InTeR
Zeitschrift zum Innovations- und Technikrecht

AI Act kompakt

Compliance, Management und Use Cases für die Unternehmenspraxis

von

Peter Hense
Rechtsanwalt, Leipzig

und

Tea Mustać
Mag. iur., Leipzig

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Bibliografische Information Der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.de abrufbar.

ISBN 978-3-8005-1823-4

dfv Mediengruppe

Druck: Beltz Grafische Betriebe GmbH, 99947 Bad Langensalza

Printed in Germany

Vorwort

„The first question you should ask yourself when building an AI system is; can we do it without AI?“
(Common Sense im Machine Learning)

Unser Buch ist ein Frühwerk und doch eines, das die Essenz von fast drei Jahren intensiver Auseinandersetzung mit dem AI Act in sich trägt. Die Erkenntnisse und Einsichten, die auf den folgenden Seiten von AI Act kompakt gesammelt sind, speisen sich aus unserer langjährigen Begleitung von Machine-Learning-Projekten in Forschung und Entwicklung. Von Dynamic Pricing über biometrische Identifikation bis hin zu Social CRMs und Systemen zur Sprach- und Emotionserkennung – wir haben all diese Technologien bereits auf unseren Tischen seziert. Das ist die technische Seite. Seit 2022 jedoch fokussieren wir uns auf die spezifische Regulierung von Machine Learning, also das, was heute als „künstliche Intelligenz“ die Runde macht.

Die frühzeitige Organisation von Compliance entlang der AI Supply Chain für Unternehmen und Organisationen weltweit zwang uns dazu, uns schon lange vor der offiziellen Einführung des AI Acts mit Themen wie Model Disgorgement durch die FTC, Bias Audits in New York und dem ersten umfassenden AI-Gesetz, dem Colorado AI Act, zu beschäftigen. Ohne unsere enge Vernetzung mit Kolleg:innen aus verschiedensten Fachdisziplinen weltweit wären wir nicht in der Lage gewesen, die Entwicklungen zu durchdringen und entsprechend zu handeln, besonders nicht angesichts des Booms generativer AI Systems. Doch wir hatten das Glück, auf gute Freunde zählen zu können.

Teils aus Neugier, teils im Auftrag, aber stets mit Begeisterung haben wir seit 2017 bei der IEEE an der Standardisierung von Algorithmic Bias Consideration (P7003) mitgewirkt, bereits 2018 Algorithmic Impact Assessments durchgeführt, 2020 unmittelbar vor der Pandemie die ersten Fundamental Rights Impact Assessments verfasst und Ende 2022 die ersten Bias Audits von Automated Employment Decision Tools nach dem New Yorker Local Law 144 begleitet. 2023 überprüften wir das automatisierte Kreditscoring von Banken nach der Schufa auf Diskriminierungsfreiheit und zählen heute zu den Vorreitern bei der Implementierung von AI-Managementsystemen nach ISO 42001. Und dennoch fühlen wir uns angesichts der schieren Menge und Vielfalt des Themas „künstliche Intelligenz“ immer wieder wie Anfänger. Mehr als einmal mussten wir unsere Annahmen revidieren und unsere Bewertungen anpassen – das Technologiefolgenrecht hinkt der Technologie selbst eben oft hinterher.

In diesem Buch geht es nicht um juristische Haarspalterei – dafür war uns die Zeit zu schade. Vielmehr wollen wir Verständnis schaffen und praxisnahe

Lösungen präsentieren für all jene, die High-Risk AI Systeme designen, entwickeln, anbieten und einsetzen. Und das sind, entgegen manchen Wunschvorstellungen, recht viele Organisationen. Mit *AI Act kompakt* erhalten Sie einen kernigen, informativen und persönlich geprägten Einblick in das, was wir dem AI Act entnehmen. Eingeflossen sind tausende Stunden Arbeit und Austausch mit Kolleg:innen aus Data Science, Statistik, ML Engineering, Cybersicherheit, Soziologie, Standardisierung und Recht. Wir nehmen für uns nicht in Anspruch, in jedem Punkt alles zu wissen. Aber unsere Leser:innen können sich darauf verlassen, dass das, was wir schreiben, wohlüberlegt ist und oft in Diskussionen mit anderen Expert:innen gereift ist.

Der AI Act ist handwerklich kein gutes Gesetz. Er wimmelt von Eigentümlichkeiten, sprachlichen Verwirrungen, Wiederholungen, Lücken und Widersprüchen. Aber die großen Linien sind erkennbar, und wir haben uns alle Mühe gegeben, nicht aus jeder sprachlichen Mücke einen rechtlichen Elefanten zu machen, sondern der Praxis eine Handreichung zu bieten, mit der Provider und Deployer den richtigen Weg einschlagen können.

Und wir hatten Freude an der Arbeit – so wie auch an unserem Podcast „RegInt: Decoding AI Regulation“, in dem wir seit 2023 monatlich diejenigen informieren und unterhalten, die an Regulierung, Technologie und den Hintergründen von AI interessiert sind. Wir haben die verfügbare Literatur der letzten Jahre gesichtet und die aktuellen Forschungsergebnisse der Jahre 2020 bis 2024 dort einbezogen, wo sie uns zum Verständnis der gesetzgeberischen Begriffe und Intentionen relevant erschienen. Der AI Act fiel nicht vom Himmel; er basiert in wesentlichen Teilen auf genau diesen Forschungsergebnissen und gesellschaftlichen Entwicklungen – dem Lobbying von Unternehmen genauso wie dem Engagement zivilgesellschaftlicher NGOs.

Einen großen Mehrwert unseres Buches sehen wir in einem weiteren Schwerpunkt: den Standards, Berichten und Guidelines von ISO, IEC, IEEE sowie CEN/CENELEC. Wir geben sogar Einblicke in solche, die sich noch im nichtöffentlichen Entwurfsstadium befinden. Warum? Weil ohne das in diesen Standards verdichtete Fachwissen die Kernanforderungen des AI Acts nur schwer zu verstehen sind. Standardisierung hat den Vorteil, dass juristische, naturwissenschaftliche und geisteswissenschaftliche Stakeholder auf eine gemeinsame Terminologie und ein gemeinsames Verständnis zurückgreifen können. Glauben Sie uns: Das Wissen um und aus interdisziplinären Standards ist bei der praktischen Umsetzung von AI-Act-Compliance deutlich wichtiger als die Lektüre der neuesten juristischen Fachzeitschrift.

Und nun, viel Spaß beim Lesen!

Leipzig, im September 2024 *Tea und Peter*

Inhaltsverzeichnis

II. Design

1. Die Idee

„Never forget that only dead fish swim with the stream."
(*Malcolm Muggeridge*)

Um den Entwicklungs- und Bereitstellungsprozess eines AI Systems effektiv zu starten, sollten wir uns zunächst den anspruchsvollsten Fragen widmen:

– Warum ist dieses System notwendig?
– Welche Probleme soll das System lösen?
– Welche Ziele verfolge ich mit diesem System?
– Welche Teile eines Prozesses sollen automatisiert werden?
– Braucht die Welt noch einen Chatbot?

Manche Leserinnen und Leser dieses Buches mögen über diesen Einstieg schmunzeln, doch unsere praktische Erfahrung bestätigt, dass eine bedrückend hohe Zahl von Unternehmen AI Systems entwickeln, beschaffen oder bereitstellen, nur weil es alle anderen auch tun. Dies ist in jeder Hinsicht eine äußerst schlechte Strategie.

Um nicht nur ein nützliches und qualitativ hochwertiges AI System zu entwickeln und zu betreiben, sondern auch ein System, das den Anforderungen des AI Acts entspricht, sollten Sie zunächst die zuvor gestellten Fragen beantworten. Dadurch können Sie die Ziele Ihres AI Systems klar definieren. Diese Ziele helfen Ihnen dann dabei:

– den vorgesehenen Zweck des Systems zu bestimmen;
– die Risikokategorie zu antizipieren, in die das System fallen könnte;
– eine *Business Impact Analysis* durchzuführen, um festzustellen, ob Sie über die notwendigen Ressourcen zur Entwicklung eines konformen Systems verfügen (die Entwicklung konformer Hochrisikosysteme wird nicht gerade günstig);
– angemessene Designentscheidungen zu treffen.

Beispiel: Wir möchten ein AI System entwickeln, um die Effizienz einer bestimmten Verwaltungsdienstleistung zu steigern und Verwaltungsangestellten dadurch zu helfen, indem eingehende E-Mails automatisch nach Thema und Dringlichkeit kategorisiert werden.

1. Warum ist dieses System notwendig?

Es ist notwendig, weil derzeit die Bearbeitung von Anfragen über einen Monat dauert, selbst wenn die Anfragen dringend und mit wenig Aufwand zu beantworten sind. Durch eine bessere Organisation der E-Mails würde sichergestellt, dass sie schneller die zuständige Abteilung und die

verantwortliche Person erreichen. Dies würde die Reaktionszeiten erheblich verkürzen. Darüber hinaus würde die Bestimmung des Dringlichkeitsgrads gewährleisten, dass die dringendsten Angelegenheiten bevorzugt bearbeitet werden.

2. Welche Probleme soll mein System lösen?

Langsame und ineffiziente öffentliche Dienstleistungen, ungleicher Zugang zu grundlegenden öffentlichen Dienstleistungen, eine zunehmende Anzahl von Beschwerden aufgrund langsamer Reaktionszeiten sowie die steigende Anzahl von E-Mails zum selben Thema aufgrund verzögerter Antworten.

3. Was möchte ich mit diesem System erreichen?

Die langsamen und ineffizienten öffentlichen Dienstleistungen verbessern, den allgemeinen Zugang zu essenziellen öffentlichen Dienstleistungen erleichtern und die Anzahl der Beschwerden reduzieren.

4. Welche Teile welches Prozesses möchte ich automatisieren?

Den ersten Schritt, also die Kategorisierung und automatische Weiterleitung an die zuständige Abteilung und verantwortliche Person.

5. Braucht die Welt noch einen Chatbot?

Es handelt sich nicht um einen Chatbot, und die Welt braucht auch wirklich keinen neuen.

Sobald wir diese Fragen beantwortet haben, können wir schlussfolgern, dass ein AI System erforderlich ist, wenn auch ein eher einfaches. Obwohl das System im Kontext der öffentlichen Verwaltung eingesetzt wird, trifft es keine wichtigen Entscheidungen in Bezug auf Rechte oder den Zugang zu öffentlichen Dienstleistungen. Das bedeutet höchstwahrscheinlich, dass das System nicht als hochriskant eingestuft wird. Da das System voraussichtlich ein geringes Risiko darstellt, verfügen wir wahrscheinlich über die Ressourcen, um es zu entwickeln und bereitzustellen. Nun bleibt nur noch zu entscheiden, ob die Entwicklung ausgelagert oder intern durchgeführt wird, und die entsprechenden Designentscheidungen zu treffen, um angemessene Qualitäts- und Genauigkeitsniveaus zu erreichen. Die Aufgabe ist zwar nicht trivial, aber wir haben endlich einen vernünftigen Startpunkt gefunden.

2. Legal Requirements Engineering

Vor diesem Hintergrund entwickelt sich Legal Requirements Engineering zunehmend zu einer relevanten **Disziplin und Arbeitsmethode** für Juristinnen und Juristen, da Gesetzgebungsvorhaben der EU aufgrund ihrer in-

terdisziplinären und hybriden Natur – die Einflüsse aus Standards, externen Richtlinien und verschiedenen wissenschaftlichen Disziplinen vereinen – immer komplexer werden. Besonders im Kontext des AI Act zeigen sich die **unterschiedlichen Perspektiven** der Beteiligten aus verschiedenen Professionen, wie Technologie, Statistik, Organisationswissenschaften, Sozialwissenschaften und speziellen Rechtsgebieten auf die Gesetzgebung. Diese unterschiedlichen Sichtweisen erschweren die einheitliche Interpretation und Umsetzung von Vorschriften, was die Notwendigkeit eines strukturierten Ansatzes im Legal Requirements Engineering unterstreicht. Legal Requirements Engineering ist ein strukturiertes Verfahren zur Erfassung, Analyse, Dokumentation und Verwaltung rechtlicher Anforderungen, die in technischen Systemen oder Produkten umgesetzt werden müssen. Ziel ist es, sicherzustellen, dass alle relevanten Gesetze, Richtlinien, Motive, Hintergrundinformationen und Standards **in die Systementwicklung integriert** werden, um **nachhaltige Rechtskonformität** zu gewährleisten. Der Prozess beginnt für die Betroffenen, in-house oder externe Berater und Beraterinnen, mit der **Identifikation** und Erfassung aller relevanten Facetten einer Norm, die für das spezifische Projekt relevant sind, darunter Case Law und Behördenentscheidungen. Danach folgt die Analyse, in der die rechtlichen Anforderungen hinsichtlich ihrer Auswirkungen auf das Systemdesign, die Architektur und die Funktionalität bewertet werden. Anschließend werden die rechtlichen Anforderungen **systematisch dokumentiert**, um als Grundlage für die technische Entwicklung zu dienen. Diese Dokumentation muss klar und präzise sein, um für alle Beteiligten aller Disziplinen verständlich zu bleiben. Eine einfache, klare Sprache ist unerlässlich. Die **Integration** dieser Anforderungen in das technische Systemdesign und die Entwicklungsprozesse erfolgt daraufhin, wobei Compliance-Mechanismen eingebaut werden, um die Einhaltung der Anforderungen zu überwachen. Es folgt die **Überprüfung und Validierung**, die regelmäßig durchgeführt wird, um sicherzustellen, dass das System weiterhin konform ist und auf Änderungen in den rechtlichen Rahmenbedingungen reagiert. Schließlich umfasst Legal Requirements Engineering auch das **Management der Anforderungen über den gesamten Lifecycle des AI Systems** hinweg, insbesondere im Hinblick auf sich ändernde Gesetze, Standards und Verwaltungspraxis.

3. Zweckbestimmung

Everything is foreseeable ex post.

Vor der Entwicklung eines AI Systems steht die Frage, welche Probleme das System lösen kann und welchem Zweck es dienen soll. Es ist angesichts der überwältigenden technischen Gestaltungsoptionen unmöglich, ein Sys-

tem zu entwickeln, ohne den konkreten Anwendungsfall vor Augen zu haben. Wer noch auf der Suche nach Use Cases für AI ist, dem bietet sich die Lektüre des jüngsten **Technical Reports ISO/IEC TR 24030:2024 (Information technology – Artificial intelligence (AI) – Use cases)** an, der auf nahezu 170 Seiten detailliert Anwendungsfälle erläutert, die von Healthcare und Agriculture über FinTech und Windenergieanlagen bis hin zu Digital Marketing reichen.

Beispiele für Use Cases aus dem TR 24030:2024:

- Im Bereich der **Landwirtschaft** ist ein Use Case die Echtzeit-Segmentierung und **Vorhersage von Pflanzenwachstumsdynamiken** (Use Case 126). Hier wird eine AI-basierte Lösung entwickelt, die auf eingebetteten Systemen mit geringem Energieverbrauch basiert und neuronale Netzwerke (Convolutional Neural Networks – CNNs und Long-Short-Term Memory – LSTM) verwendet, um Wachstumsmuster von Pflanzen in Echtzeit zu analysieren und vorherzusagen. Die verwendeten Algorithmen ermöglichen eine präzise Überwachung von Umweltbedingungen und die Optimierung von Ressourceneinsatz durch Sensorfusion und Bildanalyse.
- Im Bereich des **E-Commerce** kommt AI verstärkt bei der Erkennung von **Nutzerabsichten** durch Deep Learning (Use Case 43) zum Einsatz. Hier wird ein System beschrieben, das auf Basis von Deep-Learning-Techniken wie Recurrent Neural Networks (RNNs) die Intention von Nutzern in Echtzeit erkennt und darauf basierend angepasste Interaktionen anbietet. Dieses System analysiert sowohl Text- als auch Sprachdaten, um Nutzeranfragen zu interpretieren und eine personalisierte Antwort zu generieren.
- In der **Bildungsbranche** werden AI Systems verwendet, um **Lernplattformen** zu personalisieren und Lernprozesse effizienter zu gestalten. Ein Beispiel hierfür ist das adaptive Lernsystem für personalisiertes Lernen (Use Case 102), das auf Machine Learning basiert und für jeden Lernenden maßgeschneiderte Lehrpläne erstellt. Hierbei analysiert das System kontinuierlich die Fortschritte der Lernenden und passt das Lehrmaterial entsprechend an, um den Lernerfolg zu maximieren. Das System verwendet prädiktive Algorithmen, um den Lernfortschritt vorauszusagen und potenzielle Lernschwächen frühzeitig zu erkennen.
- Im **Energiesektor** werden KI-Anwendungen in **Smart Energy Grids** (Use Case 166) eingesetzt, um Energieflüsse in Echtzeit zu überwachen und zu steuern. Diese KI-Systeme nutzen prädiktive Modelle, um den Energiebedarf basierend auf historischen und Echtzeitdaten vorherzusagen, und passen die Energieverteilung entsprechend an. Hierbei kommen Algorithmen des maschinellen Lernens zum Einsatz, die sowohl wetterbedingte als auch nutzerseitige Einflüsse auf den Energieverbrauch berücksichtigen, um eine optimierte und nachhaltige Energieversorgung zu gewährleisten.

– Im **Gesundheitswesen** werden KI-Systeme zur Unterstützung von Diagnosen und zur Optimierung klinischer Prozesse eingesetzt. Der Anwendungsfall zur Analyse von CT-Scans der Brust zur **Früherkennung von Lungenkrebs** (Use Case 105) beschreibt ein System, das auf Computer Vision und maschinellem Lernen basiert und medizinische Bilder in Echtzeit analysiert. Hierbei kommen Convolutional Neural Networks (CNNs) zum Einsatz, die auf große Datensätze trainiert wurden, um subtile Anomalien zu erkennen, die auf frühe Stadien von Lungenkrebs hinweisen.
– In der **Fintech-Branche** spielen KI-Systeme eine Schlüsselrolle bei der **Erkennung von Betrug aufgrund von Kollusion** (Use Case 20). Diese Systeme verwenden fortschrittliche Mustererkennungsalgorithmen, um betrügerische Aktivitäten in Finanztransaktionen zu identifizieren. Machine-Learning-Modelle analysieren dabei große Mengen von Transaktionsdaten in Echtzeit und lernen, ungewöhnliche Verhaltensmuster zu erkennen, die auf potenziellen Betrug hinweisen.

Wesentliche Entwicklungsfragen wie die Wahl des Modells und der Methoden, die in den obigen Use Cases angerissen sind, sowie die Art der benötigten Trainingsdatensätze lassen sich nur dann beantworten, wenn das Einsatzgebiet des Systems klar definiert ist. Auch hier können technische Standards die Kommunikation erleichtern, da sie organisationsübergreifend Konzepte und Sprache im Umgang mit AI Systems festlegen, wie die **ISO/IEC 22989:2022 (Information technology – Artificial intelligence – Artificial intelligence concepts and terminology)**. Insofern sind die gesetzlichen Anforderungen und die Natur des Entwicklungsprozesses eng miteinander verbunden. Allerdings verlangt der Gesetzgeber von Providern auch, **vorhersehbare Fehlanwendungen** mit einzuplanen, die vernünftigerweise zu erwarten sind. Von einem umsichtigen Systemdesign profitiert auch die Robustheit des AI Systems.

Art. 3.13 definiert eine vernünftigerweise **vorhersehbare Fehlanwendung** als:

> „*die Verwendung eines KI-Systems in einer Weise, die nicht seiner Zweckbestimmung entspricht, die sich aber aus einem vernünftigerweise vorhersehbaren menschlichen Verhalten oder einer vernünftigerweise vorhersehbaren Interaktion mit anderen Systemen, auch anderen KI-Systemen, ergeben kann*".

Was mit Blick auf ein konkretes System als vernünftigerweise vorhersehbare Fehlanwendung einzuordnen ist, lässt sich nur mit Blick auf den Zweck festlegen, für den das System bestimmt ist.

Den Begriff „**Zweckbestimmung**" definiert Art. 3.12 AI Act als:

> „*die Verwendung, für die ein KI-System laut Anbieter bestimmt ist, einschließlich der besonderen Umstände und Bedingungen für die*

> *Verwendung, entsprechend den vom Anbieter bereitgestellten Informationen in den Betriebsanleitungen, im Werbe- oder Verkaufsmaterial und in diesbezüglichen Erklärungen sowie in der technischen Dokumentation.*“

Komplizierter ist es, zweckwidrige Nutzungen zu betrachten, die **durch menschliches Verhalten entstehen** können. Statt einseitig auf die Festlegung einwirken zu können, muss der Provider anhand objektiver Kriterien prognostizieren, was „vernünftigerweise vorhersehbar“ ist. Dieser sehr theoretische Betrachtungswinkel stellt die Praxis vor eine große Herausforderung. Hilfe bieten praktische Standards, wie der Technical Report ISO/TR 24971:2020 für die Anwendung der ISO 14971:2019 (Medical devices – Application of risk management to medical devices). Sie identifizieren drei Kategorien des Fehlgebrauchs, die vernünftigerweise vorhersehbar sind. Diese lassen sich auf alle AI Systems übertragen:

1. Bedienungsfehler, Ausrutscher, Irrtümer (slip, lapse, mistake),
2. vorsätzlicher Missbrauch (intentional acts of misuse) und
3. die vorsätzliche Verwendung von Geräten für andere als die vom Hersteller vorgesehenen Anwendungsfelder oder für Anwendungsfelder, für die keine Zulassung besteht.

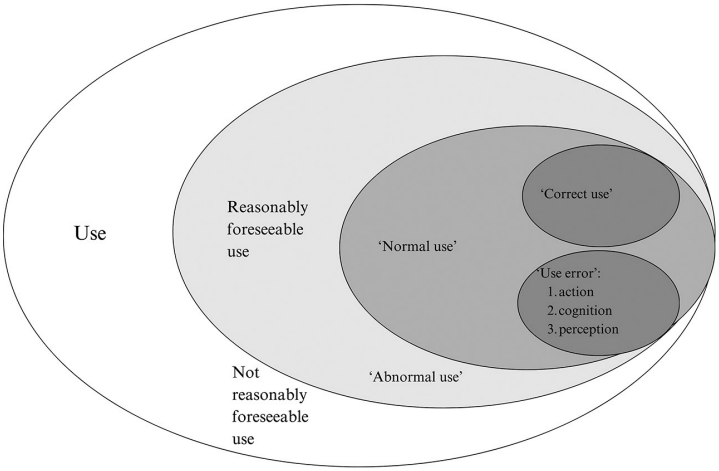

Abbildung 3: Venn-Diagramm der verschiedenen Arten der Verwendung von Produkten/AI Systems

Im Bereich der Medizinprodukte können weitere Anleihen von der **IEC 62366-1:2020 (Medical devices – Part 1: Application of usability engineering to medical devices = DIN EN 62366)** genommen werden, in wel-

cher der Begriff „Benutzungsfehler“ eingeführt wurde, der die „vernünftigerweise vorhersehbare Fehlanwendung“ mit einschließt.

Eine weitere Hilfestellung bietet der Leitfaden für die Anwendung der **Maschinenrichtlinie 2006/42/EG**. Dort finden sich mehrere Beispiele dafür, was im Zusammenhang mit Maschinen als „vernünftigerweise vorhersehbare Fehlanwendung“ betrachtet werden könnte. Zumindest einige dieser Beispiele lassen sich auch auf AI Systems anwenden. Zu den Beispielen gehören:

– der Verlust der Kontrolle über die Maschine durch den Bediener;
– reflexartiges Verhalten einer Person im Falle einer Fehlfunktion, eines Zwischenfalls oder eines Ausfalls, während sie die Maschine benutzt;
– Verhaltensweisen, die auf mangelnde Konzentration oder Unachtsamkeit zurückzuführen sind;
– Verhaltensweisen, die darauf zurückzuführen sind, dass Personen den Weg des geringsten Widerstands einschlagen, während sie eine Aufgabe erledigen;
– Verhaltensweisen, die sich aus dem Zwang ergeben, die Maschine unter allen Umständen in Betrieb zu halten;
– das Verhalten bestimmter Gruppen von Personen, z. B. von Kindern.

Die Kombination der beiden genannten Punkte vermittelt einen Eindruck davon, welche Überlegungen der Gesetzgeber in Bezug auf AI Systems angestellt hat. Auf der Grundlage des besten Wissens über das Produkt und das menschliche Verhalten sind **alle vernünftigerweise vorhersehbaren Verwendungen** zu berücksichtigen, die sich aus Anwendungsfehlern, rücksichtslosem Gebrauch und vorsätzlichem Missbrauch ergeben können, wobei alle diese Gebrauchsarten eine gewisse Überschneidung aufweisen können. Allerdings konzentrieren sich die genannten Standards und Reports vorwiegend auf die Reduktion von Risiken, die mit Anwendungsfehlern verbunden sind. Die anderen Kategorien berücksichtigen sie nur unzureichend. Die hierzu im nationalen und europäischen Produkthaftungsrecht ergangene Rechtsprechung füllt jedoch ganze Kommentare, sodass ein Blick in die Spezialliteratur an dieser Stelle dringend empfohlen wird.

Um zu bestimmen, was in einem bestimmten Fall „vernünftigerweise vorhersehbar“ ist, müssen die Provider einen zweistufigen Prozess aus **1. Usability Engineering** und **2. Human Factors Engineering** durchlaufen. Beide Schritte sind notwendig, um detaillierte Hinweise zu erteilen, wie das System von wem und wofür verwendet werden soll. Außerdem geben sie Auskunft über das Verhalten, die Fähigkeiten, die Einschränkungen und andere Merkmale von Menschen, die das System nutzen und mit ihm interagieren. Damit schaffen sie die Grund-voraussetzung, um geeignete Maßnahmen zur Risikominderung zu entwickeln.

a) Usability Engineering

Die beabsichtigte Nutzung und der beabsichtigte Zweck können zusammenfallen.[20] Bei ihrer Gestaltung sind alle vorherigen Eingabedaten zu berücksichtigen. Hierzu können gehören:

– ursprüngliche Projektentwurfspläne,
– Benutzeranforderungen,
– Daten aus früheren Projekten und Versionen,
– Daten über ähnliche Systeme,
– Standards und gesetzliche Anforderungen usw.[21]

Eine detaillierte Überprüfung der verfügbaren Daten ermöglicht es, den beabsichtigten Zweck des Systems in Form einer übergeordneten Erklärung zu definieren, die mindestens Folgendes enthält:

– vorgesehene Benutzer,
– voraussichtliches Niveau der Anwenderkenntnisse,
– Einsatzumgebung,
– Funktionalitäten des Systems,
– voraussichtliche Auswirkungen auf die Umwelt,
– Funktionsprinzipien.

Hilfreich kann auch die Angabe **konkreter Nutzungsszenarien** sein, für die das System vorgesehen ist. Auf der Grundlage dieser Szenarien können wir später konkretere potenzielle Risiken identifizieren, die mit der normalen und korrekten Nutzung des Systems verbunden sind, z. B. Risiken, die durch einen Systemausfall oder eine Fehlfunktion entstehen.

20 ISO 14971:2019 Medical devices – Application of risk management to medical devices.
21 MD101 Consulting, IEC 62366-1:2020 and Usability engineering for software, https://blog.cm-dm.com/post/2018/07/06/IEC-62366-1-and-Usability-engineering-for-software (letzter Aufruf: August 2024).

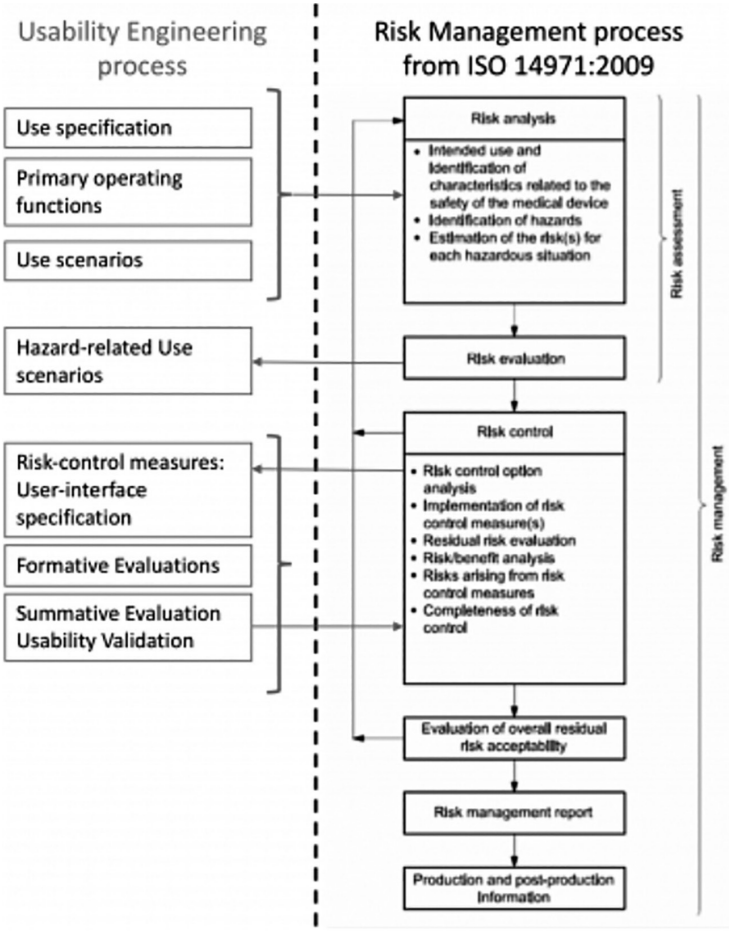

Abbildung 4: MD101 Consulting, IEC 62366-1 and Usability engineering for software, https://blog.cm-dm.com/post/2018/07/06/IEC-62366-1-and-Usability-engineering-for-software (letzter Aufruf: August 2024)

b) Human Factors Engineering

Wesentlich komplexer ist es, die vorhersehbaren Risiken im Zusammenhang mit dem Umgang von Menschen mit AI Systems zu bewerten. Dieser Schritt ist für eine umfassende Risikoanalyse und eine angemessene Risikominderung jedoch erforderlich. Beides zusammen ist wiederum für eine rechtskonforme Produktgestaltung notwendig.