30 Minuten an den Kunden zuzustellen. Notwendig ist hierzu bislang naturgemäß das Vorhandensein einer geeigneten Freifläche, auf der die Drohne das bestellte Paket ablegen kann (meist der eigene Garten). Auf dieser Fläche wird von dem Besteller ein Schild ausgelegt, welches die Drohne aus der Luft erkennen und zielgenau ansteuern kann.

Datenschutzrechtliche Relevanz entfaltet dieser erste Anwendungsfall insofern, als die Transportdrohne zum einen zahlreicher Empfängerinformationen bedarf, um das zu transportierende Paket zustellen zu können. Diese personenbezogenen Daten (etwa Name, Anschrift, ggf. Telefonnummer, Inhalt der Sendung, Sendungsnummer, Gefahrendeklaration der Sendung, Versenderinformationen) werden entweder auf der Drohne selbst gespeichert oder aber aus einer „Speditionscloud" abgerufen. Zum anderen aber muss die Transportdrohne selbst zahlreiche Umgebungsinformationen erheben und verarbeiten, um sich im Luftraum orientieren, Straßen und Häuser erkennen und auf Hindernisse (Personen oder Gegenstände) adäquat reagieren zu können. Die Drohne muss weiterhin das Zielterrain scannen, um (etwa im Falle von Amazon Prime Air) das im Garten aufgestellte Anflugschild oder aber eine spezielle Paketbox auffinden und identifizieren zu können. Diese erhobenen Umgebungs- und Bodeninformationen enthalten mitunter personenbezogene oder –beziehbare Daten, insbesondere etwa dann, wenn private Grundstücke überflogen werden oder sich Passanten im Erfassungsbereich der optisch-elektronischen Einrichtungen befinden.

Jedenfalls hinsichtlich der Empfängerinformationen, die entweder unmittelbar auf der Drohne gespeichert, verarbeitet oder genutzt oder aber aus der „Speditionscloud" abgerufen und anschließend verarbeitet oder genutzt werden, kommt noch eine *Einwilligung* des Bestellers in Betracht, welcher diese etwa während des Bestellvorgangs erteilen kann. Etwas anderes gilt jedoch hinsichtlich der personenbezogenen Umgebungsdaten, die bei dem Transport der Ware an den Besteller anfallen. Denn eine datenschutzrechtliche Einwilligung nach dem BDSG erfordert grundsätzlich eine *vorherige* Zustimmung des Betroffenen. Eine solche ist bei willkürlichen Passanten aber erstens deshalb nicht einholbar, da vor der konkreten Paketzustellung regelmäßig nicht bekannt sein wird, welche Personen sich in dem betroffenen Flugkorridor befinden werden. Zweitens sind die betroffenen Passanten dem Speditionsunternehmen aber auch unbekannt, sodass dieser schon mangels Kontaktinformationen keine Einwilligung einholen kann. Drittens wäre ein solches Vorgehen selbstverständlich aber auch vollkommen unpraktikabel und daher bereits aus diesem Grund auszuschließen. Falsch wäre es in diesem Kontext aber auch, davon auszugehen, eine konkludente Einwilligung der Passanten läge dann vor, wenn diese wissentlich (etwa da diese durch entsprechende Hinweisschilder auf den Umstand hingewiesen werden) Gebiete betreten, die von datenerhebenden Drohnen überflogen werden. Denn das für die Wirksamkeit einer Einwilligung notwendige Kriterium der Freiwilligkeit ist dann nicht gegeben, wenn für den Einwilligenden ein faktischer Zwang entsteht. Ein solcher wird regelmäßig aber dann vorliegen, wenn der Passant durch die Nichteinwilligung ein bestimmtes öffentliches Gelände nicht mehr betreten dürfte [2].

Da die Erhebung und Verarbeitung der Umgebungs- und Passantendaten keinen Zwecken eines Beschäftigungsverhältnisses dient, scheidet in diesem Fall § 32 BDSG als *gesetzlicher Rechtfertigungstatbestand* aus. Fraglich ist bei der Suche nach einem einschlägigen Erlaubnistatbestand dann nur, ob hierbei auf § 6b BDSG oder auf den allgemeinen § 28 BDSG abgestellt werden muss. § 6b BDSG ist im Rahmen einer Videoüberwachung mittels optisch-elektronischer Einrichtungen grundsätzlich spezieller und daher dem § 28 BDSG vorzuziehen. Doch findet dieser Erlaubnistatbestand nur dann Anwendung, wenn hierbei eine „Beobachtung", also eine nicht nur ganz kurzzeitige Observation, vorliegt [6]. Wird das zu überfliegende Terrain von der Drohne insofern nur ganz kurzzeitig erfasst und werden die Daten umgehend ausgewertet und anschließend wieder gelöscht, könnte die Anwen-

dung des § 6b BDSG ausgeschlossen und auf § 28 BDSG zurückzugreifen sein. Dies ist abhängig von der konkreten Systemausgestaltung, also davon, wie lange die Drohne ein zu überfliegendes Terrain „im Auge behält". Im Ergebnis kann dies vorliegend aber dahingestellt bleiben, da sich die datenschutzrechtliche Zulässigkeit sowohl bei § 6b Abs. 1 Nr. 3 BDSG als auch bei § 28 Abs. 1 Nr. 2 BDSG danach bestimmt, ob der Datenumgang für die *Wahrung der berechtigten Interessen* der verantwortlichen Stelle *erforderlich* ist und kein Grund zu der Annahme besteht, dass *schutzwürdige Interessen des Betroffenen* überwiegen. In beiden Fällen ist zudem *der Zweck des Datenumgangs konkret festzulegen*.

Das Tatbestandskriterium der *berechtigten Interessen* umfasst dabei grundsätzlich jedes tatsächliche Interesse wirtschaftlicher oder ideeller Natur [2] und damit auch eigene Geschäftszwecke. Mit der geschäftsmäßigen Beförderung einer bestellten Ware an den Endverbraucher liegt ein solches berechtigtes Interesse im Sinne der Tatbestandsnorm vor. Im Rahmen des zusätzlich zu beachtenden Tatbestandskriteriums der *schutzwürdigen Interessen* der Betroffenen ist dieses berechtigte Interesse der datenschutzrechtlich verantwortlichen Stelle (Speditionsunternehmen) sodann mit den Interessen des Betroffenen (Passant) abzuwägen. Die Interessen des Betroffenen wiegen dabei umso höher, je größer der datenschutzrechtliche Eingriff ist. Es liegt dabei in der Hand des Speditionsunternehmens, diesen Eingriff so schonend wie möglich auszugestalten: So ist die einzusetzende Transportdrohne bereits im Rahmen der Systementwicklung bestmöglich datenschutzkonform auszugestalten („Privacy by Design"). Dies betrifft unter anderem die zwingende Einhaltung der Grundsätze zur Datenvermeidung und zur Datensparsamkeit und insofern die Beschränkung der Datenerhebung, -verarbeitung und -nutzung auf ein unumgängliches Mindestmaß. Schließlich erfordern die datenschutzrechtlichen Erlaubnistatbestände auch, dass der *Zweck des Datenumgangs konkret festgelegt* wird. Dies entspricht dem datenschutzrechtlichen sog. Zweckbindungsgrundsatz, wonach für einen bestimmten Verwendungszweck erhobene Daten nur zu diesem Zweck verarbeitet und genutzt werden dürfen.

Beispiel 2: Automatisierter Gesundheitsroboter zur Betreuung von Pflegebedürftigen in deren Zuhause. Auch im Gesundheits- und Pflegewesen befinden sich automatisierte Systeme in der Entwicklung. Zwar ist zweifelhaft, ob solche Pflegeroboter jemals dieselbe Sensibilität und Fachkunde wie menschliche Pflegekräfte aufweisen können werden (auch da zur Betreuung und Pflege von Bedürftigen eine Vielzahl an unterschiedlichen Handlungen vorzunehmen sind und diese auch je nach Patient variieren, also nicht pauschal vorprogrammiert werden können). Dennoch werden automatisierte Dienstleistungsroboter zukünftig menschliche Pflegekräfte jedenfalls unterstützen können.

Dabei sind verschiedene Formen des Einsatzes von Gesundheits-/Pflegerobotern im Zuhause des Pflegebedürftigen denkbar: So könnte der Roboter von dem Pflegebedürftigen zunächst auch selbst erworben und betrieben werden, ohne dass hierbei noch andere Stellen involviert wären. Berücksichtigt man jedoch, dass solche Systeme äußerst kostspielig sind und zudem auch einer permanenten fachgerechten Wartung und Aktualisierung bedürfen, werden sich hierbei vielmehr Kooperationsmodelle mit privaten Pflegediensten etablieren, welche im Rahmen von Pflegedienstleistungsverträgen automatisierte Gesundheitsroboter beim Patienten einsetzen werden.

Datenschutzrechtliche Relevanz entfaltet dieses zweite Anwendungsbeispiel insofern, als automatisierte Dienstleistungsroboter zu ihrem Einsatz im Gesundheitswesen zahlreicher personenbezogener Daten über den Patienten selbst (etwa Name, Alter, Krankheitsbild) und dessen Umfeld (etwa über sein Zuhause/Zimmer sowie über andere im Haushalt lebende Personen) bedürfen, um die jeweilige Pflegeleistung ordnungsgemäß ausführen zu können. Im obigen Anwendungsszenario, bei dem ein automatisierter Gesundheitsroboter von einem privaten Pflegedienst eingesetzt wird, wäre ebendieser Pflegedienst *verantwortliche Stelle* im Sinne des Datenschutzrechts. Dabei ist zu beachten, dass für den Einsatz von IT-Systemen im Gesundheitswesen grundsätzlich mehrere Datenschutzvorschriften in Betracht kommen können und nicht automatisch auf das BDSG abgestellt werden darf. So ist ein datenschutzrelevantes Handeln einer Krankenkasse etwa nach dem Sozialgesetzbuch (hier: SGB V) zu beurteilen. Erhebt, verarbeitet oder nutzt ein öffentliches Krankenhaus personenbezogene Daten, kann dagegen auch das jeweilige Landesdatenschutzgesetz (LDSG) einschlägig sein, wenn es sich dabei um ein Krankenhaus eines Bundeslandes handelt.

Da im vorliegenden Sachverhalt aber ein privater Dienstleister und mithin eine nichtöffentliche Stelle handelt, ist hierbei weiterhin auf das BDSG zurückzugreifen. Welche datenschutzrechtlich relevanten Vorgänge dabei stattfinden, ist erneut von der konkreten Systemausgestaltung abhängig. So ist etwa denkbar, dass die von dem automatisierten System erhobenen Daten lediglich in dem System selbst verarbeitet werden. Andererseits kommt aber auch eine Übermittlung der Daten an den Pflegedienst oder an von diesem beauftragte IT-Dienstleister (sog. Auftragsdatenverarbeitung) mit anschließender Datenverarbeitung in Frage („Gesundheitscloud").

Auch im Rahmen dieses Anwendungsfalles kommt zunächst eine *Einwilligung* des Patienten gegenüber dem privaten Pflegedienst in Betracht. Neben den gewöhnlichen Einwilligungsvoraussetzungen (Freiwilligkeit, Informiertheit, Bestimmtheit) ist hierbei zusätzlich § 4a Abs. 3 BDSG zu beachten. Dieser bestimmt, dass beim Vorliegen von besonderen Arten personenbezogener Daten die Einwilligung ausdrücklich auf diese Daten bezogen sein muss. Im Ergebnis bedeutet dies, dass hierbei erhöhte Anforderungen an die Bestimmtheit und an die Genauigkeit der datenschutzrechtlichen Einwilligung zu stellen sind und auch nur eine ausdrückliche Einwilligung des Patienten in Betracht kommt [5]. Gerade bei Pflegebedürftigen ist aber zudem zu beachten, dass zur Erzielung einer rechtswirksamen Einwilligung der Patient auch einwilligungsfähig, also imstande sein muss, die Tragweite seiner Entscheidung zu erkennen [4]. Hinsichtlich der im Umfeld des Patienten befindlichen Personen kommt eine datenschutzrechtliche Einwilligung gegenüber dem Pflegedienst jedenfalls für die dauerhaft im Zuhause des Patienten lebenden Personen in Betracht (etwa Ehepartner oder Kinder). Erhebt das automatisierte System aber auch von Besuchern (etwa Freunden, Handwerkern u. a.) personenbezogene Daten, wird eine Einwilligung hierbei aus Praktikabilitätsgründen ausgeschlossen und nach einem einschlägigen gesetzlichen Erlaubnistatbestand zu suchen sein.

Im Rahmen eines *gesetzlichen Erlaubnistatbestandes* ist erneut § 28 BDSG heranzuziehen, da in diesem Anwendungsszenario weder ein Beschäftigungsverhältnis nach § 32 BDSG (der private Pflegedienst steht in keinem Arbeitnehmerverhältnis zu dem Patienten), noch ein öffentlicher Raum nach § 6b BDSG vorliegt. Da im Falle eines Pflege-/Gesundheitsroboters unter anderem auch Gesundheitsdaten und damit „besondere Arten personenbezogener Daten" nach § 3 Abs. 9 BDSG erhoben und verarbeitet werden, sind im Verhältnis zu dem Patienten die Spezialbestimmungen der § 28 Abs. 6-9 BDSG zu beachten, die gegenüber dem Abs. 1 der Vorschrift strengere Regelungen enthalten. Insbesondere kann dabei nach § 28 Abs. 7 Satz 1 BDSG eine Erhebung, Verarbeitung oder Nutzung von besonderen Arten personenbezogener Daten dann gerechtfertigt sein, „wenn dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch *sonstige Personen* erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen". Weiterhin kann nach § 28 Abs. 7 Satz 3 BDSG eine Datenerhebung, -verarbeitung oder –nutzung besonderer Arten personenbezogener Daten unter gewissen Voraussetzungen aber auch durch *Angehörige eines anderen Berufes* erfolgen, „dessen Ausübung die Feststellung, Heilung oder Linderung von Krankheiten oder die Herstellung oder den Vertrieb von Hilfsmitteln mit sich bringt". Ob die Voraussetzungen der gesetzlichen Rechtfertigungstatbestände erfüllt sind, kann im Rahmen dieser Ausführungen weder pauschal bejaht, noch verneint werden. Vielmehr erfordert dies eine präzise Prüfung im konkreten Einzelfall und ist mitunter abhängig von dem konkreten Einsatzzweck des automatisierten Systems und von der organisatorischen Ausgestaltung des privaten Pflegedienstes.

Gegenüber anderen im Umfeld des Patienten befindlichen Personen kann dagegen erneut auf § 28 Abs. 1 Nr. 2 BDSG zurückgegriffen werden, da Gesundheitsdaten und mithin besondere Arten personenbezogener Daten nur von dem Patienten, nicht aber von Dritten erhoben werden.

Fazit und Ausblick

Automatisierte Systeme werden schon in naher Zukunft unseren Himmel, unsere Straßen, unsere Industrie und Wirtschaft sowie unsere Wohnungen bevölkern und uns minutenschnell mit bestellter Ware beliefern, uns zu einem Ziel befördern während wir schlafen und unseren Alltag zuhause in allen Facetten erleichtern. In der Industrie 4.0 werden gar unsere automatisierten

Produkte automatisiert erschaffen werden und auch im Dienstleistungssektor werden wir zukünftig vermehrt Roboter antreffen.

Neben all den Chancen und Erleichterungen, die sich durch die Automatisierung ergeben werden, werden diese technischen Neuerungen jedoch auch neuartige Gefährdungen mit sich bringen, die zu Personenverletzungen, Sachbeschädigungen, Datenpannen und generell zu Kontrollverlust führen können. Diese Gefährdungen stellen jedoch kein spezifisches Phänomen der Automatisierung dar. Vielmehr haftet jeder technischen Neuerung stets auch ein Risiko an.

Dabei liegt es an uns, diesen Gefährdungen durch eine sichere und rechtskonforme Technikgestaltung entgegenzuwirken. Gefordert sind dabei nicht nur die Hersteller automatisierter Systeme. Die Automatisierung von bislang menschlich durchgeführten Arbeiten wird vielmehr auch eine gesellschaftliche und gesetzgeberische Herausforderung sein. Anstatt der technischen Entwicklung hinterherzusehen, sind insofern bereits heute die notwendigen Weichenstellungen zu treffen, um diese Herausforderungen für die Zukunft zu meistern.

Literatur

1. Bitkom (2016) Drohnen und Roboter sind die Paketboten der Zukunft. https://www.bitkom.org/Presse/Presseinformation/Drohnen-und-Roboter-sind-die-Paketboten-der-Zukunft.html, letzter Zugriff: 5.4.2017
2. Brink S (2016) § 6b BDSG. In: Wolff/Brink (Hrsg) Beck'scher Online-Kommentar Datenschutzrecht. C.H. Beck, München
3. Eckert C (2014) IT-Sicherheit. Oldenbourg, München
4. Franzen M (2017) § 4a BDSG. In: Erfurter Kommentar zum Arbeitsrecht. C.H. Beck, München
5. Kühling J (2016) § 4a BDSG. In: Wolff/Brink (Hrsg) Beck'scher Online-Kommentar Datenschutzrecht. C.H. Beck, München
6. Schmid A (2015) Rechtliche Bewertung ziviler Drohnenflüge. K&R, S 217–222