**Juni 2026**
14. Jahrg.
84364
**Seite 65–132**

# InTeR

## Zeitschrift zum Innovations- und Technikrecht

**2**

*Prof. Dr. Stefan Müller*
65 **Gewandelte Erscheinungsformen – zur Modernisierung des Designrechts**

*Tom Hubert und Prof. Dr. Anne Paschke*
66 **Mobile (Land-)Maschinen und Roboter zwischen Automatisierung und Autonomie**

*Prof. Dr. Thomas Hoeren und Stefan Pinelli*
73 **Künstliche Intelligenz, Robotik und Quantencomputing**

*Prof. Dr. Christoph Schmidt*
80 **Das Besteuerungsverfahren als datengetriebenes Entscheidungssystem: Automationsgrade, Rechtsgrundlagen und Grenzen**

*Dr. Frank Sarre*
88 **Algorithmus trifft Recht: Informatik und EU Data Act im Wechselspiel?**

*Ilan Leonard Selz und Yakin Surjadi*
96 **Vom Datenschutzrecht zum Datenwirtschaftsrecht: Paradigmenwechsel durch den Data Act bei Nutzerzugriffen auf Smart-Device-Daten**

*Marie Carnap und Paul Jäde*
101 **Der Entwurf des Reallaboregesetzes: Chance für nachhaltigkeitsbezogene Innovation im Produktbereich?**

*Prof. Dr. Dagmar Gesmann-Nuissl*
107 **Rechtsprechungsreport „Innovations- und Technikrecht"**
- Anm. zu EuGH, Urt. v. 19.3.2026 – C-526/24, S. 107–112
- Anm. zu BGH, Urt. v. 11.3.2026 – I ZR 28/25, S. 112–116
- Anm. zu AG München, Urt. v. 13.2.2026 – 142 C 9786/25, S. 116–119
- Anm. zu OLG Düsseldorf (20. Zivilsenat), Urt. v. 2.4.2026 – I-20 W 2/26, S. 119–121
- Anm. zu EuGH (Zweite Kammer), Urt. v. 26.3.2026 – C-338/24, S. 121–126
- Anm. zu BGH (XI. Zivilsenat), Urt. v. 3.3.2026 – XI ZR 20/24, S. 126–130

130 **InTeRessantes**



dfv Mediengruppe · Frankfurt am Main

Prof. Dr. Thomas Hoeren und Stefan Pinelli, Münster/Wolfsburg*

# Künstliche Intelligenz, Robotik und Quantencomputing

## Ein Rechtsrahmen für eine integrierte Technologieentwicklung

*Die rechtliche Einordnung von Künstlicher Intelligenz, Robotik und Quantencomputing erfordert einen grundlegenden Perspektivwechsel.[1] Die technologische Entwicklung ist nicht nur primär unter dem Gesichtspunkt potenzieller Haftungs- und Sicherheitsrisiken zu betrachten, sondern im Kontext eines bestehenden und sich fortentwickelnden Rechtsrahmens, der die Voraussetzung für eine sichere und vertrauenswürdige Nutzung dieser Technologien bildet. Der Fokus verschiebt sich damit von einer ausschließlich risikozentrierten Betrachtung hin zu einem Verständnis des Rechts als integralem Ordnungs- und Ermöglichungsrahmen technologischer Transformation.[2]*

### I. Einstieg: Drei Technologiestränge – ein Transformationscluster

Die Konvergenz von Künstlicher Intelligenz, Quantencomputing und Robotik markiert einen grundlegenden technologischen Entwicklungsschritt. Diese Technologien sind aus unserer Sicht nicht isoliert zu betrachten, sondern bilden gemeinsam ein integriertes Transformationscluster, das die strukturellen Grundlagen zentraler wirtschaftlicher und gesellschaftlicher Bereiche nachhaltig verändert. Insbesondere industrielle Produktionsprozesse, medizinische Versorgungssysteme, logistische Infrastrukturen sowie Formen menschlicher Mobilität werden durch das Zusammenwirken algorithmischer Entscheidungsprozesse, physischer Handlungssysteme und neuartiger Rechenkapazitäten neu strukturiert.

#### 1. KI als gegenwärtiger Automatisierungs- und Entscheidungshebel

Künstliche Intelligenz ist gegenwärtig der zentrale technologische Treiber für die Automatisierung komplexer Entscheidungsprozesse. Machine-Learning-basierte Systeme übernehmen zunehmend Funktionen, die bislang menschlicher Bewertung vorbehalten waren, etwa in der industriellen Qualitätssicherung, der vorausschauenden Wartung oder der autonomen Navigation. Regulatorisch bedeutsam ist dabei insbesondere, dass solche Systeme nicht auf deterministischen Programmstrukturen beruhen, sondern ihr Verhalten auf der Grundlage datenbasierter Trainingsprozesse entwickeln. Dies führt zu spezifischen Anforderungen an Nachvollziehbarkeit, Risikobewertung und rechtlicher Verantwortungszuweisung innerhalb bestehender regulatorischer Rahmenbedingungen.

#### 2. Quantencomputing als Beschleuniger künftiger Rechen- und Optimierungsprozesse

Quantencomputing eröffnet das Potenzial einer erheblichen Beschleunigung bestimmter Rechenoperationen[3], insbesondere bei komplexen Optimierungsproblemen, der Simulation molekularer Prozesse sowie beim Training leistungsfähiger KI-Modelle. Diese gesteigerte Rechenleistung wird nicht sämtliche Anwendungsbereiche gleichermaßen erfassen, entfaltet jedoch dort, wo sie eingesetzt wird, eine grundlegende Verschiebung der technischen Möglichkeiten. Zugleich stellt Quantencomputing die bisherigen Grundlagen kryptographischer Sicherheit in Frage.[4] Insbesondere Quantenalgorithmen wie der Shor-Algorithmus ermöglichen prinzipiell die effiziente Faktorisierung großer Zahlen und fordern damit etablierte Verschlüsselungsverfahren wie RSA heraus.[5] Hieraus ergibt sich die Notwendigkeit einer Migration hin zu quantensicheren kryptographischen Verfahren der Post-Quantum-Cryptography, die künftig eine zentrale Voraussetzung für die langfristige Sicherheit digitaler und physischer Systeme darstellen werden.[6]

#### 3. Robotik als physische Ausführungsinstanz

Robotik fungiert als physische Ausführungsinstanz algorithmischer Entscheidungsprozesse und bildet damit die Schnittstelle zwischen digitaler Informationsverarbeitung und realweltlicher Handlung.[7] Während klassische Robotersysteme primär auf deterministisch vorgegebene Bewegungsabläufe beschränkt waren, ermöglichen moderne KI-gestützte Systeme eine adaptive und kontextabhängige Interaktion mit ihrer Umgebung.[8] Die physische Umsetzung algorithmischer Entscheidungen verleiht diesen Systemen eine unmittelbare Wirkungsdimension, da Fehlentscheidungen nicht lediglich zu fehlerhaften Datenoutputs führen, sondern potenziell physische Schäden oder Gefährdungen verursachen können. Perspektivisch wird die Integration quantengestützter Optimierungsverfahren die Fähigkeit robotischer Systeme weiter erhöhen, komplexe Entscheidungs- und Koordinationsprozesse in Echtzeit zu bewältigen.

#### 4. Physical AI als Schnittstelle

Der Begriff Physical AI bezeichnet KI-Systeme, deren Funktion nicht auf die Verarbeitung und Auswertung von Daten beschränkt ist, sondern die unmittelbar physische Prozesse steuern und reale Handlungen auslösen. Hierzu

---

* Mehr über die Autoren erfahren Sie auf S. III.

1 Vgl. ErwG 1 und 4 der Verordnung (EU) 2024/1689 (KI-Verordnung – AI Act); *Europäische Kommission,* White Paper on Artificial Intelligence, 2020, S. 2 ff.; *Floridi et al.,* AI4People – An Ethical Framework for a Good AI Society, Minds & Machines 2018, 689 (insb. 692 ff.). Die Fußnoten beschränken sich auf das zur Belegfunktion Erforderliche.

2 Siehe dazu auch *Hoeren/Pinelli,* KIR 2026, 5-9.

3 Vgl. *Europäische Kommission,* Quantum Technologies Flagship, 2018; National Institute of Standards and Technology (NIST), Post-Quantum Cryptography Standardization, 2024.

4 Siehe dazu auch *Hoeren/Pinelli,* CR 412025, 834-840.

5 Vgl. *Shor,* SIAM J. Comput. 26 1997, 1484 ff.

6 Dazu ebenfalls Hoeren/Pinelli, Quantum Computing and Law – Challenges for Data Protection, Evidence Law and Product Liability 2025, abrufbar unter SSRN: https://ssrn.com/abstract=5978700 oder http://dx.doi.org/10.2139/ssrn.5978700 (zuletzt abgerufen am 15.4.2026).

7 Vgl. *Calo,* California Law Review 2015, 513, 514 f.

8 *Lenz,* in: Lenz, Produkthaftung, 2. Auflage 202, § 9 Rn. 104, 105; *Schwarz-Schilling/Lundborg/Wernick* in: Sassenberg/Faber Industrie 4.0 und Internet-HdB, 3. Auflage 2025, § 1 Industrie 4.0 und Industrial Internet of Things Rn. 112-124.

zählen insbesondere adaptive Industrieroboter, chirurgische Assistenzsysteme, autonome Transportsysteme sowie robotische Assistenzsysteme in sensiblen Anwendungsbereichen wie Medizin und Pflege. Der entscheidende Unterschied zu rein digital operierenden KI-Systemen liegt in der unmittelbaren physischen Wirkungsdimension ihrer Entscheidungen. Während Fehlklassifikationen bei rein informationellen Systemen primär zu fehlerhaften Outputs führen, können Fehlentscheidungen im Kontext von Physical AI unmittelbare Auswirkungen auf die körperliche Unversehrtheit von Personen, die Integrität von Sachwerten oder die Funktionsfähigkeit technischer Systeme haben. Physical AI verlagert damit algorithmische Entscheidungsprozesse aus dem digitalen Raum in einen physisch wirksamen Handlungskontext und begründet hierdurch spezifische Anforderungen an Sicherheit, Nachvollziehbarkeit und regulatorische Governance.

## II. Begriff und Systematik: Was ist Physical AI – und warum ist das rechtlich neu?

Physical AI begründet keine eigenständige Rechtskategorie, sondern beschreibt eine technische Systemklasse, bei der sich bestehende regulatorische Anforderungen systemisch verdichten. Charakteristisch ist die funktionale Kopplung von Anforderungen der funktionalen Sicherheit, der IT-Sicherheit, der Daten-Governance sowie der KI-spezifischen Compliance. Diese Dimensionen bestimmen die Sicherheit und rechtliche Zulässigkeit des Gesamtsystems. Physical AI stellt damit keine neue regulatorische Kategorie dar, sondern eine Fallgruppe, in der bestehende Normstrukturen in ihrer integrierten Anwendung besonders verdichtet zur Wirkung gelangen. Der Begriff ist kein bloßes Marketinglabel, sondern eine analytische Regulierungsfallgruppe für Konstellationen, in denen sich regulatorische Anforderungen systemisch überlagern und nur in ihrer integrierten Anwendung vollständig erfasst werden können.

### 1. Abgrenzung zu rein digitaler KI

Klassische KI-Anwendungen wie Sprachmodelle, Empfehlungssysteme oder Systeme zur Betrugserkennung operieren primär innerhalb eines informationellen Referenzrahmens. Ihre Outputs beschränken sich auf die Generierung von Texten, Wahrscheinlichkeitswerten oder Entscheidungsvorschlägen und entfalten ihre Wirkung zunächst ausschließlich im digitalen Raum. Physical AI hingegen steuert Aktoren, die algorithmische Entscheidungen unmittelbar in physische Handlung übersetzen. Hierzu zählen insbesondere robotische Greifsysteme, autonome Transportsysteme oder medizinische Robotik, die aktiv auf ihre Umgebung einwirken und physische Kräfte ausüben.

Diese Verkörperung algorithmischer Entscheidungsprozesse begründet eine qualitativ neue Risikodimension. Fehlfunktionen verbleiben nicht auf der Ebene fehlerhafter Information, sondern können unmittelbar physische Schäden, Gefährdungen von Personen oder Beeinträchtigungen technischer Systeme verursachen. Physical AI erweitert damit den Wirkungsbereich algorithmischer Systeme vom digitalen in den physisch wirksamen Handlungskontext und erfordert eine entsprechend integrierte regulatorische Betrachtung.

### 2. Typische Use Cases

Physical AI findet bereits heute in einer Vielzahl praktischer Anwendungsfelder Einsatz.[9] In industriellen Produktionsumgebungen ermöglichen adaptive Robotersysteme eine unmittelbare Interaktion mit menschlichen Arbeitskräften und übernehmen eigenständig Steuerungs- und Entscheidungsfunktionen innerhalb komplexer Fertigungsprozesse. In der Logistik kommen autonome Transportsysteme und robotische Lagersysteme zum Einsatz, die Materialflüsse selbstständig koordinieren und optimieren.

Auch im medizinischen Kontext gewinnt Physical AI zunehmend an Bedeutung, etwa durch robotische Assistenzsysteme, die KI-basierte Bildanalyse mit präziser physischer Steuerung verbinden. Im Bereich der Mobilität manifestiert sich Physical AI insbesondere in autonomen Transport- und Drohnensystemen, die eigenständige Navigationsentscheidungen treffen und physisch umsetzen. Gemeinsam ist diesen Anwendungen, dass algorithmische Entscheidungsprozesse nicht auf digitale Outputs beschränkt bleiben, sondern unmittelbar physische Wirkung entfalten.

### 3. Der qualitative Unterschied: Governance in Echtzeit

Physical AI vereint regulatorische Anforderungen aus mehreren bislang getrennt betrachteten Bereichen. Hierzu gehören insbesondere Anforderungen der funktionalen Sicherheit (Safety), der IT- und Systemintegrität (Security) sowie der rechtmäßigen und kontrollierten Verarbeitung von Daten (Data Governance).

Der entscheidende Unterschied liegt darin, dass diese Dimensionen bei Physical AI funktional miteinander verflochten sind. Die Sicherheit eines Systems hängt nicht allein von seiner mechanischen Konstruktion ab, sondern ebenso von der Integrität seiner Software, der Qualität der zugrunde liegenden Daten und der Widerstandsfähigkeit gegenüber externen Manipulationen. Physical AI erfordert daher eine integrierte regulatorische Perspektive, die technische Sicherheit, algorithmische Steuerung und Compliance als funktional verknüpfte Elemente eines Gesamtsystems begreift.

## III. Der bestehende Rechtsrahmen als Ermöglichungsarchitektur

Entgegen der häufig geäußerten Annahme eines regulatorischen Vakuums existiert bereits heute ein differenziertes und funktionsfähiges Regelungsgefüge für Physical AI.

Der rechtliche Ordnungsrahmen ergibt sich aus einem funktional abgestuften Zusammenspiel mehrerer komplementärer Regime, insbesondere aus dem AI Act, dem Produktsicherheits- und Maschinenrecht, der Cybersecurity-Regulierung sowie dem Datenschutzrecht.[10]

9 https://appinventiv.com/blog/benefits-and-use-cases-of-physical-ai/ (zuletzt abgerufen am 15.4.2026).

10 Vgl. Verordnung (EU) 2024/1689 (AI Act); Verordnung (EU) 2023/1230 (Maschinenverordnung); Richtlinie (EU) 2022/2555 (NIS2-Richtlinie); Verordnung (EU) 2016/679 (DSGVO). Das ganze regulatorische Geflecht ist aber wegen der diversen Digital-Omnibus-Verfahren im Wandel; siehe *Gebehenne/Siebler/Hennemann,* EuDIR 2026, im Erscheinen.

### 1. AI Act als horizontale Compliance-Schicht

#### *a) Risikobasierter Ansatz als Strukturprinzip*

Die KI-Verordnung (EU) 2024/1689 („AI Act") etabliert einen risikobasierten Ordnungsrahmen für den Einsatz künstlicher Intelligenz. Ausgangspunkt ist die Differenzierung nach dem Gefährdungspotenzial eines KI-Systems. Die Verordnung unterscheidet zwischen verbotenen Anwendungen, Hochrisiko-Systemen, Systemen mit begrenztem Risiko sowie Anwendungen mit minimalem Risiko. Diese abgestufte Struktur ermöglicht durchaus eine risikoadäquate Ausgestaltung der regulatorischen Anforderungen und schafft eine Grundlage für den rechtssicheren Einsatz von KI-Systemen.[11]

#### *b) Physical AI als Hochrisiko-Konstellation*

Physical-AI-Systeme sind regelmäßig als Hochrisiko-KI im Sinne des AI Act einzuordnen, da sie entweder als Sicherheitskomponente im Kontext produktsicherheitsrechtlicher Vorgaben fungieren oder unter die in Anhang III der Verordnung definierten Hochrisikobereiche fallen, insbesondere in den Sektoren kritischer Infrastruktur, Beschäftigung und Gesundheit. Typische Beispiele sind kollaborative Industrieroboter oder medizinrobotische Systeme. Für diese Systeme gelten umfassende regulatorische Anforderungen, insbesondere im Hinblick auf Risikomanagement, technische Dokumentation, Nachvollziehbarkeit sowie organisatorische und technische Governance-Strukturen.[12]

#### *c) Pflichtenpaket als Legal Design*

Für Hochrisiko-KI etabliert der AI Act ein umfassendes Governance-Paket, das den gesamten Lebenszyklus eines Systems strukturiert erfasst. Hierzu gehören insbesondere ein kontinuierliches Risikomanagementsystem zur Identifikation, Bewertung und Minderung potenzieller Risiken, Anforderungen an die Data Governance einschließlich der Qualität und Geeignetheit von Trainings-, Validierungs- und Testdatensätzen, umfassende technische Dokumentationspflichten sowie Logging- und Nachvollziehbarkeitsanforderungen. Ergänzend verlangt der Rechtsrahmen Mechanismen des Human Oversight, um eine angemessene menschliche Kontrolle über automatisierte Entscheidungsprozesse sicherzustellen. Diese regulatorischen Anforderungen sind integraler Bestandteil eines rechtlich strukturierten Systemdesigns. Sie übersetzen technische Zuverlässigkeit, Transparenz und Kontrollierbarkeit in verbindliche rechtliche Mindeststandards und schaffen damit die Grundlage für vertrauenswürdige und rechtskonforme KI-Systeme.[13]

#### *c) Mehrwert: Standardisierung, Vertrauensbildung, Marktzugang*

Der AI Act entfaltet seine Wirkung insbesondere als Instrument regulatorischer Standardisierung. Die Entwicklung harmonisierter technischer Standards schafft einen normativen Referenzrahmen, an dem sich die Konformitätsbewertung von KI-Systemen orientiert. Die Einhaltung solcher Standards begründet eine Vermutungswirkung der Rechtskonformität und reduziert damit regulatorische Unsicherheit für Anbieter und Betreiber. Zugleich fördern einheitliche Anforderungen die Marktkohärenz innerhalb des Binnenmarktes, indem sie die grenzüberschreitende Verkehrsfähigkeit konformer Systeme erleichtern. Der Rechtsrahmen wirkt damit nicht primär beschränkend, sondern als strukturierende Voraussetzung für Vertrauen, Skalierbarkeit und Marktzugang.[14]

### 2. Produktsicherheitsrecht und Maschinenrecht als Basisschicht

#### *a) Maschinenverordnung (EU) 2023/1230 als Modernisierungsschub*

Die Maschinenverordnung (EU) 2023/1230, die ab dem 20. Januar 2027 Anwendung findet, ersetzt die bisherige Maschinenrichtlinie und überführt das Produktsicherheitsrecht in ein unmittelbar geltendes, unionsweit harmonisiertes Regime. Sie trägt den technologischen Entwicklungen softwaregesteuerter und KI-basierter Systeme Rechnung, indem sie explizit Anforderungen an sicherheitsrelevante Softwarefunktionen, Updatefähigkeit sowie den Schutz vor Cyberrisiken integriert (vgl. insbesondere Art. 3 Nr. 3 sowie Anhang III der VO (EU) 2023/1230). Zugleich präzisiert sie die Verantwortlichkeiten entlang der Entwicklung, Integration und Modifikation von Maschinen. Die Maschinenverordnung bleibt damit der zentrale Rechtsrahmen für die Verkehrsfähigkeit physischer Systeme und definiert die grundlegenden Sicherheitsanforderungen als Voraussetzung für deren rechtmäßige Bereitstellung und Nutzung im Binnenmarkt.

#### *b) Konformitätsbewertung und CE-Kennzeichnung*

Das CE-Kennzeichen bildet das zentrale Marktinstrument des europäischen Produktsicherheitsrechts. Es dokumentiert, dass ein Produkt die einschlägigen unionsrechtlichen Anforderungen erfüllt und rechtmäßig im Binnenmarkt in Verkehr gebracht werden darf. Voraussetzung hierfür ist die Durchführung eines Konformitätsbewertungsverfahrens gemäß Kapitel III der VO (EU) 2023/1230; hierzu treten insbesondere die technische Dokumentation, eine systematische Risikoanalyse sowie die Prüfung der Einhaltung der maßgeblichen Sicherheitsanforderungen, flankiert durch die EU-Konformitätserklärung und die CE-Kennzeichnung nach Art. 21 und 24 VO (EU) 2023/1230. Bei bestimmten Hochrisiko-Maschinen ist zudem die Einbindung einer notifizierten Stelle erforderlich. Die Konformitätsbewertung ist dabei nicht als formaler Verwaltungsakt zu verstehen, sondern als strukturiertes Governance-Instrument, das die Sicherheit des Produkts sicherstellt, Transparenz schafft und die Grundlage für Vertrauen in technische Systeme im Binnenmarkt bildet.

#### *c) Zusammenspiel mit dem AI Act*

Der AI Act und die Maschinenverordnung begründen keine widersprüchliche Doppelregulierung, sondern eine komplementäre Regulierungsarchitektur. Während die Maschinenverordnung die physische Sicherheit technischer Systeme adressiert und insbesondere Anforderungen an mechanische Integrität, elektrische Sicherheit und Schutzmechanismen festlegt, reguliert der AI Act die algorithmische Steuerungsebene, insbesondere im Hinblick auf Datenqualität, Nachvollziehbarkeit und die Vermeidung systemischer Fehlentscheidungen.[15] Am Beispiel eines kollaborativen Industrieroboters zeigt sich diese funktionale Auf-

11 Vgl. Art. 5-7 sowie Art. 50 AI Act (Transparenzpflicht).
12 Vgl. Art. 6i. V. m. Anh. III AI Act.
13 Vgl. Art. 9-15 AI Act.
14 Vgl. Art. 40, 41 AI Act.
15 Vgl. Art. 9-15 AI Act; Art. 10-12 Maschinenverordnung.

gabenteilung deutlich: Die Maschinenverordnung gewährleistet durch konstruktive Sicherheitsanforderungen, etwa Kraft- und Momentbegrenzungen, den physischen Schutz von Personen, während der AI Act sicherstellt, dass die zugrunde liegenden KI-Systeme in der Lage sind, ihre Umgebung zuverlässig zu erfassen und sicherheitsrelevante Entscheidungen etwa zur Kollisionsvermeidung nachvollziehbar und regelkonform zu treffen.

### 3. Cybersecurity als neue Grundbedingung physischer Systeme

#### *a) Cyber Resilience Act (CRA)*

Der Cyber Resilience Act (EU) 2024/2847 etabliert erstmals verbindliche Cybersecurity-Anforderungen für Produkte mit digitalen Elementen und schafft damit einen einheitlichen regulatorischen Mindeststandard für deren Sicherheit.[16] Zentrales Strukturprinzip ist der Ansatz des Security by Design, wonach Sicherheitsanforderungen nicht nachträglich implementiert, sondern von Beginn an integraler Bestandteil der Systemarchitektur sein müssen. Hieraus ergeben sich konkrete Pflichten für Hersteller, insbesondere im Hinblick auf sichere Standardkonfigurationen, ein kontinuierliches Vulnerability Management, Transparenzanforderungen etwa in Form einer Software Bill of Materials sowie die Gewährleistung von Sicherheitsupdates über den vorgesehenen Lebenszyklus des Produkts. Cybersecurity wird damit nicht als nachgelagerte Schutzmaßnahme, sondern als konstitutive Voraussetzung für die Verkehrsfähigkeit digitaler und physischer Systeme normativ verankert.

#### *b) NIS2-Richtlinie: Betreiberpflichten und organisatorische Resilienz*

Die Richtlinie (EU) 2022/2555 (NIS2-Richtlinie) erweitert den Anwendungsbereich unionsrechtlicher Cybersecurity-Pflichten erheblich und etabliert ein umfassendes Regime organisatorischer und technischer Sicherheitsanforderungen für Betreiber wesentlicher und wichtiger Einrichtungen.[17] Unternehmen, die kritische Dienstleistungen erbringen, sind verpflichtet, angemessene Risikomanagementmaßnahmen zur Gewährleistung der Sicherheit ihrer Netz- und Informationssysteme zu implementieren. Dies erfasst nicht nur klassische IT-Infrastrukturen, sondern ausdrücklich auch Operational Technology (OT), insbesondere Steuerungs- und Kontrollsysteme physischer Anlagen. Für Physical-AI-Systeme folgt hieraus, dass deren rechtliche Einordnung nicht isoliert auf der Ebene der Produktsicherheit erfolgt, sondern auch die betriebliche Einbettung und die organisatorische Resilienz des Betreibers regulatorisch relevant werden. Autonome Logistiksysteme oder vernetzte Robotiklösungen können daher als Bestandteil kritischer Infrastrukturen in den Anwendungsbereich der NIS2-Richtlinie fallen und unterliegen entsprechend erweiterten Compliance- und Sicherheitsanforderungen.

#### *c) Cybersecurity als Voraussetzung für Safety*

Ein grundlegender regulatorischer Paradigmenwechsel besteht darin, Cybersecurity nicht mehr als isolierte IT-Sicherheitsfrage, sondern als integralen Bestandteil der funktionalen Sicherheit physischer Systeme zu begreifen. Die Sicherheit eines Physical-AI-Systems bemisst sich nicht allein an seiner mechanischen oder konstruktiven Zuverlässigkeit, sondern ebenso an seiner Widerstandsfähigkeit gegenüber externen Manipulationen und unbefugten Eingriffen. Ein System, dessen Steuerungs- oder Kommunikationsstrukturen kompromittiert werden können, ist unabhängig von seiner physischen Robustheit als unsicher zu qualifizieren. Daraus folgt, dass Sicherheits- und Konformitätsbewertungen Cybersecurity-Risiken systematisch einbeziehen müssen. Die Analyse potenzieller Angriffsszenarien ist damit nicht fakultativer Bestandteil technischer Risikoprüfung, sondern regulatorisch notwendige Voraussetzung für die rechtliche und tatsächliche Sicherheit physischer KI-Systeme.

### 4. Datenschutzrecht als Infrastruktur für legitime Datennutzung

Die Datenschutz-Grundverordnung (EU) 2016/679 bildet das zentrale rechtliche Fundament für den Umgang mit personenbezogenen Daten im Kontext von Physical AI. Sie untersagt Datenverarbeitung nicht grundsätzlich, sondern bindet sie an definierte Rechtmäßigkeits-, Transparenz- und Governanceanforderungen. Jede Verarbeitung bedarf einer Rechtsgrundlage im Sinne des Art. 6 DSGVO und unterliegt dem Prinzip der Zweckbindung. Bei risikobehafteten Verarbeitungen ist zudem eine Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO durchzuführen. Ergänzend verpflichtet die DSGVO zur Implementierung technischer und organisatorischer Maßnahmen im Sinne des Art. 32 DSGVO zur Sicherstellung der Integrität und Sicherheit der Verarbeitung. Datenschutz fungiert damit nicht zwingend als Innovationshemmnis, sondern als rechtliche Infrastruktur legitimer und vertrauenswürdiger Nutzung von personenbezogenen Daten.[18]

### 5. Der Data Act als Bestandteil der regulatorischen Architektur

Der Data Act erweitert diese regulatorische Architektur wesentlich, indem er die rechtliche Einordnung und Zugänglichkeit der von Physical-AI-Systemen erzeugten Daten präzisiert. Physical-AI-Systeme generieren fortlaufend Betriebs- und Sensordaten, die auch als Produktdaten im Sinne des Data Act qualifiziert werden können. Die Verordnung begründet insoweit Zugriffsrechte zugunsten der Nutzer sowie unter bestimmten Voraussetzungen zugunsten Dritter und schafft damit einen Rechtsrahmen für die kontrollierte Nutzung maschinengenerierter Daten.

Zugleich normiert sie Anforderungen an Interoperabilität, Datenportabilität und den Wechsel zwischen digitalen Infrastrukturen. Dadurch wird sichergestellt, dass Physical-AI-Systeme nicht in geschlossenen Plattformstrukturen verbleiben, sondern einer rechtlich strukturierten Datenzugangs- und Interoperabilitätsordnung unterliegen.[19]

### 6. Haftungsrecht als Backstop, nicht als Leitnarrativ

Die neue Produkthaftungsrichtlinie (EU) 2024/2853 modernisiert das Haftungsregime für digitale und KI-gestützte Produkte und erfasst Software ausdrücklich als haftungsfähiges Produkt. Sie enthält Beweiserleichterungen und erweitert die Haftung auf nachträgliche substanzielle Ver-

16 Vgl. Art. 1 Verordnung (EU) 2024/2847 (Cyber Resilience Act – CRA); ErwG 1-2.
17 Vgl. Art. 1 und 21 Richtlinie (EU) 2022/2555 (NIS2-Richtlinie).
18 Vgl. Art. 5, 6, 32 und 35 DSGVO; ErwG 4, 75.
19 Vgl. Art. 1, 4–7 und 23 Verordnung (EU) 2023/2854 (Data Act); ErwG 5.

änderungen von Systemen. Für Physical AI gewinnt dabei insbesondere die Qualität der technischen Dokumentation zentrale Bedeutung, da sie die Nachvollziehbarkeit von Systemverhalten und die Einhaltung regulatorischer Anforderungen belegt. Haftungsrecht fungiert in diesem Kontext nicht als primärer Steuerungsmechanismus, sondern als sekundärer Sicherungsrahmen, der Anreize zur Implementierung robuster Gover- nance-, Dokumentations- und Sicherheitsstrukturen entlang des gesamten Systemlebenszyklus schafft.[20]

## IV. Die entscheidende Praxisfrage: Wie wird aus Normen ein funktionsfähiges Compliance-System?

Rechtsnormen entfalten ihre Steuerungswirkung erst durch ihre systematische Übersetzung in technische, organisatorische und betriebliche Prozesse. Die zentrale Herausforderung besteht daher darin, abstrakte regulatorische Anforderungen in eine funktionsfähige Compliance-Architektur zu überführen, die den gesamten Lebenszyklus eines Systems erfasst. Dies setzt eine integrierte Governance-Struktur voraus, in der rechtliche Vorgaben, technische Systemarchitektur und organisatorische Verantwortlichkeiten nicht isoliert, sondern als miteinander verzahnte Elemente eines kohärenten Compliance-Modells verstanden und implementiert werden.

### 1. Governance entlang des Lebenszyklus

Physical AI unterliegt einem durchgängigen technologischen und regulatorischen Lebenszyklus, der sich von der Systemkonzeption bis zum laufenden Betrieb erstreckt. Dieser umfasst insbesondere die Designphase, die Trainingsphase, die Deploymentphase sowie die anschließenden Update- und Monitoringphasen. Ein funktionsfähiges Compliance-System muss diesen gesamten Lebenszyklus erfassen und rechtliche Anforderungen nicht punktuell, sondern als integralen Bestandteil eines durchgängigen Governance-Prozesses implementieren.

### 2. Rollen und Verantwortlichkeiten

Physical-AI-Systeme entstehen regelmäßig im Zusammenwirken mehrerer Akteure, deren jeweilige Verantwortungsbereiche rechtlich differenziert zu bestimmen sind. Zu unterscheiden sind insbesondere der Provider, der das KI-Modell entwickelt und trainiert und für Data Governance sowie technische Dokumentation verantwortlich ist, der Integrator beziehungsweise Hersteller, der das KI-System in eine physische Maschine einbettet und die Gesamtsystemsicherheit sowie die Konformitätsbewertung einschließlich CE-Kennzeichnung gewährleistet, sowie der Betreiber oder Deployer, der das System im praktischen Einsatz verwendet und für den ordnungsgemäßen Betrieb, die Wartung und die fortlaufende Überwachung mitverantwortlich ist. Die regulatorische Herausforderung besteht darin, dass diese Rollen funktional miteinander verflochten sind und ihre Abgrenzung in der Praxis nicht immer eindeutig erfolgt. Der AI Act trägt dieser Struktur Rechnung, indem er die jeweiligen Verantwortlichkeiten entlang der Wertschöpfungskette präzise zuordnet und zugleich Dokumentations- und Schnittstellenpflichten etabliert, die eine rechtssichere Zurechnung ermöglichen.[21]

Diese Struktur führt zugleich zu einer funktionalen Differenzierung regulatorischer Verantwortung. Während klassische Produktsicherheitsmodelle von einer klar bestimmbaren Herstellerverantwortung ausgehen, entstehen bei Physical AI mehrstufige Verantwortungsstrukturen, in denen sicherheitsrelevante Systemeigenschaften durch das Zusammenwirken von Provider, Integrator und Betreiber bestimmt werden. Diese funktionale Verschränkung wird durch Softwareupdates, Systemintegration und fortlaufende Systemanpassungen weiter verstärkt. Der AI Act reagiert hierauf mit einer differenzierten Rollenarchitektur, kann jedoch in komplexen Systemkonstellationen nicht jede praktische Zurechnungsfrage abschließend vorstrukturieren. Regulatorische Verantwortung wird damit zunehmend systemisch, lebenszyklusbezogen und funktionsbezogen bestimmt.

### 3. Dokumentation als zentrales Vertrauensmedium

Dokumentation bildet ein zentrales Struktur- und Vertrauenselement regulatorischer Compliance. Sie erfüllt mehrere Funktionen zugleich: Sie dient als Nachweis gegenüber Aufsichtsbehörden, ermöglicht Transparenz und Kommunikation entlang der Lieferkette und stellt die Grundlage für die Analyse und Aufarbeitung sicherheitsrelevanter Vorfälle dar. Zugleich ermöglicht sie eine kontinuierliche Weiterentwicklung und Verbesserung des Systems im laufenden Betrieb. Der AI Act verlangt eine umfassende technische Dokumentation des KI-Systems, die Maschinenverordnung fordert eine technische Dokumentationsakte und der Cyber Resilience Act etabliert mit der Software Bill of Materials ein Instrument zur Transparenz über Softwarekomponenten. Diese Dokumentationspflichten gewährleisten regulatorische Nachvollziehbarkeit.[22]

### 4. Standards als Brücke zwischen Norm und Technik

Harmonisierte Standards übernehmen eine zentrale Vermittlungsfunktion zwischen abstrakten rechtlichen Anforderungen und deren technischer Umsetzung.[23] Sie konkretisieren gesetzliche Vorgaben in überprüfbare technische Spezifikationen und schaffen damit die operative Grundlage für Compliance. Dabei entfalten sie insbesondere zwei zentrale Wirkungen: Zum einen begründen sie eine Vermutungswirkung dahingehend, dass bei Einhaltung harmonisierter Standards die entsprechenden gesetzlichen Anforderungen als erfüllt gelten; zum anderen ermöglichen sie Interoperabilität, indem sie einheitliche technische Schnittstellen und Verfahren etablieren. Maßgebliche Akteure der Standardisierung sind insbesondere die europäischen Normungsorganisationen CEN und CENELEC, die internationalen Standardisierungsgremien ISO und IEC sowie technische Organisationen wie das IEEE, die spezifische Standards für KI- und Robotiksysteme entwickeln.

20 Vgl. Art. 4, 6 und 9 Richtlinie (EU) 2024/2853 (Produkthaftungsrichtlinie).

21 Vgl. Art. 3 und Art. 16–29 AI Act.

22 Vgl. Art. 11 AI Act; Art. 10–12 Maschinenverordnung; Art. 13, 14 CRA.

23 Vgl. Art. 40 ff. AI Act; CEN/CENELEC, European Standardisation Strategy 2022; ISO/IEC JTC 1, Artificial Intelligence Standards Overview, 2023; IEEE, Ethically Aligned Design, 2019.

### 5. Compliance by Architecture: Integration statt Addition

Die wirksamste Form regulatorischer Compliance besteht darin, rechtliche Anforderungen bereits auf der Ebene der Systemarchitektur zu berücksichtigen und nicht erst nachträglich als externe Kontroll- oder Prüfmechanismen zu implementieren. Compliance wird damit zum integralen Bestandteil des technischen Designs (Compliance-by-Architecture).[24] Dies zeigt sich insbesondere in Konzepten wie Privacy by Design durch lokale Datenverarbeitung oder Pseudonymisierung, Security by Design durch abgesicherte Kommunikationsprotokolle und kryptographisch gesicherte Update-Mechanismen sowie Safety by Design durch redundante Sicherheitsstrukturen und Fail-Safe-Mechanismen. Entscheidend ist die Integration dieser Dimensionen in eine einheitliche Systemarchitektur. Safety, algorithmische Steuerung, Cybersecurity und Daten-Governance sind keine isolierten Compliance-Bereiche, sondern funktional miteinander verflochtene Elemente eines kohärenten Gesamtsystems. Dies erfordert eine enge interdisziplinäre Zusammenarbeit zwischen technischen, organisatorischen und rechtlichen Akteuren bereits im Entwicklungsprozess.

## V. Quantencomputing als nächste Regulierungswelle

Quantencomputing befindet sich derzeit noch weitgehend im Forschungsstadium, wird aber absehbar erhebliche Auswirkungen auf Physical AI entfalten – sowohl als Beschleuniger für Optimierungs-, Simulations- und Trainingsprozesse als auch als Risikofaktor für bestehende Sicherheitsannahmen, insbesondere im Bereich der Kryptographie.[25] Für Physical-AI-Systeme rückt damit die Frage in den Vordergrund, wie Updatefähigkeit, Security over Time und Langzeit-Compliance technisch und regulatorisch abgesichert werden können.

### 1. Quantum als Gamechanger

Quantencomputing besitzt das Potenzial, zentrale Rechenoperationen in den Bereichen Optimierung, Simulation und KI-Training erheblich zu beschleunigen. Dies betrifft insbesondere Anwendungen mit hoher Komplexität, etwa die Steuerung logistischer Netzwerke, die Simulation molekularer Prozesse oder das Training umfangreicher Machine-Learning-Modelle. Aus regulatorischer Perspektive ergibt sich daraus eine veränderte Risikodynamik: Systeme, die bereits heute als Hochrisiko-KI qualifiziert werden, könnten durch quantenbasierte Beschleunigung eine gesteigerte Leistungsfähigkeit und damit zugleich ein erhöhtes Schadenspotenzial entfalten. Die Risikobewertung und die darauf aufbauenden Compliance-Mechanismen müssen daher die Möglichkeit technologischer Leistungssprünge systematisch berücksichtigen.

### 2. Quantum als Risiko für Kryptographie

Die unmittelbar gravierendste sicherheitsrechtliche Konsequenz des Quantencomputings betrifft die bestehende kryptographische Infrastruktur. Quantenalgorithmen, insbesondere Shor's Algorithm, sind grundsätzlich geeignet, etablierte asymmetrische Verschlüsselungsverfahren wie RSA, elliptische Kurven oder Diffie-Hellman zu kompromittieren und damit zentrale Vertrauensmechanismen digitaler Systeme zu unterminieren.[26] Für Physical-AI-Systeme entsteht hieraus ein spezifisches Langzeitrisiko, da deren operative Lebensdauer regelmäßig deutlich über den aktuellen Stand kryptographischer Sicherheit hinausreicht. Angriffsstrategien im Sinne eines „Harvest now, decrypt later" verdeutlichen, dass bereits heute erhobene und gespeicherte Daten künftig nachträglich entschlüsselt werden könnten. Daraus folgt die Notwendigkeit einer frühzeitigen Migration zu quantensicheren Verschlüsselungsverfahren. Die Entwicklung und Standardisierung der Post-Quantum-Cryptography, etwa durch die Veröffentlichung erster PQC-Standards durch das NIST im Jahr 2024, markiert insoweit einen entscheidenden Schritt zur Sicherung der langfristigen Integrität und Vertrauenswürdigkeit Physical-AI-basierter Systeme.

### 3. Konsequenzen für Physical AI

Die Maschinenverordnung sowie der Cyber Resilience Act verlangen bereits heute die Updatefähigkeit sicherheitsrelevanter Systemkomponenten.[27] Quantencomputing verschärft diese Anforderung erheblich, da kryptographische Verfahren künftig ausgetauscht werden müssen, ohne die grundlegende Konformität des Systems in Frage zu stellen. Dies setzt modular aufgebaute Systemarchitekturen und klar definierte Update- und Sicherheitsmechanismen voraus. Physical-AI-Systeme müssen daher so konzipiert sein, dass ihre kryptographische Integrität über den gesamten Lebenszyklus hinweg gewährleistet und bei veränderten Sicherheitsanforderungen anpassungsfähig bleibt.

Die bestehenden regulatorischen Rahmenwerke tragen dieser Entwicklung bereits strukturell Rechnung, indem sie Anforderungen an IT-Sicherheit, Updatefähigkeit und die fortlaufende Absicherung technischer Systeme über ihren gesamten Lebenszyklus etablieren. Sie schreiben jedoch keine spezifischen kryptographischen Verfahren vor, sondern beschränken sich auf funktionale Sicherheitsanforderungen und gewährleisten damit regulatorische Technologieneutralität. Die regulatorische Architektur bleibt damit offen für die Integrationsfähigkeit zukünftiger Sicherheitsstandards, insbesondere quantenresistenter Kryptographie, ohne dass eine grundlegende Anpassung der bestehenden Rechtsstruktur erforderlich würde. Die Vorbereitung auf Post-Quantum-Cryptography wird damit primär zu einer Frage technischer Standardisierung und Compliance-Implementierung, nicht zu einer eigenständigen gesetzlichen Regulierung.

## VI. Offene Fragen und Diskussionsimpulse

Trotz des bereits bestehenden differenzierten Rechtsrahmens verbleiben zentrale Fragen, die einer weiteren rechtlichen Klärung bedürfen. Dies betrifft insbesondere dynamische Systeme, bei denen unklar ist, ab welchem Grad einer Änderung eine erneute Konformitätsbewertung erforderlich wird. Hinzu treten Herausforderungen im Bereich der Verantwortungszuordnung innerhalb komplexer Liefer- und Integrationsketten, die eine präzisere rechtliche Strukturierung der beteiligten Akteursrollen erfordern. Auch die Anforderungen an Nachvollziehbarkeit und Evi-

24 Vgl. Art. 25 DSGVO; Art. 15 AI Act.
25 Vgl. NIST, NIST Releases First 3 Finalized Post–Quantum Encryption Standards, v. 13.8.2024.
26 Vgl. *NIST,* NIST Releases First 3 Finalized Post–Quantum Encryption Standards, v. 13.8.2024; *Shor,* SIAM J. Comput. 26 1997, 1484 ff.
27 Vgl. Art. 10–12 Maschinenverordnung; Art. 13, 14 CRA.

denz, etwa im Hinblick auf Logging- und Incident-Forensics-Standards, sind bislang nicht abschließend konkretisiert. Weitere Diskussionsfelder ergeben sich aus der internationalen Dimension regulatorischer Divergenzen, den arbeitsrechtlichen Implikationen des Einsatzes physischer KI-Systeme sowie den besonderen Anforderungen im Bereich medizinischer Robotik. Vor diesem Hintergrund stellt sich schließlich die grundlegende Frage, ob langfristig ein eigenständiges, kohärentes Governance-Konzept für Physical AI erforderlich sein wird.

## VII. Fazit: Das Glas ist halbvoll – Rechtsrahmen als Innovationsmotor

Der europäische Rechtsrahmen für Physical AI weist weder ein regulatorisches Defizit noch eine innovationshemmende Überregulierung auf. Vielmehr besteht bereits eine kohärente und funktionsfähige Regulierungsarchitektur aus AI Act, Maschinenrecht, Cybersecurity-Regulierung und Datenschutzrecht, die unterschiedliche Dimensionen physischer KI-Systeme systematisch adressiert. Diese Normen wirken nicht isoliert, sondern ergänzen sich funktional und schaffen in ihrem Zusammenspiel die rechtlichen Voraussetzungen für eine sichere, vertrauenswürdige und nachhaltige Entwicklung sowie den rechtssicheren Einsatz physischer KI-Systeme.

### 1. Strukturgeber: Vertrauen, Standardisierung, Skalierung

Rechtliche Anforderungen übernehmen im Kontext von Physical AI eine zentrale strukturierende Funktion, indem sie Vertrauen bei Nutzern, Marktteilnehmern und Investoren schaffen. Ein CE-gekennzeichnetes und AI-Act-konformes System signalisiert, dass definierte Sicherheits-, Qualitäts- und Governanceanforderungen eingehalten werden und das Produkt innerhalb eines normativ abgesicherten Rahmens betrieben werden kann. Standardisierung reduziert dabei regulatorische und technische Unsicherheiten, indem sie einheitliche Referenzpunkte für Entwicklung, Konformitätsbewertung und Betrieb bereitstellt und zugleich Interoperabilität ermöglicht. Einheitliche europäische Regelungen schaffen darüber hinaus die Voraussetzung für Skalierung: Systeme, die den unionsrechtlichen Anforderungen entsprechen, können ohne zusätzliche nationale Zulassungsverfahren im gesamten Binnenmarkt bereitgestellt und betrieben werden. Der Rechtsrahmen wirkt damit als Infrastruktur für Marktzugang, Vertrauen und technologische Diffusion.

### 2. Physical AI als Testfeld integrierter Regulierung

Physical AI fungiert als Verdichtungspunkt der verschiedenen regulatorischen Dimensionen, da hier algorithmische Entscheidungsprozesse, physische Systemwirkung, Cybersecurity und Datenverarbeitung unmittelbar zusammenwirken. Keine dieser Ebenen kann isoliert betrachtet werden, weil die Sicherheit, Funktionsfähigkeit und Rechtmäßigkeit des Gesamtsystems erst aus ihrem strukturierten Zusammenspiel entstehen. Physical AI wird damit zum praktischen Testfall dafür, ob die europäische Regulierung in der Lage ist, komplexe technologische Systeme durch ein kohärentes und operables Zusammenspiel unterschiedlicher Rechtsbereiche wirksam zu erfassen und zu steuern.

### 3. Quantencomputing als nächster Schritt

Die Migration auf Post-Quantum-Cryptography wird perspektivisch zu einer regulatorischen Notwendigkeit, da bestehende kryptographische Verfahren langfristig ihre Sicherheitsfunktion verlieren können. Systeme, die bereits heute über Updatefähigkeit und modulare Architekturen verfügen, sind besser in der Lage, auf diese veränderten Sicherheitsanforderungen zu reagieren. Daraus folgt als zentrale Konsequenz, dass Anpassungsfähigkeit nicht als nachgelagerte Eigenschaft, sondern als strukturelles Designprinzip technologischer Systeme verstanden werden muss. Ein heute zertifiziertes System muss daher so konzipiert sein, dass seine Sicherheit auch unter veränderten technologischen Rahmenbedingungen langfristig gewährleistet werden kann.

### 4. Zehn Thesen

1. Physical AI ist keine bloße Fortsetzung digitaler KI, sondern ein qualitativ neuer Regulierungsgegenstand, weil algorithmische Entscheidungen unmittelbar in physische Wirkungen übersetzt werden.

2. Der zentrale Ordnungsrahmen für Physical AI entsteht nicht aus einem Einzelgesetz, sondern aus einer integrierten Vierfacharchitektur: AI Act (Algorithmik), Maschinenrecht und Produktsicherheit (Safety), CRA und NIS2 (Cybersecurity) sowie Data Act / DSGVO (Daten-Governance).

3. Der AI Act ist für Physical AI weniger Verbotsrecht als eine horizontale Compliance-Schicht, die technische Qualität – etwa Risikomanagement, Logging und Human Oversight – in rechtliche Mindeststandards übersetzt.

4. Die Maschinenverordnung (EU) 2023/1230 bleibt der Primärrahmen für die Verkehrsfähigkeit physischer Systeme; AI-Act-Compliance ersetzt weder CE-Konformität noch die grundlegenden Safety-Anforderungen.

5. Cybersecurity ist bei Physical AI keine IT-Nebenpflicht, sondern eine Safety-Voraussetzung: Ein manipulierbares System ist in der Sache ein unsicheres Produkt.

6. Die Zukunftsfähigkeit von Physical AI hängt weniger von neuen Haftungsregeln ab als von der Durchsetzbarkeit von Dokumentations-, Update- und Monitoringpflichten über den gesamten Lebenszyklus.

7. Haftungsrecht wirkt bei Physical AI vor allem als Backstop: Es sanktioniert Governance-Defizite, ersetzt aber nicht die präventive Struktur des Produktsicherheits- und AI-Compliance-Regimes.

8. Quantencomputing wird Physical AI nicht nur leistungsfähiger machen, sondern auch die Sicherheitsgrundlagen verschieben, insbesondere durch den Angriff auf klassische Kryptographie; Post-Quantum-Security wird damit zu einem Kernbestandteil künftiger Produktsicherheit.

9. Die eigentliche Herausforderung liegt in der Verantwortungsdiffusion: Provider, Integratoren und Betreiber bilden eine Kette, in der rechtliche Zurechnung nur gelingt, wenn Rollenmodelle und Schnittstellenpflichten präzise definiert werden.

10. Der entscheidende Erfolgsfaktor für Physical AI in Europa ist nicht weniger Recht, sondern besseres Recht: Standardisierung, klare Governance-Modelle und interoperable Compliance-Prozesse können regulatorische Qualität in einen verlässlichen Standort- und Marktvorteil verwandeln.