Digitalisierung

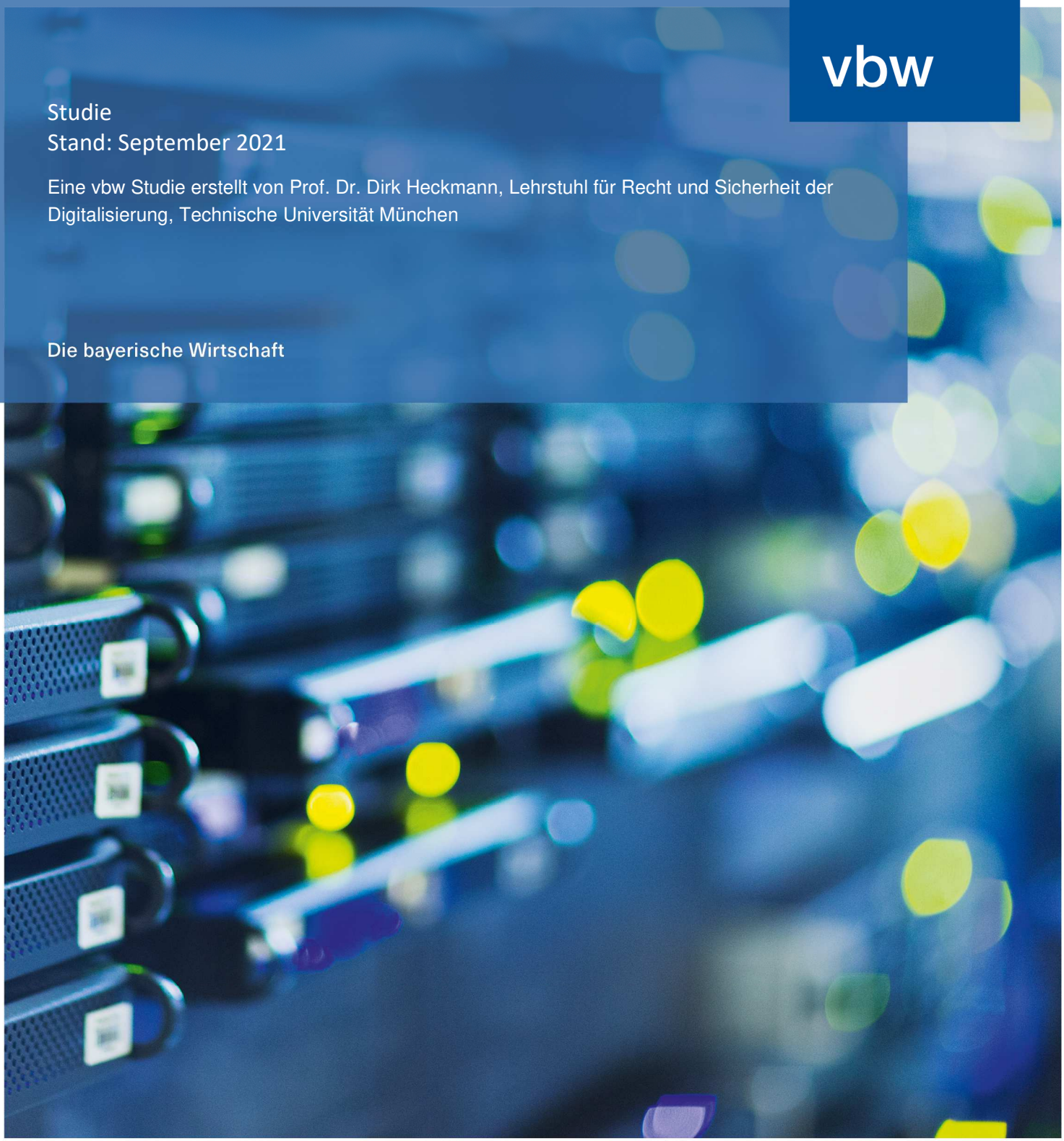
Datenschutz, IT-Sicherheit und Haftung bei automatisierten Systemen

vbw

Studie
Stand: September 2021

Eine vbw Studie erstellt von Prof. Dr. Dirk Heckmann, Lehrstuhl für Recht und Sicherheit der Digitalisierung, Technische Universität München

Die bayerische Wirtschaft



Vorwort

Intelligenter Rechtsrahmen für intelligente Systeme

Automatisierte Systeme sind seit vielen Jahren Standard in der Industrie. Seit sie neue Anwendungsbereiche erschließen und in das Blickfeld von Verbrauchern rücken, sind sie auch in den Fokus des Gesetzgebers geraten. Das autonome Fahren ist ein prominentes Beispiel, zumal die Technologie für Bayern und Deutschland – als Automobilstandorte – besonders relevant ist.

Klar ist, dass jedes automatisierte System datenschutzkonform zu betreiben ist, die Anforderungen der IT-Sicherheit zu wahren hat und im Falle eines Schadensereignisses auch die Haftung geklärt sein muss. Die meisten Fragen lassen sich allerdings auf Basis des geltenden Rechts gut beantworten. Unsere Studie zeigt auf, wie vielfältig heute schon die Rechtsquellen sind, die automatisierte Systeme erfassen, und was es grundsätzlich bei ihrem Einsatz zu beachten gilt.

Vor jeder neuen Regelung muss sich der Gesetzgeber fragen, ob tatsächlich noch eine Lücke besteht und ein Bedarf zu decken ist. Angesichts der enormen Potenziale haben wir ein vitales Interesse daran, innovationsfreundlich zu agieren. Im Zweifel sind Mut zum Experiment und Chancenorientierung gefragt. Das gilt ganz besonders für den Bereich der Künstlichen Intelligenz, wo der europäische Gesetzgeber aktuell über das Ziel hinauszuschießen droht.

Bertram Brossardt
02. September 2021

Inhalt

1 Das Wichtigste auf einen Blick

Automatisierte Systeme erfordern Nachdenken, selten aber Umdenken.

Automatisierte Systeme gehören zu den längst etablierten, unverzichtbaren Bestandteilen der Industrialisierung und halten in einer zunehmend digitalisierten und vernetzten Welt auch Einzug in alle Lebensbereiche. Die Automatisierung an sich sorgt durch selbsttätige Abläufe für effiziente, zeit- und kostensparende Prozesse – bis hin zu autonomen Systemen, die unabhängig von menschlicher Steuerung und Überwachung agieren. In Verbindung mit smarten Maschinen, den Errungenschaften der Robotik und vor allem der Möglichkeit maschinellen Lernens wird nunmehr ein Automatisierungsgrad erreicht, der je nach Kontext als hocheffizient, komfortabel oder ressourcenschonend wahrgenommen und wertgeschätzt wird. In Verbindung mit dem Einsatz Künstlicher Intelligenz lassen sich ganze Lebens- und Arbeitsbereiche neu gestalten (Smart Home, Smart City, Smart Factory und anderes mehr).

So sehr technologische Innovationen diese Entwicklung befördern, so unübersehbar die Nachfrage nach automatisierten Systemen (von autonomen Fahrzeugen oder Drohnen über Roboter bis zu KI-gestützten Fertigungsprozessen, also sowohl im Hard- als auch im Softwarebereich) ist und so evolutionär diese Entwicklungslinien sind: Sie betreffen zugleich eine Vielzahl durch sie berührter Interessen und bedürfen deshalb auch einer rechtlichen Betrachtung. Dabei soll, kann und darf das Recht die soziotechnische Weiterentwicklung nicht verhindern. Es ist vielmehr seine Aufgabe, eine maßvolle Interessenabwägung zu initiieren und bestimmte, potenziell gefährliche Entwicklungen zu kanalisieren.

Maßgeblich hierfür ist besonders das Datenschutzrecht und das IT-Sicherheitsrecht, weil mit automatisierten Systemen vielfach eine Datenverarbeitung einhergeht, für die Erlaubnistatbestände zu finden sind, soweit es um personenbezogene Daten geht, was nicht bei allen systemseitig benötigten Daten der Fall ist. Besonderer Wert ist außerdem auf die Funktionsfähigkeit, Verfügbarkeit und Integrität solcher Systeme zu legen. Für all dies wurden in den letzten Jahren zahlreiche Regelwerke auf europäischer und nationaler Ebene geschaffen (zum Beispiel die DSGVO, das IT-Sicherheitsgesetz, die EU-Drohnenverordnung. Das Gesetz zum autonomen Fahren, Novellen zum Produkthaftungsrecht und andere mehr), die dem Einsatz automatisierter Systeme keineswegs entgegenstehen, sondern für Rechts- und Betriebssicherheit sorgen sollen. Daneben ist auf Branchenstandards wie etwa IT-Sicherheitsstandards hinzuweisen, die detailliert Beschaffenheit und Betrieb regeln.

Gleichwohl können es Schadensfälle durch Funktionsmängel, Systemangriffe oder Unglücksfälle auftreten, die Haftungsfragen aufwerfen. Auch wenn es gesetzliche Anspruchsgrundlagen gibt, ist die wichtigste Handlungsempfehlung an Unternehmen für den Einsatz automatisierter Systeme, die wesentlichen Gefahrenszenarien vorauszudenken und besonders durch vertragliche Vereinbarungen mit Herstellern und Dienstleistern sowohl die Sorgfaltspflichten und Produkteigenschaften als auch die Verantwortlichkeiten so zu regeln, dass die Haftungsverteilung fair und angemessen ist.

2 Einführung

Begriffsbestimmungen, Status Quo und weitere Entwicklungsschritte

Automatisierte Systeme sind aus unserem Alltag schon heute nicht mehr wegzudenken. So sind etwa unsere Autos bereits imstande, hochautomatisierte Fahrfunktionen auszuführen und auch automatisierte Lieferdrohnen befinden sich bereits in der Test- und Erprobungsphase, teilweise sogar schon im Praxiseinsatz. Unser Zuhause wird mit dem Einsatz intelligenter Gebäudetechnik zunehmend „smart“ und automatisiert. Zukünftig werden wir insbesondere auch im privaten Bereich sowie im Dienstleistungssektor vermehrt intelligente und automatisierte Systeme antreffen, die uns etwa in Geschäften beraten oder uns im Haushalt aushelfen können. So erfreuen sich Saug- und Mähroboter längst großer Beliebtheit und erscheint die Vernetzung im Haushalt dank intelligenter Technologien auch für technische Laien attraktiv. Sprachassistenzsysteme dienen hier oft als Brückentechnologie.

Die Kehrseite dieser Automatisierung ist jedoch die Sorge vor neuartigen Gefährdungen, denen durch eine rechtskonforme und sichere Technikgestaltung entgegengewirkt werden muss. Dies betrifft zum einen die Gewährleistung von Funktions- und Informationssicherheit. Zum anderen ist bei der Entwicklung von automatisierten Systemen stets das geltende Datenschutzrecht zu beachten. Wird durch ein automatisiertes System eine Person verletzt oder eine fremde Sache beschädigt, stellt sich weiterhin auch hierbei stets die Haftungs-frage, die durch den Einsatz von automatisierten Systemen eine neue Dimension erhält. Dies nicht zuletzt deshalb, weil ein „selbständiges“ Agieren einer Maschine die Frage der Zurechnung aufwirft. Verlagert sich die Haftung von der unmittelbaren Schadensverursachung auf die dieser vorgelagerten Programmierung der Maschine? Brauchen wir gar eine neue Kategorie wie jene der E-Person?

Diese juristische Studie widmet sich der IT-sicherheitsrechtlichen, datenschutzrechtlichen und haftungsrechtlichen Perspektive des Einsatzes automatisierter Systeme. Behandelt werden nicht nur automatisierte Straßen- und Luftfahrzeuge, sondern darüber hinaus auch automatisierte Industrie- und Dienstleistungsroboter und mithin eine Vielzahl verschiedener automatisierter Systeme.

2.1 Begriffsbestimmungen

Im Rahmen der Automatisierung und Smartifizierung werden verschiedene Begrifflichkeiten verwendet, die zunächst definiert werden müssen.

2.1.1 Automatisierung, Autonomie

Zunächst wird hierunter klassischerweise die Übertragung einzelner Aufgaben vom Menschen auf einzelne künstliche Systeme (beispielsweise auf einen Industrieroboter) verstanden. Dieser Automatisierungsbegriff muss je nach Automatisierungsgrad weiter unterteilt werden. Häufig anzutreffende Begrifflichkeiten sind dabei etwa die Teilautomatisierung, die Hochautomatisierung oder die Vollautomatisierung (vergleiche hierzu noch Kapitel 2.2). Daneben existiert als Vorstufe noch das sogenannte Assistenzsystem und als höchste Form der Automatisierung die sogenannte Autonomie.

Autonomie beschreibt je nach Art und Typ des Systems eine vollständige Kontrollübernahme durch eine künstliche Intelligenz beziehungsweise (bei einfacher Befehlsfolge) einen Algorithmus. Ein autonomes System bedarf insofern in keiner Situation einer menschlichen Steuerung mehr. Bei einem autonomen Fahrzeug etwa ist ein Fahrzeugführer als solcher daher nicht mehr notwendig. Jeder Insasse des Fahrzeugs wird zum Passagier.

Neben diesem komponentenbezogenen Verständnis von Automatisierung, das den Grad an Verselbstständigung einzelner IT-Systeme / -Komponenten oder Maschinerie beschreibt, wird auch im Kontext der sogenannten „Industrie 4.0“ häufig insoweit von einer Automatisierung gesprochen, die sogenannte „Smart Factories“ ermöglichen soll, in denen gesamte Produktionszyklen automatisiert ablaufen können. Die Industrie 4.0 stellt jedoch keine vertikale Erweiterung der Automatisierungsstufen (über die Stufe der Autonomie hinaus), sondern vielmehr eine horizontale Vernetzung der automatisierten Einzelsysteme dar.

2.1.2 Algorithmen, Künstliche Intelligenz und Machine Learning

Künstliche Intelligenz (KI) beschreibt die Automatisierung intelligenten Verhaltens; hierzu zählt beispielsweise die Fähigkeit eines IT-Systems, aus rohen Sensordaten sinnvolle Informationen zu gewinnen und hierdurch selbstständig Rückschlüsse zu ziehen, die dann Auswirkung auf die weitere Programmausführung haben. Im Unterschied zu einfachen Algorithmen beziehungsweise algorithmischen Systemen geht es beim Einsatz von KI um mehr als nur eine Abfolge aus (vor-)programmierten Befehlen. Man kann das mit einer Suchmaschine verdeutlichen: So lange sich diese auf das Auffinden von katalogisierten und kategorisierten Treffern beschränkt, hat dies nichts mit KI zu tun. Von Künstlicher Intelligenz kann man aber dann sprechen, wenn die Maschine das Suchverhalten eigenständig analysiert, Vorschläge priorisiert und Muster erkennt, die sie in Suchprofilen abbildet.

Künstliche Intelligenz kann von einem IT-System etwa genutzt werden, um aus mehreren möglichen Handlungsalternativen die geeignetste und sinnvollste Option selbstständig auszuwählen (beispielsweise: Berechnung der optimalen Ausweichroute bei der Erkennung eines Hindernisses durch eine Flugdrohne). Ein Teilbereich der künstlichen Intelligenz ist dabei das sogenannte „Machine Learning“, bei der das IT-System per Beobachtung oder per „trial-and-error“-Verfahren die in einer spezifischen Situation am besten geeignete Handlungsalternative für die Zukunft erlernen kann. Durch die zusätzliche Vernetzung der

einzelnen selbstlernenden IT-Systeme kann zudem eine sogenannte „Schwarmintelligenz“ gebildet werden.

Der Einsatz von künstlicher Intelligenz ist auf jeder Automatisierungsstufe möglich. Mit zunehmendem Automatisierungsgrad steigt dabei die Notwendigkeit des Einsatzes höher entwickelter Formen von künstlicher Intelligenz.[1]

2.2 Entwicklung einer allgemeinen Abstufungslehre für automatisierte Systeme

Es wurde bereits gezeigt, dass der Automatisierungsbegriff eine weitere Unterteilung je nach Ausprägung und Grad der Automatisierung erfahren muss. Hinsichtlich automatisierter und autonomer Straßenfahrzeuge existiert hierzu eine Stufenlehre, die den Automatisierungsgrad in fünf Stufen unterteilt,[2] wobei mit steigendem Automatisierungsgrad eine zunehmende Steuerungsübernahme durch das System (technisches Können) und mithin die Möglichkeit des Fahrzeugführers, die eigene Fahrzeugkontrolle abzugeben (rechtliches Dürfen), verbunden ist. Die auf einer spezifischen Automatisierungsstufe von dem System nicht übernommenen Steuerungsarten verbleiben dagegen bei dem Fahrzeugführer, die dieser insofern weiterhin aktiv auszuführen und zu kontrollieren hat. Die verschiedenen Automatisierungsstufen sind dabei die *Assistenz*, die *Teilautomatisierung*, die *Hochautomatisierung*, die *Vollautomatisierung* und die *Autonomie*.

[1] Näher hierzu das vbw-Positionspapier Künstliche Intelligenz, Januar 2019: https://www.vbw-bayern.de/Redaktion/Frei-zugaengliche-Medien/Abteilungen-GS/Wirtschaftspolitik/2019/Downloads/Position-KI-Januar-2019_kurz_final.pdf.
[2] Dagegen enthält die DIN-Norm 19233 etwa lediglich eine Unterscheidung der Stufen „Vollautomatisierung“ und „Teilautomatisierung“.

Abbildung 1
Stufen des automatisierten Fahrens[3]

* spezifischer Anwendungsfall je nach Straßentyp, Geschwindigkeitsbereich oder Umfeldbedingungen
Quelle: bayme vbm vbw 2018

Fraglich ist, ob diese Kfz-spezifischen Automatisierungsstufen[4] nun allgemein auf alle automatisierten IT-Systeme übertragen werden können. Um obige Abstufungslehre daher auf alle automatisierten Systeme anwenden zu können, ist insofern eine Abstraktion dieses Schemas notwendig. Diese könnte folgendermaßen formuliert werden:

Stufe 1 (assistiert)

Das System ist imstande, den Menschen bei der Durchführung seiner Aufgabe zu unterstützen. Das System ist jedoch nicht imstande, die gesamte Aufgabe selbstständig auszuführen, sondern nimmt dem Menschen lediglich eine Teilaufgabe ab. Das assistierte System ist stets von einer zusätzlichen menschlichen Steuerung und Führung abhängig.
Beispiel: Sogenanntes „Exoskelett“ zur Unterstützung bei Trag- und Hebearbeiten im Gewerbe oder zur Anwendung bei querschnittsgelähmten Menschen.

Stufe 2 (teilautomatisiert)

Das System ist imstande, in *spezifischen* Situationen die zugewiesene Aufgabe selbstständig zu übernehmen. Das System muss dabei aber durchgehend überwacht werden. Notfalls muss von der beaufsichtigenden Person unverzüglich eingegriffen werden.
Beispiel: Einsatz von Fließbändern in der Industrie, gegebenenfalls mit automatisierter Geschwindigkeitsregelung, ohne eigene Fehlererkennungsmechanismen.

[3] Vgl. auch die Darstellung unter https://www.bast.de/BASt_2017/DE/Presse/Mitteilungen/2021/06-2021.html.
[4] In einem neuen Modell zum automatisierten/autonomen Fahren spricht man bei Level 1 und 2 auch von „Fahrerassistenz“, bei Level 3 und 4 von „Fahrerbasierter Automatisierung“ und bei Level 4 und 5 von „Betreiberbasierter Automatisierung“.

Stufe 3 (hochautomatisiert)

Das System ist imstande, in *spezifischen* Situationen die zugewiesene Aufgabe selbstständig zu übernehmen. Das System muss nicht durchgehend überwacht werden. Im Bedarfsfall, wenn das System ein Problem erkennt oder ein Fehler auftritt, kann eine menschliche Steuerungsübernahme oder ein regulierender Eingriff notwendig werden. Der Eingriff muss nicht unverzüglich, aber alsbald erfolgen. Das System geht zwischenzeitlich in einen Wartezustand über (sogenannter risikominimaler Zustand[5], der ab Stufe 3 auch Formen höherer Automatisierung dahingehend kennzeichnet, dass die Systemgrenzen vom System selbst erkannt werden, wodurch auch das Sicherheitsniveau solcher Systeme gesteigert und den Bedürfnissen im Praxiseinsatz gerecht wird).
Beispiel: Einsatz fortgeschrittener Industrieroboter mit zahlreichen Sensoren und Fehlererkennungsmechanismen sowie automatisierter Stoppfunktion bei unklaren Gefahrenlagen.

Stufe 4 (vollautomatisiert)

Das System ist imstande, in *spezifischen* Situationen die zugewiesene Aufgabe selbstständig zu übernehmen. Das System muss nicht überwacht werden. Ein menschlicher Eingriff ist im Rahmen der Leistungsgrenzen auch beim Vorliegen eines erkannten Problems oder eines Fehlers nicht mehr notwendig, da das System imstande ist, dieses selbstständig zu umgehen oder zu beseitigen.
Beispiel: Einsatz hochentwickelter Fertigungssysteme in der Industrie, die mittels zahlreicher Sensorik und intelligenter Fehlererkennungsmechanismen abnormale Zustände (etwa defektes / verrutschtes Transportgut) erkennen und diese in bestimmten Fällen durch den Einsatz von Fehlerbeseitigungsmechanismen selbstständig bereinigen können (etwa durch Aussonderung / Neuanordnung des defekten / verrutschten Transportguts).

Stufe 5 (autonom)

Das System ist imstande, in *allen* Situationen die zugewiesene Aufgabe selbstständig zu übernehmen. Das System muss weder überwacht werden, noch wird ein menschlicher Eingriff notwendig, da das System fähig ist, Fehler und Probleme selbstständig zu umgehen oder zu beseitigen.
Beispiel: Einsatz komplexer Fertigungsanlagen, die durch den Einsatz intelligenter Fehlererkennungsmechanismen und zahlreicher Fehlerbeseitigungsmechanismen imstande sind, jegliche auftretenden abnormalen Zustände zu erkennen und zu beseitigen.

2.3 Der Entwicklungsstand automatisierter Systeme

Im Industrie- und Dienstleistungsbereich finden bereits heute schon zahlreiche unterschiedliche automatisierte Systeme Anwendung. Dieser Entwicklungsstand soll im Folgenden zunächst überblicksmäßig und dann an den konkreten Beispielen automatisiertes Straßenfahrzeug und automatisiertes Luftfahrzeug dargestellt werden.

[5] Nunmehr für das automatisierte Fahren von Kraftfahrzeugen geregelt in § 1d Abs. 4 StVG-neu, hierzu unten ###.

2.3.1 Die Automatisierung in der Industrie

2.3.1.1 Von der Industrie 1.0 zur Industrie 4.0

Die Automatisierung von Arbeitsvorgängen in der Industrie ist nicht erst eine Erfindung der letzten Jahre, sondern bereits seit der ersten industriellen Revolution (*Industrie 1.0*) zu beobachten, als mithilfe von Wasser- und Dampfkraft mechanische Produktionsanlagen genutzt und die Herstellungsabläufe daher effizienter und mit weniger Personalbedarf ausgestaltet werden konnten. Die zweite industrielle Revolution (*Industrie 2.0*) folgte sodann bei Beginn des 20. Jahrhunderts, als im Schlachthof von Cincinnati das erste Fließband zum Einsatz kam. Das Fließband ermöglichte erstmals eine neue Form der Massenproduktion und Arbeitsteilung, indem ein Mitarbeiter nicht mehr eine Vielzahl an Arbeitsschritten, sondern nur noch spezifische Handlungsabläufe zu erledigen hatte.

Die heute in der Industrie vorzufindende Automatisierung – insbesondere durch die Robotik – ist indes aber vielmehr ein Produkt der dritten industriellen Revolution (*Industrie 3.0*) zu Beginn der 70er Jahre des 20. Jahrhunderts, als mit der Fortentwicklung der Informations- und Kommunikationstechnik Arbeitsabläufe mithilfe von Computertechnik automatisiert werden konnten. Diese automatisierten IuK-Systeme konnten seitdem beständig weiterentwickelt werden, sodass heutige Industrieroboter eine unüberschaubare Vielzahl an Arbeiten verrichten können. Dies betrifft etwa die Ausführung schwerer Hebe- und Tragarbeiten bei den Automobilherstellern oder die Verrichtung präziser Lötarbeiten bei den Chipherstellern.

Im Rahmen der vierten industriellen Revolution erfolgt nun eine dezentrale oder zentrale digitale Vernetzung der einzelnen Komponenten und Maschinen. Diese stehen hierdurch in einem permanenten Informationsaustausch zueinander. Die Vernetzung der Einzelkomponenten wird durch den Einsatz intelligenter Algorithmen ergänzt, sodass die einzelnen IT-Systeme die hierbei gewonnenen Informationen auch für den Produktionsprozess gewinnbringend verwerten können. Das betrifft etwa die Meldung über die derzeitige Eigenauslastung des jeweiligen Systems an die anderen Komponenten, die daraufhin die Zustellung weiterer Bauteile besser koordinieren können. So ist beispielsweise denkbar, dass die Lackierstation in der Automobilproduktionshalle die verbleibende Arbeitszeit für das derzeit zu lackierende Bauteil an die Zustellroboter oder die Fließbänder meldet, die daraufhin entweder bereits das nächste zu lackierende Bauteil liefern, oder aber bei noch andauerndem Lackierprozess auf eine andere Lackierstation ausweichen. Diese Vernetzung und die Echtzeitauswertung von Daten wird insbesondere zu einer Steigerung der Produktivität führen, weil hierdurch Leerlaufzeiten sowie Materialverschwendung vermieden werden können.

Mittels der Vernetzung einzelner Komponenten ist es möglich, ganze Produktionsabläufe zu automatisieren. Im Rahmen der bereits aufgezeigten allgemeinen Automatisierungsstufenlehre ist hierbei bereits heute eine Automatisierung auf der Stufe der *Hochautomatisierung* vollständig etabliert, bei der das System Fehler im Produktionsablauf zumindest selbstständig feststellen kann und dann in einen Wartezustand übergeht, bis dieser (durch

menschlichen Eingriff) behoben wurde. Doch auch *vollautomatisierte* Industrieanlagen befinden sich heute schon im Praxiseinsatz, welche Fehler im Produktionsablauf nicht nur erkennen, sondern gar selbst und ohne fremde Hilfe beseitigen können.

Einer Branchenumfrage zufolge setzen fast zwei Drittel der befragten Unternehmen im Rahmen von Industrie 4.0 bereits spezielle Anwendungen wie vernetzte Produktionsanlagen, Echtzeit-Kommunikation zwischen Maschinen oder intelligente Roboter ein.[6]

2.3.1.2 Ausgewählte Beispiele der Automatisierung in der Industrie

Als typisches Beispiel für eine Automatisierung im Sinne von Industrie 4.0 kann das Elektronik- und Gerätewerk der Siemens AG im bayerischen Amberg genannt werden, das aufgrund seiner intelligenten und automatisierten Produktionsanlagen zu den modernsten Werken der Welt zählt.[7] Eine große Herausforderung der Automatisierung ganzer Fabrikationshallen liegt dabei gerade auch in der Lokalisierung und Identifizierung der verschiedenen Bauteile durch die einzelnen Produktionsstationen. Hierzu kommen heute optische zweidimensionale Codes (sogenannte QR-Codes) zum Einsatz, die auf jedes einzelne Bauteil aufgeklebt oder gedruckt werden.[8] Diese Codes können sodann von zahlreichen intelligenten Kamerasystemen in der Smart Factory erfasst und von der jeweiligen Produktionseinheit interpretiert werden. Zudem werden hierzu häufig auch sogenannte RFID-Systeme (Radio-Frequency Identification) eingesetzt, deren (meist passive) Sender es aufgrund der kleinen Größe und der minimalen Kosten erlauben, eine Vielzahl an – auch sehr kleinen – Bauteilen zu bestücken. Durch den Einsatz dieser Identifikationstechniken sowie weiterer Automatisierungslösungen konnte auch hier bereits die Stufe der *Vollautomatisierung* erreicht werden.[9]

Ein weiteres Beispiel bilden sogenannte automatisierte „Flurförderfahrzeuge“ oder sonstige automatisierte Fördersysteme, die etwa von der BMW Group oder von ThyssenKrupp eingesetzt werden.[10] Laut Herstellerangaben sind diese automatisierten Systeme dabei imstande, per Lasernavigation geleitet, selbstständig Waren innerhalb eines Werks oder Werksgeländes zu transportieren.[11] Je nach konkreter Ausführung sind diese Förderfahrzeuge dann bereits auf der Stufe der *Vollautomatisierung* oder der *Autonomie* einzuordnen, wenn diese Hindernisse selbstständig erkennen und umfahren können und daher auf keine fremde Hilfe oder Überwachung mehr angewiesen sind.[12]

---

[6] https://www.heise.de/hintergrund/Statistik-der-Woche-So-weit-ist-Deutschland-bei-Industrie-4-0-6018907.html.
[7] https://www.plattform-i40.de/PI40/Redaktion/DE/Anwendungsbeispiele/076-elektronikwerk-amberg-die-digitale-fabrik/beitrag-elektronikwerk-amberg-die-digitale-fabrik.html (abgerufen am 19.07.2021).
[8] http://www.mittelstand-digital.de/MD/Redaktion/DE/PDF/rfid-steuert-produktion-und-logistik-pdf,property=pdf,bereich=md,sprache=de,rwb=true.pdf (abgerufen am 19.07.2021).
[9] Vgl. https://www.merkur.de/wirtschaft/merkel-besuch-siemens-amberg-zr-4758778.html (abgerufen am 19.07.2021).
[10] http://www.jungheinrich.de/automatische-foerderzeuge/referenzen-automatische-foerderzeuge/ (abgerufen am 19.07.2021).
[11] http://www.jungheinrich.de/automatische-foerderzeuge/ (abgerufen am 19.07.2021).
[12] Der Hersteller selbst spricht dagegen nur von einer „teilweisen oder vollständigen Automatisierung“ außerhalb der hier zugrunde gelegten Automatisierungsstufenlehre, vgl. http://www.jungheinrich.de/automatische-foerderzeuge/ (abgerufen am 19.07.2021).

Weiterhin sind auch sogenannte automatisierte „Portalroboter“ zu nennen, also solche, die oberhalb von Ladeflächen zum Be- und Entladen eingesetzt und durch unterschiedliche Positionierung ihrer Portalarme einen einfachen Zugang an Maschinen und Arbeitsstationen ermöglichen. Auch er vermag Arbeiten selbstständig durchzuführen und zu koordinieren. Je nach Ausgestaltung eines solchen Portalroboters, also danach, ob dieser Fehler im Ablauf automatisch erkennen und auch korrigieren kann oder zur Korrektur des Fehlers noch menschlicher Hilfe bedarf, sind auch diese bereits auf der Stufe der *Vollautomatisierung*, zumindest aber auf der Stufe der *Hochautomatisierung*, einzuordnen.

Die Entwicklung automatisierter Werkzeugroboter und deren potenzielle Anwendungsfelder in nahezu allen Industriebereichen sind in den vergangen Jahren massiv vorangeschritten. Zu nennen ist hier etwa das Panda-Robotersystem des Münchner Start-ups Franka Emika.[13] Der Panda umfasst einen Arm und seinen Controller. Der feinfühlige und agile Arm verfügt über 7 Achsen und Drehmomentsensoren in jeder Achse und lässt sich in allen denkbaren Industrieanwendungen perfekt einsetzen. Gesteuert wird er über eine leicht zu bedienende App-Oberfläche und ist damit nicht nur extrem nutzerfreundlich, sondern auch besonders leicht in Betrieb zu nehmen. Dabei ist dieses Robotersystem in seinem modularen Aufbau in der Lage, sämtliche Automatisierungsstufen zu unterstützen, jeweils in Abhängigkeit zu seinem Einsatzgebiet und der mit ihm verknüpften Software. In ihm verbinden sich KI und Robotik.

Neben automatisierten Industrierobotern und Fließbändern kommen in der Industrie auch automatisierte Softwareprodukte zum Einsatz, wie etwa die Software „Automic“, die im Kontext der Industrie 4.0 gesamte Produktions- und Lieferketten automatisiert. Hierbei soll etwa bei einem deutschen Sportartikelhersteller künftig ermöglicht werden, dass ein Kunde im Ladengeschäft ein individuell designtes Produkt bestellt und diese Bestellung sodann unmittelbar, also ohne weitere Zwischenstationen und ohne zeitliche Verzögerung, in die Produktionsabteilung weitergereicht und hergestellt wird. Weiterhin soll durch Automic ermöglicht werden, dass im Ladengeschäft verkaufte und im Lager nicht mehr vorhandene Produkte automatisiert nachbestellt werden und insofern Lieferverzögerungen und damit leere Regale vermieden werden können.

2.3.2 Die Automatisierung im Dienstleistungssektor

Die Entwicklung von Dienstleistungsrobotern, insbesondere sogenannte „Humanoide“ / „Androide“, also dem menschlichen Körper nachempfundener Roboter, die dem Menschen im Alltag behilflich sind, ist bereits seit den Anfängen der Informations- und Kommunikationstechnologie ein Wunschtraum Vieler. So wurde in dem Film Metropolis etwa schon 1927 ein Humanoide vorgeführt, der einem weiblichen Maschinenmenschen glich. Und bereits 1939 wurde der erste tatsächliche humanoide Roboter „Elektro“ auf der Westinghouse Weltausstellung in New York präsentiert, der sogar einen Wortschatz von 700 Wörtern besaß, selbstverständlich aber noch von einem Menschen ferngesteuert werden

[13] https://www.franka.de (abgerufen am 21.07.2021).

musste, also noch kein algorithmisches System oder gar Künstliche Intelligenz besaß, auf dessen Grundlage automatisierte Aktionen ausgeführt werden konnten.

Heute existiert eine Vielzahl an Robotik-Unternehmen, die Service- und Dienstleistungsroboter für die unterschiedlichsten Einsatzszenarien herstellen. Für den privaten Bereich sind etwa bereits heute in jedem Elektronikfachmarkt automatisierte Staubsauger- oder Wischroboter erhältlich, die ihre Aufgaben bereits *hoch*- oder gar *vollautomatisiert* ausführen können (je nachdem, ob der Roboter auf Hindernisse selbst reagieren kann; bestimmte Hindernisse sind bislang aber noch unüberwindbar (etwa Treppen), sodass die Stufe der *Autonomie* hier noch nicht erreicht werden kann). In jedem Baumarkt sind zudem auch *hoch- oder vollautomatisierte* Rasenmäherroboter erhältlich. Für das Gewerbe wird unter anderem auch „Pepper“, ein 1,20 Meter großer japanischer Roboter, künftig eine Rolle spielen. Dieser soll etwa in Banken und Geschäften Flyer verteilen, Wartende belustigen oder gar Verkaufsgespräche führen. Selbst die Kreuzfahrtschifffflotte AIDA setzt Pepper bereits vereinzelt auf ihren Schiffen ein, wo dieser den Passagieren beim Einchecken und zur Orientierung auf dem Schiff hilft beziehungsweise Ausflugstipps gibt.

Auch im medizinischen Sektor sowie in der Krankenpflege sind Dienstleistungsrobotern bereits im Einsatz. Das betrifft zum Beispiel Assistenzrobotik in der Medizin wie sie im MIRO Innovation Lab entwickelt wird, aber auch Automatisierungslösungen und Assistenzsysteme im Bereich Pflege wie bei moio.care – das intelligente Pflegepflaster. Ebenso dienen robotikgestützte Pollenzählungen der Prävention und intelligente Bild- und Texterkennung ist im Gesundheitswesen universell einsetzbar.[14]

Auch das bereits erwähnte Panda-Robotersystem von Franka Emika kann im Dienstleistungssektor eingesetzt werden. Als Reaktion auf die weltweite COVID-19-Pandemie stellte das Unternehmen im Sommer 2020 etwa ein neues Modell namens „SR-NOCS“ vor. SR-NOCS steht für „Swab Robot for Naso- and Oropharyngeal Covid-19 Screening“ (Tupferroboter für den Nasen- und Rachenabstrich bei der Covid-19-Diagnostik). NOCS ist nach Aussage von Franka Emika der weltweit erste Abstrichroboter dieser Art und soll Coronatests sicherer und schneller machen.[15]

Bei der Entwicklung von Service- und Dienstleistungsrobotern spielt die Erforschung künstlicher Intelligenz eine Schlüsselrolle. Denn gerade bei diesen ist erforderlich, dass sie sich in den Alltag ihrer Halter oder Kunden bestmöglich integrieren. Aufgrund der Unvorhersehbarkeit alltäglicher Situationen und aufgrund der Unterschiedlichkeit der Persönlichkeit, Vorlieben und Stimmung des jeweiligen Halters oder Kunden können hierbei nicht alle Szenarien ab Werk einprogrammiert werden. Der Roboter muss insofern vielmehr selbst beziehungsweise auf Basis des Nutzer-Feedbacks ein adäquates und optimales Verhalten im Laufe des Betriebs erlernen.

---

[14] Näher zu diesen und weiteren Beispielen https://www.vbw-zukunftsrat.de/Gesundheit-und-Medizin/Anwendungen.
[15] https://www.handelsblatt.com/unternehmen/mittelstand/familienunternehmer/franka-emika-ceo-simon-haddadin-dieser-gruender-baut-den-ersten-abstrichroboter-fuer-coronatests/25995562.html?ticket=ST-11491153-bDYpZe9CtbUKmKoXuggQ-ap2 (abgerufen am 21.07.2021).

2.3.3 Automatisierte Straßenfahrzeuge

Die Automatisierung des Kfz ist keineswegs eine „Erfindung“ der letzten Jahre. So sprach etwa bereits im Jahre 1958 Frank Rowsome im Magazin „Popular Science“ vom sogenannten „Auto Pilot“, der schließlich 1962 dann als sogenannter „Tempomat“ eingeführt wurde. Der Tempomat, aber auch das 1978 entwickelte Antiblockiersystem (ABS), die Antischlupfregelung (ASR) aus den 90er Jahren sowie das Elektronische Stabilitätsprogramm (ESP), stellen bereits die Vorfahren der heutigen Automatisierung im Kfz dar. Diesen frühen *Assistenzsystemen* folgten schließlich – auf der nächsten Stufe – der Parklenk- und der Spurhalteassistent, die beim Parken vollständig, beim Fahren auf der Autobahn hilfsweise, die Steuerung über das Lenkrad übernehmen, während der Fahrzeugführer weiterhin die Geschwindigkeit durch Gas geben oder Bremsen kontrollieren muss. Das 2010 eingeführte automatische Notbremssystem kann umgekehrt das Fahrzeug bei erkannten Hindernissen selbstständig abbremsen, während der Fahrer weiterhin die Lenkbewegung kontrolliert.

In Erweiterung des Parklenkassistenten werden seit den 2010er Jahren nunmehr sogenannte Parkmanöverassistenten in moderne Kfz verbaut, die nicht nur die Lenkbewegung, sondern auch das Beschleunigen und Bremsen beim Einparken übernehmen und in dieser spezifischen Situation also einen Fahrer bereits ersetzen können. Dem Fahrer kommt dabei nur noch eine Überwachungsfunktion zu (*Teilautomatisierung*). Er kann notfalls durch eigene Lenk- oder Bremsimpulse korrigierend eingreifen. Mittlerweile ist es durch das sogenannte „Schlüsselparken“ sogar möglich, dass sich der Fahrzeugführer während des Parkvorgangs auch außerhalb des Fahrzeugs befindet und diesem mittels des Schlüssels nur noch eine Parklücke aufzeigen muss, in welche das Fahrzeug dann automatisiert einparkt. Ein korrigierendes Eingreifen des überwachenden Fahrzeugführers ist weiterhin per Notstopp möglich, der etwa mit einem Schalter auf dem Schlüssel ausgelöst werden kann. In Zukunft wird durch das sogenannte „Valet Parking“ auch ein *vollautomatisiertes* Ein- und Ausparken möglich sein. Das Fahrzeug muss hierzu dann nur noch im Einfahrtsbereich eines Parkhauses oder Parkplatzes abgestellt werden. Geleitet durch zahlreiche im Kfz und im Parkhaus angebrachte Sensoren und intelligente Steuerungsalgorithmen kann dieses daraufhin selbstständig einen freien Parkplatz finden, dort einparken und später, nachdem der Fahrzeughalter sein Fahrzeug per Smartphone, Tablet oder Fernbedienung „ruft“, wieder automatisiert ausparken.

Auch beim Stau-„Assistenten“ ist das automatisierte Kfz mittlerweile in der Lage, in der spezifischen Stausituation die vollständige Kontrolle über die Längs- (vor / zurück) und Querachse (links / rechts) zu übernehmen. Jedoch hat der Fahrzeugführer den Vorgang bislang noch dauerhaft zu überwachen und sicherzustellen, dass er notfalls unverzüglich korrigierend (durch Gegenlenkung oder Bremsen) eingreifen kann (*Teilautomatisierung*). Eine Beschäftigung mit anderen Dingen ist daher derzeit noch nicht zulässig. Zukünftig soll durch das sogenannte Staufolgefahren / Fahren im Stau aber auch die Notwendigkeit einer permanenten Fahrzeugüberwachung durch den Fahrzeugführer entfallen und diesem dann ermöglicht werden, sich während der Fahrt mit anderen Dingen zu beschäftigen. Erkennt das System dann die Notwendigkeit einer Steuerungsübernahme durch den Fahrzeugführer, so wird dieser per Warnhinweis darauf aufmerksam gemacht (*Hochautomatisierung*). Dem Fahrzeugführer bleibt dann eine gewisse Übernahmezeit.

Zusammenfassend ist die Automatisierung in Straßenfahrzeugen derzeit also noch auf spezifische Szenarien (Fahren im Stau / Parken) beschränkt. Gerade das Valet Parking ist zudem auf das Vorhandensein einer entsprechenden Infrastruktur in Parkhäusern oder auf Parkplätzen angewiesen. Perspektivisch soll aber auch das Fahren auf der Autobahn automatisiert werden. Einen wichtigen Beitrag zu dieser Fortentwicklung der Kfz-Automatisierung leistet unter anderem die Teststrecke für automatisiertes und autonomes Fahren auf der Bundesautobahn A9, auf der bereits heute schon *hoch- und vollautomatisierte* Fahrfunktionen getestet werden können. Auch das automatisierte Fahren innerhalb der Stadt wird derzeit bereits getestet. Aufgrund der erhöhten Komplexität des automatisierten Fahrens in innerstädtischen Gebieten lassen sich hierbei bisher aber noch keine gesicherten Zukunftsprognosen aussprechen.

Neben dem technischen Entwicklungsbedarf erfordert der Einsatz von automatisierten Fahrfunktionen auch eine Weiterentwicklung des Rechts. Im Juni 2017 wurden erstmalig spezifische gesetzliche Bestimmungen für Kraftfahrzeuge mit hoch- und vollautomatisierten Fahrfunktionen geschaffen. Diese wurden im Mai 2021 durch das „Gesetz zum *autonomen Fahren*“ für weitere Stufen der Automatisierung und Vernetzung in eine neue Entwicklungsstufe gebracht (siehe dazu unten Kapitel 2). Es bleiben allerdings sowohl auf nationaler als auch auf internationaler Ebene noch weitere Anpassungen erforderlich.

2.3.4 Automatisierte und autonome unbemannte Luftfahrzeuge (Drohnen)

Unbemannte Luftfahrzeuge sind äußerst anfällig für Umwelteinflüsse wie Wind und Wetter, da sie im Gegensatz zu Straßenfahrzeugen keinen Kontakt zu einem festen Bezugspunkt haben, wie dies bei Straßenfahrzeugen etwa die Straße ist. Diese Umwelteinflüsse bedürfen eines ständigen Gegenlenkens durch die Drohne, damit das Luftfahrzeug stabil in der Luft gehalten werden kann.

Zu diesem Zweck sind so gut wie alle auf dem Markt erhältlichen modernen zivilen Drohnen bereits heute mit zahlreichen hochsensiblen Sensoren und elektronischen Positionsbestimmungssystemen ausgerüstet. Hierzu gehören unter anderem Kompass, Gyroskop, Beschleunigungsmesser, Barometer und GPS-Modul.

Je nach Ausgestaltung können zudem weitere Module wie (Ultraschallsensoren, Kameras und andere visuelle Positionsbestimmungssysteme verbaut sein, um Hindernisse automatisiert erkennen und umfliegen zu können.

Hierdurch sind moderne Flugdrohnen bereits heute unter anderem in der Lage:

- ihre Position stabil zu halten,
- Umwelteinflüsse selbstständig auszugleichen,
- vorgegebene Zielkoordinaten (sogenannte „Waypoints“) *hoch- oder vollautomatisiert* selbstständig anzufliegen,
- ein vorgegebenes Objekt (sogenannter „Point of Interest“) *hoch- oder vollautomatisiert* selbstständig zu umfliegen,

– ein vorgegebenes Objekt *hoch- oder vollautomatisiert* zu verfolgen (sogenannte „Follow Me“-Funktion),
– Hindernisse zu erkennen und *vollautomatisiert* zu umfliegen.

Moderne Flugdrohnen sind also auch heute schon in der Lage, Flüge in spezifischen Situationen automatisiert durchzuführen. Der von der DHL GmbH getestete „Paketkopter“, der bereits erfolgreich Medikamente auf die Nordseeinsel Juist und Pakete auf eine Alm bei Reit im Winkl ausgeliefert hat, ist nur eines von mehreren Beispielen. Auch vom Online-Warenhaus Amazon wird derzeit der „Amazon Prime Air“-Dienst getestet.

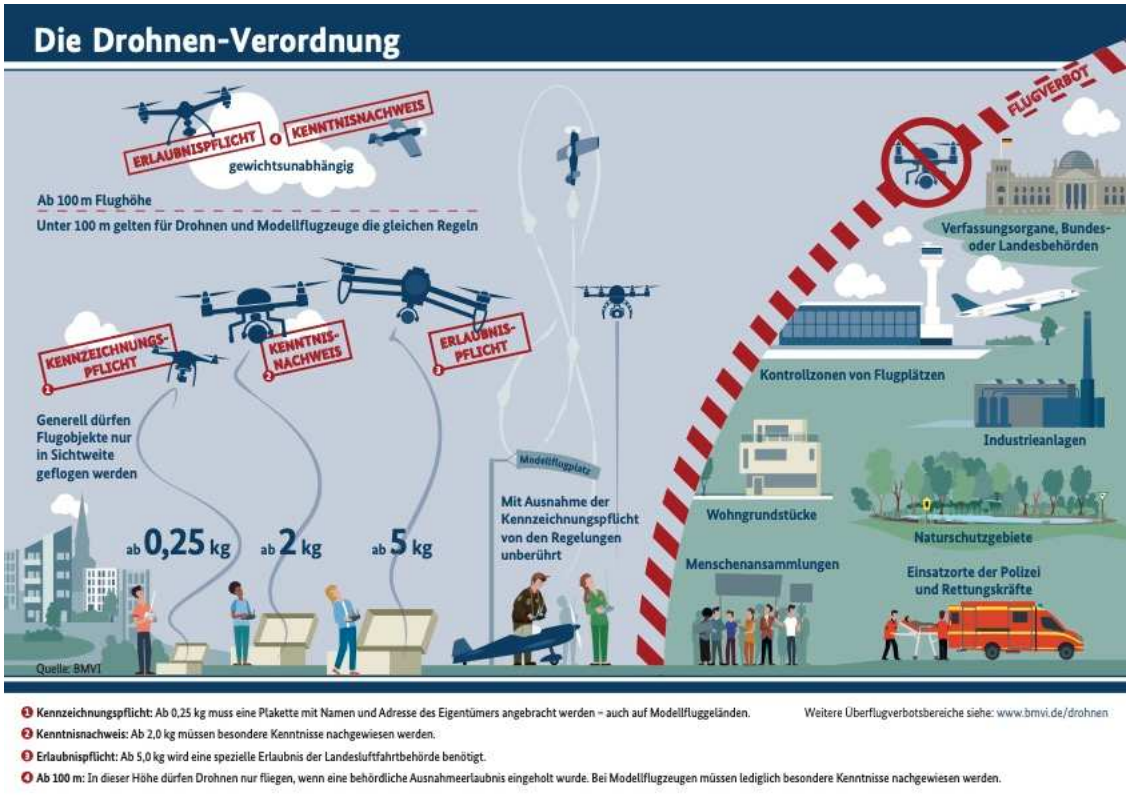
Bis Drohnen tatsächlich in unserem Alltag vollautomatisiert oder autonom Lieferungen zustellen oder sonstige Aufgaben übernehmen können, besteht aber auch hier noch erheblicher Forschungsbedarf, der insbesondere auch im sicheren Erkennen und Ausweichen von anderen Flugobjekten und Gegenständen besteht. Gerade in dicht besiedelten städtischen Gebieten kann dies derzeit noch nicht vollumfänglich gewährleistet werden. Neben der Weiterentwicklung der verwendeten Sensorik und der zur Anwendung kommenden softwaregestützten Erkennungs- und Ausweichalgorithmen bedarf es hierbei zukünftig auch neuer Konzepte zur sicheren Integration von Flugdrohnen in den kontrollierten und unkontrollierten Luftraum.

Auf europäischer Ebene wird das „Drohnen-Recht“ im Wesentlichen durch die sogenannte EU-Drohnen-Verordnung (Durchführungsverordnung (EU) 2019/947 der Kommission vom 24. Mai 2019 über die Vorschriften und Verfahren für den Betrieb unbemannter Luftfahrzeuge[16] geprägt. Sie enthält „detaillierte Bestimmungen für den Betrieb unbemannter Luftfahrzeugsysteme (genauer: unbemannter Luftfahrzeuge und Luftfahrzeugsysteme - unmanned aircraft system, UAS) sowie für das Personal, darunter auch für Fernpiloten und an diesem Betrieb beteiligte Organisationen“ (Art. 1) und begründet 3 Betriebskategorien (Anwendungsszenarien) von UAS[17]: offen, speziell und zulassungspflichtig. Diese Kategorien beschreiben das von den UAS ausgehende Risiko und fordern gleichsam „aufsteigend“ zu diesen Risiken eine zunehmende Regulierung und staatliche Aufsicht. Die Einzelheiten werden der nationalen Gesetzgebung überlassen.

Dort gilt für den Einsatz von automatisierten Drohnen zunächst das Luftverkehrsrecht, also das Luftverkehrsgesetz (LuftVG), die Luftverkehrsordnung (LuftVO) und die Luftverkehrszulassungsordnung (LuftVZO), besonders aber die sogenannte „DrohnenVO“ (Verordnung zur Regelung des Betriebs von unbemannten Fluggeräten v. 30.03.2017, zuletzt geändert durch Gesetz vom 14.6.2021[18]). Sie greift die Vorgaben der EU-Drohnen-Verordnung auf.

[16] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0947&rid=1.
[17] Hierzu näher https://www.drohnen.de/20336/drohnen-gesetze-eu/.
[18] https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*[@attr_id=%27bgbl121s1766.pdf%27]#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1766.pdf%27%5D__1628336171567.

Abbildung 2
Die Drohnen-Verordnung



Bildquelle:BMVI[19]

2.4 „Smartifizierung“ und Vernetzung zu einer „Smart World“

Nicht nur in der Industrie 4.0 erfolgt derzeit eine Vernetzung bislang isolierter Einzelkomponenten und -systeme zu einem automatisierten und intelligenten Gesamtsystem. Vielmehr erfährt diese „Smartifizierung“ von Alltagsgegenständen und Prozessen im „Internet of Things“ derzeit und zukünftig eine ubiquitäre Entwicklung, die quasi alle Lebensbereiche betreffen wird (sogenannte „Smart World“). Bereits heute finden sich in Privatwohnungen schon zahlreiche smarte und vernetzte IT-Komponenten und Geräte wie etwa Smart-TVs, smarte Kühlschränke, sonstige smarte Küchengeräte, smarte Waschmaschinen und eine große Palette an Smart-Home-Geräten wie vernetzte dimmbare Lichtschalter oder zeitgesteuerte Jalousien. Auch unmittelbar am Körper tragen wir bereits das Smartphone und vermehrt auch Smart Watches oder Fitnesstracker. Zukünftig werden noch weitere smarte Bekleidungsgegenstände („Smart Wearables“) hinzukommen. Auch im Straßenverkehr

[19] https://www.bmvi.de/SharedDocs/DE/Publikationen/LF/flyer-die-neue-drohnen-verordnung.pdf?__blob=publicationFile.

entwickelt sich ein sogenannter „Smart Traffic“, bestehend aus „Connected Cars“ und einer „Smart Infrastructure“, die miteinander und untereinander vernetzt sind und in einem permanenten Informationsaustausch stehen.[20] Hierin einbezogen ist auch die Digitalisierung der Energiewirtschaft[21] („Smart Metering“, „Smart Grid“): So wird smarte Energiesteuerung zum Bestandteil des Smart Home, sorgt darüber hinaus aber auch für die Vernetzung der Gebäude, die nicht nur wie bisher Energie von Stromanbietern beziehen, sondern mit ihren Solardächern selbst auch solche in das Energienetz einspeisen. Eine bedarfsgerechte Steuerung insbesondere in Bezug auf erneuerbare Energien setzt einen hohen Digitalisierungsgrad voraus.

Aufgrund dieser alles erfassenden Vernetzung des Alltags entsteht zunehmend ein digitaler Erlebnisraum, der eine Vielzahl an Komponenten miteinander verbindet. Durch diese „Smartifizierung“ wird dabei auch eine Gesamtautomatisierung unseres Alltags ermöglicht, insofern diese Smart Devices untereinander kommunizieren und bestimmte Prozesse miteinander koordinieren (etwa das Abstellen aller Haushaltsgeräte oder das Aktivieren der Alarmanlage, wenn die Smart Watch an das Smart Home meldet, dass der Nutzer derzeit auswärts unterwegs ist).

2.5 Überblick über die wesentlich betroffenen Rechtsbereiche

Die Automatisierung und Vernetzung von Systemen werfen eine Reihe an Rechtsfragen auf. Zu unterscheiden sind dabei solche, die alle automatisierten Systeme unabhängig von ihrer konkreten Ausgestaltung und Form betreffen und besondere Rechtsfragen, die nur für spezifische automatisierte Systeme relevant werden.

2.5.1 Allgemeine Rechtsbereiche

2.5.1.1 Datenschutzrecht

Die Automatisierung von Systemen ist nur durch den Einsatz zahlreicher Sensortechnik sowie durch Algorithmen, die die hierbei erhobenen Sensorinformationen verarbeiten, möglich.

Naturgemäß betreffen diese Informationen nicht nur sachbezogene Informationen über das Umfeld des automatisierten Systems, sondern auch personenbezogene Daten über in der Nähe befindliche Personen. Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten unterliegt nach der Datenschutz-Grundverordnung (DSGVO) einem soge-

[20] Hierzu näher *Heckmann/Paschke*, IT-Sicherheit, in: Bräutigam/Kraul, Internet of Things, 2021, § 10.
[21] Vgl.hierzu das vbw-Positionspapier Digitalisierung der Energiewirtschaft: https://www.vbw-bayern.de/Redaktion/Frei-zugaengliche-Medien/Abteilungen-GS/Wirtschaftspolitik/2020/Downloads/vbw_Position_Digitalisierung_der_Energiewirtschaft_Dezember_2020.pdf sowie die Handlungsempfehlungen des Zukunftsrates der Bayerischen Wirtschaft „Klima 2030. Nachhaltige Innovationen“: https://www.vbw-zukunftsrat.de/klima2030/Klima%202030-Handlungsempfehlungen-lang.pdf.

nannten Verbot mit Erlaubnisvorbehalt. Nach Art. 6 Abs. 1 DSGVO ist eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten nur zulässig, wenn ein gesetzlicher Erlaubnistatbestand vorliegt.

2.5.1.2 IT-Sicherheitsrecht

In Deutschland existiert bislang kein einheitliches und umfassendes IT-Sicherheitsrecht. Sowohl das aus dem Jahre 2015 stammende IT-Sicherheitsgesetz 1.0 sowie das Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 18.05.2021 (IT-Sicherheitsgesetz 2.0)[22] treffen nur stellenweise Bestimmungen zur adäquaten Absicherung von IT-Systemen, insbesondere für die Betreiber kritischer Infrastrukturen.

Im Rahmen der *Informationssicherheit* als Teilgebiet der IT-Sicherheit bleibt daher meist nur ein Rückgriff auf Art. 32 DSGVO , der grobe IT-Sicherheitsvorgaben und -zielsetzungen enthält.[23] Insbesondere das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt aber auch umfangreiche organisatorische, technische, personelle und infrastrukturelle Handlungsempfehlungen zur Steigerung der IT-Sicherheit bereit (insbesondere die IT-Grundschutzkataloge).

Im Rahmen der *Funktionssicherheit*, als weiteres Teilgebiet der IT-Sicherheit, ist dagegen auf das Produktsicherheitsgesetz (ProdSG) mit seinen Produktsicherheitsverordnungen (ProdSV) sowie auf zahlreiche weitere DIN-, EN-, ISO- und IEC-Richtlinien zurückzugreifen.

2.5.1.3 Haftungsrecht

Werden bei dem Einsatz automatisierter IT-Systeme Personen verletzt oder Sachen beschädigt, stellt sich anschließend stets die Haftungsfrage. Neben spezifischen Haftungsnormen aus dem Straßenverkehrsrecht, dem Luftverkehrsrecht oder dem Datenschutzrecht muss dabei stets auch das allgemeine Vertragsrecht sowie das Deliktsrecht aus dem Bürgerlichen Gesetzbuch (BGB) in Betracht gezogen werden. Neben der eigentlichen deliktischen Haftung kommt darüber hinaus auch ein Schadensersatzanspruch aus § 823 Abs. 2 BGB in Betracht, wenn eine Strafrechtsnorm des StGB und mithin ein sogenanntes Schutzgesetz verletzt wurde.

Gerade bei automatisierten Systemen, bei denen die späteren Handlungsabläufe bereits zum Zeitpunkt der Systementwicklung und -programmierung vorgegeben werden, könnte weiterhin auch der Produkthersteller nach dem Produkthaftungsgesetz verpflichtet sein, entstandene Schäden zu ersetzen. Denn da mit zunehmendem Automatisierungsgrad eine menschliche Steuerung immer weiter zurücktritt, wird die Ursache eines schadensauslösenden Ereignisses zukünftig vermehrt auf den Hersteller zurückzuführen sein. Oft werden gar mehrere Haftungsadressaten in Frage kommen, etwa sowohl der Halter als auch der Hersteller des automatisierten Systems. Es stellt sich dann die Frage, wie zwischen den

[22] Ausführlich unten Kapitel 3.4.5.
[23] Ausführlich unten Kapitel 3.5.2.

verschiedenen Adressaten eine billige und adäquate Haftungsverteilung vorgenommen werden kann.[24]

2.5.2 Besondere Rechtsbereiche

Je nach Art und Weise, Einsatzzweck und konkreter Systemausgestaltung können bei der Entwicklung und bei dem Betrieb eines automatisierten Systems zudem ganz spezifische Vorschriften relevant werden. So ergeben sich bei dem Einsatz eines automatisierten Straßen- oder Luftfahrzeugs etwa besondere Bestimmungen aus dem jeweiligen Fahrzeugzulassungsrecht. Bei dem Einsatz von automatisierten Drohnen im öffentlichen Raum sind je nach Einsatzort etwa auch besondere Bestimmungen des Bundesnaturschutzgesetzes oder des Bundesimmissionsschutzgesetzes zu beachten. Zudem können bei rechtswidrigen Gefährdungen des Luftraums spezifische Normen des StGB relevant werden. Werden zur Realisierung von automatisierten Systemen dagegen Telekommunikationsinfrastrukturen verwendet, kann weiterhin etwa auch das TKG zu beachten sein.

[24] Hierzu ausführlich Kapitel 4.

3 Exkurs: Das Gesetz zum autonomen Fahren

Auf dem Weg in eine volldigitalisierte Verkehrsinfrastruktur

Am 20.05.2021 hat der Deutsche Bundestag das Gesetz zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes – Gesetz zum autonomen Fahren beschlossen.[25] Der Bundesrat stimmte am 28.05.2021 zu. Es ist am 28.07.2021 in Kraft getreten. Die im vorliegenden Kontext relevanten Gesetzesänderungen beziehungsweise Erweiterungen betreffen das Straßenverkehrsgesetz (StVG), in das die neuen §§ 1d bis 1l eingefügt werden. Schon mit der Novelle aus dem Jahr 2017[26] wurde durch Einfügung der §§ 1b und 1c StVG automatisiertes Fahren reguliert. Dies wird durch die nunmehrige Erweiterung unter der expliziten Bezeichnung „Gesetz zum *autonomen Fahren*" für weitere Stufen der Automatisierung und Vernetzung in eine neue Entwicklungsstufe gebracht: Während das "alte" Gesetz nur das Verhalten unter bestimmten Fahrzeug- und Verkehrsbedingungen regelte, geht es in der Novelle 2021 auch um technische Anforderungen an den Bau, die Beschaffenheit und die Ausrüstung von Kraftfahrzeugen mit autonomen Fahrfunktionen sowie Prüfung und Verfahren für die Erteilung einer Betriebserlaubnis.

Mit diesem Gesetz wird insbesondere die Erhöhung der Verkehrssicherheit bezweckt, in der Annahme, dass Maschinen beziehungsweise die mit ihnen installierte Informationstechnik weniger (Fahr-) Fehler begehen als der Mensch – besonders wenn dieser unter Alkoholeinfluss steht, sich selbst überschätzt oder aus unterschiedlichen Gründen die Verkehrsvorschriften missachtet.[27] Während diese Grundannahme von vielen Expertinnen und Experten geteilt wird, wird aber auch darauf hingewiesen, dass technische Mängel ebenso ein Unfallrisiko darstellen und auf Fehlverhalten anderer Verkehrsteilnehmer, etwa Fußgänger, nur dann adäquat reagiert werden kann, wenn diesbezüglich kritische Situationen erkannt und richtig eingeordnet werden und eine gefahrenabwehrende Kommunikation mit diesen Akteuren gelingt.[28] Dies ist eine von vielen anspruchsvollen Anforderungen an die Gestaltung der entsprechenden Systeme.

Inhalt und Systematik des Gesetzes lassen sich wie folgt zusammenfassen:

Mit der Legaldefinition in § 1d StVG-neu wird die Kategorie eines „Kraftfahrzeugs mit autonomer Fahrfunktion in festgelegten Betriebsbereichen" eingeführt. Dies geht über die bisher gesetzlich geregelten Automatisierungsstufen hinaus und ist in zweifacher Hinsicht bemerkenswert: Zum einen wird das Kraftfahrzeug trotz „autonomer Fahrfunktion" nicht

---

[25] Gesetzesentwurf der Bundesregierung, Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes – Gesetz zum autonomen Fahren, Bearbeitungsstand: 08.02.2021, abrufbar unter www.bmvi.de/SharedDocs/DE/Artikel/DG/gesetz-zum-autonomen-fahren.html, zuletzt aufgerufen am 19.07.2021.
[26] Achtes Gesetz zur Änderung des Straßenverkehrs vom 16.6.2017, BGBl. I S. 1648.
[27] Gesetzesbegründung, S. 18.
[28] *Haupt*, NZV 2021, 172, 173.

gleichberechtigt neben andere im Straßenverkehr geführte Kraftfahrzeuge gestellt, sondern per definitionem auf einen festgelegten Betriebsbereich[29] (§ 1d Abs. 2 StVG-neu) reduziert. Zum anderen unterliegt dieses Fahrzeug trotz autonomen, also „selbst"bestimmten Fahrbetriebs einer technischen Aufsicht, als die immer eine natürliche Person bereitstehen muss, um die entsprechenden Fahrfunktionen zu aktivieren oder deaktivieren beziehungsweise bestimmte Fahrmanöver freizugeben (§ 1d Abs. 3 StVG-neu). Letzteres hat auch Bedeutung für die Haftung bei fehlerhaftem Fahrbetrieb und der Verursachung von Schäden (hierzu näher Kapitel 4.2.2.4.5). *Haupt* spricht hier von „ferngesteuertem Fahren"[30], was freilich den Aspekt der technischen Aufsicht mit diesem Bild nur zu einem Teil beschreibt und zu Missverständnissen einlädt.

Von großer praktischer, aber auch rechtlicher Bedeutung ist schließlich der Begriff des „risikominimalen Zustands", den § 1d Abs. 4 StVG-neu definiert: Als solcher gilt ein „Zustand, in den sich das Kraftfahrzeug mit autonomer Fahrfunktion auf eigene Veranlassung oder auf Veranlassung der Technischen Aufsicht selbstständig versetzt, um unter angemessener Beachtung der Verkehrssituation die größtmögliche Verkehrssicherheit für andere Verkehrsteilnehmende und Dritte zu gewährleisten." Dabei fällt auf, dass das Gesetz den Begriff des Risikos in einer Weise verwendet, dass der Betrieb eines Kraftfahrzeugs mit autonomer Fahrfunktion eine Unfall- beziehungsweise Schadensfreiheit keineswegs garantieren, sondern lediglich minimieren muss. Bemerkenswert ist überdies, dass „autonomes Fahren" in diesem Kontext sowohl von der Technischen Aufsicht als auch „von selbst" veranlasst sein kann.

§ 1e StVG-neu regelt das rechtliche Regime der vorgenannten Fahrzeuge im Zulassungsrecht. Neben den üblichen Zulassungsvoraussetzungen (Zulassung zur Teilnahme am öffentlichen Straßenverkehr, Erteilung einer Betriebserlaubnis) ist der Betrieb eines Kraftfahrzeugs mittels autonomer Fahrfunktion nur zulässig, wenn das Kraftfahrzeug in einem „genehmigten, festgelegten Betriebsbereich eingesetzt wird" (§ 1e Abs. 1 Nr. 3 StVG-neu) und es bestimmten technischen Voraussetzungen entspricht (§ 1e Abs. 1 Nr. 1, Abs. 2 StVG-neu). Unter den teilweise noch untergliederten 10 Punkten des Anforderungskatalogs in § 1e Abs. 2 StVG-neu sind besonders hervorzuheben:

- Fähigkeit zur selbstständigen Bewältigung der Fahraufgabe innerhalb des Betriebsbereichs (Nr. 1)
- Fähigkeit zur Einhaltung der Verkehrsvorschriften inklusive Schadensvermeidung und Schadensreduzierung (Nr. 2a)
- „ethische Programmierung" möglicher Dilemma-Konstellationen entsprechend der Leitlinien der Ethikkommission für automatisiertes und vernetztes Fahren (Bewertung von kollidierenden Rechtsgütern, keine Abwägung „Leben gegen Leben") (Nr. 2 b und c)[31]

[29] Dieser Betriebsbereich kann zum Beispiel ein bestimmter Autobahnabschnitt (so etwa *Haupt*, NZV 2021, 172, 174) aber auch ein Werksgelände oder die Transferstrecke zwischen einem Bahnhof und einer Reha-Klinik sein. Es ist davon auszugehen, dass autonomes Fahren in eher kleinen Schritten zugelassen wird, um die Funktionstüchtigkeit und die Auswirkungen zu erproben.
[30] *Haupt*, NZV 2021, 172.
[31] Kritisch bewertet wird die Umsetzung zur Lösung von Dilemma-Situationen von *Schrader,* ZRP 2021, 109, 110.

– Fähigkeit zur Erkenntnis der Notwendigkeit zur Versetzung des Kfz in einen risikominimalen Zustand, insbesondere bei technischen Störungen oder Erreichen der Systemgrenzen und Kommunikation mit der Technischen Aufsicht zum sicheren Betrieb (Nr. 3-5, 7)
– Selbständiges Erkennen von Funktionsstörungen und diesbezügliche Kommunikation mit der Technischen Aufsicht (Nr. 6)
– Gewährleistung ausreichend sicherer Funkverbindungen[32], insbesondere zur Technischen Aufsicht und zur Versetzung des Kfz in einen risikominimalen Zustand bei Nichtverfügbarkeit oder einem Angriff auf die Funkverbindung[33] (Nr. 10).

Eine weitere zentrale Vorschrift ist § 1f StVG-neu. Dieser regelt die Pflichten der Beteiligten beim Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion. Abgegrenzt werden die Pflichten der Halter (Abs. 1), der Technischen Aufsicht (Abs. 2) und der Hersteller (Abs. 3). Danach ist der Halter zur Erhaltung der Verkehrssicherheit verpflichtet, insbesondere durch Wartung der erforderlichen Systeme. Darüber hinaus hat der Halter die Aufgaben der Technischen Aufsicht – wenn auch nicht zwingend in eigener Person – zur erfüllen. Hierzu zählen unter anderem die Freischaltung alternativer Fahrmanöver, die Deaktivierung der autonomen Fahrfunktion oder die Bewertung des Funktionsstatus. Eine herausragende Rolle kommt dem Hersteller eines Kraftfahrzeugs mit autonomer Fahrfunktion zu. Letztlich ist das, was ein solches Fahrzeug später im autonomen Betrieb zu leisten hat, im Wesentlichen bereits durch die elektronische und elektrische Architektur des Kraftfahrzeugs, insbesondere die Programmierung der entsprechenden Systeme, die sichere Funkverbindung etc. angelegt. So gesehen wird ein Großteil jener Entscheidungen, die bei normalen Kraftfahrzeugen durch den Fahrzeugführer getroffen wird, bei Kraftfahrzeugen mit autonomer Fahrfunktion gleichsam vorverlagert in die Ausgestaltung des autonomen Systems.

Nachdem beim autonomen Fahren zwangsläufig eine Vielzahl von Daten entsteht und auch gebraucht wird, regelt § 1g StVG-neu sehr ausführlich und differenziert, welche Daten von wem in welchem Kontext erhoben, gespeichert und genutzt werden dürfen.[34] Hervorhebenswert ist die Regelung in § 1g Abs. 3 StVG-neu:

> *Der Hersteller muss den Halter präzise, klar und in leichter Sprache über die Einstellungsmöglichkeiten zur Privatsphäre und zur Verarbeitung der Daten informieren, die beim Betrieb des Kraftfahrzeugs in der autonomen Fahrfunktion verarbeitet werden. Die diesbezügliche Software des Kraftfahrzeugs muss dem Halter entsprechende Einstellungen ermöglichen.*

---

[32] *Haupt* weist zu Recht darauf hin, dass diese wichtige, unverzichtbare Anforderung vielfach noch nicht erfüllbar ist, NVZ 2021, 172, 174.
[33] Die Gefahr von Hackerangriffen darf nicht unterschätzt werden, nicht zuletzt, weil dies das wichtige Vertrauen der Menschen in die digitale Verkehrsinfrastruktur erschüttern würde, *Haupt*, NVZ 2021, 172, 175. Darauf hat bereits die Ethikkommission für automatisiertes und vernetztes Fahren hingewiesen, vgl. Abschlussbericht Ethikkommission, S. 23.
[34] Zur Forderung, die übermittelten Daten zu anonymisieren oder sogar ein verkehrsmittelübergreifendes Mobilitätsdatengesetz einzuführen vgl. *Haupt*, NVZ 2021, 172, 175 m.w.N.; vgl. ausführlich betreffend Datenerhebung und -verarbeitung *Steege*, Gesetzesentwurf zum autonomen Fahren (Level 4), SVR 2021, 128, 134f.

Dies entspricht den Anforderungen in Art. 12 Abs. 1 DSGVO und wird auch den Anforderungen gerecht, die die Ethikkommission für automatisiertes und vernetztes Fahren in ihrem Abschlussbericht 2017 formuliert hat.[35]

§ 1h StVG-neu regelt die (De-)Aktivierung von Funktionen für einen automatisierten beziehungsweise autonomen Betrieb entsprechender Kraftfahrzeuge und das diesbezügliche Genehmigungsverfahren und trägt damit dem Umstand Rechnung, dass das Straßenverkehrsrecht stets auch in einem internationalen Kontext gesehen werden muss und andere Staaten nicht zwangsläufig denselben oder einen vergleichbaren rechtlichen Standard für das autonome Fahren gesetzt haben. Darüber hinaus geht es aber auch generell darum, „dass aktuell nicht genehmigungsfähige Funktionen bereits verbaut werden dürfen. Diese dürfen dann auch aktiviert werden, sobald deren Nutzung einmal zulässig sein wird."[36]

§ 1i StVG-neu ermöglicht die Erprobung des Betriebs von Kraftfahrzeugen mit automatisierten und autonomen Fahrfunktionen unter bestimmten Voraussetzungen. Dazu zählt insbesondere eine permanente Überwachung der Fahrt durch eine anwesende Person, die als technische Aufsicht mit allen Fahrfunktionen vertraut ist und jederzeit in den Fahrbetrieb eingreifen kann (praktisch wie ein Fahrlehrer neben dem Fahrschüler). Zuständig sind nicht (mehr) die Landesbehörden, sondern einheitlich das Kraftfahrtbundesamt.

Abschließend widmen sich die §§ 1j, 1k und 1l StVG-neu der Ermächtigung zum Erlass einer Rechtsverordnung (insbesondere zu technischen und organisatorischen Einzelheiten[37]), den Besonderheiten bei Einsatzfahrzeugen der Bundeswehr, Polizei, Feuerwehr etc. sowie einer Evaluierung des Gesetzes zwischen 2024 und 2030.

Was das Haftungsregime im Straßenverkehrsrecht betrifft, verbleibt es bei der Halterhaftung nach §§ 7, 18 StVG. Die Haftungsgrenzen nach § 12 StVG, die bereits für hoch- und vollautomatisierte Fahrzeuge im Vergleich zu konventionellen Fahrzeugen erhöht wurden, gelten auch für autonome Kraftfahrzeuge.[38]

In einer ersten Gesamtbetrachtung ist positiv zu bewerten, dass durch diese jüngste Gesetzesnovelle bereits das „autonome Fahren" in den Blick der Legislative gerät, was im internationalen Kontext eher noch die Ausnahme darstellt und Deutschland eine gewisse Vorreiterrolle bei der Herstellung von Rechtssicherheit in diesem Bereich zuteilt. Schon die Errichtung und Arbeit der Ethikkommission für automatisiertes und vernetztes Fahren 2016/2017 stieß zumindest europaweit auf große Anerkennung und Interesse. Deren Erkenntnisse wurden vielfach rezipiert.

---

[35] Vgl. Abschlussbericht Ethikkommission, S 25, In dieser Kommission war der Verf. dieser Studie für genau diesen Teil der Berichterstattung zuständig.
[36] *Haupt*, NVZ 2021, 172, 175; *Steege*, SVR 2021, 128, 134f.
[37] Klärungsbedürftig ist unter anderem auch, welche Qualifikation die Person haben muss, die die Technische Aufsicht innehat, was im Verhinderungsfall gilt und wie Aufsicht im Detail wahrgenommen werden kann, hierzu *Haupt*, NVZ 2021, 172, 175; kritisch diesbezüglich auch *Steege*, SVR 2021, 128, 132f.
[38] Vgl. *Schrader*, ZRP 2021, 109, 111, der das fehlende Tätigwerden des Gesetzgebers in Sachen Haftung kritisch bewertet, wohingegen *Lutz*, DAR 2021, 182, 185 Änderungen des derzeitigen straßenverkehrsrechtlichen Haftungssystems nicht für erforderlich hält.

Auf der anderen Seite können die neuen Regelungen aber nur ein weiterer (Zwischen-) Schritt auf dem Weg in ein neues Recht der digitalen Verkehrsinfrastruktur sein.[39] Zum einen wird es darauf ankommen, ob die erwartete Rechtsverordnung für die gewünschte Konkretisierung und Klarstellung sorgen kann. Zum anderen muss sich das Zusammenspiel von Kfz-Hersteller, IT-Experten, Technischer Aufsicht und dem vorprogrammierten Fahrzeug in der Praxis erst beweisen. Das Gesetz zum autonomen Fahren bietet insoweit freilich eine agile Plattform, derer sich die zuständigen Behörden und unmittelbar mit dem Fahrbetrieb befassten Akteure auch bedienen müssen, immer in selbstkritischer Reflektion impulsgebend für eine ständige Weiterentwicklung dieser technischen und rechtlichen Innovation.

Wissenschaftlich begleitet wird diese Entwicklung unter anderem von der Forschungsstelle für Mobilitätsrecht an der TU Braunschweig[40], die ab dem 1.10.2021 von Anne Paschke geleitet wird und sich schwerpunktmäßig dann mit Rechtsfragen der Digitalisierung im Mobilitätssektor sowie dem europäischen Mobilitätsdatenraum befassen wird. Als Gastwissenschaftlerin am TUM Center for Digital Public Services (unter der Leitung des Verfassers der vorliegenden Studie) wird sie auch mit der TU München kooperieren und die Expertise der Forschungseinrichtungen bündeln.

[39] *Schrader*, ZRP 2021, 109.
[40] https://mobilitaetsrecht.net.

4 Datenschutz und IT-Sicherheit

Zusammenspiel von Datenschutz, Funktionssicherheit und Informationssicherheit

4.1 Begriffsbestimmungen

4.1.1 Datenschutz

Mit dem *Datenschutz* wird das Recht auf informationelle Selbstbestimmung gewährleistet (Art. 2 Abs. 1, Art. 1 Abs. 1 GG), also der Schutz des Einzelnen vor einer rechtswidrigen Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten. „Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (näher hierzu 4.3.2). Nicht vom Datenschutz erfasst sind also reine Sachdaten wie Wetterdaten, Bilanzen oder Konstruktionspläne (letztere unterliegen aber dem Geheimnisschutz des geistigen Eigentums und dürfen aus diesen Gründen nicht ohne Weiteres weitergegeben werden). Auch Maschinendaten sind zunächst Sachdaten, können aber einen Personenbezug haben, wenn und soweit man von ihnen etwa Rückschlüsse auf das Arbeitsverhalten von Arbeitnehmern ziehen kann, die diese Maschinen bedienen oder deren Produkte weiterverarbeiten. Ebenso kann etwa die Routenführung eines autonomen Fahrzeugs Auskunft geben über Aufenthaltsorte der hierdurch transportierten Passagiere.
Das Datenschutzrecht regelt, ob und unter welchen näheren Voraussetzungen (pesonenbezogene) Daten rechtmäßig erhoben, verarbeitet oder genutzt werden dürfen.

4.1.2 Funktionssicherheit und Informationssicherheit

Der Begriff der IT-Sicherheit ist zu untergliedern in die Teilbereiche Funktionssicherheit („Safety“) und Informationssicherheit („Security“).

Unter dem Begriff der *Funktionssicherheit*[41] ist ein IT-System zu fassen, dessen Ist-Funktionalität ohne Abweichungen der erwarteten Soll-Funktionalität entspricht.[42] Vereinfacht gesagt, nimmt ein funktionssicheres System also keine unzulässigen Zustände an[43] – es funktioniert wie vorgesehen, sodass es insbesondere seiner Umwelt (Personen / anderen Sachen / der Natur) keinen Schaden zufügt. Das IT-System soll hinsichtlich seiner Fehlerfrei-

[41] Vgl. zur funktionalen Sicherheit beim automatisierten Fahren bereits vbw, Automatisiertes Fahren – Datenschutz und Datensicherheit, 2018, S. 29ff.
[42] *Eckert*, IT-Sicherheit, 10. Aufl. 2018, S. 6.
[43] *Eckert*, IT-Sicherheit, 10. Aufl. 2018, S. 6.

heit unbedenklich eingesetzt werden können. Insbesondere auf höheren Automatisierungsstufen, auf denen eine dauerhafte Überwachung des Systems durch einen Menschen nicht mehr notwendig ist und das automatisierte System bislang menschlich durchgeführte Arbeitsabläufe eigenständig ersetzt, ist die Gewährleistung von Funktionssicherheit unverzichtbar. Dabei ergibt sich eine Verpflichtung zu einer funktionssicheren Systemausgestaltung bereits aus dem Produktsicherheitsgesetz, das in § 3 Abs. 1 ProdSiG normiert, dass durch ein Produkt die Sicherheit und Gesundheit von Personen nicht gefährdet werden darf. Weiterhin lässt sich eine solche Verpflichtung auch aus dem Strafrecht herleiten, welches beispielsweise die fahrlässige Körperverletzung unter Strafe stellt, wenn also aufgrund eines unsicheren Systems etwa eine Person verletzt wird. Neben diesen gesetzlichen Verpflichtungen zur funktionssicheren Systemausgestaltung ergibt sich dies aber auch mittelbar aus dem Haftungsrecht, da der Entwickler und Hersteller eines Systems Haftungsfolgen von vornherein vermeiden möchte und daher auf eine funktionssichere Technikgestaltung achten wird.

Mit *Informationssicherheit*[44] wird dagegen der Schutz der auf einem System gespeicherten und verarbeiteten Informationen gegen fremde Einsicht (Schutz der Vertraulichkeit), Veränderung (Schutz der Integrität) und Löschung (Schutz der Datenverfügbarkeit) verstanden. Ein Unterfall der Informationssicherheit ist dabei die sogenannte *Datensicherheit*, die explizit den Schutz der auf einem System gespeicherten und verarbeiteten personenbezogenen Daten bezweckt.

4.2 Zusammenspiel der IT-Sicherheit und des Datenschutzrechts

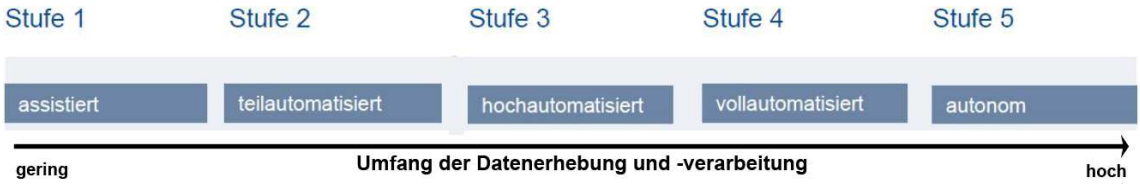
Die IT-Sicherheit und das Datenschutzrecht sind keine voneinander isolierbaren Bereiche. Vielmehr stehen die Funktionssicherheit (Safety), das Datenschutzrecht (Privacy) und die Informationssicherheit (Security) in ständiger Wechselwirkung zueinander.

Zum Beispiel ist es zur Erzielung von Funktionssicherheit gerade notwendig, dass zahlreiche Sensordaten über das Umfeld des Systems erhoben und verarbeitet werden. So kann ein automatisiertes Fahrzeug oder ein automatisierter Dienstleistungsroboter sein Umfeld (etwa die in der Nähe befindlichen Personen oder Sachen) nur dann bestmöglich schützen, wenn das System Kenntnis von seiner Umwelt hat (dies geschieht per Erhebung von Sensordaten) und diese Informationen zur Vermeidung von Unfällen und Beschädigungen auch gewinnbringend auswertet (dies geschieht per Verarbeitung der im vorherigen Schritt erhobenen Sensordaten). Mit steigendem Automatisierungsgrad steigt daher auch die Anzahl und der Umfang der notwendigen Datenerhebungen und -verarbeitungen, da die bislang menschlich durchgeführten Handlungen zunehmend durch automatisierte und intelligente Algorithmen ersetzt werden und diese auf Informationen beziehungsweise Daten angewiesen sind. Soweit die mittels Sensoren erfassten Informationen personenbeziehbar sind (was nicht immer, aber auch nicht selten der Fall ist), sind die datenschutzrechtlichen

[44] Vgl. zur Informationssicherheit beim automatisierten Fahren bereits vbw, Automatisiertes Fahren – Datenschutz und Datensicherheit, 2018, S. 29ff.

Anforderungen mit jenen der Gewährleistung von Funktions- und Informationssicherheit in Einklang zu bringen.

Abbildung 3
Umfang der Datenerhebung nach Automatisierungsstufe

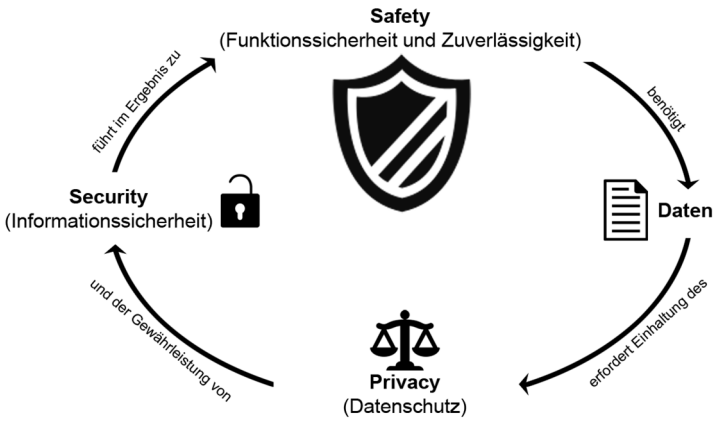


Quelle des Originals: bayme vbm vbw

Eine Erhöhung der *Funktionssicherheit* führt insofern zu dem Dilemma, dass aufgrund zahlreicher Datenerhebungen und -verarbeitungen der *Datenschutz* zunächst verschlechtert wird. Dieses Dilemma kann nur durch eine den Grundsätzen des Datenschutzrechts entsprechende technische Ausgestaltung (beispielsweise durch die technische Sicherstellung und Realisierung der Grundsätze der Datenvermeidung und der Datensparsamkeit) aufgelöst werden (Privacy by Design, Art. 25 Abs. 1 DSGVO).

Diese datenschutzrechtlich legitim erhobenen und gespeicherten Daten müssen sodann hinreichend gegen Fremdzugriff geschützt werden, was Aufgabe der *Informationssicherheit* ist.

Abbildung 4
Zusammenhang zwischen IT-Sicherheit und Datenschutz



Quelle: eigene Darstellung

4.3 Datenschutz in automatisierten Systemen

Es wurde schon gezeigt, dass bereits die Automatisierung von IT-Systemen an sich, insbesondere aber die Gewährleistung von Funktionssicherheit, von der Erhebung und Verarbeitung zahlreicher Sensordaten abhängig ist.[45]

Zu klären ist in diesem Zusammenhang, welche Rechtsgrundlagen für eine solche Datenerhebung und -verarbeitung in Betracht kommen können, welche Arten von Daten hierbei betroffen sind, welche allgemeinen datenschutzrechtlichen Grundsätze existieren und welche konkreten Rechtfertigungsvoraussetzungen für die Nutzung zu Primärzwecken (Realisierung der Automatisierung sowie Gewährleistung der Funktionssicherheit) dabei bestehen.

4.3.1 Rechtsquellen des Datenschutzrechts

4.3.1.1 Datenschutzgrundverordnung (DSGVO)

In erster Linie kommt bei der Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten in Deutschland die Datenschutzgrundverordnung (DSGVO) zur Anwendung. Als europäische Verordnung besitzt sie allgemeine und unmittelbare Geltung für die Mitgliedsstaaten der EU.[46] Sie enthält umfassende Bestimmungen für Verantwortliche zur Verarbeitung von personenbezogenen Daten und richtet sich innerhalb ihres Anwendungsbereiches unterschiedslos an öffentliche wie nicht-öffentliche Stellen. Gleichwohl eröffnet die DSGVO den Mitgliedsstaaten an verschiedenen Stellen die Möglichkeit, einzelne Teilbereiche des Datenschutzrechts in nationalen Regelungen umzusetzen und näher auszugestalten oder zu spezifizieren (sogenannte Öffnungsklauseln).[47]

4.3.1.2 Nationale Datenschutzbestimmungen

Das Bundesdatenschutzgesetz (BDSG) richtet sich gemäß § 1 Abs. 1 BDSG an öffentliche Stellen des Bundes und der Länder bei jedweder Verarbeitung personenbezogener Daten sowie an nichtöffentliche Stellen, soweit sie Daten entsprechend der DSGVO verarbeiten.[48] Handelt es sich bei dem datenschutzrechtlich Verantwortlichen nicht um eine öffentliche Stelle des Bundes, sondern um eine öffentliche Stelle eines Landes, ist der Anwendungsbereich des BDSG dagegen nur dann eröffnet, wenn der Datenschutz nicht durch Landesgesetze geregelt ist und soweit die Stelle Bundesrecht ausführt. Dabei ist zu beachten, dass der Anwendungsbereich der nationalen Regelungen grundsätzlich nur dann eröffnet ist, solange nicht die DSGVO unmittelbar gilt.[49] Dies ist insbesondere dann anzunehmen, wenn

---

[45] Zu der allgemeinen rechtlichen Herausforderung von Big Data vgl. *Heckmann*, vbw Studie: Big Data als Chance und Herausforderung für Unternehmen, 2016. Zur Unterscheidung zwischen personenbezogenen und sachbezogenen Daten vgl. noch Kapitel 3.3.2.
[46] *Heckmann/Scheurer* in: Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl., Kap. 9 Rn. 70.
[47] *Heckmann/Scheurer* in: Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl., Kap. 9 Rn. 73f.
[48] *Ernst* in: Paal/Pauly DSGVO BDSG, 3. Aufl. 2021, § 1 BDSG Rn. 2, 5.
[49] Vgl. dazu klarstellend § 1 Abs. 5 BDSG.

der Regelungsbereich der DSGVO gar nicht erfasst ist (so zum Beispiel im Bereich der nationalen Sicherheit[50]) oder, wenn Regelungen der DSGVO aufgrund von Öffnungsklauseln durch nationale Gesetze spezifiziert oder konkretisiert werden (so zum Beispiel zur Datenerhebung im Rahmen von Beschäftigungsverhältnissen nach § 26 BDSG).

Innerhalb der nationalen Regelungen wiederum hat das Bundesdatenschutzgesetz die Rolle eines Auffanggesetzes.[51] Nach § 1 Abs. 2 BDSG ist das Bundesdatenschutzgesetz nur anwendbar, wenn nicht speziellere bereichsspezifische Datenschutzgesetze vorliegen, die vorrangig anzuwenden sind.[52] Solche sind etwa das Telemediengesetz (TMG)[53] für die Betreiber von Telemedienangeboten (oft Webseiten) oder das Telekommunikationsgesetz (TKG) für die Betreiber von Telekommunikationsanlagen. Für die Betreiber von E-Health-Produkten ist weiterhin das Sozialgesetzbuch (SGB) relevant.

Ein eigenständiges, spezifisches Datenschutzrecht für automatisierte Systeme existiert dagegen nicht. Auch hinsichtlich des automatisierten Fliegens (konkret: des Betriebs unbemannter Flugkörper wie Drohnen) enthalten die Luftfahrtgesetze (insbesondere das LuftVG und die LuftVO) bislang keine spezifischen Datenschutzvorschriften.[54] Eine Ausnahme bietet das automatisierte Fahren: Hier enthält nunmehr § 1g StVG-neu durch das Gesetz über das autonome Fahren seit Ende Juli 2021 umfangreiche Regelungen zur Datenverarbeitung. Diese sind aber nicht ohne weiteres auf andere automatisierte Systeme übertragbar. Daher ist zur datenschutzrechtlichen Bewertung von automatisierten Systemen weiterhin auf die allgemeinen Datenschutzgesetze (insbesondere die DSGVO) zurückzugreifen.

4.3.2 Unterscheidung zwischen personenbezogenen und sachbezogenen Daten[55]

Sowohl die DSGVO (Art. 1 Abs. 1 DSGVO) als auch die datenschutzrechtlichen Spezialgesetze sind nur bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten anwendbar.[56] Zu unterscheiden ist demnach, ob die von einem automatisierten System erfassten Sensordaten personenbezogener oder sachbezogener Natur sind.

---

[50] *Ernst* in: Paal/Pauly DSGVO BDSG, 3. Aufl. 2021, § 1 BDSG Rn. 13.
[51] BT-Drs. 18/11325, 79; *Gola/Reif* in: Gola/Heckmann, BDSG, 13. Aufl. 2019, § 1 BDSG Rn. 11.
[52] *Ernst* in:Paal/Pauly DSGVO BDSG, 3. Aufl. 2021, § 1 BDSG Rn. 6f.
[53] Anmerkung: Die bereichsspezifischen Datenschutzvorschriften aus dem Telemediengesetz (TMG) und dem Telekommunikationsgesetz (TKG) werden zum 01.12.2021 in ein eigenes Gesetz, das Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien vom 23.06.2021, BGBl. 2021 I, S. 1982 (TTDSG) überführt. Zur bislang umstrittenen Frage der Anwendbarkeit der datenschutzrechtlichen Vorschriften des TMG neben der DSGVO siehe *Heckmann* in: Heckmann, juristPK Internetrecht, 6. Aufl 2019 (Vorauflage), Kap. 1 Rn. 21 m.w.N.
[54] Obgleich das LuftVG etwa schon spezifische Datenschutzvorschriften enthält. Diese betreffen bislang etwa aber nur die Einrichtung einer Flugsicherung (§ 27c LuftVG) und eines Flugwetterdienstes (§ 27e LuftVG), die Durchführung von Vorfeldinspektionen (§ 29 LuftVG) und die Erstellung von Luftfahrtdateien (§ 64 LuftVG).
[55] Vgl. etwa zu den beim automatisierten Fahren anfallenden Arten von Daten bereits das Positionspapier vbw, Automatisiertes Fahren – Datenschutz und Datensicherheit, 2018, S. 4f.
[56] So auch Art. 1 Abs. 1 DSGVO.

Dabei ist zu beachten, dass nach Art. 4 Nr. 1 DSGVO als personenbezogene Daten nicht nur persönliche oder sachliche Verhältnisse einer *identifizierten*, also bereits bestimmten, Person gelten, sondern es hierbei auch ausreicht, wenn die jeweilige Person zumindest *identifizierbar,* also bestimmbar, ist (Personenbeziehbarkeit). Nach Art. 4 Nr. 1 DSGVO ist eine Person identifizierbar, wenn sie direkt oder indirekt, insbesondere „mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“. Unbeachtlich ist dabei, ob eine solche Identifikation tatsächlich stattfindet, vielmehr reicht die wahrscheinliche Möglichkeit aus, dass eine Identifizierung erfolgen kann.[57]

Nach Erwägungsgrund 26 S. 3 und 4 zur DSGVO sollen, um festzustellen, ob eine natürliche Person identifizierbar ist, alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren. Dabei sollen „alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind“.[58]

Auch nach Inkrafttreten der DSGVO umstritten ist dabei jedoch die Frage, inwieweit das Zusatzwissen Dritter berücksichtigt werden muss. Dabei soll es nach einer Auffassung ausreichen, wenn der Betroffene zwar nicht von der verantwortlichen Stelle selbst, aber von irgendeiner – noch so entfernten – Person oder Stelle erkannt und identifiziert werden könnte (absolute Theorie).[59] Nach einer anderen Auffassung käme es vielmehr auf eine Identifizierbarkeit durch die verantwortliche Stelle selbst an (relative Theorie).[60] Dieser Streitfrage hat sich auch der EuGH im Rahmen der Personenbeziehbarkeit von dynamischen IP-Adressen angenommen und dabei einen Mittelweg zwischen beiden Ansätzen gewählt.[61] Nach dem EuGH sei zwar grundsätzlich der Theorie einer relativen Personenbeziehbarkeit zu folgen. Dennoch käme es hierbei nicht zwingend auf die Kenntnisse und Identifizierungsmöglichkeiten der verantwortlichen Stelle selbst an. Vielmehr sei es für eine Personenbeziehbarkeit auch ausreichend, wenn die Identifizierung lediglich mittels Zusatzwissens eines Dritten ermöglicht wird und die verantwortliche Stelle sich an diesen Dritten vernünftigerweise wenden könnte.[62] Aus dem Wortlaut lässt sich keine klare Lösung entnehmen, vorzugswürdig – auch im Hinblick auf die Rechtsprechung des EuGH – ist jedoch ein vermittelnd relativer Ansatz, nach dem entscheidend ist, welche Möglichkeiten und Mittel dem Verantwortlichen nach allgemeinem Ermessen zur Verfügung stehen.[63]

---

[57] *Arning/Rothkegel* in: Taeger/Gabel DSGVO BDSG, 3. Aufl. 2019, Art. 4 DSGVO Rn. 31.
[58] Vgl. EG 26 S. 4.
[59] *Arning/Rothkegel* in: Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, Art. 4 DSGVO Rn. 33.
[60] *Arning/Rothkegel* in: Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, Art. 4 DSGVO Rn. 34.
[61] EuGH Urt. v. 12.05.2016 – C-582/14 – BeckRS 2016, 81027.
[62] EuGH Urt. v. 12.05.2016 – C-582/14 – BeckRS 2016, 81027.
[63] Vgl. zu Erwägungsgrund 26; *Heckmann/Scheurer* in: Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl., Kap. 9 Rn. 122 f; vgl. zu IP-Adressen: EuGH, Urt. V. 19.10.2016 – C582/14, MMR 2016, 842, 843; im Ergebnis auch *Klar/Kühling* in: Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, Art. 4 DSGVO Rn. 26.

Im Rahmen von automatisierten Systemen, die oft mit Kameratechnik bestückt sind, könnte diese Streitfrage aber ohnehin dahinstehen, wenn die sich in dem Sensorerfassungsbereich des Systems befindlichen Personen im Detail erfasst werden und die dabei erhobenen Daten etwa auch deren Gesichtszüge beinhalten. Denn wird eine Person derart detailliert erfasst, liegt unter Umständen bereits eine Identifizierung vor; die Frage der Identifizierbarkeit stellt sich insofern nicht mehr.[64] Möchte man dieser weiten Auffassung nicht folgen, so muss zumindest im Rahmen der Identifizierbarkeit berücksichtigt werden, dass die heute frei zur Verfügung stehenden Instrumente, etwa der Face Recognition und der intelligenten Personensuche in sozialen Medien, eine Identifizierung bei einer Personenablichtung leichter ermöglichen als dies etwa bei dynamischen IP-Adressen der Fall ist. Im Ergebnis wird daher immer dann, wenn eine Person auf einer Kameraaufzeichnung anhand ihrer Gesichtszüge erkennbar ist beziehungsweise ihre Identifikation ermöglicht wird, ein personenbezogenes Datum vorliegen, auch wenn die Person der verantwortlichen Stelle bislang noch unbekannt ist.[65] Bei Übersichtsaufnahmen aus größerer Entfernung oder Aufnahmen mit sehr geringer Auflösung – beispielsweise beim Einsatz von Rückfahrkameras oder Notbremssystemen, denen es nur darauf ankommt, einen Menschen an sich zu identifizieren – ist ein Personenbezug oftmals nicht gegeben.[66]

Etwas anderes könnte sich nur dann ergeben, wenn das verwendete automatisierte System zur Informationsbeschaffung Emotionserkennung datenschutzkonform aufsetzt[67] oder erst gar keine solchen Kamerasysteme verwendet, sondern mittels sonstiger, „neutraler“ Sensoren (etwa mittels Ultraschall oder kapazitativer Berührungssensoren) ausgestattet ist, die von sich aus nicht imstande sind, personenbezogene Merkmale zu erheben, oder wenn intelligente Kamerasysteme verwendet werden, die immer dann keine Daten erheben, wenn sich eine Person im Erfassungsradius befindet (in diesem Fall stellt das System mittels „neutraler“ Sensoren lediglich fest, dass sich *eine* Person im Erfassungsradius befindet, erstellt dann aber keine personenbeziehbare Bild- oder Videoaufnahme). Doch auch in diesen Fällen kann eine Identifizierbarkeit dann doch vorliegen, wenn durch die Heranziehung zusätzlicher Kenntnisse (etwa des Schichtplans) oder zusätzlicher Sensorwerte (sogenannte Sensorfusion) theoretisch und nach der dargestellten Wahrscheinlichkeit doch noch ein eindeutiger Personenbezug hergestellt werden könnte.

Weiter darf nicht allein aus dem Grund, dass bei der technischen Ausgestaltung eines automatisierten Systems auf den Einsatz von Kameratechnik verzichtet wird, generell und ungeprüft darauf geschlossen werden, dass hierbei nur „neutrale“ Sensoren zum Einsatz kämen, die stets nur mittels Zusatzwissens einen Personenbezug zulassen würden. Betrachtet man die Erfassungsdetaildichte und -schärfe von 3D-Lidar-Systemen, die eine Abtastung ihrer Umgebung mittels Laserlicht vornehmen und die häufig beim automatisier-

[64] Auch nach Art. 4 Nr. 1 DSGVO liegt ein Personenbezug dann vor.
[65] *Arning/Rothkegel* in: Taeger/Gabel DSGVO BDSG, 3. Aufl. 2019, Art. 4 DSGVO Rn. 31.
[66] Vgl. vor Inkrafttreten der DSGVO *Scholz* in: Simitis, BDSG, 8. Aufl. 2014, § 6b BDSG Rn. 67.
so auch vor Inkrafttreten der DSGVO *Schmid*, K&R 2015, 217, 220; zum Einsatz bei Drohnen: *Lurtz*, ZD-A 2019, 06646.
[67] So etwa bei der Lösung von Pyramics, die 2017 mit dem For..Net Award, dem Preis für datenschutzkonforme Innovationen der Forschungsstelle für IT-Recht und Netzpolitik ausgezeichnet wurde: https://www.for-net.info/for-net-award/for-net-award-2017/.

ten Fahren zum Einsatz kommen, so ist hier – abgesehen von Abweichungen in der Farbdarstellung – nur schwerlich ein signifikanter datenschutzrechtlicher Unterschied zu der Verwendung von Kameras feststellbar.

Eine Datenerhebung mittels optisch-elektronischer Instrumente oder sonstiger Sensoreinrichtungen kann dabei sowohl bewusst und absichtlich (etwa durch die Erfassung der Personen im Umfeld des Systems, um diese zu schützen) oder in Form von unerwünschten Begleitdaten erfolgen. Neben dieser Datenerfassung im Außenbereich des Systems kann etwa im Rahmen von automatisierten Kfz auch eine Datenerhebung im Innenraum (etwa die Anzahl anwesender Passagiere oder Informationen über die Erfüllung der Anschnallpflicht der Insassen, etc.) und auch unabhängig von Sensordaten (etwa die Auswertung des Fahrverhaltens und Generierung eines Fahrprofils) erfolgen. Weiterhin können automatisierte Systeme personenbezogene Informationen auch aus bestehenden Datenbanken abrufen, speichern und selbst verarbeiten. Auch hier gelten die allgemeinen Regeln zur Personenbeziehbarkeit von Informationen: Soweit sich aus den erfassten Daten – gegebenenfalls in Verbindung mit zugänglichen weiteren Informationen – Rückschlüsse auf bestimmte Personen ziehen lassen, müssen die datenschutzrechtlichen Anforderungen eingehalten werden. Geht es hingegen um statistische Daten oder Messungen ohne Rückbeziehbarkeit in Bezug auf bestimmte oder bestimmbare Personen, liegen reine Sachdaten vor, für die die DSGVO keine Vorgaben macht.

Typisch sachbezogen sind auch etwa Systeminformationen zum Zustand und zur Abnutzung des Systems, zum Fortschritt des derzeitigen Arbeitsablaufes, zur Betriebszeit, zur Systemtemperatur, zum Akkustand und zum Energieverbrauch, bei automatisierten Straßen- und Luftfahrzeugen aber auch zu den Wetterbedingungen und zur Witterung. Auch solche zunächst sachbezogenen Informationen können im Einzelfall und insbesondere in Verbindung mit weiteren Informationen aber dann personenbezogene Daten darstellen, wenn sich hieraus dennoch Rückschlüsse auf die rechtliche, wirtschaftliche oder soziale Position des Betroffenen herleiten lassen oder diese Daten zur Beschreibung seiner individuellen Verhältnisse geeignet sind.[68] Letzteres kann vorliegen, wenn aus den zunächst sachbezogenen Daten des Fahrzeugs (Strecke, Laufzeit etc.) etwa das Fahrverhalten des Fahrzeugführers ausgelesen werden kann, so dass diese Informationen ebenfalls personenbezogene Daten darstellen.

4.3.3 Allgemeine Datenschutzgrundsätze

Die DSGVO, das BDSG, aber auch die weiteren nationalen datenschutzrechtlichen Spezialgesetze haben allgemeine datenschutzrechtliche Grundsätze gemeinsam, die sich überwiegend übergesetzlich aus dem Grundrecht auf informationelle Selbstbestimmung beziehungsweise der Charta der Grundrechte der Europäischen Union ergeben. Die wichtigsten dieser Grundsätze, insbesondere die der DSGVO, sollen nun zusammen mit ihrer Relevanz beim Einsatz automatisierter Systeme dargestellt werden.

---

[68] *Schild* in: BeckOK Datenschutzrecht, Wolff/Brink, 36. Ed. 01.05.2021, Art. 4 DSGVO Rn. 24; bejahend zu *Damman* in: Simitis, BDSG, 8. Aufl. 2014, § 3 BDSG Rn. 60; *Klar/Kühling* in: Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, Art. 4 DSGVO Rn. 13.

Praxistipp

Schon in der Entwicklungsphase eines automatisierten Systems muss auf eine datenschutzkonforme Technikausgestaltung geachtet werden. Insofern sollen die Datenschutzgrundsätze bereits ab Werk berücksichtigt und implementiert werden (sogenanntes „Privacy by Design“, Art. 25 Abs. 1 DSGVO).

4.3.3.1 Verbotsprinzip mit Erlaubnisvorbehalt

Aus Art. 6 Abs. 1 DSGVO ergibt sich das sogenannte „Verbotsprinzip mit Erlaubnisvorbehalt“. Hiernach ist eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten nur zulässig, wenn dies gesetzlich erlaubt ist. Im Rahmen der weiteren datenschutzrechtlichen Untersuchung wird sich daher stets die Frage stellen, ob für eine spezifische datenschutzrelevante Handlung jeweils ein gesetzlicher Erlaubnistatbestand vorliegt. Eine solche datenschutzrechtliche Erlaubnis kann sich insbesondere ergeben, wenn (vereinfach gesagt)

- die betroffene Person wirksam in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat und dies auf ihrer freiwilligen Entscheidung sowie jener Information über Art und Ausmaß dieser Verarbeitung beruht, die ihr von der verarbeitende Stelle vorab zur Verfügung gestellt wurde (sogenannte informierte Einwilligung) oder
- eine gesetzliche Grundlage die Datenverarbeitung ausdrücklich erlaubt oder
- eine Abwägung der Interessen des Betroffenen mit jenen der verarbeitenden Stelle ergibt, dass letztere deutlich überwiegen.

Das sogenannte Verbotsprinzip will keineswegs Datenverarbeitung und Datennutzung, sondern lediglich einen willkürlichen Umgang mit personenbezogenen Daten verhindern. Greift auch nur einer der Erlaubnistatbestände, ist die Datenverarbeitung grundsätzlich zulässig. Es sind dann nur die in der DSGVO näher geregelten Grundsätze und Vorkehrungen zu beachten, von denen die wichtigsten im Folgenden kurz dargestellt werden.

4.3.3.2 Prinzip der Datenminimierung

Nach Art. 5 Abs. 1 lit. c) DSGVO ist bei der Verarbeitung personenbezogener Daten darauf zu achten, dass diese dem Zweck angemessen sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind (Datenminimierung). Dieses Prinzip der Datenminimierung normiert insofern, dass nicht mehr Daten erhoben oder verarbeitet werden dürfen, als dies tatsächlich erforderlich ist. Zudem sind Daten nach Ablauf dieser Erforderlichkeit unverzüglich zu löschen und, wenn möglich und nicht unverhältnismäßig, zu anonymisieren oder zu pseudonymisieren (vgl. auch Art. 17 DSGVO).[69]

[69] Vgl. zur Anonymisierung und Pseudonymisierung auch vbw, Positionspapier Automatisiertes Fahren – Datenschutz und Datensicherheit, 2018, S. 21f.

Aus diesem Gebot der Datenminimierung und der Konkretisierung nach der Vorschrift zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (vgl. Art. 25 DSGVO – Privacy by Design/Default)[70] ergibt sich die Verpflichtung des Verantwortlichen eines automatisierten Systems, den Umfang der Datenerhebung und -verarbeitung schon im Rahmen der technischen Systemausgestaltung gering zu halten.

Werden per Sensor etwa Informationen über das Umfeld erhoben, sind schon im Zeitpunkt dieser Datenerhebung irrelevante und entbehrliche Informationen zu ignorieren *(Stufe 1)*. Dies bedarf insofern einer Beschränkung der Erfassungsreichweite der Sensoren, um nicht im Rahmen von unerwünschten Begleitdaten auch unnötige personenbezogene Daten zu erheben. Weiterhin befinden sich hierzu derzeit auch intelligente Sensor-/Kamerasysteme in der Entwicklung, die dann, wenn sich ein Mensch im Erfassungsbereich befindet, keine Daten erheben. Dennoch wird sich eine Datenerhebung auf dieser ersten Stufe nicht immer vermeiden lassen, da das automatisierte System entweder auf eine kontinuierliche Datenerhebung oder aber gerade auf die Erhebung von personenbezogenen oder -beziehbaren Daten angewiesen sein könnte.

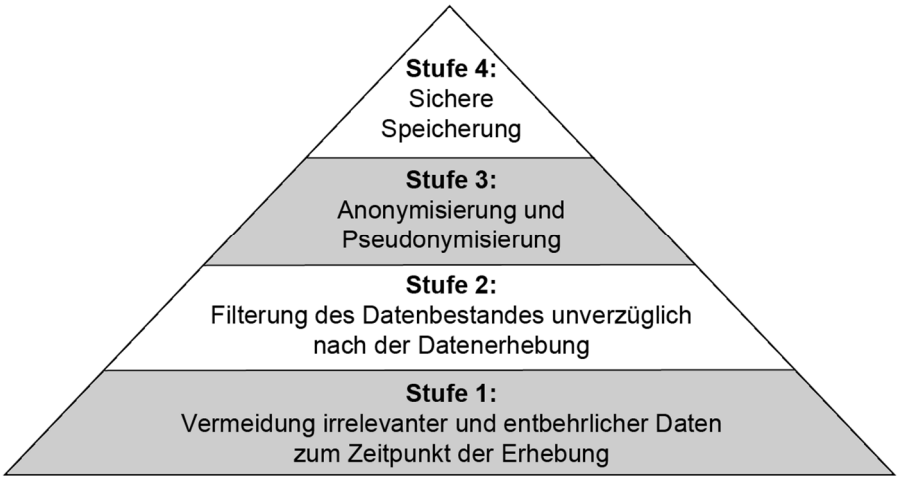
Unverzüglich nach dieser Datenerhebung ist der erhobene Datenbestand dann nach dennoch erhobenen, aber unnötigen Daten zu durchsuchen und sind diese auszufiltern *(Stufe 2)*.

Relevante personenbezogene Daten, die nicht ausgefiltert werden können, da diese für die weitere Systemausführung notwendig sind, sind – soweit möglich – unverzüglich zu anonymisieren oder zumindest zu pseudonymisieren *(Stufe 3)*.

Die verbleibenden Restdaten sind dann verschlüsselt und gegen fremde Einsicht geschützt zu speichern und unverzüglich zu löschen, wenn diese nicht mehr benötigt werden *(Stufe 4)*.

[70] *Heberlein* in: Ehmann/Selmayr, Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 5 DSGVO Rn. 23.

Abbildung 5
Pyramide der Datenvermeidung bei automatisierten Systemen



Quelle: eigene Darstellung

4.3.3.3 Zweckbindungsgrundsatz

Bei der Nutzung automatisierter Systeme ist zwischen Primär- und Sekundärzwecken zu unterscheiden. Während die Primärzwecke der grundsätzlichen Realisierung des automatisierten Systems sowie der Gewährleistung von Funktionssicherheit dienen, sollen die Daten im Rahmen der sekundären Zwecke auch für darüberhinausgehende Aufgaben (etwa Forschung, Entwicklung, Marketing, Nutzungsberichte etc.) verwendet werden.

Nach dem sogenannten Zweckbindungsgrundsatz gem. Art. 5 Abs. 1 lit. b) DSGVO sind bei der Verarbeitung von personenbezogenen Daten die von der verantwortlichen Stelle, also dem „Datenverarbeiter“, entsprechend seinem (legitimen) Geschäftsmodell vorher festgelegten Verarbeitungszwecke aber strikt einzuhalten und die Daten dürfen nicht in einer mit diesem Zweck nicht zu vereinbarenden Weise weiterverarbeitet werden.[71] Dies unterbindet zum einen eine Datenerhebung für unbestimmte Zwecke „auf Vorrat“. Zum anderen wird hierdurch auch eine spätere Zweckänderung erschwert, die dann gegebenenfalls nur nach zusätzlicher Einwilligung des Betroffenen möglich ist.

4.3.3.4 Grundsatz der Speicherbegrenzung

Die Speicherung personenbezogener Daten darf nach Art. 5 Abs. 1 lit. e) DSGVO im Grundsatz ausschließlich so erfolgen, dass die Identifizierung der betroffenen Personen nur so

[71] Vgl. auch *Heckmann/Scheurer* in: Heckmann/Paschke, jurisPK Internetrecht, 7. Aufl. 2021, Kap. 9 Rn. 220.

lange ermöglicht wird, wie es für die Zwecke der Verarbeitung erforderlich ist. Hierdurch wird der Grundsatz der Zweckbindung um eine zeitliche Komponente ergänzt, nach der Daten nur innerhalb des maßgeblichen Zeitraums verarbeitet werden dürfen; dabei sind auch Löschkonzepte zu entwickeln, die konkrete Fristen vorgeben und technische Maßnahmen bereitstellen.[72] Im Rahmen von automatisierten Systemen ist darauf zu achten, dass die eingesetzten Sensoren und Systeme, die personenbezogene Daten erfassen können, diese zeitlich nur so lange erfassen, solange es für die Funktionstüchtigkeit des jeweiligen Systems erforderlich ist. Im Anschluss daran müssen Daten anhand von kurzen Löschkonzepten gelöscht werden.

4.3.3.5 Grundsatz der Vertraulichkeit und Integrität

Personenbezogene Daten müssen nach Art. 5 Abs. 1 lit. f) DSGVO in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen. Durch Art. 5 Abs.1 lit. f) DSGVO wird die Datensicherheit als Grundsatz der Datenverarbeitung normiert. Der Grundsatz findet weitere Ausprägungen in den Pflichten des Verantwortlichen nach Art. 24, 25 und 32 DSGVO.[73]

4.3.3.6 Grundsatz der Transparenz

Nach Art. 5 Abs. 1 lit. a) DSGVO müssen personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffenen Person nachvollziehbaren Weise verarbeitet werden. Neben dem Grundsatz der Verarbeitung nach Treu und Glauben ist hier der Grundsatz der Transparenz geregelt.[74] Nach Erwägungsgrund 39 S. 3 zur DSGVO sollen Informationen und Mitteilungen zur Verarbeitung leicht zugänglich und verständlich in klarer und einfacher Sprache abgefasst werden, wobei besonders die Information über den Verantwortlichen, sowie die Zwecke der Verarbeitung und sonstige Informationen relevant sind. Nur, wer um Datenverarbeitungsvorgänge weiß und in die Lage versetzt wird, sie zu verstehen, kann mögliche Risiken und Gefahren feststellen und darauf reagieren.[75] Der Transparenzgrundsatz findet seine konkrete Ausprägung in den Informationspflichten nach Art. 12 ff. DSGVO, aber auch im Rahmen von Privacy by Design und Default gemäß Art. 25 DSGVO sowie einigen weiteren Normen.[76]

---

[72] *Herbst* in: Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, Art. 5 DSGVO Rn. 65; *Heckmann/Scheurer* in: Heckmann/Paschke, jurisPK Internetrecht, 7. Aufl. 2021, Kap. 9 Rn. 230 f.
[73] Vgl. dazu Kapitel 3.4; *Heckmann/Scheurer* in: Heckmann/Paschke, jurisPK Internetrecht, 7. Aufl. 2021, Kap. 9 Rn. 232 ff., 482 ff.
[74] Vgl. dazu *Heckmann/Scheurer* in: Heckmann/Paschke, jurisPK Internetrecht, 7. Aufl. 2021, Kap. 9 Rn. 217 ff.
[75] Vgl. dazu *Heckmann/Scheurer* in: Heckmann/Paschke, jurisPK Internetrecht, 7. Aufl. 2021, Kap. 9 Rn. 218.
[76] *Herbst* in: Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, Art. 5 DSGVO Rn. 19.

4.3.4 Beispiel: Zulässigkeit der Datenerhebung und -verarbeitung nach der DSGVO bei Verwendung einer automatisierten Industriedrohne

Nach dem Grundsatz des Verbotsprinzips mit Erlaubnisvorbehalt aus Art. 6 Abs. 1 DSGVO ist eine Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn das Gesetz dies erlaubt, insbesondere wenn eine Einwilligung des Betroffenen vorliegt. Das Vorliegen dieser Rechtmäßigkeitsvoraussetzungen kann dabei stets nur für den konkreten Einzelfall beurteilt werden. Das Vorgehen bei der datenschutzrechtlichen Rechtmäßigkeitsprüfung soll im Folgenden daher anhand eines solchen konkreten Einzelfalles beispielhaft aufgezeigt werden. Hierfür soll folgendes Szenario zugrunde gelegt werden:

Das Werksgelände eines Industrieunternehmens wird von einer öffentlichen Straße in zwei Teile getrennt. Auf beiden Teilen des Werksgeländes finden sich Produktionsstätten. Zum Transport kleinerer Bauteile von dem einen Werksgelände über die öffentliche Straße hinweg zu dem anderen Werksgelände sollen künftig automatisierte Industriedrohnen eingesetzt werden, die zur Erfassung ihrer Umgebung intelligente Kamerasysteme, also optisch-elektronische Einrichtungen, verwenden.

Datenschutzrechtliche Relevanz erhält dieser Anwendungsfall dadurch, dass die automatisierte Transportdrohne zahlreicher Sensorinformationen (insbesondere durch Kamerasysteme und sonstige optisch-elektronische Einrichtungen) zur 1) Orientierung im Raum, 2) Routenbestimmung, 3) Erkennung und Vermeidung von Hindernissen und 4) zum Schutz von in der Nähe befindlichen Personen und Sachen bedarf.

Da die DSGVO sowohl Daten, die sich auf identifizierte als auch auf identifizierbare Personen beziehen schützt, (vgl. Art. 4 Nr. 1 DSGVO sowie Kapitel 3.3.2) ist davon auszugehen, dass sich unter den erhobenen und verarbeiteten Sensorinformationen auch zahlreich datenschutzrechtlich relevante Daten befinden werden. Dies betrifft zumindest Informationen über die sich auf den Werksgeländen befindlichen Arbeitnehmer, die eine Identifizierbarkeit ermöglichen.[77] Doch auch hinsichtlich der Passanten auf dem überflogenen öffentlichen Grundstück ist ein Personenbezug dann zu bejahen, wenn hierbei deren Gesichtszüge oder das sonstige äußere Erscheinungsbild erkennbar aufgezeichnet wird und die Personen daher identifiziert oder mit noch verhältnismäßigem Aufwand identifizierbar sind.[78]

Im Sinne der oben bereits dargestellten „Pyramide der Datenvermeidung bei automatisierten Systemen“ sind dabei technisch alle möglichen und verhältnismäßigen Maßnahmen einzusetzen, um das Anfallen von personenbezogenen Daten bereits zum Zeitpunkt der Erhebung zu vermeiden (Stufe 1). Trotz dieser ersten Schutzmaßnahme werden von der Drohne aber zahlreiche personenbezogene Daten erhoben werden, die anschließend teilweise gefiltert (Stufe 2) und anonymisiert oder pseudonymisiert (Stufe 3) werden. Bereits diese anfängliche Datenerhebung von personenbezogenen Daten, auch wenn diese Daten

[77] Die hierbei erhobenen und verarbeiteten Daten enthalten zumindest die Informationen, dass sich eine bestimmte Person zu einer bestimmten Zeit an einem bestimmten Ort aufgehalten hat, sodass Identifizierbarkeit angenommen werden kann.
[78] Vgl. *Schild* in: BeckOK Datenschutzrecht, Wolff/Brink, 36. Ed. 01.05.2021, Art. 4 DSGVO Rn. 14 f sowie bereits Kapitel 3.3.2.

später wieder ausgefiltert oder anonymisiert werden, bedarf einer gesetzlichen Grundlage oder einer Einwilligung der Betroffenen. Weiterhin verbleiben auch nach der Filterung und (jedenfalls bei der) Pseudonymisierung personenbezogene oder -beziehbare „Restdaten“ bei der Drohne, wenn die Drohne gerade diese zur Erledigung ihrer Aufgaben benötigt. Diese Datenverarbeitung und -nutzung bedarf einer weiteren gesetzlichen Grundlage oder einer Einwilligung der Betroffenen.

4.3.4.1 Bezüglich der Arbeitnehmer auf dem Werksgelände

4.3.4.1.1 Datenschutzrechtlicher Erlaubnistatbestand zur Datenerhebung und -verarbeitung nach DSGVO und BDSG

Die Datenerhebung und -verarbeitung der Arbeitnehmerdaten auf dem Werksgelände könnte zunächst durch einen gesetzlichen Erlaubnistatbestand der DSGVO oder des BDSG gerechtfertigt sein. Wäre ein solcher Erlaubnistatbestand einschlägig, bedürfte es keiner zusätzlichen Einwilligung der Betroffenen. Für die Datenerhebung und Datenverarbeitung der Industriedrohne kommen im Verhältnis zu den Arbeitnehmern primär Art. 6 DSGVO, aber auch § 4 BDSG, der eine spezielle Ermächtigungsgrundlage für die Videoüberwachung enthält, sowie § 26 BDSG, der eine spezielle Ermächtigung für die Datenverarbeitung im Beschäftigungsverhältnis vorsieht, in Betracht.

Hinsichtlich des § 4 BDSG muss aber bereits festgestellt werden, dass hierbei dem Wortlaut nach nur „öffentlich zugängliche Räume“ betroffen sind, wovon im Rahmen eines durch Mitarbeiterausweise und Zugangskontrollen gesicherten Betriebsgeländes grundsätzlich nicht ausgegangen werden kann. Außerdem findet § 4 BDSG keine Anwendung für nichtöffentliche Stellen.[79]

Für Drohnenflüge auf dem nicht-öffentlichen Werksgelände müsste die Erhebung und Verarbeitung der automatisiert ausgewerteten Bilddaten also auf Art. 6 DSGVO oder § 26 BDSG gestützt werden. § 26 BDSG spezifiziert die DSGVO im Rahmen einer Öffnungsklausel zur Datenverarbeitung von Beschäftigten für Zwecke des Beschäftigungsverhältnisses und ist anwendbar, soweit die Daten zur Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses verarbeitet werden. Maßgeblich für den sachlichen Anwendungsbereich gegenüber der DSGVO ist insoweit der Begriff des „Beschäftigungskontextes“ nach der Öffnungsklausel des Art. 88 Abs. 1 DSGVO, die den Rahmen für konkretisierende nationale Regelungen festlegt.[80] Für andere nicht ausdrücklich festgelegte Bereiche der Datenverarbeitung – auch im Beschäftigtenkontext - gilt weiterhin die DSGVO[81]; insbesondere ist diesbezüglich an eine Rechtfertigung durch Interessenabwägung nach Art. 6 Abs. 1 lit. f) DSGVO zu denken. Im Rahmen von Überwachungssystemen erfolgt die Prü-

[79] *Schröder*, ZD 2021, 302.
[80] *Franzen*, Erfurter Kommentar zum BDSG, 21. Aufl. 2021, § 26 BDSG Rn. 7.
[81] Vgl. *Gräber/Nolden* in: Paal/Pauly, DSGVO BDSG, 3. Aufl. 2021, § 26 BDSG Rn. 8-10.

fung der Rechtmäßigkeit im Zweifel nach der DSGVO, da diese von § 26 BDSG nicht ausdrücklich aufgegriffen werden.[82] Für den Einsatz von Drohnen kann im Einzelfall aber eine Verarbeitung nach § 26 BDSG vorliegen, wenn die eingesetzte Drohne für den Arbeitsablauf und somit für die Durchführung der Beschäftigungsverhältnisse notwendig ist, da dann ein solcher Kontext vorliegt.

Nach § 26 Abs. 1 S. 1 BDSG dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses dann erhoben, verarbeitet oder genutzt werden, wenn dies unter anderem für die Durchführung des Beschäftigungsverhältnisses *erforderlich* ist oder zur Aufklärung möglicher Pflichtverletzungen im Rahmen der Beendigung nötig ist.[83]

Durch das Kriterium der Erforderlichkeit wird dabei jedoch deutlich, dass an die technische Ausgestaltung der automatisierten Industriedrohne hohe Anforderungen hinsichtlich der Datensparsamkeit und Datenminimierung zu stellen sind. Zudem wurde auch im Kontext von Videoüberwachungsmaßnahmen am Arbeitsplatz, die jedenfalls technisch mit den hier in Rede stehenden datenerhebenden und –verarbeitenden automatisierten Systemen vergleichbar sind, im Schrifttum und in der Rechtsprechung bereits zum früher einschlägigen und fast vollständig übernommenen § 32 Abs. 1 S. 1 BDSG a. F. ausgeführt, dass dieser äußerst restriktiv anzuwenden ist. Vorliegend ist aber zu bedenken, dass der Einsatz der Kameratechnik in der Industriedrohne lediglich dem ordnungsgemäßen Funktionieren der Drohne und sogar dem Schutz des Arbeitnehmers dient, eine Überwachung also weder angedacht ist noch tatsächlich stattfindet. Der Kameraeinsatz bei Industriedrohnen ist insofern doch nicht mit einer typischen Videoüberwachung eines Betriebes vergleichbar, sodass der Eingriff in das Recht auf informationelle Selbstbestimmung des Arbeitnehmers, im Vergleich zur tatsächlichen Videoüberwachung, hier geringer ausfällt.

Gerade hinsichtlich der Erfüllung der Tatbestandsmerkmale des § 26 Abs. 1 Satz 1 BDSG kommt es auf eine strikte Einhaltung der oben dargestellten *Pyramide der Datenvermeidung bei automatisierten Systemen* an. Je nach Art und Weise des konkret eingesetzten automatisierten Systems sowie abhängig von dem Ausmaß der dabei durchgeführten Datenerhebung und -verarbeitung wird in entsprechenden Fällen hilfsweise aber auf eine Einwilligung des Arbeitnehmers zurückgegriffen werden müssen.

4.3.4.1.2 Einwilligung in die Datenerhebung und -verarbeitung

Die Möglichkeit für die Erteilung einer datenschutzrechtlichen Einwilligung im Beschäftigtenkontext ergibt sich aus § 26 Abs. 2 BDSG. Dieser spezifiziert die Anforderung an die Einwilligung nach der DSGVO in Bezug auf die Besonderheiten des Beschäftigtenkontext. Die Grundelemente der Einwilligung ergeben sich aus Art. 4 Nr. 11 DSGVO. Danach erforderlich ist eine unmissverständliche Erklärung oder Handlung in freiwilliger, informierter

---

[82] *Gräber/Nolden* in: Paal/Pauly DSGVO BDSG, 3. Aufl. 2021, § 26 BDSG Rn. 11; vgl. auch *Heckmann/Scheurer* in: Heckmann/Paschke, jurisPK Internetrecht, 7. Aufl. 2021, Kap. 9, Rn. 987ff.
[83] So zur Fortgeltung der BAG Rechtsprechung unter der DSGVO: *Maschmann* in: Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, § 26 BDSG Rn. 45a.

Weise, durch die das Einverständnis mit der Verarbeitung erkennbar ist.[84] Die Freiwilligkeit der Einwilligung liegt vor, wenn die Möglichkeit gegeben ist, die Einwilligung auch zu verweigern, ohne dabei Nachteile zu erleiden.[85]

Eine solche Einwilligungslösung ließe sich zunächst innerbetrieblich – etwa im Rahmen einer von den Angestellten zu unterzeichnenden Betriebsvereinbarung – in Erwägung ziehen.[86] In der Rechtswissenschaft umstritten war nach der früheren Gesetzeslage, ob eine solche Einwilligung den hierfür notwendigen Tatbestand der „Freiwilligkeit" erfüllen kann, als sich die Arbeitnehmer stets in einer gewissen Über- / Unterordnungsposition befinden. Nach dem neu gefassten BDSG konkretisiert § 26 Abs. 2 BDSG die Anforderungen an die Freiwilligkeit im Beschäftigtenkontext und die Form der Einwilligung. Gemäß § 26 Abs. 2 S. 1 BDSG sind bei der Beurteilung der Freiwilligkeit die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen eine mögliche Einwilligung erteilt wird, zu berücksichtigen. Nach § 26 Abs. 2 S. 2 BDSG kann Freiwilligkeit insbesondere dann vorliegen, wenn für die beschäftigte Person durch die Datenverarbeitung ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen.

Die arbeitnehmerdatenschutzrechtliche Relevanz verdeutlicht auch der hier in Rede stehende Anwendungsfall: Besonders bei der Kameraerfassung von Arbeitnehmern entsteht für diese schnell eine gewisse Drucksituation – da diese Art der Datenerhebung (auch wenn dies tatsächlich nicht gegeben ist) einen gewissen Überwachungscharakter besitzt, welchem der Arbeitnehmer durchgängig ausgesetzt ist.

Wie bereits erläutert wurde, dient der Einsatz der optisch-elektronischen Einrichtungen in der Industriedrohne aber lediglich dem ordnungsgemäßen Funktionieren der Drohne und gar dem Schutz der Arbeitnehmer. Eine Überwachung ist dabei also weder angedacht, noch findet eine solche tatsächlich statt, sodass der Eingriff in das Recht auf informationelle Selbstbestimmung des Arbeitnehmers hierbei im Vergleich zur herkömmlichen Videoüberwachung geringer ausfällt. Dieser Eingriff wird unter strikter Beachtung der oben bereits dargestellten *Pyramide der Datenvermeidung bei automatisierten Systemen* weiter minimiert, indem die personenbezogenen Arbeitnehmerdaten alsbald anonymisiert oder wieder vom System gelöscht werden, wenn diese für das Funktionieren des Systems nicht mehr relevant sind. Dies kann unter Umständen auch innerhalb weniger Sekunden bereits der Fall sein.

Ist im vorliegenden Beispielsfall sichergestellt, dass das automatisierte System keine (Total-)Überwachungsgefahr institutionalisiert und werden die stattfindenden Datenerhebungs- und Datenverarbeitungsschritte ausführlich in der Einwilligungserklärung erläutert, so kann eine „freiwillige" Einwilligung der Arbeitnehmer in entsprechenden Anwendungsszenarien zumindest in Betracht kommen.

---

[84] Vgl. auch *Maschmann* in: Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, § 26 BDSG Rn. 62.
[85] Vgl. auch *Maschmann* in: Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, § 26 BDSG Rn. 62.
[86] Vgl. dazu § 26 Abs. 4 BDSG, der ausdrücklich die Möglichkeit einer Vereinbarung durch Kollektivvereinbarungen vorsieht.

4.3.4.2 Bezüglich der Passanten auf dem öffentlichen Terrain

4.3.4.2.1 Datenschutzrechtlicher Erlaubnistatbestand zur Datenerhebung und -verarbeitung nach DSGVO und BDSG

Für Passanten und Dritte, die sich wie im Anwendungsbeispiel in öffentlich zugänglichen Räumen bewegen, ergibt sich die Zulässigkeit der Datenerhebung und -verarbeitung aus einer Interessensabwägung nach Art. 6 Abs. 1 S. 1 lit. f) DSGVO.[87] Zwar hat der Gesetzgeber mit § 4 BDSG eine nationale Vorschrift zur Konkretisierung der Videoüberwachung als besondere Form der Datenverarbeitung geschaffen, die unter anderem eine Zulässigkeit zur Wahrnehmung des Hausrechts regelt. Allerdings eröffnet die DSGVO in Art. 6 Abs. 1 S. 1 lit. e), Abs. 3, Abs. 2 DSGVO lediglich die Möglichkeit zur Konkretisierung durch öffentliche Stellen, während die Öffnungsklausel nicht-öffentliche Stellen – wie ein privates Firmengelände – nicht mehr umfasst, sodass die Rechtfertigungsgründe der DSGVO maßgeblich sind.[88]

Danach ist die Verarbeitung unter anderem dann zulässig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Auch hier ist eine Videoüberwachung zwar nur dann zulässig, wenn sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und die schutzwürdigen Interessen der Betroffenen nicht überwiegen. Das Tatbestandskriterium der berechtigten Interessen umfasst dabei aber jedes tatsächliche Interesse wirtschaftlicher oder ideeller Natur und damit auch eigene Geschäftszwecke (hier der Transport von Bauteilen auf das angrenzende Werksgelände und insofern die Aufrechterhaltung des ordnungsgemäßen Betriebs des Unternehmens).[89] Die Einhaltung des gesetzlichen Tatbestands ist insofern keineswegs ausgeschlossen, sondern bei Beachtung bestimmter technischer und rechtlicher Erforderlichkeits- und Verhältnismäßigkeitsmaßstäbe durchaus erfüllbar. Bei Drohnenflügen über eine öffentliche Straße müsste etwa die technische Gestaltung der Drohne so konzipiert sein, dass bei sämtlichen Datenerhebungs- und Datenverarbeitungsschritten der Eingriff in die Rechte der Betroffenen möglichst gering gehalten wird und nur insoweit geschieht, wie dies für die ordnungsgemäße Funktion der Drohne zwingend notwendig ist. Dies kann erneut durch strenge Umsetzung der bereits dargestellten Pyramide der Datenvermeidung bei automatisierten Systemen erfolgen.

Eine früher regelmäßig diskutierte Hinweispflicht wie in § 4 Abs. 2 BDSG folgt aus den einschlägigen Regelungen der DSGVO nicht grundsätzlich.[90] Insoweit wäre regelmäßig Art. 14

---

[87] Als Voraussetzung gilt hierfür erneut, dass die Einsichtnahme der Drohne in den öffentlichen Raum mit einer gewissen Zeitdauer erfolgt („Beobachtung") und mithin eine „Videoüberwachung" im Sinne der Vorschrift vorliegt. Wie oben bereits erläutert wurde, ist aber davon auszugehen, dass das ordnungsgemäße Funktionieren einer automatisierten Industriedrohne von einer kontinuierlichen Umgebungserfassung abhängig sein wird und das Tatbestandsmerkmal mithin vorliegt.
[88] So u.a. *Buchner* in: Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, § 4 BDSG Rn. 11; *Wilhelm* in: BeckOK Datenschutzrecht, Wolff/Brink, 36. Ed. 01.05.2021, § 4 BDSG Rn. 28; *Grabenschröer/Reuther* in: Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, § 4 BDSG Rn. 43.
[89] Vgl. *Buchner/Petri* in: Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, Art. 6 DSGVO Rn. 146a.
[90] Vgl. dazu: *Schröder*, ZD 2021, 302, 307.

DSGVO im Rahmen der Informationspflichten anzuwenden, der aber eine Ausnahme vorsieht, wenn die Erteilung der Informationen unmöglich oder unverhältnismäßig wäre (Art. 14 Abs. 5 DSGVO), was zumindest zugunsten der Aufklärung von Passanten bei einem fahrenden automatisierten Fahrzeug anzunehmen wäre (im Gegensatz zum aufzuklärenden Fahrer).[91] Eine Hinweispflicht könnte sich letztlich aus dem Transparenzgrundsatz nach Art. 5 Abs. 1 lit. a) DSGVO ergeben, der eine proaktive Förderung der Transparenz vorsieht; allerdings folgt hieraus nicht zwangsläufig eine konkrete Handlungspflicht im Hinblick auf die geringen Beeinträchtigungen.[92] Auch im Beispielsfall der Transportdrohne erscheint eine individuelle Information der Passanten entbehrlich. Es genügt ein allgemeines Hinweisschild, wie man es auch von der Videoüberwachung bei Kriminalitätsschwerpunkten kennt – jedenfalls solange das Betriebsgelände durch Dritte frei zugänglich ist.

4.3.4.2.2 Einwilligung in die Datenerhebung und -verarbeitung

Da es sich bei Passanten zumeist um unbekannte Dritte handelt, ist eine allgemeine Einwilligungslösung hier schon faktisch unmöglich. Nicht legitim wäre dabei auch, auf der Straße entsprechende Hinweisschilder aufzustellen und dann anzunehmen, dass der Passant, der die Straße dennoch betritt, in die Datenerhebung und -verarbeitung durch das Betreten konkludent einwilligt.[93] Eine datenschutzrechtliche Einwilligung muss, wie bereits ausgeführt, stets freiwillig erfolgen, was dann regelmäßig nicht gegeben ist, wenn hierbei ein faktischer Zwang (hier: Entzug der Möglichkeit, eine öffentliche Straße zu nutzen) ausgeübt wird. Anders könnte das beurteilt werden, wenn es um ein faktisch zugängliches Betriebsgelände geht und der Passant (anders als ein Beschäftigter) nicht auf die Straßennutzung (etwa als Abkürzung) angewiesen ist.

4.4 Funktionssicherheit (Safety) automatisierter Systeme

Naturgemäß sind die technischen Anforderungen an die Funktionssicherheit eines automatisierten Straßenfahrzeugs anders als etwa bei einem automatisierten Luftfahrzeug und erneut anders bei einem automatisierten Rasenmähroboter. Die zur Erzielung von Funktionssicherheit notwendigen Maßnahmen und Konstruktionsvorschriften sind insofern hochgradig einzelfall- und systemabhängig und lassen sich daher nicht pauschal für alle automatisierten Systeme verallgemeinern. Vielmehr sind hierbei stets die spezifischen Gefahren und Eigenheiten des jeweiligen Systems zu berücksichtigen. Auch im Rahmen dieser Studie können daher nicht alle für ein spezifisches automatisiertes System in Betracht kommenden Vorschriften aufgeführt werden. Vielmehr soll dem Leser lediglich ein (nicht abschließender) Überblick über die denkbaren Rechtsnormen gegeben werden.

---

[91] *Schröder*, ZD 2021, 302, 307.
[92] *Schröder*, ZD 2021, 302, 307.
[93] Vgl. weiterhin bereits oben in Kapitel 4.3.4.2.1 zu der Problematik, dass intelligente automatisierte Flugdrohnen künftig ihre Flugrouten dynamisch bestimmen können werden und es daher ohnehin fraglich ist, ob mit statisch aufgestellten Hinweisschildern Rechtssicherheit erzielt werden kann.

Es ist weiterhin darauf hinzuweisen, dass der Gesetzgeber oftmals nicht zwischen den Begriffen der Funktionssicherheit und der Informationssicherheit unterscheidet. Vielmehr wird hierbei meist auf den unpräzisen Begriff der IT-Sicherheit zurückgegriffen. Eine Abgrenzung zwischen Normen, die die Gewährleistung von Funktionssicherheit bezwecken und Normen, die die Gewährleistung von Informationssicherheit bezwecken ist insofern meist nicht trennscharf möglich. In der folgenden differenzierten Darstellung wird daher stets auf den schwerpunktmäßigen Normzweck abgestellt.

4.4.1 ProdSG und ProdSV

Hinsichtlich der Sicherheit neu auf den Markt kommender Produkte kommt als zentrale Norm zunächst das Produktsicherheitsgesetz (ProdSG) zur Anwendung. Nach § 3 Abs. 1 ProdSG darf ein Produkt, das einer oder mehrerer der Rechtsverordnungen nach § 8 Abs. 1 ProdSG unterliegt, nur dann auf dem Markt bereitgestellt werden, wenn es die in dieser Rechtsverordnung vorgesehenen Anforderungen erfüllt und die Sicherheit und Gesundheit von Personen oder sonstiger in den Rechtsverordnungen aufgeführter Rechtsgüter bei bestimmungsgemäßer oder vorhersehbarer Verwendung nicht gefährdet. Durch diese nach § 8 ProdSG ergehenden Produktsicherheitsverordnungen (ProdSV) können insbesondere auch Anforderungen an die Beschaffenheit von Produkten geregelt werden. Die ProdSV setzen dabei meist auch europäische Produktrichtlinien in nationales Recht um. Zum Zeitpunkt der Aktualisierung der vorliegenden Studie existieren bereits 14 ProdSV, die allesamt nach spezifischen Themengebieten verfasst sind. Für das Inverkehrbringen von automatisierten Systemen kann dabei insbesondere die 1. ProdSV (Verordnung über das Inverkehrbringen elektrischer Betriebsmittel zur Verwendung innerhalb bestimmter Spannungsgrenzen) und die 9. ProdSV (Maschinenverordnung) in Betracht kommen. Eine spezifische ProdSV für automatisierte Systeme existiert zum Stand dieser Ausarbeitung dagegen nicht.

Auch außerhalb der ProdSV bleibt das ProdSG weiterhin relevant. Denn in § 3 Abs. 2 ProdSG bestimmt das Produktsicherheitsgesetz weiter, dass auch ein Produkt, dass nicht dem § 3 Abs. 1 ProdSG und daher keiner ProdSV unterliegt, nur dann auf dem Markt bereitgestellt werden darf, wenn es bei bestimmungsgemäßer oder vorhersehbarer Verwendung die Sicherheit und Gesundheit von Personen nicht gefährdet. Hierbei sind nach § 3 Abs. 2 Satz 1, Satz 2 Nr. 1 ProdSG auch die Eigenschaften des Produkts und nach Nr. 2 zudem die Einwirkungen des Produkts auf andere Produkte zu berücksichtigen. Gerade letzteres zeigt die Relevanz der zunehmenden Vernetzung von Produkten (auch, aber nicht nur im „Internet der Dinge“) und die Wechselbezüglichkeit der jeweiligen Produktsicherheit im „Zusammenspiel“ der Produkte (zum Beispiel von Smart Speakern, Haushaltsgeräten und automatisierten Bestellsystemen).

4.4.1.1.1 Exkurs: Öffentlich-rechtliche Haftung nach der Marktüberwachungsverordnung (EU) 2019/1020

Am 16.07.2021 ist die Verordnung (EU) 2019/1020 über Marktüberwachung und die Konformität von Produkten (Marktüberwachungsverordnung, MÜ-VO) in Kraft getreten. Als

Verordnung entfaltet sie umgehend unmittelbare Wirkung in allen Mitgliedstaaten der EU. Ihre Zwecke sind (unter anderem) ein hohes Schutzniveau bei öffentlichen Interessen wie Gesundheit und Sicherheit sowie Verbraucher- und Umweltschutz infolge konsequenter Durchsetzung des europäischen Produktsicherheitsrechts.[94]

Art. 14 Abs. 4 lit. k) der MÜ-VO etabliert die Befugnis nationaler Marktüberwachungsbehörden, die Entfernung von Inhalten von einer Plattform (in der MÜ-VO bezeichnet als „Online-Schnittstelle“), das heißt insbesondere einer Website, anzuordnen, wenn ein ernsthaftes Risiko nicht anders beseitigt werden kann.[95]

Software ist nicht ohne weiteres von dieser Verordnung erfasst.[96] Ob ein bestimmtes automatisiertes System betroffen sein kann, wird dem Einzelfall nach zu bestimmen sein.[97]

4.4.2 IT-Sicherheitsstandards

Neben den ProdSV können weiterhin eine Vielzahl an technischen Regelungen in den diversen und äußerst spezifischen DIN-, EN-, IEC-, ISO- und TC-Standards festgeschrieben sein, die im Folgenden beispielhaft aufgeführt werden sollen. Technische Normen als allgemein anerkannte Regeln der Technik entfalten dabei zunächst zwar keine direkte Bindungswirkung. Eine mittelbare Bindungswirkung kann sich aber dann ergeben, wenn das einschlägige Fachrecht[98] etwa die Einhaltung des Standes der Technik voraussetzt oder aber zur Vermeidung von Haftungsfolgen dem späteren Vorwurf der Fahrlässigkeit durch die Umsetzung des geltenden Technikstandes vorgewirkt werden soll.

Je nach Art und Weise sowie dem Einsatzzweck des automatisierten Systems betrifft dies etwa die EN 61131, die sich mit den Grundlagen speicherprogrammierbarer Steuerung befasst, sowie EN 61499 als Erweiterung für verteilte Steuerungen. In der DIN EN ISO 13482:2014-11 sind Sicherheitsanforderungen für persönliche Assistenzroboter normiert. Hinsichtlich der Sicherheitsanforderungen von Industrierobotern ist weiterhin die DIN EN ISO 10218-1 sowie die DIN EN ISO 10218-2 zu beachten. Die ISO/TS 15066 beinhaltet gar spezifische Anforderungen an Industrieroboter, die in einem kollaborativen Betrieb mit Menschen stehen sollen. Diese Sicherheitsstandards regeln sowohl den Betrieb des Roboters beziehungsweise Robotiksystems an sich mit seinem immanenten Gefahrenpotential (etwa bei dysfunktionalen Aktionen, Risikobeurteilung, Risikominderung etc.) als auch die Interaktion mit Menschen (Gestaltung des Kollaborationsraumes, Schutzmaßnahmen, Stoppfunktionen, Geschwindigkeits- und Abstandsüberwachung, Leistungs- und Kraftbegrenzung etc.).

---

[94] *Schucht*, GewA 2020, 259.
[95] *Schucht*, GewA 2020, 259, 262 f.
[96] *Wende*, RDi 2021, 341, 345.
[97] Der sachliche Anwendungsbereich der MÜ-VO erstreckt sich auf über 70 EU-Harmonisierungsrechtsvorschriften, wodurch sich im Ergebnis Bezüge zum gesamten EU-Produktrecht erstellen lassen, *Handorn/Schucht*, MPR 2021, 59, 60.
[98] Vgl. etwa im Bereich der Geräte- und Produktsicherheit § 14 Abs. 1 Nr. 3, Abs. 2 Satz 3 GPSG, aus dem Umweltrecht § 5 Abs. 1 Nr. 2 BImSchG oder ganz allgemein Art. 25 Abs. 1 DSGVO (Datenschutz durch Technikgestaltung).

Die ISO/IEC 15408 enthält dagegen generelle funktionale Sicherheitsanforderungen für IT-Produkte und IT-Systeme. Weiterhin kann auch die Norm ISO 9787:2013, die die Koordination von Robotern betrifft, und im Rahmen der Industrie 4.0 auch die Norm ISO/IEC 24771:2014 hinsichtlich der Vernetzung und des Informationsaustauschs zwischen einzelnen Industriekomponenten, beachtlich sein. Im Rahmen von industriellen Kommunikationsnetzen und automatisierten Industriekomponenten ist weiterhin die IEC 62443-Reihe (vormals ANSI/ISA99) relevant.[99] Hinsichtlich sicherheitsrelevanter elektrischer und elektronischer Systeme in Kfz ist weiterhin etwa ISO 26262 zu berücksichtigen. Bei dem Einsatz von intelligenten Transportsystemen ist zudem auch der Standards-Katalog ISO/TC 204 zu beachten, der eine ganze Palette an zu beachtenden Standards und Normen zu diesem Einsatzzweck vorsieht. Darüber hinaus existieren noch zahlreiche weitere spezifische zu beachtende Standards und Normen.[100]

4.4.3 MPG

Gerade dann, wenn automatisierte Systeme im medizinischen Bereich eingesetzt werden (etwa zur Betreuung von Pflegebedürftigen oder Kranken), stellen sich besonders hohe Anforderungen an die Funktionssicherheit des Systems, da hierbei ein besonders vorsichtiger und sensibler Umgang notwendig ist und Produktfehler insofern zu schweren Personenverletzungen führen können. Hierbei ist dann zuvorderst das Medizinproduktegesetz (MPG) zu beachten.

4.4.4 ArbSchG und TRBS

Während insbesondere das ProdSG und die sich daraus ergebenden ProdSV Regelungen für das *Inverkehrbringen* von Produkten beinhalten und insofern von dem Entwickler und dem (Zwischen-)händler eines Produkts zu beachten sind, könnten sich für den das automatisierte System einsetzenden Unternehmer auch Pflichten aus dem Arbeitsschutzgesetz (ArbSchG), der Betriebssicherheitsverordnung (BetrSichV) sowie aus den technischen Regeln für die Betriebssicherheit (TRBS) ergeben.

4.4.5 IT-Sicherheitsgesetz

Spezialgesetzlich sind das *IT-Sicherheitsgesetz 1.0* (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme v. 17.07.2015) und das IT-Sicherheitsgesetz 2.0 (Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme v. 18.05.2021) zu nennen, die grundsätzlich aber nur auf die Betreiber kritischer Infrastrukturen Anwendung

---

[99] Besonders relevant werden hierbei die beiden Teile IEC62443-3-1 und IEC62443-3-3 (*Security technologies for industrial automation and control systems* sowie *Security for industrial process measurement and control – network and system security*) sein.
[100] Vgl. etwa nur DIN EN ISO 11354 (Fortgeschrittene Automatisierungstechnologien und deren Anwendung - Anforderungen für das Erreichen einer Prozessinteroperabilität in Fertigungsunternehmen), DIN EN 62714 (Datenaustauschformat für Planungsdaten industrieller Automatisierungssysteme) oder DIN EN ISO 12813:2016-04 (Elektronische Gebührenerhebung - Kommunikation zur Übereinstimmungsprüfung für autonome Systeme).

finden. Solche kritischen Infrastrukturen sind nach § 2 Abs. 10 BSIG „Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden“. Welche Betreiber dieser Sektoren nun tatsächlich als kritische Infrastrukturen im Sinne des § 2 Abs.10 BSIG gelten, wurde gem. §§ 2 Abs. 10, 10 Abs. 1 BSIG per Rechtsverordnung des Bundesministeriums des Innern bestimmt.[101] Das IT-Sicherheitsgesetz 1.0 sowie das IT-Sicherheitsgesetz 2.0 stellen dabei nur Artikelgesetze dar, die zahlreiche bereits vorher bestehende Gesetze an den neuen Rechtsstand anpassen. Dies betrifft etwa das bereits angesprochene BSI-Gesetz (BSIG), aber auch zahlreiche weitere Spezialgesetze wie etwa das Atomgesetz (AtG), das Energiewirtschaftsgesetz (EnWG), das Telekommunikationsgesetz (TKG) oder das Telemediengesetz (TMG). Gerade in diesen Spezialgesetzen wurden durch das IT-Sicherheitsgesetz dann zudem auch erhöhte IT-Sicherheitsanforderungen für solche Adressaten erlassen, die gerade keine Betreiber kritischer Infrastrukturen sind (vgl. etwa § 13 Abs. 7 TMG[102], der auf alle Telemediendiensteanbieter Anwendung findet).

Die Betreiber kritischer Infrastrukturen haben dabei gemäß § 8a Abs. 1 BSIG „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der *Verfügbarkeit*, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind“. Bereits aus dem Wortlaut der Norm ergibt sich, dass das IT-Sicherheitsgesetz demnach sowohl die Gewährleistung der Funktionssicherheit als auch der Informationssicherheit bezweckt. Im Kontext von automatisierten Systemen kann das IT-Sicherheitsgesetz dann eine Rolle spielen, wenn ebensolche Betreiber kritischer Infrastrukturen automatisierte Systeme zur Erledigung ihrer Aufgaben einsetzen, was besonders auch den Einsatz von Software im sinne algorithmischer Systeme betrifft, die etwa Normabweichungen messen und in der Folge notwendige Aktionen zur Gefahrenbeherrschung, aber auch zur Dokumentation bis hin zur Auslösung von Alarmen in Gang setzen können. Die nach § 8a Abs. 1 BSIG geforderten organisatorischen und technischen Vorkehrungen können auch die Ausgestaltung der automatisierten Systeme selbst betreffen. Ab dem 1. Mai 2023 umfasst die Verpflichtung, angemessene organisatorische und technische Vorkehrungen zu treffen, auch den Einsatz von Systemen zur Angriffserkennung (§ 8a Abs. 1a BSIG). Dabei sollen die Systeme in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen.

---

[101] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) v. 22.04.2016, BGBl I S. 958 ff; derzeit liegt ein Referentenentwurf für eine zweite Verordnung zur Änderung der BSI-Kritisverordnung vor, abrufbar: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/zweite-verordnung-aenderung-bsi-kritis-vo-refe.pdf;jsessionid=300C4D4C6E55FDDC5E3FA08725BDB29F.1_cid295?__blob=publicationFile&v=2 (abgerufen am 19.07.2021).

[102] Anmerkung: Die bereichsspezifischen Datenschutzvorschriften aus dem Telekommunikationsgesetz (TKG) und dem Telemediengesetz (TMG) werden zum 01.12.2021 in ein eigenes Gesetz, das Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien vom 23.06.2021, BGBl. 2021 I, S. 1982 (TTDSG) überführt. Die Regelung des § 13 Abs. 7 TMG findet sich dann in § 19 Abs. 4 TTDSG.

Nach § 8a Abs. 2 BSIG können zur Erfüllung dieser Pflichten branchenspezifische Sicherheitsstandards mit konkreten Maßnahmenkatalogen vorgeschlagen und aufgestellt werden. Das BSIG enthält, wie bereits die DSGVO oder das BDSG, dagegen keine konkreten Handlungsempfehlungen. Nach § 8a Abs. 3 BSIG muss in Form von Sicherheitsaudits, Prüfungen oder Zertifizierungen regelmäßig auch eine Erfüllung dieser Pflichten nachgewiesen werden.

Das IT-Sicherheitsgesetz hat jedoch nicht nur Auswirkungen auf Betreiber kritischer Infrastrukturen, sondern auch auf einzelne Unternehmen. So kann das BSI gegenüber großen Unternehmen, die Telekommunikations- oder Telemediendienste anbieten, gezielte Anordnungen zur Abwehr konkreter erheblicher Gefahren im Bereich der IT-Sicherheit treffen (§§ 7c, d BSIG). Sofern solche Unternehmen also automatisierte Systeme einsetzen, können auch Maßnahmen zur Abwendung von Gefahren durch das BSI angeordnet werden.

Seit Inkrafttreten des IT-Sicherheitsgesetz 2.0 am 28.05.2021 werden nicht mehr nur einzelne Anordnungen gegenüber Unternehmen ermöglicht, sondern es werden zusätzlich zu den Betreibern kritischer Infrastrukturen Unternehmen im besonderen öffentlichen Interesse gesondert reguliert (§ 2 Abs. 14 BSIG).[103] Dabei handelt es sich um Rüstungshersteller, Unternehmen von erheblicher volkswirtschaftlicher Bedeutung und Betrieben die mit Gefahrstoffen umgehen. Für die Bestimmung der erheblichen volkswirtschaftlichen Bedeutung von Unternehmen wird nach § 2 Abs. 14 BSIG eine Rechtsverordnung erlassen, die wirtschaftliche Kennzahlen festlegt, um die Unternehmen trennscharf festlegen zu können. Diese Unternehmen müssen ab dem 01.05.2023 – beziehungsweise für Unternehmen, die sich aufgrund ihrer wirtschaftlichen Bedeutung bemessen, zwei Jahre nach Inkrafttreten der konkretisierenden Verordnung – mindestens alle zwei Jahre eine Selbsterklärung zur IT-Sicherheit beim BSI vorlegen, aus der hervorgeht, welche Zertifizierungen durchgeführt wurden (Abs. 2 Nr. 1), welche Sicherheitsaudits und Prüfungen durchgeführt oder festgelegt wurden (Abs. 2 Nr. 2) und wie sonst sichergestellt wird, dass die für das Unternehmen besonders schützenswerten IT-Systeme, Komponenten und Prozesse angemessen geschützt werden, wobei der Stand der Technik eingehalten wird (Abs. 2 Nr. 3).

4.4.6 Gewährleistung der Funktionssicherheit durch das Zulassungsrecht

Zur Sicherstellung und zum Nachweis, dass die notwendigen Maßnahmen zur Gewährleistung von Funktionssicherheit bei automatisierten Straßen- oder Luftfahrzeugen eingehalten wurden, dient das Fahrzeugzulassungsrecht.

Die entsprechenden Vorschriften finden sich für Straßenfahrzeuge in der Fahrzeugzulassungsverordnung (FZV) und für Luftfahrzeuge in der Luftverkehrszulassungsordnung (LuftVZO). Bei Luftfahrzeugen wird hierbei zwischen einer Musterzulassung (vgl. §§ 1 ff. LuftVZO) und einer Verkehrszulassung (vgl. §§ 6 ff. LuftVZO) unterschieden. Während die Mus-

[103] Vgl. dazu umfassend: *Heckmann*, bayme vbm Leitfaden IT-Sicherheit (im Erscheinen), S. 38 ff.

terzulassung die Funktionssicherheit neuer Flugzeugmodelle, also ganzer Baureihen, sicherstellt, wird die Verkehrszulassung bei der anschließenden Einzelzulassung eines Luftfahrzeugs relevant. Eine ähnliche Zweiteilung kennt das Zulassungsrecht bei Kraftfahrzeugen. Nach § 3 Abs. 1 FZV dürfen Fahrzeuge „auf öffentlichen Straßen nur in Betrieb gesetzt werden, wenn sie zum Verkehr zugelassen sind. Die Zulassung wird auf Antrag erteilt, wenn das Fahrzeug einem genehmigten Typ entspricht …".

Hinsichtlich des Zulassungsrechts für automatisierte Straßenfahrzeuge sind weiterhin etwa das *Wiener Übereinkommen* (Übereinkommen über den Straßenverkehr v. 8.11.1968) in seiner neuesten Fassung (letzte Änderungen des Wiener Übereinkommens in Deutschland vom 23.03.2016), das zur Umsetzung des Übereinkommens in nationales Recht hierfür notwendige Transformationsgesetz sowie weitere EU-Richtlinien (etwa RL 2007/46/EG und neuere EU-RL) und ergänzende ECE-Normen zu beachten.

4.5 Informationssicherheit (Security) automatisierter Systeme

Auch hinsichtlich der Informationssicherheit von IT-Systemen existiert bislang kein einheitlicher Rechtsrahmen. Vielmehr sind hierbei erneut eine Vielzahl an Rechtsnormen zu beachten, wobei nochmals darauf hingewiesen werden muss, dass eine Abgrenzung zwischen Rechtsnormen, die die Gewährleistung der Funktionssicherheit bezwecken und Rechtsnormen, die die Gewährleistung der Informationssicherheit bezwecken, nicht trennscharf vorgenommen werden kann und daher jeweils lediglich auf den schwerpunktmäßigen Normzweck abgestellt wird.

Praxistipp

Schon in der Entwicklungsphase eines automatisierten Systems sollte auf eine sichere Technikausgestaltung geachtet werden. Insofern sollen die IT-Sicherheitsgrundsätze bereits ab Werk bestmöglich berücksichtigt und implementiert werden (sogenanntes „Security by Design").

4.5.1 IT-Sicherheitsvorgaben im Kontext des Datenschutzes

Vor Inkrafttreten der DSGVO war die zentrale IT-Sicherheitsnorm § 9 BDSG a. F. i. V. m. der entsprechenden Anlage.[104] Hinsichtlich der Datensicherheit der erhobenen und auf den automatisierten Systemen gespeicherten Daten sind nunmehr insbesondere die Bestimmungen der DSGVO zu beachten.

[104] Vgl. dazu *Heckmann*, bayme vbw, Leitfaden IT-Sicherheit, S. 35 f.

So gibt bereits Art. 5 Abs. 1 lit. f) DSGVO den Grundsatz vor, dass die Sicherheit („Integrität und Vertraulichkeit“) personenbezogener Daten hinreichend gewährleistet werden muss und diese insbesondere vor einer unbefugten oder unrechtmäßigen Verarbeitung, vor unbeabsichtigten Verlust, vor unbeabsichtigter Zerstörung und vor unbeabsichtigter Beschädigung durch geeignete technische und organisatorische Maßnahmen geschützt werden müssen.

Dieser Grundsatz wird von Art. 24 DSGVO im Rahmen der Pflichten des Verantwortlichen aufgegriffen. Danach hat dieser unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der DSGVO erfolgt, wobei auch IT-sicherheitsrechtliche Maßnahmen erfasst sein können.[105]

Die genannten Grundsätze werden von Art. 32 DSGVO erneut aufgegriffen und im Hinblick auf die IT-Sicherheit konkretisiert. Danach wird unter anderem bestimmt, dass „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen […] der Verantwortliche […] geeignete technische und organisatorische Maßnahmen [treffen muss], um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“. Dies erfordert ausdrücklich ein Sicherheitsmanagement und auch in Art. 30 Abs. 1 lit. g) DSGVO wird der Verantwortliche verpflichtet, die Maßnahmen im vorgeschriebenen Verarbeitungsverzeichnis zu beschreiben und dokumentieren; das Outsourcing auf Auftragsverarbeiter ist dabei grundsätzlich möglich (Art. 28 Abs. 3 S. 2 lit. e) DSGVO).[106]

Im Vergleich zu der früher maßgeblichen Anlage zu § 9 BDSG a. F. (vor Inkrafttreten der DSGVO) enthält Art. 32 Abs. 1 DSGVO zwar keine wortlautgleichen IT-Sicherheitszielbestimmungen. Doch bestimmt auch Art. 32 Abs. 1 DSGVO weiter, dass von den zu treffenden Maßnahmen auch die „Pseudonymisierung und Verschlüsselung personenbezogener Daten“ (a), „die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen“ (b), „die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen“ (c) sowie „ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“ (d) eingeschlossen seien. Hinsichtlich der Datensicherheit führen die Bestimmungen des Art. 32 Abs. 1 DSGVO daher im Ergebnis zu einem mit der Anlage zu § 9 BDSG a. F. vergleichbaren Schutzniveau.

Komplettiert werden die datenschutzrechtlichen Vorschriften zur IT-Sicherheit durch die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche

[105] Vgl. dazu *Heckmann*, bayme vbw, Leitfaden IT-Sicherheit, S. 18 f.
[106] Vgl. dazu *Heckmann*, bayme vbw Leitfaden IT-Sicherheit, S. 65 ff.

Voreinstellungen („privacy by design“ und „privacy by default“) in Art. 25 DSGVO. Diese Grundsätze sind als (bußgeldbewehrte) Pflicht des Verantwortlichen ausgestaltet und können auch Bezüge zur IT-Sicherheit enthalten, zum Beispiel durch die notwendige Sicherungen gegen den Verlust von Daten oder Schutz vor unberechtigtem Zugriff, die schon bei der Entwicklung berücksichtigt werden müssen.[107] An dieser Stelle sei erwähnt, dass diese Grundsätze gerade nicht für den (nicht i. S. v. Art. 4 Nr. 7 DSGVO verantwortlichen) Hersteller etwaiger Software gelten.[108]

4.5.2 IT-Sicherheitsgesetz

Die Betreiber kritischer Infrastrukturen haben künftig gem. § 8a Abs. 1 BSIG „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, *Integrität, Authentizität und Vertraulichkeit* ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind“. Das IT-Sicherheitsgesetz bezweckt damit einerseits die Gewährleistung von Funktionssicherheit (Verfügbarkeit), andererseits aber auch die Sicherstellung von Informationssicherheit (Integrität, Authentizität und Vertraulichkeit).

Zwar ist das IT-Sicherheitsgesetz zunächst nur für die Betreiber kritischer Infrastrukturen, Unternehmen im besonderen öffentlichen Interesse oder große Anbieter von Telekommunikations- oder Telemediendiensten relevant. Vielfach werden aber auch diese zur Erledigung ihrer Aufgaben automatisierte Systeme einsetzen, etwa zur Steuerung und Überwachung ihrer Anlagen oder einzelner Komponenten. In diesem Fall finden die Bestimmungen des IT-Sicherheitsgesetzes auch auf die technische Ausgestaltung der automatisierten Systeme Anwendung.

4.5.3 NIS-Richtlinie

Die europäische NIS-Richtlinie (NIS-RL) bezweckt die Erhöhung der Sicherheit von Netz- und Informationssystemen in den EU-Mitgliedstaaten. Hält man sich vor Augen, dass Automatisierung stets auch mit Vernetzung einhergeht (schon jetzt ist europaweit das Notrufsystem eCall verpflichtend), eine Vernetzungspflicht von automatisierten Kfz diskutiert wird[109] und wohl aus Sicherheitsaspekten heraus unumgänglich ist, wird deutlich, dass die NIS-Richtlinie gerade auch auf die Entwickler und Betreiber automatisierter Systeme Anwendung finden kann. Die NIS-RL wurde bereits am 6.7.2016 vom europäischen Gesetzgeber verabschiedet und ist daraufhin am 8.7.2016 in Kraft getreten. Als europäische Richtli-

---

[107] Vgl. dazu *Heckmann*, bayme vbw Leitfaden IT-Sicherheit, S. 18.
[108] Dies wurde zwar im Gesetzgebungsprozess erwogen, letztlich aber darauf verzichtet. Genauer hierzu m.w.N. und für das Bestehen einer solchen Pflicht des Herstellers zur Einhaltung datenschutzrechtlicher Standards argumentierend, vgl. *Specht-Riemenschneider*, MMR 2020, 73.
[109] http://www.golem.de/news/einbaupflicht-gefordert-usa-setzen-beim-vernetzten-fahren-auf-wlan-1612-125097.html (abgerufen am 19.07.2021).

nie entfaltet die NIS-RL aber keine unmittelbare Rechtswirkung, sondern muss erst umgesetzt werden. Die Umsetzung in Deutschland erfolgte durch das NIS-RL-Umsetzungsgesetz vom 29.07.2017, in Kraft getreten am 30.06.2017.[110]

Im Rahmen der NIS-RL und ihrer Umsetzung wurden neue Sicherheitsanforderungen und Meldepflichten für die Betreiber sogenannter „wesentlicher Dienste“ und für die Anbieter „digitaler Dienste“ definiert. Die wesentlichen Dienste sind dabei von den weitergehenden kritischen Infrastrukturen nach § 2 Abs. 10 BSIG umfasst, sodass die Umsetzung der Richtlinie in das bestehende Recht aufgenommen werden konnte, da die Mitgliedsstaaten nach Art. 3 NIS-RL auch strengere Regelungen zur Umsetzung einführen können.[111] Neu eingefügt wurden insbesondere die Anforderungen an die Anbieter von digitalen Diensten, die nun nach § 2 Abs. 11, 12 BSIG legaldefiniert werden; sie umfassen im Wesentlichen Online-Dienste, Online-Suchmaschinen und Cloud-Computing-Dienste.[112]

Nicht ausgeschlossen ist daher, dass auch spezifische Entwickler und Anwender von automatisierten Systemen Betreiber von kritischen Infrastrukturen sind oder „digitale Dienste“ (etwa automatisierte Softwareprodukte) bereitstellen oder nutzen und daher auch bei der Ausgestaltung dieser automatisierten Systeme auf die Erfordernisse der NIS-RL, beziehungsweise auf das ergangene nationale Umsetzungsgesetz, zu achten ist.

Derzeit in Planung ist die NIS RL 2.0. Die EU-Kommission hat im Dezember 2020 einen Vorschlag für eine NIS-RL 2.0 veröffentlicht, der bisher evaluierte Mängel der NIS-RL beheben soll.[113] Dabei sollen mit den Bereichen Abwasser, Weltraum und öffentliche Verwaltung weitere Sektoren in den Bereich der kritischen Infrastruktur aufgenommen werden und bestehende Teilsektoren erweitert werden.[114] Auch wird nicht mehr zwischen Betreibern wesentlicher Dienste und Anbietern digitaler Dienste unterschieden, sondern nach den Maßgaben der wesentlichen und wichtigen Einrichtungen, die nach bestimmten Kriterien in den Anlagen festgelegt werden.[115] Adressiert werden mittlere und große Unternehmen, jedoch keine Kleinunternehmen nach Art. 2 Abs. 1 NIS RL 2.0. Dabei werden für die Unternehmen nach Art. 18 Abs. 2 NIS RL 2.0 Mindestanforderungen an die Sicherheit definiert, die weiter konkretisiert werden sollen.

4.5.4 Cybersecurity Act / Rechtsakt zur Cybersicherheit und EU-Cybersicherheitspolitik

Auf europäischer Ebene bietet der Cybersecurity Act (CSA) der Union weitere Regelungen für die IT- beziehungsweise Cybersicherheit. Der Begriff der Cybersicherheit wird vorwie-

---

[110] https://www.kritis.bund.de/SubSites/Kritis/DE/Aktuelles/Meldungen/170630_NIS_Richtlinie.html abgerufen am 19.07.2021).
[111] *Buchberger* in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 2 BSIG Rn. 12.
[112] Vgl. dazu *Buchberger* in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 2 BSIG Rn. 13ff.
[113] https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union (abgerufen am 19.07.2021).
[114] *Kipker/Birreck/Niewöhner/Schnorr*, MMR 2021, 214.
[115] *Kipker/Birreck/Niewöhner/Schnorr*, MMR 2021, 214.

gend unionsrechtlich eingesetzt, mittlerweile aber zum Beispiel auch in der deutschen Cybersicherheitsstrategie 2021 aufgegriffen. Er dient als Oberbegriff für die Themenfelder der IT-Sicherheit, Informationssicherheit oder Datensicherheit.[116] Die am 27.06.2019 in Kraft getretene Verordnung festigt und stärkt die Rolle der Agentur der Europäischen Union für Cybersicherheit (ENISA) als europäisches Pendant zum BSI.[117] Dies sah auch schon die Cybersicherheitspolitik der EU-Kommission aus dem Jahr 2017 vor.[118] Der Cybersecurity Act adressiert die Mitgliedsstaaten und ihre Organe, aber auch private Wirtschaftsunternehmen, verpflichtet sie aber nicht direkt. Er soll die Cybersicherheit in der EU stärken, indem unter anderem ein einheitlicher Rahmen für die *Sicherheitszertifizierung* von Produkten oder Prozessen geschaffen wird.[119] Die Cybersicherheitspolitik der EU-Kommission aus dem Jahr 2020 sieht außerdem eine zukünftige Erweiterung der unionsrechtlichen Cybersicherheit vor: Dabei soll ein offenes, globales, aber sicheres Internet verwirklicht werden. Dafür sollen unter anderem die NIS-RL überarbeitet werden (siehe oben), ein europäisches Cyberschutzschild und kompetente Stellen eingerichtet werden, eine sichere Kommunikationsinfrastruktur mit der Umsetzung von 5G zeitnah umgesetzt und Notfallpläne eingerichtet werden.[120] Damit auch IoT-Anwendungen sicher vernetzt sind, sollen transparente Sicherheitslösungen, Zertifizierungen und Sorgfaltspflichten für Hersteller vernetzter Geräte eingeführt werden.[121] Begleitend wird künftig ein Europäisches Kompetenzzentrum im Bereich der Cybersicherheit eingerichtet, das die Kapazitäten für Cybersicherheit in der EU erhöhen soll und durch nationale Koordinierungsstellen unterstützt wird.[122] Weitere Änderungen ergeben sich aus der Warenkauf-Richtlinie von 2019[123], die notwendige Sicherheitsaktualisierungen (Updates) für die Anbieter bestimmter Waren und Dienstleistungen im Online- und Einzelhandel verpflichtend vorsieht. Die deutsche Umsetzung der Richtlinie soll ab 1. Januar 2022 in Kraft treten (vergleiche dazu Kapitel 4.2.1).[124]

4.5.5 Handlungsempfehlungen des BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht regelmäßig eigene *Handlungsempfehlungen* und *Maßnahmenkataloge*, die der Anwender zur Umsetzung seiner IT-Sicherheitsverpflichtungen zu Rate ziehen kann. Die Handlungsempfehlungen des BSI stellen nur freiwillige Standards mit richtungsweisendem Charakter dar. Insofern steht dem Betreiber offen, seine Verpflichtungen auch durch andere Standards und Maßnahmenkataloge zu erfüllen. Im Rahmen der Handlungsempfehlungen des BSI sind

---

[116] *Kipker*, Cybersecurity, 1. Aufl. 2020, Rn. 4.
[117] *Martini* in: Paal/Pauly, DSGVO BDSG, 3. Aufl. 2021, Art. 32 DSGVO Rn. 17.
[118] Vgl. dazu *Heckmann*, bayme Leitfaden IT-Sicherheit, 2021, S. 10.
[119] *Martini* in: Paal/Pauly, DSGVO BDSG, 3. Aufl. 2021, Art. 32 DSGVO Rn. 17a; vgl. ausführlich zum Cybersecurity Act: *Heckmann*, bayme vbm Leitfaden IT-Sicherheit, S. 21 ff.
[120] Vgl. dazu ausführlich *Heckmann*, bayme vbm Leitfaden IT-Sicherheit, 2021, S. 13 ff.
[121] Vgl.dazu ausführlich *Heckmann*, bayme vbm Leitfaden IT-Sicherheit, 2021, S. 13 ff.
[122] Vgl.dazu ausführlich *Heckmann*, bayme vbm Leitfaden IT-Sicherheit, 2021, S. 26 ff.
[123] Richtlinie (EU) 2019/771.
[124] Vgl. dazu unten; https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/Warenkaufrichtlinie.html (abgerufen am 19.07.2021).

dann insbesondere die *BSI IT-Grundschutz-Kataloge* relevant, die grundlegend in Gefährdungs- und in Maßnahmenkataloge unterteilt werden. [125]

Die Gefährdungskataloge enthalten insofern eine Aufzählung der denkbaren Gefährdungslagen beim Einsatz von IT. Diese betreffen neben technischem Versagen auch organisatorische Mängel, menschliche Fehlhandlungen oder höhere Gewalt. Die Maßnahmenkataloge enthalten sodann konkrete Handlungsempfehlungen, um diesen Gefährdungslagen bestmöglich zu begegnen. Auch diese betreffen insofern nicht nur technische und infrastrukturelle, sondern auch organisatorische und personelle Gegenmaßnahmen.

Aufgrund des modularen Aufbaus der IT-Grundschutzkataloge sind diese grundsätzlich offen ausgestaltet und nicht auf spezifische Systeme beschränkt. Denn anstatt spezifische Gesamtsysteme darzustellen, enthalten die IT-Grundschutzkataloge vielmehr nur Darstellungen einzelner, in einem Gesamtsystem verbauter IT-Komponenten. Dies führt dazu, dass der Anwender sein zu prüfendes Gesamtsystem zunächst in seine Einzelkomponenten auftrennen und entkoppeln muss und dann im Rahmen der komponentenbezogenen Bestimmungen der IT-Grundschutzkataloge sein System modelliert und analysiert. Welche Bestimmungen der IT-Grundschutzkataloge daher für ein automatisiertes System relevant sind, ist erneut abhängig von der Art und der Ausgestaltung des Systems.

Beispiel: In einer Produktionshalle sollen intelligente Roboter miteinander kommunizieren. Der einsetzende Unternehmer überlegt, ob er bei der Verwendung von Wireless LAN (WLAN) spezifische IT-Sicherheitsstandards zu beachten hat. In dem IT-Grundschutzkatalog-Baustein B4.6 befinden sich Ausführungen zum sicheren Einsatz von WLAN. Dieser Baustein untergliedert sich in Ausführungen zur Gefährdungslage (höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen, vorsätzliche Handlungen) sowie in konkrete Maßnahmenempfehlungen zur Beseitigung oder Minimierung dieser Gefahren. Aufgrund dieser Maßnahmenempfehlungen wird der Unternehmer sein WLAN etwa dem Stand der Technik entsprechend verschlüsseln und auch alle eingesetzten Access Points und Router dementsprechend absichern. Weiterhin wird er einen Notfallplan mit Verhaltensregeln bei zukünftigen WLAN-Sicherheitsvorfällen bereithalten.

4.5.6 ISO/IEC 27000-Standards

Auch die sogenannte ISO/IEC 27000-Familie, die von der International Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC) herausgegeben wird, stellt eine Reihe an IT-Sicherheitsstandards und damit ebenfalls *freiwillige* Handlungsempfehlungen für die Betreiber von IT dar (soweit diese nicht über gesetzliche Generalklauseln einen verpflichtenden Charakter erhalten). Auch im Rahmen der ISO/IEC 27000-Reihe existieren (bislang) keine automatisierungsspezifischen Richtlinien, sodass je nach verwendeten Einzelkomponenten ein Querschnitt aus allen ISO/IEC 27000-Dokumenten in Betracht kommt.

---

[125] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html (abgerufen am 19.07.2021).

4.5.7 Weitere IT-Sicherheitsstandards

Die bereits oben im Rahmen der Funktionssicherheit genannten ISO / IEC / EN / DIN-Normen (vergleiche hierzu Kapitel 3.4.2) enthalten stellenweise auch Vorschriften zur Informationssicherheit von IT-Systemen und sind in diesem Kontext gleichwohl heranzuziehen. Dies betrifft beispielsweise die ISO/IEC 15408, die neben funktionalen Sicherheitsanforderungen für IT-Produkte und IT-Systeme (Teil 2) auch Anforderungen an die Vertrauenswürdigkeit dieser Systeme beinhaltet (Teil 3).

5 Haftung

Haftungskonstellationen und Haftungsnormen bei automatisierten Systemen

5.1 Haftungsszenarien

Ebenso vielfältig wie die Einsatzszenarien von automatisierten Systemen – man denke hierbei nur an die unterschiedlichen Ausgestaltungen (etwa Industrieroboter, Dienstleistungsroboter, automatisierte Straßenfahrzeuge, automatisierte Drohnen, algorithmische Systeme zur Anlagensteuerung, Monitoring etc.) und an die grenzenlosen Einsatzgebiete (etwa in der Industrie, im Transportwesen, im Pflege- und Gesundheitswesen, durch den Staat, im Haushalt, etc.) – sind auch die denkbaren Gefährdungsszenarien, die von solchen Systemen ausgehen können. Denn jede technische Entwicklung bringt naturgemäß auch neuartige Gefährdungspotentiale mit sich, die gerade am Anfang einer neuen Produktgattung einer stetigen Produktverbesserung und Weiterentwicklung bedürfen. Nicht alle technischen Fehlerquellen lassen sich insofern bereits in der Entwicklungsphase „am Reißbrett“ identifizieren und eliminieren. Oftmals bedarf es hierzu vielmehr einer Erprobung im tatsächlichen Einsatz. Doch nicht nur technische Fehlfunktionen können Auslöser von Personenverletzungen oder Sachbeschädigungen sein – auch eine fehlerhafte Bedienung oder eine fehlerhafte Wartung des Systems kommt in Betracht.

Setzt ein Dienstleister oder ein Unternehmen ein automatisiertes System, etwa einen automatisierten Industrieroboter, ein, oder aber stellt dieser selbst solche automatisierten Systeme her, stellt sich insofern stets die Frage, welche Haftungsszenarien hierbei in Betracht kommen, wenn durch die Verwendung des Systems Sachen beschädigt oder Personen verletzt werden. Zu klären ist hierbei zunächst, welche Fehlerquellen überhaupt zu einer fehlerhaften technischen Reaktion führen können und wer Betroffener eines solchen technischen Fehlverhaltens sein kann (wer also hierdurch verletzt werden kann oder wessen Sachen hierdurch beschädigt werden können). Anschließend stellt sich stets die wichtige Frage, welche Haftungsadressaten bei etwaigen Schadensersatzforderungen herangezogen werden können.

5.1.1 Fehlerquellen bei automatisierten Systemen

Als Fehlerquellen eines automatisierten Systems[126] kommen zunächst eine *fehlerhafte Softwareprogrammierung* oder aber ein *Hardwareversagen* in Betracht. Automatisierte Systeme sind insbesondere auf die Erhebung und Verarbeitung zahlreicher Sensordaten angewiesen, um eine exakte und fehlerfreie Programmausführung zu gewährleisten.

[126] Vgl. zu weiteren Haftungsquellen vbw Positionspapier Datenwirtschaft, Oktober 2020, S. 28 ff. https://www.vbw-bayern.de/Redaktion/Frei-zugaengliche-Medien/Abteilungen-GS/Wirtschaftspolitik/2020/Downloads/Position-Datenwirtschaft-Oktober-2020_final.pdf.

Durch den hardwareseitigen Ausfall von Sensoren beziehungsweise durch Abweichungen in der Messgenauigkeit können daher ebenso technische Fehlreaktionen ausgelöst werden wie durch eine softwareseitige Störung bei der Datenverarbeitung, wenn die korrekt erhobenen Daten also fehlerhaft ausgewertet werden.

Neben diesen Fehlern in der Hard- oder Software ist bei automatisierten Systemen auch auf die *vorgegebene Programmierung* zu schauen. Werden bestimmte Verhaltensweisen und Algorithmen im Rahmen der Entwicklung falsch vorgegeben, kann dies insofern zu objektiv unerwünschten Reaktionen führen, die aber weder auf einem Software- noch auf einem Hardwareversagen beruhen, sondern lediglich Folge eines inadäquat ausgestalteten Systems sind. Aber selbst bei einem adäquat ausgestalteten System stellt sich bei hochentwickelter KI-Technologie immer mehr die Frage wie mit selbsterlerntem (sicherheitsgefährdendem) Verhalten umgegangen werden soll, was ungewollt ist, von dem aber selbst die Entwickler nicht wissen, wieso es aufgetreten ist (sogenannte Black-Box-Effekte).[127] Zwar kann solches spezifisches Verhalten im Einzelfall oft nicht vorhergesagt werden, gleichwohl wird der Hersteller/Entwickler grundsätzlich Kenntnis darüber haben, dass seine Technologie bestimmtes atypisches Verhalten hervorbringen kann.[128] Anknüpfungspunkte für die Zuteilung von Verantwortung bleiben also stets das Agieren von Entwicklern und Anwendern beziehungsweise eine Kombination der beiden.[129] So könnte zum Beispiel das System mit den "falschen" Daten gefüttert sein oder kein korrektes Feedback gegeben werden oder es nicht bestimungsgemäß eingesetzt werden – all dies sollte auch bei der Vertragsgestaltung zwischen dem "Hersteller" der KI und dem Anwender berücksichtigt werden.

Doch selbst wenn sowohl die Hard- und Software ordnungsgemäß funktioniert und dem System weiterhin auch eine adäquate Technikgestaltung zugrunde liegt, kann es dann zu Funktionsstörungen kommen, wenn ein *unberechtigter Dritter Zugriff auf das System* erhält und dieses insofern „kapert“ (sogenanntes „Hijacking“). Im Rahmen der Realisierung von IT-Sicherheit sind daher zum einen die auf dem System gespeicherten personenbezogenen Daten (Teilbereich der Informationssicherheit), zum anderen aber auch das System selbst vor einer unautorisierten Kontrollübernahme (Teilbereich der Funktionssicherheit) zu schützen.

Ein automatisiertes System, etwa ein automatisierter Industrieroboter, bedarf weiterhin stets einer *fachmännischen Installation am Einsatzort sowie einer ständigen Wartung und Aktualisierung* der Betriebssoftware. Durch eine mangelhafte Wartung, Fehler beim Daten-Input oder durch den Betrieb einer veralteten Firmware können insofern zahlreiche Funktionsstörungen ausgelöst werden, welche wiederum zu der Verletzung von Personen oder der Beschädigung von Sachen führen können.

---

[127] *Seehafer/Kohler*, EuZW 2020, 213, 215 f.
[128] *Wagner*, AcP 2017, 707, 750 ff.
[129] Vgl. insoweit den Ansatz für eine zivilrechtliche Haftung, den das EU Parlament in seinem Entwurf vom 20.10.2020 für eine Verordnung über Haftung für den Betrieb von Systemen mit künstlicher Intelligenz vorgestellt hat, 2020/2014(INL).

Zuletzt stellt der Endnutzer stets auch selbst eine Fehlerquelle dar, da ein automatisiertes System *lediglich innerhalb seiner Leistungsgrenzen und nur in der vorgeschriebenen ordnungsgemäßen Art und Weis*e eingesetzt werden darf. Hierfür verantwortlich kann bei der Verwendung eines automatisierten Industrieroboters etwa der für das System zuständige Angestellte sein, der das System stets fachmännisch zu bedienen hat und sich im Wege von Schulungen auch regelmäßig über technische Neuerungen weiterbilden muss. Gerade bei der privaten Verwendung von automatisierten Dienstleistungsrobotern im Zuhause des Anwenders tragen zudem auch die Käufer und Inhaber des Systems die Pflicht, ihr automatisiertes System nur ordnungsgemäß nach Anleitung oder Instruktion einzusetzen und zu bedienen sowie fachmännisch warten und aktualisieren zu lassen.

5.1.2 Betroffene bei Funktionsstörungen automatisierter Systeme

Kommt es zu einer Funktionsstörung oder einem sonstigen Fehlverhalten eines automatisierten Systems, ist zuvorderst der unmittelbare Nutzer und Anwender gefährdet, also derjenige, der sich in der räumlichen unmittelbaren Nähe des Systems befindet. Dies kann bei dem Einsatz eines automatisierten Industrieroboters etwa der sich im Umfeld befindliche Arbeitnehmer sein, bei einem Krankenpflegeroboter der zu behandelnde Patient oder aber die bedienende Pflegekraft.

Neben diesen unmittelbar betroffenen Personen kann auch das einsetzende Unternehmen Nachteile durch eine Funktionsstörung des automatisierten Systems tragen. Denn wird das fehlerhafte System selbst oder werden andere Maschinen oder Sachen des Unternehmens beschädigt oder muss das fehlerhafte System zur zukünftigen Korrektur des Fehlers zeitaufwendig aktualisiert oder repariert werden, kann hierdurch ein massiver Produktionsrückstau entstehen. Dies wiederum kann zu Produktionsverzögerungen, zu Auftragsstornierungen oder gar zu Schadensersatzforderungen und mithin zu Umsatzeinbußen führen.

Hält man sich den oben im Datenschutzteil besprochenen Fall (vergleiche Kapitel 3.3.4) des Einsatzes einer Industriedrohne vor Augen, die zur Wahrnehmung ihrer Aufgaben auch öffentliches Terrain überfliegen muss, wird weiterhin schnell deutlich, dass auch unbeteiligte Passanten verletzt oder deren Sachen beschädigt werden können, wenn die eingesetzte Drohne abstürzt oder sonst mit einem Passanten kollidiert. Neben einer solchen körperlichen oder gesundheitlichen Verletzung des Passanten oder der Beschädigung einer seiner Sachen kommt hierbei auch eine Verletzung des Rechts auf informationelle Selbstbestimmung und des Persönlichkeitsrechts in Betracht, wenn personenbezogene oder -beziehbare Daten über diese Person rechtswidrig erhoben, verarbeitet oder genutzt werden. Die Literatur zu „diskriminierenden“ algorithmischen Systemen beziehungsweise KI füllt mittlerweile ganze Bibliotheken. Dieses Thema war auch Gegenstand der Arbeit der Datenethikkommission der Bundesregierung.[130]

[130] Vgl. den Abschlussbericht der Datenethikkommission vom 23.10.2019, dort u.a. S. 176 ff.: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6

5.1.3 Haftungsadressaten bei Funktionsstörungen automatisierter Systeme

Wird bei dem Einsatz eines automatisierten Systems eine Person verletzt, eine Sache beschädigt oder ein sonstiges Recht (etwa das Datenschutzrecht) beeinträchtigt, kommen mehrere Haftungsadressaten in Betracht. Ausgehend von der jeweiligen Fehlerquelle (vergleiche oben Kapitel 4.1.1) wird hierbei regelmäßig zunächst derjenige herangezogen werden, der den Fehler zu vertreten hat. Im Rahmen der im deutschen Recht stellenweise vorzufindenden Gefährdungshaftung kann dieser Grundsatz jedoch dort durchbrochen sein, wo der Halter eines Systems (etwa bei automatisierten Fahrzeugen) auch ohne eigenes Verschulden haftet.

Je nach Art und Weise sowie Einsatzort des automatisierten Systems kommen als Haftungsadressaten grundsätzlich in Betracht:
- der Hersteller und Entwickler des automatisierten Systems, seiner Hardware und Software
- bei der Entwicklung gegebenenfalls beteiligte weitere Dritte (etwa Zulieferer für die Firmware oder einzelner technischer Komponenten, App-Entwickler etc.),
- gegebenenfalls Zwischenhändler, die das System an den Endnutzer vertreiben,
- das einsetzende Unternehmen,
- bei Industrie- und Dienstleistungsrobotern der mit dem System betraute Arbeitnehmer,
- bei Dienstleistungsrobotern für den Privatgebrauch der Endnutzer,
- bei einer auf einen unbefugten Eingriff oder Angriff durch Dritte (etwa durch Hacker) zurückzuführenden Fehlreaktion auch dieser Dritte.[131]

Weiterhin kommt auch eine Haftung des Netzbetreibers bei einem Netzausfall in Betracht, da automatisierte und vernetzte Systeme hochgradig von einem stabilen Datenaustausch untereinander abhängig sind. Im Falle von in der Öffentlichkeit agierenden Systemen wird dies zukünftig zuvorderst über das Mobilfunknetz (insbesondere über den in Deutschland seit 2019 zur Verfügung stehenden 5G-Standard beziehungsweise den perspektivischen Nachfolgestandard 6G)[132] geschehen. Eine solche Haftung wird sich insbesondere aus den zwischen dem Telekommunikationsanbieter und dem Betreiber des automatisierten Systems geschlossenen Verträgen ergeben. Meist behält sich der Telekommunikationsanbieter hierbei aber einen gewissen Prozentanteil an legitimen Ausfallzeiten vor, für die dann kein Schadensersatz verlangt werden kann.

5.2 Maßstäbe und Rechtgrundlagen der Haftung

Eine Haftung kann sich im deutschen Recht aus allgemeinen Vorschriften (etwa aus dem BGB), oder aber aus Spezialgesetzen (etwa aus dem StVG, dem LuftVG oder dem

[131] Vgl. allgemein *De la Durantaye* in: BeckOK IT-Recht, Borges/Hilber, 2. Ed. 01.05.2020, § 831 BGB Rn. 9.
[132] Zu den verschiedenen Generationen von digitalen Mobilfunkstandards *Marx* in: Heckmann/Paschke, jurisPK Internetrecht, 7. Aufl. 2021, Kap. 1.2 Rn. 12.

ProdHaftG) ergeben. Weiter kann sich eine Haftung einerseits aus einer vertraglichen Beziehung des Beschädigten zum Schädiger ergeben, also etwa dann, wenn eine vertragliche Pflicht gebrochen wurde. Andererseits kann sich eine Haftung aber auch außervertraglich, etwa aus dem Deliktsrecht, ergeben. Die einzelnen Haftungsnormen unterscheiden sich weiterhin auch nach ihrem Verschuldensmaßstab: abzugrenzen ist hierbei die Verschuldenshaftung zu der Haftung aus vermutetem Verschulden zu der Gefährdungshaftung.

5.2.1 Vertragliche Haftung

Schließen Parteien wirksam einen Vertrag, so erhält der Gläubiger aus dem vertraglichen Schuldverhältnis einen Anspruch gegen den Schuldner, also das Recht, von diesem ein Tun oder Unterlassen zu fordern (vergleiche § 194 Abs. 1 BGB). Welches Tun oder Unterlassen hierbei konkret gefordert werden kann, ist dabei abhängig von dem jeweiligen Vertragsverhältnis. Bei einem Kaufvertrag wird der Verkäufer einer Sache nach § 433 Abs. 1 BGB etwa verpflichtet, dem Käufer die Sache zu übergeben und das Eigentum an der Sache – frei von Sach- und Rechtsmängeln – zu verschaffen. Der Käufer ist nach § 433 Abs. 2 BGB dagegen verpflichtet, dem Verkäufer den vereinbarten Kaufpreis zu zahlen und die Sache abzunehmen. Beim Werkvertrag dagegen wird der Unternehmer nach § 631 Abs. 1 BGB zur Herstellung des versprochenen Werkes und der Besteller zur Entrichtung der vereinbarten Vergütung verpflichtet. Auch hierbei hat der Unternehmer dem Besteller gemäß § 633 Abs. 1 BGB das Werk frei von Sach- und Rechtsmängeln zu verschaffen. Weiterhin relevant ist auch der Dienstleistungsvertrag nach §§ 611 ff. BGB.

Aus dem Grundsatz der Privatautonomie (aus Art. 2 Abs. 1, Art. 1 Abs. 1 GG) folgt, dass die Parteien in ihrer Vertragsgestaltung grundsätzlich frei sind. Diese können daher also nicht nur Verträge schließen, deren Typus ausdrücklich gesetzlich geregelt ist (etwa einen Kaufvertrag oder einen Werkvertrag), sondern grundsätzlich jede Art von Vertragsverhältnis, das den Schuldner und den Gläubiger dann an eine Vielzahl von unterschiedlichen Pflichten bindet. In diesem Kontext relevant sind insbesondere auch sogenannte gemischte Verträge, bei denen umfassende Rechte und Pflichten beider Vertragsparteien vereinbart werden, die unterschiedliche Vertragsarten betreffen. So werden in dem Verhältnis Anbieter (Hersteller oder Verkäufer des automatisierten Systems) und Anwender (der das System einsetzende Unternehmer oder die das System erwerbende Privatperson) etwa oftmals Kombinationen aus Kaufverträgen/Werk(lieferungs)verträgen (beispielsweise die Anschaffung und Herstellung des Systems selbst) und Dienstleistungsverträgen (beispielsweise die ständige Wartung und Aktualisierung des Systems beziehungsweise die Versorgung mit „Patches“, also Updatepaketen mit Fehlerverbesserungen) in einem übergreifenden „Roboterbeschaffungs- und Roboterwartungsvertrag“ vereinbart werden. Insoweit beginnt die Haftung für Abweichungen von vertraglich zugesicherten Eigenschaften bereits bei der allgemeinen Sachmängelgewährleistung, für die es aufgrund der Neuartigkeit des Vertragsgegenstandes noch keine gesicherte Rechtsprechung gibt. Gleichwohl ist vertraglichen Vereinbarungen in diesem Bereich der Vorzug zu geben.

Ab 01.01.2022 werden zwei europäische Richtlinien (Warenkauf- und Digitale-Inhalte-Richtlinie) ihre Wirkung entfalten, mit der Folge, dass das BGB eine substanzielle Veränderung erfährt[133]. Es soll fit für die Digitalisierung gemacht werden. Insbesondere werden neue Vertragstypen geschaffen, der Vertrag über digitale Produkte (§§ 327 ff. BGB-neu, betrifft zum Beispiel eine Spiele-App aus dem App-Store) und der Vertrag über Waren mit digitalem Element (§§ 327a Abs. 3 S.1, 475b Abs. 1 S.1 BGB-neu, betrifft zum Beispiel einen „smarten" Lautsprecher mit Bluetooth-Funktion). Letztgenannter Vertragstyp wird insbesondere für automatisierte Systeme (deren Funktionsfähigkeit im Kern aus dem Zusammenspiel einer Hardware- sowie einer Software-Komponente besteht) im B2C-Bereich erhebliche Relevanz haben. Rechte der Verbraucher werden gestärkt.[134] Für die Bestimmung der Mangelhaftigkeit ist nicht mehr nur in erster Linie der Zeitpunkt des Erwerbs der Sache entscheidend, vielmehr wurde nun auch eine Bereitstellungs- und Aktualisierungspflicht (betreffend das digitale Element) für einen bestimmten Aktualisierungszeitraum normiert, innerhalb derer der Verkäufer für fehlerhafte Patches (Fehlerkorrekturen) oder Updates (Produktaktualisierungen) haftet. Bei Mangelhaftigkeit des digitalen Elements kann sich der Käufer stets an den Verkäufer (und nicht etwa den Hersteller/Betreiber der Software) wenden. Der vertraglichen Beziehung zwischen Hersteller und Verkäufer wird damit in Zukunft besondere Bedeutung zukommen.[135]

Wird eine vertragliche Pflicht verletzt, kann dies der gegnerischen Partei einen Anspruch auf Schadensersatz aus den §§ 280 ff. BGB vermitteln, wenn diese Pflichtverletzung durch den Schuldner oder durch einen diesem zurechenbaren Dritten (vergleiche § 278 BGB) vorsätzlich oder fahrlässig (sogenanntes „Vertretenmüssen", vergleiche § 276 Abs. 1 S. 1 BGB) begangen wurde. Der konkrete Umfang der Schadensersatzpflicht richtet sich dabei nach den §§ 249 ff. BGB, wonach beispielsweise Behandlungskosten zu erstatten sowie beschädigte Sachen zu reparieren und zu ersetzen sind. Eine vertragliche Haftungsbegrenzung ist möglich und richtet sich nach allgemeinen haftungsrechtlichen Grundsätzen (etwa kein Haftungsausschluss bei Vorsatz).

5.2.2 Außervertragliche Haftung

Neben der vertraglichen Haftung kommt auch eine außervertragliche Haftung in Betracht. Diese bedarf grundsätzlich keines vorherigen Vertragsverhältnisses zwischen dem Schädiger und dem Geschädigten und kann daher als eigenständige Anspruchsgrundlage eines unbeteiligten Dritten oder aber neben einem weiterhin bestehenden vertraglichen Anspruch bestehen.

---

[133] Gesetz zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (bmjv.de)
[134] *Wende*, RDi 2021, 341, 343 f.
[135] *Mayer/Möllnitz*, RDi 2021, 333, 334, 343; *Wende*, RDi 2021, 341, 345.

5.2.2.1 Verschuldenshaftung

Im Deliktsrecht haftet grundsätzlich nur derjenige, der eine Verletzungshandlung vorsätzlich oder fahrlässig (sogenanntes Verschulden) begangen hat (vergleiche § 823 Abs. 1 BGB). Das Vorliegen eines Verschuldens stellt demnach grundsätzlich eine notwendige Tatbestandsvoraussetzung dar, die grundsätzlich die klagende Partei positiv beweisen muss. Gelingt der Nachweis nicht, so ist der Anspruch nicht durchsetzbar. Die zentrale Deliktshaftungsnorm des § 823 Abs. 1 BGB stellt etwa eine solche Verschuldenshaftung dar.

5.2.2.2 Haftung aus vermutetem Verschulden

Im Gegensatz dazu wird ein Verschulden bei manchen Haftungstatbeständen zulasten des Schädigers widerlegbar vermutet. Hierbei muss also nicht die klagende Partei das Vorliegen eines Verschuldens beweisen, sondern vielmehr kann sich der Beklagte lediglich exkulpieren, also den Gegenbeweis erbringen, um einer Haftung zu entgehen. Eine solche Haftung aus vermutetem Verschulden liegt etwa im Rahmen der Fahrzeugführerhaftung nach § 18 Abs. 1 StVG vor. Ebenso begründet Art. 82 Abs. 1 DSGVO eine Haftung aus vermutetem Verschulden, wonach „jeder Verstoß gegen die Verordnung“ eine Schadensersatzpflicht begründet (vergleiche ausführlicher unter dem Kapitel 4.2.2.4.4).[136]

5.2.2.3 Gefährdungshaftung

Als Ausnahme von dem Grundsatz, dass nur derjenige Verursacher für einen Schaden haften muss, der diesen auch verschuldet hat, sieht das deutsche Recht stellenweise aber auch eine sogenannte Gefährdungshaftung vor. Hiernach muss auch für solche Schäden gehaftet werden, die von dem in Anspruch genommenen nicht vorsätzlich oder fahrlässig herbeigeführt wurden. Eine solche Gefährdungshaftung wird regelmäßig darin begründet und gerechtfertigt, dass von dem Anspruchsgegner eine Gefahr in die Welt gesetzt wurde, für die dieser unabhängig eines eigenen Verschuldens einzustehen hat. So sind bestimmte Verhaltensweisen zwar abstrakt gefährlich (etwa das Fahren eines Autos), aber dennoch erlaubt, da ihre soziale Nützlichkeit überwiegt. Der Halter eines Fahrzeugs handelt nicht rechtswidrig, nur weil er ein Auto hat, auch wenn er weiß, dass von einem Auto im Straßenverkehr gewisse Gefahren ausgehen. Dennoch hat der Fahrzeughalter verschuldensunabhängig diejenigen Schäden zu ersetzen, die in den Risikobereich des Fahrzeugs fallen, vergleiche § 7 StVG. Auch der Hersteller eines Produkts ist unter Umständen verschuldensunabhängig zum Schadensersatz verpflichtet, da das bloße Inverkehrbringen des Produkts schon eine Gefahr darstellt, vergleiche § 1 ProdHaftG.

[136] *Heckmann/Scheurer* in: Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 9 Rn. 610.

5.2.2.4 Konkrete außervertragliche Haftungsanspruchsgrundlagen

Im Folgenden sollen die im Kontext von automatisierten Systemen in Betracht kommenden außervertraglichen Haftungsanspruchsgrundlagen überblicksmäßig (und nicht abschließend) aufgezeigt werden.

5.2.2.4.1 § 823 Abs. 1 BGB

§ 823 Abs. 1 BGB gilt als zentraler Haftungstatbestand, wenn jemand vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, das Eigentum oder ein sonstiges absolutes Recht eines anderen widerrechtlich verletzt.

Im Rahmen des Einsatzes automatisierter Systeme kommt diese Anspruchsgrundlage insbesondere dann in Betracht, wenn ein Arbeitnehmer oder ein anderer Beteiligter verletzt wird oder dessen Sachen beschädigt werden. Haftungsadressat ist dabei derjenige, der die Pflichtverletzung und den Schaden kausal und verschuldet herbeigeführt hat. Dies kann zunächst der bedienende Arbeitnehmer sein, wenn dieser aufgrund eines eigenen Fehlverhaltens eine Fehlfunktion des Systems herbeiführt. Weiter kann aber auch das Unternehmen selbst aufgrund organisatorischen Fehlverhaltens notwendige Wartungen versäumt oder das System falsch installiert und hierdurch die Verletzung von Rechten Dritter verschuldet haben.

Ein weiterer wichtiger Fall sind Verletzungen von Rechtsgütern Dritter (Passant, andere Beteiligte), die auf einen Produktfehler zurückzuführen sind, für den der Hersteller und Entwickler einzustehen hat. Hier spricht man von der sogenannten „Produzentenhaftung“.[137] Im Bereich der automatisierten Systeme ist diese Produzentenhaftung insbesondere relevant als Ausfluss einer allgemeinen Produktbeobachtungspflicht.[138] Können durch Patches oder Updates Fehler oder Gefahren minimiert oder vermieden werden, ist der Betreiber der Software zu entsprechenden Reaktionsmaßnahmen verpflichtet. Die Frage nach der Klassifikation als Hersteller eines bestimmten Systemteils wird im Rahmen von komplex vernetzten Systemen der Industrie 4.0 immer komplizierter.

5.2.2.4.2 § 823 Abs. 2 BGB

Nach § 823 Abs. 2 BGB trifft eine Verpflichtung zum Schadensersatz auch denjenigen, der gegen ein sogenanntes Schutzgesetz verstößt. Ein solches Schutzgesetz können etwa eine Strafnorm des StGB, aber auch diverse andere Rechtsnormen sein, die nicht nur den Schutz der Allgemeinheit sondern gerade auch eines Einzelnen bezwecken (sogenannter Individualschutz).[139]

---

[137] In Abgrenzung von der Produkthaftung nach dem ProdHaftG (siehe 3.2.2.4.3), *Heydn* in: Schuster/Grützmacher, IT-Recht, 1. Aufl. 2020, § 823 BGB Rn. 4.
[138] *Lüftenegger*, RDi 2021, 293 f.
[139] *De la Durantaye* in: BeckOK IT-Recht, Borges/Hilber, 2. Ed. 01.05.2020, § 823 BGB Rn. 62.

Im Kontext des Einsatzes von automatisierten Systemen kommt als ein solches Schutzgesetz insbesondere auch das Produktsicherheitsgesetz in Betracht, das in § 3 ProdSG bestimmt, dass kein unsicheres Produkt auf den Markt gelangen darf.[140]

Aber etwa auch Normen aus dem Medizinproduktegesetz sowie aus der MPBetreibV können solche Schutzgesetze sein, die bei Zuwiderhandlung Schadensersatzansprüche nach dem § 823 Abs. 2 BGB auslösen können.

In Betracht kommt hierbei weiterhin eine Verletzung des Luftverkehrsrechts bei der Nutzung von Drohnen, die über § 823 Abs. 2 BGB (und damit neben § 33 LuftVG) ebenfalls zu Schadensersatzansprüchen führen kann.

Als Individualschutzgesetze kommen weiterhin Normen aus der DSGVO (parallel zu Art. 82 DSGVO) und dem BDSG in Betracht, etwa § 4 BDSG (Videoüberwachung durch öffentliche Stellen), Art. 6 Abs. 1 und 4 DSGVO (rechtskonforme Datenerhebung) sowie Art. 12-14 DSGVO (Informationspflichten).[141]

5.2.2.4.3 § 1 ProdHaftG

Nach § 1 Abs. 1 ProdHaftG haftet der Hersteller eines Produkts, wenn durch einen Produktfehler ein Mensch getötet, sein Körper oder seine Gesundheit verletzt oder eine fremde Sache beschädigt wird. Der Geschädigte hat insofern nachzuweisen, dass ein fehlerhaftes Produkt vorlag und seine Schädigung auf diesen Fehler zurückzuführen ist, § 1 Abs. 4 ProdHaftG. Auf ein Verschulden kommt es anders als i. R. d. Produzentenhaftung gem. § 823 Abs. 1 BGB (vergeiche oben Kapitel 4.2.2.4.1) hier aber nicht an (sogenannte Gefährdungshaftung, vergleiche oben Kapitel 4.2.2.3).Die verschuldensabhängige Haftung aus § 823 Abs. 2 BGB ist deshalb in der Praxis nur dort relevant, wo das ProdHaftG den Schaden nicht vollständig abdeckt, etwa oberhalb der Haftungshöchstsumme nach § 10 ProdHaftG oder um eine Selbstbeteiligung bei Sachschäden (§ 11 ProdHaftG) zu vermeiden.

Gerade beim Einsatz von automatisierten Systemen könnte zukünftig eine nicht zu unterschätzende Haftungsverschiebung hin zum Hersteller und Entwickler des Produkts stattfinden.[142] Im Kontext des automatisierten Fahrens etwa könnte dies zu einer Haftungsverlagerung vom Fahrzeughalter und -führer hin zum Automobilhersteller führen.[143] Denn während beim manuell gesteuerten Kfz der Hersteller nur für sogenannte Konstruktions- oder Fabrikationsfehler einzustehen hatte, könnte dieser nun auch für konkrete Fahrfehler des automatisierten Kfz aufkommen müssen, wenn die automatisierten Handlungen und Reaktionen des Fahrzeugs bereits ab Werk vorgegeben werden und diese die Ursache eines Unfalls waren. Hierbei besteht insbesondere auch die Gefahr, dass sich der Fahrzeugführer

[140] *Förster* in: BeckOGK BGB, Gsell/Krüger/Lorenz/Reymann, 58. Ed. 01.07.2021, § 823 BGB Rn. 675 ff.
[141] *De la Durantaye* in: BeckOK IT-Recht, Borges/Hilber, 2. Ed. 01.05.2020, § 823 BGB Rn. 68.
[142] Vgl. hierzu den Abschlussbericht der Ethikkommission für automatisiertes und vernetztes Fahren (an dem der Verf. dieser Studie maßgeblich beteiligt war), S.8 Nr. 10 (nachfolgend „Abschlussbericht Ethikkommission“); ebenso *Seehafer/Kohler*, EuZW 2020, 213.
[143] *Wagner*, AcP 2017, 707, 709.

bei einem Unfall künftig stets auf ein Versagen des Kfz beruft, auch wenn er das Fahrzeug selbst gesteuert hat. Dies erfordert insbesondere technische Lösungen, die den Kausalverlauf eines Unfalls protokollieren und rechtssicher nachweisen können. Diesen Ansatz verfolgt der Gesetzgeber mit dem 2017 in Kraft getretenen § 63a StVG, der vorsieht, dass die Steuerungsübernahme durch den Fahrzeugführer oder durch das automatisierte System von dem Fahrzeug protokolliert wird.[144] Mit dem Gesetz zum autonomen Fahren (siehe oben Kapitel 2) wurde zudem § 1g StVG geschaffen, der den Halter eines autonomen Fahrzeugs zur Speicherung bestimmter Daten bei gewissen Anlässen verpflichtet.[145]

Angesichts der oben skizzierten Herausforderungen, mit denen sich das aktuelle deutsche (auf die europäische Produkthaftungs-RL aus dem Jahre 1985 zurückgehende) Produkthaftungsregime konfrontiert sieht und angesichts der Tatsache, dass sich eine (Digital-)Reform des Produkthaftungsrechts anzubahnen scheint[146], sollen an dieser Stelle knapp einige zentrale Punkte der aktuellen Reform-Diskussionen wiedergegeben werden (was noch nichts über ihre jeweilige Berechtigung aussagt):[147]

- Aktualisierung des „Produkt"-Begriffs (Einbeziehung von „Software"?)[148]
- Aktualisierung des „Fehler"-Begriffs, unter anderem Konkretisierung maßgeblicher Sicherheitsstandards sowie Aktualisierung des maßgeblichen Zeitpunkts für Beurteilung der Fehlerhaftigkeit[149]
- Überarbeitung der Beweislastverteilung (zugunsten des Geschädigten)[150]

Vereinfacht lässt sich sagen: das Produkthaftungsrecht soll vom analogen ins digitale Zeitalter überführt werden.

5.2.2.4.4 Art. 82 DSGVO

Art. 82 DSGVO enthält einen zivilrechtlich eigenständigen Schadensersatzanspruch. Nach dem Wortlaut des Abs. 1 kann „jeder Verstoß gegen die Verordnung" einen Schadensersatzanspruch begründen. Hierunter fallen insbesondere Verstöße gegen die umfassend geregelten Bestimmungen zur rechtskonformen Verarbeitung von Daten

---

[144] *Roshan*, NJW-Spezial 2021, 137; *Jahnke* in: Burmann/Heß/Hühnermann/Jahnke, StraßenverkehrsR, 26. Aufl. 2020, § 1 b StVG Rn. 10 ff.
[145] Zu beachten ist jedoch, dass dessen Verhältnis zu § 63a StVG nicht eindeutig ist, jedenfalls ist § 63a StVG seinem Wortlaut nach nicht auf das „autonome Fahren" anwendbar, *Steege*, SVR 2021, 128, 136.
[146] Vgl. für eine Übersicht der wesentlichen Aspekte des Diskussionsstands das Forderungspapier der Verbraucherzentrale Bundesverband e.V. „Produkthaftung im digitalen Zeitalter" vom 07.06.2021.
[147] Zu erwähnen sei zudem, dass der Vorschlag der EU Kommission für eine KI-Verordnung vom 21.04.2021 (COM(2021), 206 final) die Frage der zivilrechtlichen Haftung beim Einsatz von KI bewusst ausklammert, vgl. Art. 53 Nr. 4 des Verordnungs-Entwurfs, der klarstellt, dass auch bei „AI regulatory sandboxes" die zivilrechtlichen Haftungsregelungen unberührt bleiben.
[148] Derzeit stark umstritten und nur im jeweiligen Einzelfall zu beantworten. Im Kontext automatisierter Systeme allerdings ist diese Frage nicht von hoher Relevanz, da solche Systeme stets eine Einheit aus Soft- und Hardware darstellen und damit grds. von dem Produkthaftungsrecht erfasst sind.
[149] Dies betrifft vor allem die Frage nach der Einführung einer – dem Produkthaftungsrecht bislang unbekannten – Produktbeobachtungspflicht.
[150] Vgl. für einen Überblick über die aktuellen Vorschläge den Bericht einer von der EU Kommission eingesetzten Expertenkommission „Liability for Artificial Intelligence and other emerging digital technologies", Expert Group on Liability and New Technologies – New Technologies Formation, 2019 sowie einen (unverbindlichen) Entwurf des EU Parlaments vom 20.10.2020 für eine Verordnung über Haftung für den Betrieb von Systemen mit künstlicher Intelligenz, 2020/2014(INL). Nähere Besprechung dieser Entwürfe: *Wende*, RDi 2021, 341; *Seehafer/Kohler*, EuZW 2020, 213.

(Art. 6 Abs. 1 S. 1 lit. a) – f) DSGVO), zur Gewährleistung der in Art. 32 DSGVO geregelten Datensicherheit sowie zu den Informations- und Mitteilungspflichten (Art. 12 ff. DSGVO).[151] Anspruchsberechtigter ist „jede Person", der ein Schaden entstanden ist. Anspruchsgegner können sowohl der Verantwortliche (Art. 4 Nr. 7 DSGVO) als auch der Auftragsverarbeiter (Art. 4 Nr. 8 DSGVO) sein.

Gerade automatisierte Systeme sind permanent auf die Erhebung und Verarbeitung zahlreicher Sensordaten angewiesen. Wie bereits gezeigt wurde, dient eine solche umfassende Datenerhebung sogar der Verbesserung der Funktionssicherheit, da nur mittels dieser Sensordaten andere Personen im Umfeld erkannt und geschützt werden können.[152] Dennoch muss jene Datenerhebung und -verarbeitung stets mit der DSGVO konform sein. Ist sie dies nicht, kommt den Betroffenen ein Schadensersatzanspruch aus Art. 82 DSGVO zu.

Zu beachten ist, dass gem. Art. 82 Abs. 3 DSGVO wiederum die Möglichkeit des Verantwortlichen oder des Auftragsverarbeiters besteht, der Haftung dann zu entgehen, wenn dieser „nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist" (sogenannte Haftung für vermutetes Verschulden, vergleiche oben Kapitel 4.2.2.3).[153]

Aktuell ist ein vom Bundesverfassungsgericht angestrengtes Verfahren vor dem Europäischen Gerichtshof (EuGH) anhängig, welches sich mit der Frage einer Erheblichkeitsschwelle i. R. v. Art. 82 DSGVO auseinandersetzt. Möglicherweise könnte es zukünftig eine Entwicklung hin zur Ahndung kleinster Datenschutzverstöße geben (Stichwort Abmahnindustrie).[154]

5.2.2.4.5 Speziell: § 7 StVG und § 18 StVG

Neben diesen – grundsätzlich für alle automatisierten Systeme relevanten – Haftungsnormen sind für spezifische automatisierte Systeme weiterhin auch Haftungsnormen aus diversen Spezialgesetzen zu beachten.

Im Rahmen von Straßenfahrzeugen ist dabei zunächst § 7 Abs. 1 StVG sowie § 18 Abs. 1 StVG relevant: Gemäß § 7 Abs. 1 StVG haftet der Fahrzeughalter verschuldensunabhängig (Gefährdungshaftung), wenn bei dem Betrieb seines Kraftfahrzeugs ein Mensch getötet, der Körper oder die Gesundheit eines Menschen verletzt oder eine Sache beschädigt wird. Daneben kann nach § 18 Abs. 1 StVG auch der Fahrzeugführer zur Haftung gezogen werden mit dem Unterschied, dass hierbei ein Verschulden (Vorsatz oder Fahrlässigkeit) vorliegen muss. Das Vorliegen dieses Verschuldens wird dabei zunächst aber vermutet und kann von dem Fahrzeugführer lediglich durch Exkulpation, also durch das Erbringen eines

---

[151] *Heckmann/Scheurer* in: Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 9, Rn. 604.
[152] Vgl. oben Kapitel 3.2.
[153] *Heckmann/Scheurer* in: Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 9 Rn. 610.
[154] Vgl. BVerfG, Beschluss v. 14.01.2021 - Az. 1 BvR 28531/19. Im konkreten Fall geht es um den Versand einer ungewollten Werbe-E-Mail an einen Anwalt. Der geltend gemachte Anspruch beläuft sich auf mindestens 500€ Schmerzensgeld.

Gegenbeweises, ausgeräumt werden.[155] Beide Haftungstatbestände sind von der vom Halter abzuschließenden Pflichtversicherung erfasst (§ 1 PflVG).[156]

Mit zunehmendem Automatisierungsgrad des Kfz stellen sich hinsichtlich dieser Haftungsnormen zwei Grundsatzfragen: zum einen ist hierbei fraglich, wie künftig eine adäquate Haftungsteilung zwischen dem Fahrzeughalter und dem Produzenten vorzunehmen ist, wenn bei höher automatisierten Systemen die Ursache eines Unfalls meist in der Fahrzeugfirmware und daher in der Sphäre des Entwicklers liegt. Zum anderen ist fraglich, ob auch bei höher automatisierten Systemen (insbesondere ab der Stufe der Vollautomatisierung, bei der eine eigene Steuerung des Fahrers stark zurücktritt) überhaupt noch ein „Fahrzeugführer" im klassischen Sinne vorhanden ist. Denn wird dem Fahrer durch eine fortgeschrittene Fahrzeugautomatisierung erlaubt, sich während der Fahrt auch mit anderen Dingen zu beschäftigen, sind zu diesem Zeitpunkt gegebenenfalls alle Insassen des Kfz nur noch als Passagiere anzusehen (unter Umständen aber mit der Möglichkeit der manuellen Steuerungsübernahme oder des Einlenkens).[157]

Auch das neue Gesetz zum autonomen Fahren (nähere Ausführungen oben Kapitel 2) ändert an dem grundsätzlichen Haftungsregime der §§ 7, 18 StVG nichts.[158] Allerdings entfällt bei einem autonomen Fahrzeug (beziehungsweise „Kraftfahrzeug mit autonomer Fahrfunktion", so der Wortlaut des § 1d Abs. 1 StVG-neu) naturgemäß die Fahrerhaftung. Es verbleib mithin die Halterhaftung als Gefährdungshaftung. Allerdings stellt das Gesetz die Figur der „Technischen Aufsicht" als eine natürliche Person vor, die das Fahrzeug deaktivieren und Fahrmanöver freigeben kann (§ 1d Abs. 3 StVG-neu).[159] Eine Haftung dieser Person wird allerdings in dem Gesetz nicht verortet, auch die Gesetzesbegründung schweigt hierzu.[160] Für die Technische Aufsicht verbleibt damit die Haftung nach allgemeinen deliktsrechtlichen Grundsätzen (vergleiche oben Kapitel 4.2.2.4.1).[161]

5.2.2.4.6 Speziell: § 33 LuftVG

Als spezifische Haftungsnorm bei dem Einsatz automatisierter Industrie- oder Dienstleistungsdrohnen kommt weiterhin § 33 Abs. 1 LuftVG in Betracht. Hiernach haftet der Halter des Luftfahrzeugs, wenn bei dem Betrieb durch einen Unfall jemand getötet, sein Körper oder seine Gesundheit verletzt oder eine Sache beschädigt wird.[162] Zu Regulierung etwai-

---

[155] *Förster* in: BeckOK BGB, Gsell/Krüger/Lorenz/Reymann 58. Ed. 01.07.2021, § 823 BGB Rn. 650.
[156] *Schrader*, ZRP 2021, 109, 111.
[157] Vgl. zu den Rechtsfragen des automatisierten Fahrens auch vbw, Positionspapier - Zukunft automatisiertes Fahren: Rechtliche Hürden beseitigen, 2018, S. 17ff.
[158] *Lutz*, DAR 2021, 182, 185; *Schrader*, ZRP 2021, 109, 111.
[159] Vgl. ausführlicher unten Kapitel 2.1.
[160] *Schrader* stellt fest, dass diese Person in Bezug auf den Fahrvorgang handelt, es folglich nahe läge, etwaiges Fehlverhalten über eine Verschuldenshaftung – ähnlich der Fahrerhaftung nach § 18 StVG - zu regeln, ZRP 2021, 109, 111.
[161] *Schrader*, ZRP 2021 109, 111.
[162] Hinsichtlich der Haftung bei der Beförderung von Fluggästen existieren dagegen spezifische Haftungsnormen, vgl. etwa §§ 44 ff. LuftVG. Diese sollen im Rahmen dieses Gutachtens aber außer Betracht gelassen werden.

ger Schäden durch die Nutzung von Drohnen ist der Abschluss einer spezifischen Haftpflichtversicherung Pflicht. Die normale Privathaftpflichtversicherung deckt durch Drohnen verursachte Schäden in der Regel nicht ab.[163]

Auch hierbei stellt sich im Laufe der Fortentwicklung des Automatisierungsgrades bei Industrie- und Dienstleistungsdrohnen die Frage, wie eine adäquate Haftungsteilung zwischen dem Luftfahrzeughalter und dem Produzenten des Luftfahrzeugs realisiert werden kann, da mit zunehmenden Automatisierungsgrad die Ursache eines Unfalls auch hierbei meist Folge eines Soft- oder Hardwarefehlers und daher eher der Sphäre des Entwicklers und Herstellers zuzuschreiben sein wird.[164] Bei den in Entwicklung befindlichen Lufttaxis wird man genauer unterscheiden müssen, welchen Automatisierungsgrad diese erreichen sollen. Hier ist die Bandbreite zwischen modernen Helikoptern und „Personenbeförderungsdrohnen“ groß.

[163] Vgl. *Wilke/Schimikowski*, RuS 2019, 490.
[164] Vgl. *Wagner*, AcP 2017, 707, 709.

6 Ausblick: Entwurf für einen Artificial Intelligence Act

Regulierung Künstlicher Intelligenz

Automatisierte Systeme werden zukünftig unser Leben mitbestimmen. Dabei spielt Künstliche Intelligenz eine zunehmend wichtigere Rolle. Selbstlernende Maschinen sind in der Lage, ihren eigenen Einsatz zu optimieren, Fehler zu erkennen und Prozesse zu verbessern. KI-unterstützte Entscheidungen sind ein wesentliches Element der Automatisierung, weil sie die Abläufe von der Menschenhand auf die Maschine übertragen und damit erst jene Autonomie entwickeln, die deren erwünschte Effekte (Beschleunigung, Präzisierung, Entlastung etc.) befördert.

Diese umfassende Automatisierung sowie Vernetzung und damit „Smartifizierung" unseres beruflichen und privaten Alltags bringt neuartige Rechtsfragen mit sich, die mehrheitlich, wie in der vorliegenden Studie aufgezeigt, bereits durch das geltende Recht beantwortet werden können.

Gleichzeitig verbleibt erkennbar Bedarf für eine Aktualisierung beziehungsweise Neufassung automatisierungsspezifischer gesetzlicher Rahmenbedingungen. So befinden wir uns beim KI-Einsatz nicht selten im grundrechtssensiblen Bereich. Wenn etwa die Prüfungsaufsicht bei elektronischen Fernprüfungen zumindest in Massenfächern durch KI-Systeme wie Proctorio ersetzt werden soll, bedarf es einer gesetzlichen Regelung (Vorbehalt des Gesetzes), um den Eingriff in die Privatsphäre und die Persönlichkeitsrechte der Prüflinge zu rechtfertigen. Die am TUM Center for Digital Public Services entwickelte Bayerische Fernprüfungserprobungsverordnung (BayFEV)[165] stellte im September 2020 die bundesweit erste Rechtsgrundlage auch für den KI-Einsatz abei einer automatisierten Videoaufsicht dar.[166]

Die über solche speziellen Fallgestaltungen hinausreichende „Regulierungslücke" wurde in den letzten Jahren seitens des Gesetzgebers durchaus erkannt, exemplarisch für ein solches spezifisches nationales Gesetzgebungsvorhaben wurde das bereits im Sommer 2021 verabschiedete „Gesetz zum autonomen Fahren" in Kapitel 3 vorgestellt. Eine weitere (vermeintliche) solche Lücke versucht der europäische Gesetzgeber perspektivisch mit dem weltweit ersten Regulierungsentwurf für einen Artificial Intelligence Act (EU) zu schließen. Dieser soll im Folgenden vorgestellt werden.

[165] https://www.tum-cdps.de/projekte/rechtssichere-elektronische-fernpruefungen-fuer-bayerns-hochschulen/.
[166] Näher zu Inhalt und Konzept der BayFEV Heckmann/Rachut, OVuR 2021, 194 ff.

Am 21.04.2021 präsentierte die EU-Kommission den Vorschlag für einen „Artificial Intelligence Act“.[167] Der Artificial Intelligence Act wird (falls verabschiedet) als Verordnung unmittelbar in allen EU-Mitgliedstaaten anwendbar sein, eine Umsetzung in nationales Recht wäre demnach nicht erforderlich. Der Entwurf des Artificial Intellicence Act markiert einen wichtigen Schritt in der politischen Diskussion um die Regulierung von künstlicher Intelligenz und wurde durch zahlreiche Aktivitäten der EU-Organe vorbereitet. Neben der Arbeit der Hochrangigen Expertenkommission für Künstliche Intelligenz ist hier vor allem das Weißbuch zur Künstlichen Intelligenz[168] aus dem Jahr 2020 zu nennen. Das Europäische Parlament hatte bereits 2017 die Einrichtung einer Europäischen Agentur für Robotik und Künstliche Intelligenz gefordert.[169] 2018 hatte die Kommission bereits einen „Koordinierten Plan für künstliche Intelligenz“ vorgestellt,[170] der zeitgleich mit dem Entwurf des Artificial Intelligence Act aktualisiert wurde.[171] Im größeren Kontext reiht sich der Entwurf des Artificial Intelligence Act ein in das politische Ziel einer „Digital Decade“, das die EU-Kommission 2021 ausgerufen hat und in dem ein „European way“ beschritten werden soll.[172] In jedem Fall handelt es sich um ein äußerst ambitioniertes und weltweit bislang einzigartiges Regulierungsvorhaben im Bereich der Künstlichen Intelligenz.[173]

Grundlegendes Ziel des Artificial Intelligence Act ist die Schaffung eines EU-weit einheitlichen und hohen Schutzniveaus für zwingende Allgemeininteressen, vor allem Gesundheit, Sicherheit und fundamentale Grund- und Freiheitsrechte von Individuen.[174] Gleichzeitig soll im digitalen Binnenmarkt der freie Waren- und Dienstleistungsverkehr für KI-Systeme zwischen Mitgliedstaaten ermöglicht werden.[175]

Der sachliche Anwendungsbereich des Artificial Intelligence Act wird durch die erstmalige Legaldefinition von KI-Systemen in Art. 3 Abs 1 Artificial Intelligence Act festgelegt. Danach ist ein KI-System eine Software, die auf Basis einer oder mehrerer in Anhang I des Artificial Intelligence Act aufgeführten Techniken und Konzepte entwickelt worden ist und im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren. Die folgenden Techniken und Konzepte sollen als KI-Techniken i. S. d. Artificial Intelligence Act gelten:

---

[167] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, COM(2021) 206 final.
[168] Weißbuch zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, COM(2020) 65 final.
[169] Entschließung des Europäischen Parlaments v. 16.2.2017 mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103(INL).
[170] Anhang der Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Koordinierter Plan für künstliche Intelligenz, COM(2018) 785 final.
[171] Annexes to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Fostering a European approach to Artificial Intelligence, COM(2021) 205 final (bislang nur in englischer Sprache verfügbar).
[172] Annexes to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. 2030 Digital Compass: the European way for the Digital Decade, COM(2021) 118 final.
[173] *Gorzala*, RdW digital exklusiv 2021/34, S. 5.
[174] Erwägungsgrund 1 Artificial Intelligence Act.
[175] Erwägungsgrund 1 Artificial Intelligence Act.

- Konzepte des maschinellen Lernens, mit beaufsichtigtem, unbeaufsichtigtem und bestärkendem Lernen unter Verwendung einer breiten Palette von Methoden, einschließlich Deep Learning (Anhang I lit. a) Artificial Intelligence Act);
- Logik- und wissensgestützte Konzepte, einschließlich Wissensrepräsentation, induktiver (logischer) Programmierung, Wissensgrundlagen, Inferenz- und Deduktionsmaschinen, (symbolischer) Schlussfolgerungs- und Expertensysteme (Anhang I lit. b) Artificial Intelligence Act);
- Statistische Ansätze, Bayessche Schätz-, Such- und Optimierungsmethoden (Anhang I lit. c) Artificial Intelligence Act).

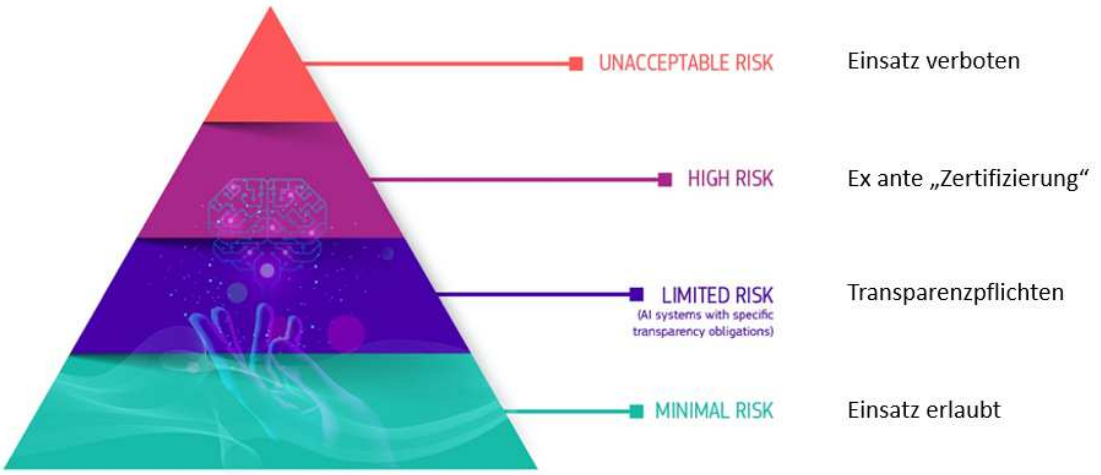
Der räumliche Anwendungsbereich des Artificial Intelligence Act soll sich erstrecken auf:

- Anbieter, die KI-Systeme in der Union in Verkehr bringen oder in Betrieb nehmen, unabhängig davon, ob diese Anbieter in der Union oder in einem Drittland niedergelassen sind (Art. 2 Abs. 1 lit. a) Artificial Intelligence Act);
- Nutzer von KI-Systemen, die sich in der Union befinden (Art. 2 Abs. 1 lit. b) Artificial Intelligence Act);
- Anbieter und Nutzer von KI-Systemen, die in einem Drittland niedergelassen oder ansässig sind, wenn das vom System hervorgebrachte Ergebnis in der Union verwendet wird (Art. 2 Abs. 1 lit. c) Artificial Intelligence Act).

Kern des Artificial Intelligence Act ist ein abgestufter risikobasierter Regulierungsansatz. Danach werden KI-Systeme je nach Risikograd in vier Kategorien unterteilt und mit dem jeweiligen Risikograd korrespondierenden Regelungen unterworfen.

Abbildung 6

Risikograde von KI-Systemen und geplante Regulierung



Quelle: Europäische Kommission , eigene Bearbeitung

KI-Systeme mit unannehmbarem Risiko

Auf der höchsten Stufe identifiziert der Artificial Intelligence Act zunächst KI-Systeme, die eine klare Bedrohung für die grundlegenden Werte der EU wie die Sicherheit, die Lebensgrundlagen und die fundamentalen Grundrechte der Menschen darstellen. Diese als besonders schädlich eingestuften KI-Systeme sollen verboten werden (Art. 5 Abs. 1 Artificial Intelligence Act).

Zu dieser Kategorie von KI-Systemen mit unannehmbarem Risiko zählen:

- Systeme zur unterbewussten, unterschwelligen Manipulation oder zur Ausnutzung des Alters, psychischer oder physischer Schwächen, die einen physischen oder psychischen Schaden von Personen verursachen oder verursachen können (Art. 5 Abs. 1 lit. a) und b) Artificial Intelligence Act);
- Systeme für Social Scoring durch öffentliche Behörden, wenn dadurch Personen oder Personengruppen nachteilig oder unvorteilhaft behandelt werden, und zwar entweder in einem sozialen Kontext, der nicht in Zusammenhang mit den Umständen der ursprünglichen Datenerhebung oder -erzeugung steht, oder in einer Weise, im Hinblick auf ihr soziales Verhalten oder dessen Tragweite ungerechtfertigt oder unverhältnismäßig ist (Art. 5 Abs. 1 lit. c) Artificial Intelligence Act);
- Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken (Art. 5 Abs. 1 lit. d) Artificial Intelligence Act). Derartige Echtzeit-Fernidentifizierungssysteme sollen nur unter bestimmten Voraussetzungen ausnahmsweise zulässig sein (etwa zur zielgerichteten Suche von Opfern von Straftaten und vermissten Kindern, zur Abwendung substanzieller Gefahren für Leben oder körperlicher Unversehrtheit natürlicher Personen oder eines Terroranschlags, Art. 5 Abs. 1 lit. d) sublit. i) - iii) Artificial Intelligence Act). Auch in diesen Ausnahmefällen bedürfen Echtzeit-Fernidentifizierungssysteme einer Genehmigung einer Justizbehörde oder einer anderen unabhängigen Stelle und unterliegen angemessenen Beschränkungen im Hinblick auf die zeitliche und geografische Geltung und die abgefragten Datenbanken.

Hochrisiko-KI-Systeme

Auf der zweithöchsten Stufe identifiziert der Artificial Intelligence Act KI-Systeme, von denen ein hohes Risiko ausgeht, weil sie sich potenziell nachteilig auf die Sicherheit der Menschen oder ihre Grundrechte auswirken können.

Zu solchen Systemen gehören einerseits Sicherheitskomponenten von Produkten, die unter sektorale Rechtsvorschriften der EU – wie etwa das Medizinprodukterecht im Medizinsektor – fallen (Art. 6 Abs. 1 Artificial Intelligence Act). Bei diesen Systemen wird davon ausgegangen, dass von ihnen ein hohes Risiko ausgeht, wenn sie gemäß diesen sektoralen Rechtsvorschriften einer Konformitätsbewertung durch Dritte unterzogen werden müssen.

Zudem definiert Anhang III des Artificial Intelligence Act die folgenden weiteren Hochrisiko-Anwendungsbereiche von KI-Systemen:

- Biometrische Identifizierung und Kategorisierung natürlicher Personen (Anhang III Nr. 1 Artificial Intelligence Act);

- Verwaltung und Betrieb kritischer Infrastrukturen (Anhang III Nr. 2 Artificial Intelligence Act);
- Allgemeine und berufliche Bildung (Anhang III Nr. 3 Artificial Intelligence Act);
- Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit (Anhang III Nr. 4 Artificial Intelligence Act);
- Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistungen (Anhang III Nr. 5 Artificial Intelligence Act);
- Strafverfolgung (Anhang III Nr. 6 Artificial Intelligence Act);
- Migration, Asyl und Grenzkontrolle (Anhang III Nr. 7 Artificial Intelligence Act);
- Rechtspflege und demokratische Prozesse (Anhang III Nr. 8 Artificial Intelligence Act).

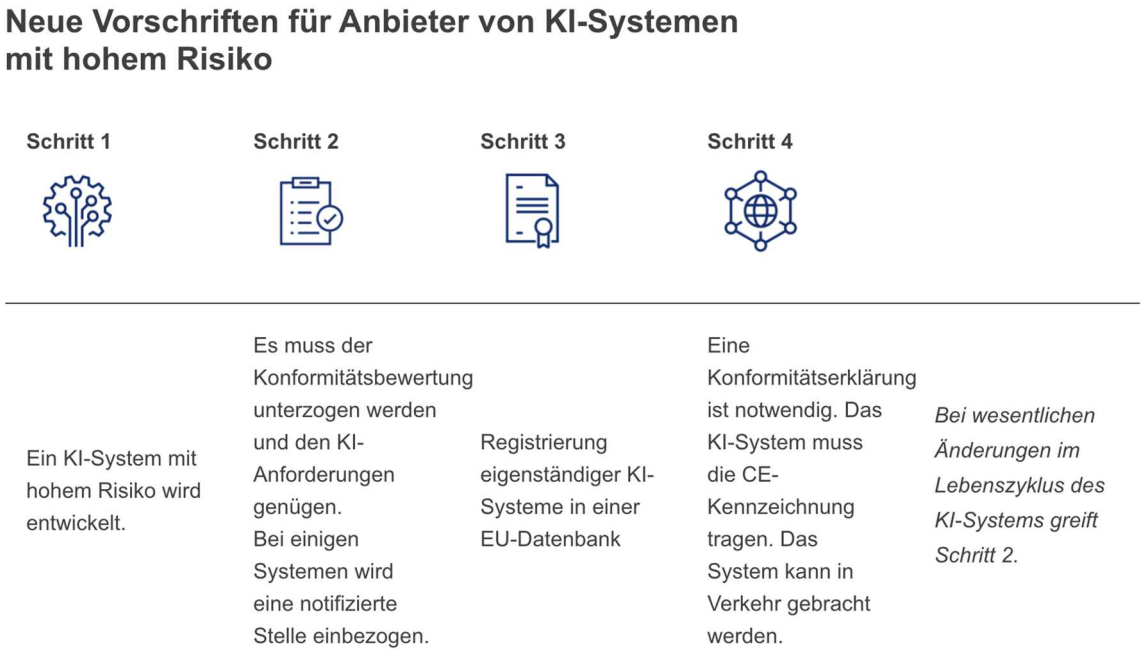
Für solche Hochrisiko-KI-Systeme sieht der Artificial Intelligence Act strenge Vorgaben vor (Art. 8 ff. KI-VO-E), die bereits erfüllt sein müssen, bevor sie auf den Markt gebracht werden dürfen:

- Angemessene Risikomanagementsysteme: Anbieter von Hochrisiko-KI-Systemen müssen ein kontinuierliches, iteratives Risikomanagementsystem für den gesamten Lebenszyklus des KI-Systems einrichten (Art. 9 Artificial Intelligence Act). Dieses ist regelmäßig zu aktualisieren. Zudem ist ein Qualitätsmanagementsystem einzurichten (Art. 17 Artificial Intelligence Act).
- Daten-Governance: Hochrisiko-KI-Systeme, die mit Daten trainiert werden, müssen eine entsprechende Daten-Governance implementieren und dürfen nur relevante, repräsentative, fehlerfreie und vollständige Trainings-, Validierungs und Testdatensätze verwenden, um Risiken und diskriminierende Ergebnisse so gering wie möglich zu halten (Art. 10 Artificial Intelligence Act).
- Technische Dokumentation: Hochrisiko-KI-Systeme bedürfen einer technischen Dokumentation, die bestimmte Mindestinhalte aufweist und stets aktuell gehalten werden muss, um die Rückverfolgbarkeit von Ergebnissen zu ermöglichen (Art. 11 Artificial Intelligence Act.
- Aufzeichnungspflichten: Hochrisiko-KI-Systeme müssen eine Funktion enthalten, die eine automatische Aufzeichnung von Vorgängen und Ereignissen („Logs“) während des Betriebs ermöglicht (Art. 12 Artificial Intelligence Act.
- Transparenz- und Informationspflichten: (Art. 13 KI-VO-E) Nutzern von Hochrisiko-KI-Systemen muss eine präzise, vollständige, korrekte und eindeutige Anleitung zur Verfügung gestellt werden, damit diese die Ergebnisse des KI-Systems entsprechend interpretieren können (Art. 13 Artificial Intelligence Act).
- Menschliche Aufsicht: Hochrisiko-KI-Systeme müssen zur Risikominimierung so gestaltet sein, dass sie effektiv durch Menschen überwacht werden können (Art. 14 Artificial Intelligence Act).
- Schließlich sind Hochrisiko-KI-Systeme – entsprechend dem jeweiligen Einsatzbereich – so zu gestalten, dass sie während ihres gesamten Lebenszyklus ein hohes Maß an Genauigkeit, Robustheit und Cybersicherheit erreichen (Art. 15 Artificial Intelligence Act).

Anbieter von Hochrisiko-KI-Systemen müssen die Konformität mit den vorgenannten Compliance-Vorgaben grundsätzlich in eigener Verantwortung bewerten und eine schriftliche EU-Konformitätserklärung abgeben (Art. 48 Artificial Intelligence Act).

Eingeführt wird auch eine CE-Kennzeichnung, welche Anbieter für zunächst fünf Jahre bei Erfüllung der Voraussetzungen an ihrem Produkt anbringen dürfen (Art. 49 Artificial Intelligence Act). Zudem richtet die EU-Kommission eine zentrale EU-Datenbank für eigenständige Hochrisiko-KI-Systeme ein (Art. 60 Artificial Intelligence Act). Anbieter von Hochrisiko-KI-Systemen müssen diese vor Inverkehrbringen oder Inbetriebnahme in die EU-Datenbank eintragen (Art. 51 Artificial Intelligence Act).

Abbildung 7
Compliance-Anforderungen an Hochrisiko-KI-Systeme



Quelle: Europäische Kommission

Unterhalb der Hochrisikoschwelle stellt der Artificial Intelligence Act besondere Transparenzverpflichtungen für bestimmte *KI-Systeme mit geringem Risiko* auf (Art. 52 Artificial Intelligence Act). KI-Systeme wie Chatbots, die mit natürlichen Personen interagieren, müssen ihre Nutzer darüber informieren, dass sie mit einer Maschine und keiner echten Person interagieren (Art. 52 Abs. 1 Artificial Intelligence Act). Die betroffenen Personen sollen so in die Lage versetzt werden, eine informierte Entscheidung darüber zu treffen, ob sie derartige Anwendungen weiter nutzen und mit diesen interagieren wollen. Auch die Verwendung eines Emotionserkennungssystems oder eines Systems zur biometrischen Kategorisierung sowie sogenannter „Deep Fakes“, also durch Systeme manipulierte oder generierte unreale Bild-, Audio- und Videodateien, muss grundsätzlich offengelegt werden (Art. 52 Abs. 2 und 3 Artificial Intelligence Act).

Alle anderen *KI-Systeme mit minimalem Risiko* werden von dem Artificial Intelligence Act nicht erfasst und können (natürlich unter Einhaltung des allgemein geltenden Rechts) entwickelt und verwendet werden.

Noch handelt es sich beim Artificial Intelligence Act um einen ersten Gesetzesentwurf. Dieser muss anschließend noch seinen Weg durch das EU-Parlament und den Rat der Europäischen Union nehmen. Im weiteren Verfahren ist damit zu rechnen, dass neben Parlament und Rat auch sämtliche potenziell betroffenen Stakeholder im Rahmen ihrer Möglichkeiten auf den Gesetzgebungsprozess Einfluss nehmen werden.[176]

Eine abschließende Beurteilung wäre daher verfrüht. Zu begrüßen ist, dass die EU-Kommission einen risikobasierten Regulierungsansatz mit je nach identifizierten Risiken abgestuften Regelungen (Verbot, Compliance-, Transparenzverpflichtungen) verfolgt. Bisweilen wird die sehr weit gefasste Definition von KI-Systemen kritisiert, die auch Verfahren wie Suchmethoden oder Expertensysteme und damit nicht nur KI im engeren Sinne, sondern im Ergebnis nahezu jedes Computerprogramm erfasse.[177] Positiv ist in jedem Fall, dass der Artificial Intelligence Act einen technologieneutralen Definitionsansatz wählt, der im Lichte neuer technischer Entwicklungen angepasst werden kann.[178] Zu Recht moniert wird weiterhin, dass der Entwurf des Artificial Intelligence Act eine zentrale rechtliche Herausforderung beim Einsatz autonomer Systeme, die Haftung (dazu ausführlich unter Kapitel 4), vollständig ausklammert.[179]

Ebenfalls positiv hervorzuheben ist, dass die EU-Kommission parallel zu den regulatorischen Vorgaben für KI-Systeme einen Fokus auf Innovationsförderung, gerade im Bereich der KMU und Startups, setzt: Nach Art. 53 Artificial Intelligence Act können die Mitgliedstaaten „KI-Reallabore“ (regulatory sandboxes) einrichten. Diese sollen eine kontrollierte Umgebung bieten, in der innovative KI-Technologien für eine begrenzte Zeit auf der Grundlage eines mit den zuständigen Behörden vereinbarten Testplans entwickelt, erprobt und validiert werden können. Beim Zugang zu den KI-Reallaboren sollen KMU und Startups bevorzugt werden (Art. 55 Artificial Intelligence Act). Ob die KI-Reallabore zur Erfolgsgeschichte werden, wird naturgemäß maßgeblich von den Rahmenbedingungen der Förderung und der (nicht nur finanziellen) Ausstattung durch die Mitgliedstaaten abhängen.

[176] *Geminn*, ZD 2021, 354, 359; *Gorzala*, RdW digital exklusiv 2021/34, S. 5.
[177] *Engelmann/Brunotte/Lütkens*, RDi 2021, 317; *Bomhard/Merkle*, RDi 2021, 276, 278.
[178] Art. 4 Artificial Intelligence Act ermächtigt die EU-Kommission, durch sogenannte delegierte Rechtakte die Liste der vom Artificial Intelligence Act erfassten Techniken und Konzepte zu aktualisieren und zu ergänzen.
[179] *Geminn*, ZD 2021, 354, 359; *Bomhard/Merkle*, RDi 2021, 276, 283.

Ansprechpartner/Impressum

Christine Völzow
Geschäftsführerin
Leiterin Abteilung Wirtschaftspolitik

Telefon 089-551 78-251
christine.voelzow@vbw-bayern.de

Impressum

Alle Angaben dieser Publikation beziehen sich ohne jede Diskriminierungsabsicht grundsätzlich auf alle Geschlechter.

Herausgeber

vbw
Vereinigung der Bayerischen Wirtschaft e. V.

Max-Joseph-Straße 5
80333 München

www.vbw-bayern.de

Weiterer Beteiligter / Verfasser

Prof. Dr. Dirk Heckmann
Lehrstuhl für Recht und Sicherheit der Digitalisierung
Technische Universität München

Dr. Alexander Schmid (Erstauflage 2017)