1.3.4 Autonome Softwaresysteme und Unternehmerverantwortung

Stichwörter: Arbeitsschutz, Datenschutz, Ju-RAMI 4.0, Personenschaden, Sachschaden, Sicherheit und Gesundheit bei der Arbeit

› Warum ist das Thema wichtig?

Cyber-physische Systeme (CPS)[1] übernehmen in 4.0-Prozessen[2] zunehmend Aufgaben der (Teil-)Steuerung der Arbeitsabläufe. Über intelligente Software[3] mit ihren Modellen der künstlichen Intelligenz (KI) können CPS Veränderungen in Abläufen vor- und Anpassungsbedarfe wahrnehmen, können Ereignisse interpretieren, Handlungsoptionen auslösen und eigenständig entscheiden. 4.0-Technologien[4] kommunizieren mit ihrem Umfeld und interagieren mit dem Menschen im Arbeitsprozess. Damit können CPS in rechtliche Verantwortungsbereiche des Unternehmers eingreifen (zum Beispiel in Regelungsbereiche des Bürgerlichen Gesetzbuches, Strafgesetzbuches, Datenschutzrechts, Arbeitsschutzrechts). Zu vielen dieser durch autonome Systeme ganz oder teilweise gesteuerten 4.0-Prozesse ist eine klare Einordnung in den bestehenden Rechtsrahmen nicht immer möglich.[5] Es ist wichtig, diese rechtlich nicht eindeutigen Aspekte zu kennen, die sich dann ergeben, wenn die intelligente Software (inkl. KI) die (Teil-)Steuerung in Prozessen übernimmt.

Diese Umsetzungshilfe besitzt keine rechtliche Verbindlichkeit, sondern beschreibt einige grundsätzliche Fragen der Unternehmerverantwortung in 4.0-Prozessen, die jeweils speziell rechtlich zu klären sind.

› Worum geht es bei dem Thema?

Die Autonomie der intelligenten Software (inkl. KI) ist zwar technologischer Art *(technische Deutungsmuster › siehe Umsetzungshilfen 1.3.2 Interaktion zwischen Mensch und Software 4.0; 1.3.3 Handlungsträgerschaft im Verhältnis Mensch und intelligente Software)* und ihr Grad hängt davon ab, wie komplex und differenziert die Interaktion der intelligenten Software (inkl. KI) mit ihrer jeweiligen Umwelt konzipiert worden ist. › *Siehe Umsetzungshilfen 1.1.4 Ethische Werte für die intelligente Software (inkl. KI); 2.3.3 Datenqualität in 4.0-Prozessen.* Die Autonomie der intelligenten Software (inkl. KI) führt aber auch dazu, dass sie nach diesen technischen Deutungsmustern selbst Schlüsse aus den Daten der Umwelt zieht und lernt sowie in Prozessen entscheidet, diese ganz oder teilweise steuert und kontrolliert. Damit tauchen Fragen der Haftung im Zusammenhang mit einer Verantwortlichkeit für Handlungen und Unterlassungen von intelligenter Software (inkl. KI) auf, die nicht automatisch auf einen bestimmten menschlichen Akteur zurückgeführt werden können. Derzeit kann im Rahmen des geltenden Rechts intelligente Software (inkl. KI) nicht für Handlungen oder Unterlassungen haftbar gemacht werden, die zu Sach- und Personenschäden führen können. Insofern stehen Hersteller, Betreiber, Eigentümer und Nutzer für Handlungen oder Unterlassungen der intelligenten Software in Verantwortung. Dies ist vor allem dann eine Frage, wenn die intelligente Software autonom und selbstlernend in Bereiche eingreift, die im Arbeitsprozess der Unternehmerverantwortung unterliegen.

Im Folgenden soll an einigen Beispielen dargestellt werden, in welchen Bereichen autonome und selbstlernende intelligente Software in Verantwortungs- und Rechtsbereiche des Unternehmers eingreifen kann (in Anlehnung an „Ju-RAMI 4.0“[6]):

- **Personenschaden** – Beispiele:
  - Infolge eines Sensors, der fehlerhafte Daten liefert, verletzt ein autonom fahrender Gabelstapler auf dem Firmengelände einen Menschen.
  - Ein CPS erkennt eine nicht ergonomische Körperhaltung und Bewegung eines Beschäftigten und korrigiert sie über ein Assistenzsystem; die Hinweise sind jedoch nicht korrekt und führen zu einem zusätzlichen Gesundheitsschaden bei dem Beschäftigten.

Diese Umsetzungshilfe gibt Experten und Interessierten Anregungen, wie Arbeit 4.0 zu gestalten ist. Die Empfehlungen sollten an die jeweilige konkrete betriebliche Situation angepasst werden.

[1] Cyber-physische Systeme (CPS) verbinden und steuern als autonome technische Systeme Arbeitsmittel, Produkte, Räume, Prozesse und Menschen beinahe in Echtzeit. Die komplette oder teilweise Steuerung übernimmt intelligente Software auf Grundlage von Modellen der künstlichen Intelligenz. Genutzt werden dazu unter anderem auch Sensoren/Aktoren, Verwaltungsschalen, Plattformen/Clouds.

[2] Unter 4.0-Prozessen werden hier alle Arbeitsprozesse verstanden, in denen cyber-physische Systeme (CPS) oder andere autonome technische Systeme (wie Plattformen, Messenger-Programme) beteiligt sind. 4.0-Prozesse sind in den Arbeitsprozessen bisher selten vollständig, aber in Ansätzen in allen Betrieben umgesetzt.

[3] Intelligente Software steuert cyber-physische Systeme (CPS) und andere autonome technische Systeme (wie Messenger-Programme). Intelligente Software nutzt Modelle künstlicher Intelligenz zusammen mit anderen Basistechnologien wie zum Beispiel Algorithmen, semantischen Technologien, Data-Mining. Intelligente Software ist autonom und selbstlernend.

[4] 4.0-Technologie bezeichnet hier Hardware und technologische Produkte (wie Assistenzmittel/Smartphones, Sensoren/Aktoren in smarten Arbeitsmitteln, Fahrzeugen, Produkten, Räumen usw., smarte Dienstleistungen, Apps), die von intelligenter Software (inkl. KI) ganz oder teilweise gesteuert werden.

[5] vgl. u. a. Di Fabio 2016, S. 17f.; Europäisches Parlament 2015, Kapitel „Haftung“; Hilgendorf & Seidel 2016a, S. 12; Tschol 2014

[6] „Ju-RAMI 4.0“ ist ein juristisches Referenzarchitekturmodell, das helfen soll, die Kluft zwischen 4.0-Technik, 4.0-Prozessen und Recht mithilfe einer Systematisierung und Visualisierung vorhandener Problemzusammenhänge zu überwinden, Hilgendorf & Seidel 2016a/2016b.

[7] StGB = Strafgesetzbuch

Rechtssituation: Wer den Körper einer anderen Person vorsätzlich oder fahrlässig verletzt, kann strafrechtlich zur Verantwortung gezogen werden (vorsätzliche [§ 223 StGB[7]] oder fahrlässige Körperverletzung [§ 229 StGB]). Wird eine Person getötet, wird eine vorsätzliche (§ 212 StGB) oder fahrlässige (§ 222 StGB) Tötung untersucht.[8]

- **Verstoß gegen Sicherheit und Gesundheit bei der Arbeit** – Beispiele:
  - Eine autonome Steuerungssoftware setzt ein Zugangsverbot zu einem durch Gefahrstoffe kontaminierten Bereich außer Kraft (inklusive der smarten Sperrmechanismen an den Zugangstüren), weil der Weg durch diesen Bereich eine erhebliche Zeitersparnis bringt.
  - Eine autonome Informationssoftware einer Anlage, die die Beschäftigten über Smartglasses im Bedienen der Anlage instruiert, hat die Arbeitsschutzunterweisung gestrichen. Dies hat sie von der falsch programmierten Software von verketteten Anlagen gelernt. Nach einem Unfall kann der Unternehmer nicht nachweisen, den Beschäftigten wie vorgeschrieben unterwiesen zu haben.

  Rechtssituation: Der Arbeitgeber hat für eine sichere und gesunde Arbeit zu sorgen und dafür alle technischen, organisatorischen und personalen Maßnahmen zu planen, umzusetzen und zu kontrollieren (§§ 3, 4 ArbSchG sowie u. a. § 4 BetrSichV; § 7 GefStoffV; § 4 ArbStättV)[9]. Die Umsetzung der Aufgabe kann der Unternehmer delegieren, die grundlegende Verantwortung für den Arbeitsschutz bleibt beim Unternehmer.

- **Missbrauch personenbezogener Daten** – Beispiele:
  - Die Smartphones, die der Betrieb allen Führungskräften und Beschäftigten zur Verfügung gestellt hat, erfassen Bewegungs- und Kommunikationsdaten der Beschäftigten und nutzen sie für das von intelligenter Software gesteuerte Personalcontrolling, ohne dass eine entsprechende Vereinbarung mit den Führungskräften und Beschäftigten vereinbart wurde.
  - Ein smarter Bohrhammer liefert Daten über die Arbeitsweise der Beschäftigten an die Hersteller-Plattform des Arbeitsmittels, ohne dass die Beschäftigten und der Arbeitgeber dies wissen.

  Rechtssituation: Personenbezogene Daten dürfen nur dann erhoben, abgespeichert oder verarbeitet werden, wenn der Betroffene ausdrücklich zugestimmt hat oder ein Gesetz die Erhebung, Speicherung oder Verarbeitung vorsieht. Derartige Daten werden missbraucht, wenn sie zu rechtlich unzulässigen Zwecken verwendet werden.[10] Grundlage für den Datenschutz in Deutschland bilden neben dem Grundgesetz (GG), die EU-Datenschutz-Grundverordnung (EU-DSGVO) und das neue Bundesdatenschutzgesetz (BDSG n. F.).

- **Sachschaden** – Beispiele:
  - Eine fehlerhafte Programmierung eines autonom agierenden Service-Transportroboters führt zu erheblichen Schäden an Fahrzeugen auf dem Betriebsgelände.
  - Eine autonome intelligente Software, die eine Reihe verketteter Maschinen steuert, berücksichtigt wesentliche Parameter der Arbeitsumgebung nicht und es kommt zu Defekten an den Maschinen.

  Rechtssituation: Sachschäden hat grundsätzlich der Eigentümer selbst zu tragen. Ein Recht auf Ersatz des entstandenen Schadens besitzt er nur, wenn es dafür eine besondere rechtliche Grundlage gibt, zum Beispiel einen Vertrag (sogenannte vertragliche Haftung) oder eine gesetzliche Vorschrift (wie § 823 BGB[11], sogenannte gesetzliche Haftung). Wird ein Sachschaden vorsätzlich herbeigeführt, kann der Verursacher des Schadens unter Umständen auch strafrechtlich zur Verantwortung gezogen werden (§ 303 StGB, Sachbeschädigung).[12]

- **Kontrollverlust an Arbeitsmitteln** – Beispiel:
  - Eine selbstlernende Software zieht auf Grundlage ermittelter Daten den Schluss, dass ein Beschäftigter effizienter mit dem Arbeitsmittel arbeitet, wenn die Schutzeinrichtung deaktiviert ist; die Software deaktiviert daraufhin die Schutzeinrichtungen.
  - Gleichzeitig deaktiviert die intelligente Software (inkl. KI) auch an allen anderen mit dem Arbeitsmittel verketteten Einrichtungen die Schutzeinrichtung.

  Rechtssituation: Ein Kontrollverlust liegt dann vor, wenn vorgegebene Regeln nicht mehr befolgt werden und eine Rückführung in den ursprünglichen regelgeleiteten Zustand nicht oder nur unter großem Aufwand möglich ist. Kontrollverlust stellt bei intelligenter Software (inkl. KI) ein erhebliches Risiko dar. Autonom erlernte Fehler und Fehlfunktionen können sich von einem zum anderen Arbeitsmittel übertragen. Dies kann Sach- und Personenschäden verursachen.[13]

- **Vertragsbruch** – Beispiele:
  - Die autonome Organisationssoftware erhöht die Taktung eines Arbeitsprozesses entgegen der vertraglichen Vereinbarungen (zum Beispiel nach Arbeitsvertrag, Betriebsvereinbarung).
  - Die smarte Personaleinsatzplanungssoftware setzt einen Beschäftigten länger ein als im Arbeitsvertrag festgelegt.

  Rechtssituation: Der Vertragsbruch muss nicht vorsätzlich erfolgen. Wenn durch einen Vertragsbruch Sach- oder Personenschäden entstehen, führt dies in der Regel zu einer rechtlichen Schadensersatzpflicht.

[8] Hilgendorf & Seidel 2016a, S. 19
[9] ArbSchG = Arbeitsschutzgesetz; BetrSichV = Betriebssicherheitsverordnung; GefStoffV = Gefahrstoffverordnung; ArbStättV = Arbeitsstättenverordnung
[10] Hilgendorf & Seidel 2016a, S. 20
[11] BGB = Bürgerliches Gesetzbuch
[12] Hilgendorf & Seidel 2016a, S.1 9
[13] Hilgendorf & Seidel 2016a, S. 21

Die Beispiele verdeutlichen die Rechtsprobleme, die sich im Handlungsfeld Unternehmerverantwortung und autonome sowie selbstlernende intelligente Software (inkl. KI) ergeben können. Unser Rechtssystem ist auf verantwortlich handelnde Person zugeschnitten und nicht auf autonom und intelligent handelnde Software.[14] Autonome Systeme besitzen bisher keine eigene Rechtspersönlichkeit. Daher ist nach geltendem Recht der Betreiber, der Eigentümer, der Nutzer der intelligenten Software (also der Unternehmer) oder der Hersteller verantwortlich, je nach Ursache des Schadens. Aus diesem Grund sollten die Betriebe die Frage der Unternehmerverantwortung bei der Nutzung autonomer CPS möglichst sorgfältig überlegen und klären.

Welche Chancen und Gefahren gibt es?

Wer die teilweise offene Rechtssituation des Einsatzes autonomer und selbstlernender CPS kennt und berücksichtigt, kann die Potenziale der intelligenten Software (inkl. KI) vollständig nutzen, um Arbeitsprozesse effektiv, effizient, sicher und gesund zu gestalten sowie neue Marktsegmente und Dienstleistungen umzusetzen.

Wer autonome und selbstlernende CPS unter Berücksichtigung der teilweise offenen Rechtssituation unreflektiert, ohne die Risiken einzuschätzen und ohne Absicherung einsetzt, unterliegt der Gefahr, für Handlungen der Software verantwortlich gemacht zu werden, die einen erheblichen Schaden für den Unternehmer und das Unternehmen zur Folge haben.

Welche Maßnahmen sind zu empfehlen?

Beim Einsatz von autonomer und selbstlernender intelligenter Software sollte in allen Anwendungsbereichen[15] unter anderem Folgendes berücksichtigt werden:[16]

- **Information:** Sich vor dem Einsatz aller smarten Gegenstände (wie Arbeitsmittel, Raumumgebung, Anlagen, Einrichtungen, Fahrzeuge), aller smarten Prozesse (wie Prozessplanung, Organisation, Personaleinsatz) sowie von Organisations- und Steuerungssoftware, die diese Arbeitsmittel und Gegenstände vernetzt, beim Hersteller/Anbieter informieren:
  - Welche Funktionen (insbesondere Steuerungsfunktion, Vernetzung, Lernprozesse) erfüllt autonome und selbstlernende Software?
  - Was wird von der Software wie entschieden?
  - Welche Informationen/Protokolle liefert die Software über ihre Entscheidungen?
  - Welche Daten werden erhoben und wie, wo und wofür werden sie genutzt?
  - Welche Interventionsmöglichkeiten gibt es für den Betrieb und für einzelne Führungskräfte und Beschäftigte?
  - In welchem Datenformat stehen die Daten zur Verfügung und ist dieses Format kompatibel zu den im Betrieb genutzten Formaten (beziehungsweise welche Anpassungsarbeiten sind erforderlich)?

  Hierzu empfiehlt es sich, die Lizenzbedingungen des Herstellers/Anbieters der autonomen und selbstlernenden intelligenten Software durchzulesen.

- **Konzept:** Hierbei sind in Bezug auf die Verantwortung die folgenden Aspekte zu berücksichtigen:
  - Anwendungsbereiche und Nutzungsart der autonomen und selbstlernenden intelligenten Software (inkl. KI) im Betrieb (zum Beispiel als Teilprozess oder als Bestandteil des Gesamtsystems)
  - Potenziale, die die intelligente Software (inkl. KI) bietet
  - Kriterien nach denen die Software lernt und Prozesse ganz oder teilweise steuert
  - Art der benötigten Daten, Berücksichtigung von Arbeitsschutz, Datensicherheit und -schutz
  - Transparenz der Handlungsträgerschaft, Interventionsmöglichkeiten,
  - Rückholbarkeit/Löschung, Umgang mit den Daten, Besitz an den Daten
  - Art der Dokumentation
  - Stand der Gerichtsbarkeit

- **Risiken:** Einschätzen und bewerten, ob die gewählten Lösungen und Konzepte Risiken enthalten, und entsprechende Maßnahmen festlegen. Die rechtlichen Schwachstellen identifizieren und auch hier Kontrollmaßnahmen definieren.
- **Vereinbarung mit Hersteller/Anbieter:** Regeln vereinbaren, wie die im Konzept dargestellten Anforderungen realisiert und garantiert werden beziehungsweise nur Lösungen annehmen, die die Anforderungen des Konzeptes weitgehend erfüllen und klare rechtliche Regeln zulassen.
- **Einführung:** Verfahren festlegen, wie die Führungskräfte und Beschäftigten mit den autonomen Systemen arbeiten sollen. Mit den Führungskräften und Beschäftigten vereinbaren, wie mit personenbezogenen Daten umgegangen wird. Die Führungskräfte und Beschäftigten für die Arbeit mit den autonomen und selbstlernenden Systemen qualifizieren und darüber informieren, welche rechtlichen Probleme dabei auftreten können.
- **Kontrolle:** Wirksamkeit der eingesetzten autonomen und selbstlernenden intelligenten Software (inkl. KI) überprüfen. Dabei auch die rechtlichen Schwachstellen, die Erfahrungen der Führungskräfte und Beschäftigten sowie ihre Verbesserungsvorschläge berücksichtigen.
- **Dokumentation:** Die Dokumentation bietet eine Grundlage, um Probleme mit Verantwortlichkeit in den einzelnen

[14] BDI & Noerr LLP 2015, S. 14

[15] Anwendungsbereiche von CPS können sein: Insellösungen, Teilkomponenten und Teilprozesse (zum Beispiel einzelne Arbeitsplätze, Arbeitsmittel, Teile von Anlagen, Räume, Produkte, Assistenzsysteme) und verkettete Prozesse und Gesamtsystemlösungen (zum Beispiel verkettete Arbeitsmittel, Wertschöpfungskette). Außerdem geschlossene Betriebsanwendungen (autark – zum Beispiel Edge Computing, betriebliche Cloud) offene Anwendungen (zum Beispiel Public Clouds, Hersteller-Plattformen).

[16] vgl. u. a. Europäisches Parlament 2015; Probst-Klosterkamp 2017; Sauerwein 2017

Situationen überhaupt beurteilen zu können. Dazu ist sicherzustellen, dass alle Entscheidungen und Prozesse der autonomen und selbstlernenden intelligenten Software dokumentiert werden:

- Wer zu welchem Zeitpunkt jeweils entscheidet, steuert und kontrolliert.
- Wann, wie und an welchen Stellen die Handlungsträgerschaft wechselt.
- Auch die Entscheidungsfindungsschritte der intelligenten Software sollten für die Rekonstruktion und Rückverfolgung zugänglich und dokumentiert sein.

Quellen und weitere Informationsmöglichkeiten:

BDI – Bundesverband der Deutschen Industrie e. V., & Noerr LLP. (2015). *Industrie 4.0 – Rechtliche Herausforderungen der Digitalisierung*. Berlin: BDI.

Di Fabio, U. (2016). *Grundrechtsgeltung in digitalen Systemen*. München: C. H. Beck.

Europäisches Parlament (2015). *Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik*. (2015/2103(INL)-Entwurf.

Hilgendorf, E., & Seidel, U. (2016a). *Juristische Herausforderungen für digitale Wertschöpfung – strukturierte Lösungswege für KMU*. iit-Institut für Innovation und Technik in der VDI/VDE Innovation + Technik GmbH. (Hrsg.). Berlin: www.autonomik40.de.

Hilgendorf, E., & Seidel, U. (2016b). *Juristische Herausforderungen für digitale Wertschöpfung – strukturierte Lösungswege für KMU*, iit-Institut für Innovation und Technik in der VDI/VDE Innovation + Technik GmbH. (Hrsg.). Berlin: www.autonomik40.de.

Probst-Klosterkamp, M. (2017). Rechtliche Herausforderungen der Industrie 4.0 für den Mittelstand. In W. Krüger (Hrsg.), *Digitalisierung und Industrie 4.0 – Herausforderungen für den Mittelstand* (S. 92–102). Bielefeld. Fachhochschule des Mittelstandes (FHM).

Sauerwein, F. (2017). *Macht der Algorithmen. Einfluss ohne Verantwortung? – Algorithmen und Roboter treffen Entscheidungen und übernehmen Führungsaufgaben – aber können sie dafür auch Verantwortung übernehmen?* www.derstandard.de/story/2000064791531/macht-der-algorithmen-einfluss-ohne-verantwortung. Zugegriffen: 06.08.2018.

Tschohl, Christof. (2014). *Industrie 4.0 aus rechtlicher Perspektive*. In Elektrotechnik & Informationstechnik 131 (7), S. 219–222.

Zu diesem Thema könnten Sie auch folgende weitere Umsetzungshilfen interessieren:

- 1.1.3 Unternehmensethik und intelligente Software (inkl. KI)
- 1.1.4 Ethische Werte für die intelligente Software (inkl. KI)
- 1.3.2 Interaktion zwischen Mensch und intelligenter Software (inkl. KI)
- 1.3.3 Handlungsträgerschaft im Verhältnis Mensch und intelligente Software (inkl. KI)
- 2.3.3 Datenqualität in 4.0-Prozessen

Herausgeber: „Offensive Mittelstand – Gut für Deutschland" – Stiftung „Mittelstand – Gesellschaft – Verantwortung"
Kurfürsten-Anlage 62, 69115 Heidelberg, E-Mail: info@offensive-mittelstand.de; Heidelberg 2019