DIGITALISIERUNG, AUTOMATISIERUNG UND KÜNSTLICHE INTELLIGENZ IN DER INDUSTRIE
EIN BEITRAG FÜR MEHR SICHERHEIT

Wer haftet für Schäden? Mensch, Maschine oder niemand?

AUTOR:
Rechtsanwalt Dr. Andreas Eustacchio LL.M. (LSE London), spezialisiert auf neue Technologien

„Social distancing“ ist, war und wird in den kommenden Wochen unseren Alltag bestimmen, bei jeder gewollten Annäherung an bzw. jeder möglichen ungewollten Nähe zu unseren Mitmenschen. Solange das Corona-Virus (Covid-19) durch Medikamente oder einen Impfstoff nicht unter Kontrolle gebracht und die Gefahr des Wiederaufflammens der Pandemie noch nicht gebannt ist, wird unsere Gesellschaft mit diesem neuen Phänomen der Distanzierung und der Einhaltung eines Mindestabstands zur Vermeidung und Reduktion von Ansteckung leben und leben lernen.

Bei all diesen Maßnahmen geht es um die Gesundheit von uns Menschen und um die Vermeidung von möglicher Ansteckung. Kurzum: es geht um Sicherheit. Aber 100 %-ige Sicherheit kann weder *social distancing* noch das Tragen von Nasen-, Mundschutz für sich allein geben.

Aber gemeinsam mit der Einhaltung der nötigen Hygiene- und Desinfektionsmaßnahmen können sie alle gemeinsam den Schutz sehr stark erhöhen.

WAS HAT DIE DIGITALISIERUNG MIT CORONA ZU TUN?

In den vergangenen Monaten hat Covid 19 notgedrungen zu all diesen Veränderungen in den vielen Gewerbe- und Industrieunternehmen geführt. Aber was macht Corona für die Industrie? Die österreichische Industrie und deren Industriebetriebe, seit je her Vorreiter bei der Automatisierung in den Produktions- und Logistikabläufen und Rückgrat der österreichischen Wirtschaft und unseres Wohlstandes, werden in ihren Entwicklungsabteilungen und Produktionsstätten noch stärker auf die Einhaltung von *social distancing* und aller anderen notwendigen Sicherheitsmaßnahmen achten. Vor allem jetzt, wo es um das Hochfahren der Wirtschaft geht, sind all diese gemeinsamen Kraftanstrengungen für die eigene Sicherheit und für jene der vielen Mitarbeiterinnen und Mitarbeiter in den Unternehmen essenziell. Verstärkte Automatisierung und der behutsame Einsatz von intelligenten Maschinen sowie Roboterisierung können dafür als flankierende Maßnahmen einen Gewinn darstellen. Dabei geht es eben nicht um den Ersatz von Menschen, also Maschine statt Menschen, sondern um eine Unterstützung der Menschen bei ihrer Arbeit und der Fertigung von Maschinen und Waren.

Faktum ist, dass Unternehmen durch die von Covid 19 ausgelöste Wirtschaftskrise plötzlich unter einem enormen finanziellen Kostendruck stehen. Auch wenn die Produktion in Österreich nun wieder anläuft, könnten wichtige europäische und außereuropäische Absatzmärkte für österreichische Unternehmen, traditionell exportorientiert, wegbrechen. Aber auch in der Lieferkette könnten veritable Engpässe auftreten, erforderliche Zulieferteile und Komponenten aus anderen Ländern (China) nicht oder nicht zu den gewohnt günstigen Konditionen geliefert werden. Und ob der Konsum anspringt und die Waren auch ihre Endabnehmer finden, ist die große Unbekannte. Und: was passiert, wenn die Infektionen wieder zunehmen? Einen zweiten lock-down kann sich wohl niemand mehr leisten.

DIGITALER WANDEL IM RECHT?

Die Transformation hin zum digitalen Wandel ist somit gerade jetzt nicht aufzuhalten. Es wird eine Zeit nach Corona geben. Die Digitalisierung wird durch die aktuelle Corona-Situation auch noch an Schwung gewinnen, und die Digitatalisierung erfasst neben der (wieder)entdeckten Arbeitswelt mit *home-office* sowie der Fertigungsindustrie auch noch viele andere Bereiche. *Selbstlernende Systeme/deep-learning*, künstliche Intelligenz (kurz KI) oder IoT (Internet of Things) gewinnen in den Bereichen der Medizintechnik, dem Gesundheits- und Pflegebereich, im Baugewerbe, im Landmaschinenbau, in der Logistik, aber auch bei der Entwicklung autonomer Fahrzeuge an Bedeutung, nur um einige zu nennen. Die, die bereits zuvor schon in Digitalisierung Zeit und Geld investiert haben, werden daher auch einen Vorsprung haben und besser durch die Krise kommen als andere, die sich diesen Entwicklungen verwehren.

Künstliche Intelligenz und selbstlernende Maschinen gelten als unverzichtbare Bausteine der Digitalisierung.

Künstliche Intelligenz (englisch: Artificial Intelligence, kurz AI) ist ein Teilgebiet der Informatik und setzt sich mit der Automatisierung intelligenten Verhaltens auseinander. KI-Systeme sind vom Menschen entwickelte Software- und Hardware-Systeme, die auf physischer oder digitaler Ebene agieren, indem sie ihre Umgebung durch Datenerfassung wahrnehmen, die gesammelten Daten interpretieren, Schlussfolgerungen daraus ziehen oder die aus diesen Daten abgeleiteten Informationen verarbeiten und über die geeignete(n) Maßnahme(n) zur Erreichung des vorgegebenen Ziels entscheiden. Bei der allgemeinen Definition des Begriffs wird vor allem auf die Imitation des menschlichen Entscheidungsverhaltens referenziert. Durch die spezifische Programmierung eines Computers sollen auf eine einfache Art anspruchsvolle Probleme gelöst werden. In der Praxis tragen einfache Algorithmen dazu bei, ein intelligentes Verhalten zu imitieren.

Fazit: bei KI ist keine manuelle aufwändige und fehleranfällige Programmierung mehr erforderlich. Es gibt auch keine eindeutig im Vorfeld definierten Entscheidungsbäume (=data mining, machine learning und data analysis). Nicht der Programmierer/Softwareentwickler, sondern die gesammelten Daten definieren das Ziel. Und die Maschine, der Computer lernt aus unzähligen Kombinationsmöglichkeiten Schlussfolgerungen zu ziehen und zu entscheiden.

Die Europäische Kommission hat in ihrem eben erst am 19.2.2020 erschienen „Weissbuch“ die Chancen der künstlichen Intelligenz als Rohstoff für die europäische Industrie betont, dabei aber auch auf die rechtlichen Herausforderungen hingewiesen. Bei allem Potential das KI hat, unsere Welt zum Besseren zu verändern, ist Vertrauen die Grundvoraussetzung dafür, dass Menschen und Gesellschaften KI-Systeme überhaupt entwickeln, einführen und nutzen. KI ist kein Selbstzweck, sondern ein Instrument, das den Menschen dienen muss und letztlich das Wohlergehen der Menschen steigern soll, wie die Europäische Kommission schon ein Jahr zuvor, im April 2019, in einem Bericht zu KI bekräftigte. Wenn KI-Systeme und die dahinterstehenden Menschen nicht bewiesenermaßen vertrauenswürdig sind, könnten daraus resultierende unerwünschte Konsequenzen zur Folge haben, dass ihre Akzeptanz möglicherweise untergraben und dadurch die Verwirklichung der potenziell gewaltigen sozialen und ökonomischen Vorteile von KI-Systemen überhaupt verhindert wird.

HAT KI WERTE?

Ob die durch KI generierten Entscheidungen auch die richtigen und mit unseren ethischen Vorstellungen vereinbare sind, ist in der Diskussion um KI ein nicht zu unterschätzender Aspekt. Nach welchem Wertekatalog soll eine selbstlernende Maschine Entscheidungen treffen? Selbst wenn man einen Zufallsgenerator entscheiden lassen wollte, müsste irgendjemand die Maschine mit den unterschiedlichen Entscheidungsmöglichkeiten zuvor füttern.

Die Europäische Kommission propagierte im Dezember 2018 Ethik-Leitlinien für eine vertrauenswürdige KI. Das sind Empfehlungen die von KI-Entwicklern, KI-Anbietern und Nutzern gleichermaßen befolgt werden sollen, vorallem um gleiche Wettbewerbsbedingungen zu bieten. Eckpunkte sind

- die Kontrolle und die Aufsicht von KI durch Menschen,
- Verlässlichkeit, Technische Robustheit und Sicherheit
- Datenschutz, Transparenz, Nichtdiskriminierung und Fairness
- Nachprüfbarkeit sowie gesellschaftliches und ökologisches Wohlergehen

Neben diesen ethischen „Regeln“ müssen durch KI erkennbare Lücken des bestehenden Rechtsrahmens durch klare rechtliche Regeln geschlossen werden. Insbesondere bei der Haftungsfrage könnte es notwendig sein, neue Regelwerke zu schaffen. Denn KI-Technologien können neue Sicherheitsrisken für Nutzer mit sich bringen, wenn sich diese in Produkten und Dienstleistungen wiederfinden. Denken Sie an ein autonomes Fahrzeug, das aufgrund eines Fehlers in der Objekterkennungstechnik einen Gegenstand auf der Straße falsch identifiziert und einen Unfall mit Verletzungen und Sachschäden verursacht.

WER TRÄGT VERANTWORTUNG?

Wer haftet also für durch Fehler einer Maschine verursachte Schäden? Der Betreiber der Maschine, der Hersteller, der Software-Entwickler oder die Maschine oder das System selbst, in das eine Maschine eingebettet ist, ähnlich wie die Haftung einer juristischen Person (GmbH, AG)? Während Schäden, die durch ein menschliches Verhalten verursacht werden, einem Menschen zugeordnet werden können, der für diese auch einzustehen hat (also den Schaden zu ersetzen hat und/oder einer strafrechtlichen Verfolgung), ist die Zuordnung zu einem menschlichen Verhalten bei KI-Technologien und selbstlernenden Systemen schwierig bis unmöglich. Dadurch kann es für Personen, die einen Schaden erlitten haben, schwer werden, Entschädigung zu erhalten, weil ihnen schlichtweg der Zugang zu Nachweisen fehlt. Dies ist aber für die Beweisführung in einem Gerichtsverfahren essenziell (wie noch aus dem Kaprunfall in Erinnerung ist). Haftet am Ende niemand?

Abhilfe schaffen könnte man durch die Einführung einer Versicherungspflicht für den Einsatz derartiger Maschinen wie bei der Kfz-Pflichthaftpflichtversicherung mit bestimmten Versicherungssummen. Dabei stellt sich aber die Frage nach Haftungshöchstgrenzen, was aber wiederum zum Nachteil eines Geschädigten wäre, wenn diese Haftungshöchstgrenzen überschritten sind.

CHANCEN FÜR DIE INDUSTRIE NOCH BESSERE PRODUKTE ZU ERZEUGEN

Heute schon bietet die Digitalisierung für die Industrie Möglichkeiten, die Qualität und die Sicherheit von Produkten zu verbessern, etwa über den digitalen Zwilling. Das ist das digitale Abbild einer Maschine oder einer Produktionsanlage. Verfahrens- und Produktionsabläufe werden durch Software digital dargestellt, nachgebildet oder simuliert. Dadurch können Produktionsprozesse verbessert und optimiert werden und die Produktsicherheit der erzeugten Produkte erhöht werden. Die software-basierte Dokumentation von Konstruktions- und Produktionsabläufen erleichtert Herstellern damit den Nachweis, dass ein erzeugtes Produkt nicht fehlerhaft war. Anhand detaillierter Simulationsergebnisse können Unternehmen den realen Verschleißzustand und die verbleibende Lebensdauer ihrer Produktionsanlagen individuell bewerten, denn das digitale Modell und das physische Gegenstück durchleben die gleichen Prozessschritte. Es geht aber nicht nur um die Erfassung des Ist-Zustandes, sondern auch darum, rechtzeitig Wartungsmaßnahmen einzuleiten, und zwar damit im Bedarfsfall ein zielgerichteter Produktrückruf eingeleitet werden kann.

Der Hersteller kann durch die Auswertung der Nutzungsdaten über sein Produkt aber auch einen von ihm nicht bestimmten und/oder ursprünglich nicht vorhersehbaren Gebrauch durch Nutzer seiner Produkte in Erfahrung bringen. Tritt ein solcher Fall ein, müsste er aus Gründen der Sicherheit die entsprechenden Änderungen bzw Ergänzungen am Produkt ergreifen, um Produktschäden zu vermeiden. Die Digitalisierung hilft somit bei der Erfüllung der gesetzlich auferlegten Produktbeobachtungspflicht. Viele Unternehmen sind bereits heute in der Lage, die Rückverfolgbarkeit ihrer Produkte mit technischen und datenschutzrechtlich zulässigen Mitteln sicherzustellen. Nach wie vor sind nämlich viele Produkte ohne Kennnummern auf dem Markt, deren Gefahren vom Hersteller nicht mehr beherrschbar sind. Ohne den tatsächlichen Produkt-Nutzer zu kennen, kennt man aber durch die, ich nennen sie „digitale Produktbeobachtung“ zumindest den Standort des Produkts. Aber auch den muss man nicht kennen, denn ein Produktrückruf könnte in Form eines Sicherheits-Software-Updates erfolgen, ohne das Produkt physisch mit enormen Kosten zurückholen bzw. nachbessern zu müssen. Damit kann man sich einen oftmals immensen logistischen Aufwand bei der Nachrüstung von Waren ersparen!

Digitale Tests der Produkte können auch als Nachweis für Versicherungen und die von ihnen verlangten Erprobungsklauseln darstellen, wenn diese nach den anerkannten Regeln von Wissenschaft und Technik erfolgen.

DIGITALISIERTE UND VERNETZTE PRODUKTE

Aber auch die von Industrieunternehmen erzeugten Maschinen, Zulieferteile oder Konsumgüter sind immer stärker vernetzt und digitalisiert. Wir haben es mit einer immer stärkeren Verzahnung von physischen Produkten und Dienstleistungen zu tun. Was früher Wartungsverträge und „after-sales-service-Verträge“ waren, mit denen man beim Verkauf einer Maschine/Anlage im Geschäft blieb, spielen heute „Software-Updates“ eine immense wirtschaftliche Bedeutung. Häufig werden diese unter dem Vorwand von „Sicherheits-Updates“ angeboten, deren Notwendigkeit vom Nutzer schwer bis gar nicht beurteilt werden kann. Oder im umgekehrten Fall etwa bei einem Flugzeughersteller, der sicherheitsrelevante Software als Extra verkaufte. Sicherheitstools dürfen jedoch niemals Extras sein. Anstatt Maschinen zu kaufen, geht der Trend

dahin, Maschinen vermehrt im Rahmen von Dienstleistungen zu nutzen. Eigentum daran muss nicht notwendigerweise mehr erworben werden.

WIE SICHER IST SICHER?

In rechtlicher Hinsicht gibt es rechtliche Unsicherheiten, gerade bei vernetzten Produkten, wie die Verletzung des Datenschutzes, Gefahren für Datensicherheit (Cyber-Kriminalität), ethische Fragestellungen und natürlich die Haftungsfragen, wenn derartige Systeme Schäden verursachen und gerade nicht die Sicherheitserwartung erfüllen, für die sie beworben oder gekauft wurden.

Das Problem der Sicherheitserwartung zeigt sich nach wie vor auch stark bei der Entwicklung selbstfahrender Autos, bei denen man schon vor fünf Jahren vorausgesagt hatte, dass diese 2020 (also heuer) bereits auf den Straßen fahren würden. Eingetreten ist es nicht. Die Wahrheit ist, dass die Fahrzeuge nach wie vor mit Assistenzsystemen ausgestattet sind, aber weder technisch so weit sind, dass man sich ohne menschliche Kontrolle über das Fahrzeug automatisiert herumführen lassen kann, noch rechtlich – zumindest in Europa – zulässig sind. Einige Hersteller haben ihre Fahrzeuge zu Beginn der Euphorie als mit „Autopiloten“ ausgestattete Systeme angepriesen. Nach den ersten medienbekannten Unfällen in den USA hat man diese Werbelinie in Europa schleunigst aufgegeben, aus Sorge vor einer Haftung für Schäden durch Unfälle, ausgelöst durch Assistenzsysteme, die nicht funktioniert haben und einer zu hohen Erwartungshaltung. Dem Kunden hat man aus Verkaufsgründen irrig suggeriert, das Auto könne bereits selbst fahren.

Der Begriff Sicherheit ist im Englischen deutlicher, weil zwischen „safety“ und „security“ unterschieden wird:

- bei „safety“ geht es um die Unfallvermeidung, also dass das Produkt selbst keine Gefahr für Menschen darstellt. In einer Maschine sind Funktionen eingebaut, die Menschen und Umwelt schützen.
- bei „security“ ist es umgekehrt, geht es doch darum, die Maschine vor Eingriffen von außen auf die Systeme zu schützen, also den Schutz der Maschine vor dem Eingriff von Menschen oder anderen Maschinen.

Die Vernetzung gibt es auch bei anderen „smart-goods“, von der vernetzten Kaffeemaschine über das smart-home, vernetzte Wearables wie Fitnesstracker bis hin zum vernetzten Herzschrittmacher. Bei allem Komfort, der damit verbunden ist, all diese Produkte müssen funktionieren, aber gleichzeitig sicher sein! Es reicht somit nicht mehr nur, dass das Produkt funktiniert und die Funktionssicherheit vorliegt, sondern die weitreichendere Systemsicherheit ist gefragt.

Schon nach der DSGVO müssen nach dem Stand der Technik geeignete technische und organisatorische IT-Sicherheitsmaßnahmen getroffen werden, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, was auch eine Datenschutz-Folgenabschätzung erfordert. Das allein genügt aber nicht. Unternehmen vergessen bei der Entwicklung von Produkten und Systemen die produktsicherheitsrechtliche Risikofolgenabschätzung.

EU-CYBERSECURITY ACT SOLL FÜR MEHR DATENSICHERHEIT SORGEN

Der EU-Cybersecurity Act 2019 (EU-Verordnung) soll maßgeblich dazu beitragen, dass IT-Produkte, -Dienste und -Prozesse bereits in ihrer Entwicklung Anforderungen an die Cybersicherheit berücksichtigen und umsetzen. Es geht um „security by design“, also um Berücksichtigung der Sicherheit bereits bei der Entwicklung von Software. Und anders als die EU NIS-Richtlinie (Netz- und Informationssicherheits-RL 2016), die sich an Betreiber kritischer Infrastruktur (z.B. Energie, Verkehr, Bankwesen, digitale Infrastruktur), große Anbieter digitaler Dienste (also mit mehr als 50 Mitarbeitern und einem Jahresumsatz von mehr als EUR 10 Mio), und Einrichtungen des Bundes richtet, die einen Sicherheitsvorfall unverzüglich an die zuständige Behörde melden müssen, betrifft der EU-Cybersecurity Act alle Anbieter.

Unter Cybersicherheit sind alle Tätigkeiten zu verstehen, die notwendig sind, um Cyberbedrohungen abzuwehren und Nutzer solcher Systeme und sonstige betroffene Personen zu schützen. Damit verbunden soll es EU-weit einheitliche Cybersicherheits-Zertifizierungen geben. Dies soll das Vertrauen in die Sicherheit von Produkten und Dienstleistungen stärken, weil damit bescheinigt wird, dass die geprüften Produkte bestimmten Anforderungen an die Cybersicherheit gerecht werden. Es ist dies eine Art produktsicherheitsrechtliche Risikofolgenabschätzung, die Unternehmen freiwillig durchführen können. Ein System- bzw. IT-Anbieter könnte aufgrund mangelnder Sicherheitsvorkehrungen auch für dadurch verursachte Schäden verantwortlich gemacht werden. Es stellt sich die Frage, ob ein derartiger Systeme-Anbieter auch die vom Verschulden unabhängige Produkthaftung treffen kann und ob er als Hersteller nach der Produkthaftung gilt.

WELCHE ROLLE SPIELEN TECHNISCHE STANDARDS? UND WAS BEDEUTET DAS FÜR DIE PRODUKTRECHTLICHE RISIKOFOLGENABSCHÄTZUNG?

Die Einhaltung derartiger freiwilliger technischer Standards wie im EU-Cybersecurity Act vorgesehen, aber auch sonstiger technishcer Normen, wie EN, DIN, ISO, etc., sind im Prinzip nur ein Mindeststandard. Es genügt also im Haftungsfall nicht, sich zur Abwehr von Ansprüchen nur darauf zu stützen. Um ein Haftungsrisiko soweit wie möglich zu minimieren, ist neben der technischen eben auch die rechtliche Risikofolgenabschätzung erforderlich. Und diese soll jedenfalls schon bei der Entwicklung, also in der Konstruktions- bzw. Planungsphase von Produkten beginnen. Hier propagieren wir in Anlehnung an *privacy by design* nach der DSGVO ein „safety-by-design“, also sich nicht erst vor der Markteinführung mit produktsicherheitsrechtlichen Fragen auseinander zu setzen, sondern schon bei der Entwicklung des Designs/Konstruktion.

Viele Unternehmen denken, dass das Abarbeiten von Checklisten ausreicht. Also, nur zu sehen, ob Normen eingehalten wurden, ist zu wenig. Erst wenn man die Rechtsprechung der Gerichte nicht nur jener in Österreich, sondern zumindest auch anderer europäischer Länder,

kennt, ist es möglich, die nötige rechtliche Einschätzung bei der Risikobeurteilung abzugeben. Denn jeder, der sich in der Produkthaftung auskennt, weiß, dass die berechtigte Sicherheitserwartung sehr häufig über einer bestehenden Norm hinausgeht. Rechtlich sind konstruktive Maßnahmen zur Erhöhung der Sicherheit folglich immer zuerst zu setzen. Als Merksatz gilt: Warnhinweise können ein konstruktiv unsicheres Produkt nicht bzw. nicht mehr sicher machen!

SOFTWARE, IOT UND STAND DER WISSENSCHAFT DER TECHNIK

Bei Software und IoT ist die Entwicklung so schnell, dass eine technische Norm schon wieder überholt sein könnte, sobald ein Produkt auf den Markt kommt. Nehmen wir an, eine Software wurde vor Markteinführung auf Sicherheitsrisken getestet, es kommt dann aber doch zu sicherheitsrelevanten Problemen und Schäden. Im Anwendungsbereich der Produkthaftung könnte ein Hersteller bzw. Software-Entwickler, vorbringen, dass im Zeitpunkt als er die Software ausgeliefert hat, diese dem Stand der Wissenschaft und Technik entsprach und es nicht erkennbar war, dass es einen software-bug gab, es sich somit um eine Schadsoftware handelte. Mit dieser Argumentation könnte er sich von der Haftung befreien, zumindest nach den EU-Produkthaftungsregeln. Aber wer bestimmt den Stand der Wissenschaft und Technik einer Software, vorallem bei völlig neuen Software-Entwicklungen, bei denen es keinen allgemeinen Stand der Wissenschaft und Technik gibt? Das sind alles noch ungelöste Fragestellungen.

VERGESSEN SIE NICHT AUF IHRE VERTRÄGE!

Für jedes Industrieunternehmen ist es notwendig, in der Liefer- und Dienstleistungskette an die bestmögliche Vertragsgestaltung zu denken, und rechtliche Absicherungen in Verträge einzubauen. Viel zu oft wird gerade in Vertriebsverträgen auf die notwendigen Aspekte der Produkthaftung und Produktsicherheit völlig vergessen.

Es ist von zentraler Bedeutung, in Verträgen nicht nur das Produkt bzw. die Dienstleistung genau zu beschreiben, sondern auch die haftungsrechtlichen Folgen, die von unsicheren bzw. fehlerhaften Produkten/Dienstleistungen ausgehen könnten, mitzudenken. Auch Produkte, die lediglich im B2B (zwischen zwei Unternehmen) vertrieben werden, könnten ja auch von Menschen außerhalb des Vertrages, also unbeteiligten Dritten (innocent bystander), verwendet werden und deren Sicherheitserwartung ist bei der Entwicklung von Produkten auch zu berücksichtigen.

Anstatt die Vorzüge der eigenen Produkte in Verträgen weiter zu bewerben, geht es in Verträgen immer stärker um klare Grenzziehungen, also inwieweit sich welche Verhaltensweisen Dritter auf die Funktionsweise und Sicherheit des vertriebenen Produkts und auf die der Nutzer und jener Personen auswirkt, die mit dem Produkt in Berührung kommen könnten. Daher muss vertraglich klar geregelt werden, wozu ein Produkt eben nicht taugt.

Oft fehen in B2B Verträgen auch klare Regelungen, welcher der Vertragspartner bei auftretenden Sicherheitsrisken von Proudukten welche Aufgaben zu übernehmen hat. Auch hier ist es natürlich nicht besonders „sexy“, zuerst die Braut, also das Produkt, schön zu machen, um im selben Atemzug die Scheidungsfolgen mitzuberücksichtigen. Anders ausgedrückt: bereits im Vertrag den Krisenfall im Auge zu haben und zu regeln, wer die Behörden bei einem auftretenden Sicherheitsrisiko und Auftreten von Schäden informiert, und wer und unter welchen Voraussetzungen einen Produktrückruf vom Endkunden oder eine Rücknahme des Produkt vom Markt startet. Wer trägt die Kosten? Und sind die bei einer richtig gemachten Risikobeurteilung angenommenen Schadensfolgen versichert bzw. besteht für diese Versicherungsdeckung?

Häufig besteht bei einem Schadensfall durch ein Produkt/Maschine, das aus vielen unterschiedlichen Teilen, zwischen den verschiedenen Produzenten Uneinigkeit darüber, wer für den Schaden ursächlich ist, und es entbrennt Streit darüber, wer den Schaden letztlich verursacht hat, während sich in der Zwischenzeit weitere Schadensfälle ereignen. Ziel aller Unternehmer muss immer die Vermeidung weiterer Schäden sein, und das bedarf eines gut funktionierenden Krisenmanagements. Je genauer die Abläufe zwischen Vertragspartnern in schriftliche Vereinbarungen gegossen sind einerseits, diese Abläufe aber auch innerhalb der Organisationsstruktur eines Unternehmens geregelt sind andererseits, desto schneller kann im Ernstfall auf ein drohendes oder entstandenes Risiko reagiert und können Schäden minimiert werden. Nach dem Produktsicherheitsgesetz (PSG 2004) ist dabei immer das gelindeste zum Ziel führende Mittel anzuwenden.

Wenn Unternehmen nicht die erforderlichen Maßnahmen ergreifen, können die zuständigen österreichischen Behörden auch Bußgelder von bis zu EUR 25.000,00 verhängen. Das mutet im Vergleich zu den millionenschweren Strafen bei Nichteinhaltung der DSGVO fast lächerlich an, wenn man bedenkt, dass unsichere Produkte eine große Gefahr für die Gesundheit von Menschen darstellen können, deren Schutz stets im Blickfeld der Konstruktion und Produktion von Produkten stehen muss.

Zu Erzielung einer bestmöglichen Sicherheit von Produkten können Digitalisierung und KI einen wesentlichen Beitrag leisten. Sowie ein Medikament oder eine Impfung auch niemals 100%-ige Sicherheit bieten können, darf auch keiner von uns trotz des Einsatzes neuer Technologien absolute Sicherheit von Produkten erwarten, die mit diesen neuen Technologien entwickelt und produziert wurden.

Rechtsanwalt
Dr. Andreas Eustacchio
LL.M. (LSE London)
www.eustacchio.com