Rat der
Europäischen Union

**Brüssel, den 24. Februar 2020**
**(OR. en)**

**6263/20**

**JAI 148**
**COPEN 59**
**CYBER 26**
**DATAPROTECT 22**
**EJUSTICE 21**
**COSI 27**
**IXIM 29**
**ENFOPOL 54**
**FREMP 14**
**TELECOM 23**
**RELEX 149**
**MI 48**
**COMPET 56**

**ÜBERMITTLUNGSVERMERK**

| | |
|---|---|
| Absender: | Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag des Generalsekretärs der Europäischen Kommission |
| Eingangsdatum: | 20. Februar 2020 |
| Empfänger: | Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union |
| Nr. Komm.dok.: | COM(2020) 64 final |
| Betr.: | BERICHT DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT UND DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS Bericht über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung |

Die Delegationen erhalten in der Anlage das Dokument COM(2020) 64 final.

Anl.: COM(2020) 64 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 19.2.2020
COM(2020) 64 final

# BERICHT DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT UND DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS

## Bericht über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung

# BERICHT ÜBER DIE AUSWIRKUNGEN KÜNSTLICHER INTELLIGENZ, DES INTERNETS DER DINGE UND DER ROBOTIK IN HINBLICK AUF SICHERHEIT UND HAFTUNG

## 1. Einführung

Künstliche Intelligenz (KI)[1], das Internet der Dinge (IoT)[2] und die Robotik werden neue Möglichkeiten und Vorteile für unsere Gesellschaft schaffen. Die Kommission hat die Bedeutung und das Potenzial dieser Technologien sowie die Notwendigkeit erheblicher Investitionen in diesen Bereichen anerkannt.[3] Sie setzt sich dafür ein, dass Europa in den Bereichen künstliche Intelligenz, Internet der Dinge und Robotik eine weltweite Führungsrolle übernimmt. Um dieses Ziel zu erreichen, bedarf es eines klaren und berechenbaren Rechtsrahmens, mit dem die technologischen Herausforderungen angegangen werden können.

### 1.1. Der bestehende Sicherheits- und Haftungsrahmen

Das übergeordnete Ziel der rechtlichen Sicherheits- und Haftungsrahmen besteht darin sicherzustellen, dass alle Produkte und Dienstleistungen, auch solche, die neue digitale Technologien nutzen, sicher, zuverlässig und beständig funktionieren und eingetretene Schäden wirksam behoben werden. Ein hohes Maß an Sicherheit von Produkten und Systemen, die neue digitale Technologien nutzen, und robuste Mechanismen zur Behebung von Schäden (z. B. der Haftungsrahmen) tragen zu einem besseren Verbraucherschutz bei. Dadurch wird zudem Vertrauen in diese Technologien und damit eine Voraussetzung für ihren Einsatz in der Industrie und die Akzeptanz durch die Nutzer geschaffen. Dies wiederum wird die Wettbewerbsfähigkeit unserer Industrie steigern und zu den Zielen der Union in diesem Bereich beitragen.[4] Bei der Entstehung neuer Technologien wie künstlicher Intelligenz, Internet der Dinge und Robotik ist ein klarer Sicherheits- und Haftungsrahmen besonders wichtig, um sowohl Verbraucherschutz als auch Rechtssicherheit für Unternehmen zu gewährleisten.

Die Union verfügt in den Bereichen Sicherheit und Produkthaftung über einen robusten und zuverlässigen Rechtsrahmen und einen soliden Bestand an Sicherheitsstandards, die durch nationale, nicht harmonisierte Haftungsvorschriften ergänzt werden. Sie alle gewährleisten das Wohlergehen unserer Bürgerinnen und Bürger im Binnenmarkt und fördern Innovation und die Verbreitung neuer Technologien. Künstliche Intelligenz, Internet der Dinge und Robotik werden jedoch die Merkmale vieler Produkte und Dienstleistungen verändern.

In der am 25. April 2018 angenommenen Mitteilung „Künstliche Intelligenz für Europa“[5] wurde ein Bericht der Kommission angekündigt, in dem die Auswirkungen der neuen

---

1 Die Definition für künstliche Intelligenz der hochrangigen Expertengruppe (HEG-KI) ist abrufbar unter https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines.

2 Die Empfehlung ITU-T Y.2060 der Internationalen Fernmeldeunion mit der Definition des Internets der Dinge ist abrufbar unter https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060.

3 SWD(2016) 110, COM(2017) 9, COM(2018) 237 und COM(2018) 795.

4 http://ec.europa.eu/growth/industry/policy_de

5 https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=COM%3A2018%3A237%3AFIN.
Die begleitende Arbeitsunterlage der Kommissionsdienststellen SWD(2018) 137 (https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137) enthält einen ersten Überblick über

digitalen Technologien auf die bestehenden Sicherheits- und Haftungsrahmen bewertet werden. Ziel dieses Berichts ist es, die weiterreichenden Auswirkungen, die künstliche Intelligenz, Internet der Dinge und Robotik auf den Haftungs- und den Sicherheitsrahmen haben, sowie die potenziellen Lücken in diesen Rechtsrahmen zu ermitteln und zu prüfen. In diesem gemeinsam mit dem Weißbuch über künstliche Intelligenz vorgelegten Bericht werden Orientierungshilfen gegeben, die zur weiteren Erörterung dienen sollen und Teil der umfassenderen Konsultation der Interessenträger sind. Der Abschnitt zum Thema Sicherheit beruht auf der Bewertung[6] der Maschinenrichtlinie[7] und den gemeinsam mit den einschlägigen Expertengruppen[8] durchgeführten Arbeiten. Der Abschnitt zu Haftungsfragen stützt sich auf die Bewertung[9] der Produkthaftungsrichtlinie[10] und die Beiträge der einschlägigen Expertengruppen[11] sowie auf Kontakte zu Interessenträgern. Dieser Bericht zielt nicht darauf ab, einen umfassenden Überblick über die bestehenden Sicherheits- und Haftungsvorschriften zu geben, sondern konzentriert sich auf die bisher ermittelten Schlüsselfragen.

## 1.2. Merkmale von KI, IoT und Robotik

Künstliche Intelligenz, Internet der Dinge und Robotik weisen viele gemeinsame Merkmale auf. Sie können **Konnektivität**, **Autonomie** und **Datenabhängigkeit** miteinander verknüpfen, um Aufgaben ohne oder nur mit geringer menschlicher Steuerung oder Aufsicht auszuführen. KI-gestützte Systeme können zudem ihre Leistung verbessern, indem sie aus Erfahrungen lernen. Ihre **Komplexität** spiegelt sich sowohl in der Vielfalt der an der **Lieferkette** beteiligten Wirtschaftsakteure als auch in der Vielzahl von Komponenten, Teilen, Software, Systemen oder Dienstleistungen wider, die zusammen die neuen technologischen Ökosysteme bilden. Hinzu kommt die **Offenheit** für Aktualisierungen und Verbesserungen nach der Markteinführung dieser Technologien. Die enormen beteiligten Datenmengen, der Rückgriff auf Algorithmen und die **Opazität** der KI-Entscheidungsfindung erschweren die Vorhersage des Verhaltens eines KI-gestützten Produkts und das Verständnis der potenziellen Schadensursachen. Schließlich können **Konnektivität** und **Offenheit** KI-Produkte und IoT-Produkte anfällig für Cyberbedrohungen machen.

---

die Herausforderungen in Bezug auf die Haftung, die sich im Zusammenhang mit neuen digitalen Technologien ergeben.

6 SWD(2018) 161 final.

7 Richtlinie 2006/42/EG.

8 Netzwerk zur Verbrauchersicherheit, eingerichtet gemäß der Richtlinie 2001/95/EG über die allgemeine Produktsicherheit, Expertengruppen zur Maschinenrichtlinie 2006/42/EG und zur Funkanlagenrichtlinie 2014/53/EU, bestehend aus Mitgliedstaaten, Branchenvertretern und anderen Interessenträgern wie Verbraucherverbänden.

9 COM(2018) 246 final.

10 Richtlinie 85/374/EWG.

11 Die Expertengruppe für Haftung und neue Technologien wurde eingesetzt, um der Kommission mit Fachwissen über die Anwendbarkeit der Produkthaftungsrichtlinie und der nationalen Vorschriften für die zivilrechtliche Haftung zur Seite zu stehen und sie bei der Ausarbeitung von Leitprinzipien für mögliche Anpassungen der geltenden Rechtsvorschriften im Zusammenhang mit neuen Technologien zu unterstützen. Die Expertengruppe besteht aus zwei Untergruppen, der „Untergruppe Produkthaftung“ und der „Untergruppe neue Technologien“, siehe http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592&NewSearch=1&NewSearch=1
Bericht der „Untergruppe neue Technologien“ über die Haftung für künstliche Intelligenz und andere neue Technologien, siehe https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

## 1.3. Chancen, die sich durch künstliche Intelligenz, Internet der Dinge und Robotik ergeben

Die Stärkung des Vertrauens der Nutzer in neue Technologien und die Erhöhung ihrer gesellschaftlichen Akzeptanz, die Verbesserung von Produkten, Verfahren und Geschäftsmodellen sowie die Unterstützung der europäischen Hersteller bei der Steigerung ihrer Effizienz sind nur einige der Chancen, die künstliche Intelligenz, Internet der Dinge und Robotik bieten.

Neben Produktivitäts- und Effizienzgewinnen hat künstliche Intelligenz auch das Potenzial, Menschen in die Lage zu versetzen, noch nicht erreichte Intelligenz zu entwickeln, neue Entdeckungen zu ermöglichen und zur Lösung einiger der größten Herausforderungen der Menschheit beizutragen. Dies reicht von der Behandlung chronischer Krankheiten und der Vorhersage von Krankheitsausbrüchen über die Verringerung der Zahl der Verkehrstoten bis hin zur Bekämpfung des Klimawandels oder der Antizipation von Bedrohungen für die Cybersicherheit.

Diese Technologien können viele Vorteile mit sich bringen, indem sie die Sicherheit von Produkten verbessern und sie weniger anfällig für bestimmte Risiken machen. So könnten beispielsweise vernetzte und automatisierte Fahrzeuge die Straßenverkehrssicherheit verbessern, da die meisten Verkehrsunfälle derzeit durch menschliches Versagen[12] verursacht werden. Darüber hinaus sind IoT-Systeme so konzipiert, dass sie große Datenmengen aus verschiedenen Quellen empfangen und verarbeiten können. Dieser gesteigerte Umfang an Informationen könnte dazu genutzt werden, dass sich Produkte selbst anpassen und somit sicherer werden. Neue Technologien können zu einer besseren Wirksamkeit von Produktrückrufen beitragen, da beispielsweise Produkte die Nutzer vor einem Sicherheitsproblem warnen könnten[13]. Tritt bei der Verwendung eines vernetzten Produkts ein Sicherheitsproblem auf, können die Hersteller direkt mit den Nutzern kommunizieren, um einerseits die Nutzer vor den Risiken zu warnen und andererseits, sofern möglich, das Problem beispielsweise durch Bereitstellung einer Aktualisierung der Sicherheitssoftware direkt zu beheben. So führte beispielsweise ein Smartphone-Hersteller während einer Rückrufaktion eines seiner Geräte im Jahr 2017 eine Software-Aktualisierung durch, um die Batteriekapazität der zurückgerufenen Telefone[14] auf Null zu setzen, damit die Nutzer die gefährlichen Geräte nicht mehr nutzen konnten.

Darüber hinaus können neue Technologien dazu beitragen, die Rückverfolgbarkeit von Produkten zu verbessern. So können beispielsweise Unternehmen und Marktüberwachungsbehörden aufgrund der für das Internet der Dinge charakteristischen Konnektivität gefährliche Produkte verfolgen und Risiken entlang der Lieferketten erkennen.[15]

---

[12] Schätzungen zufolge sind rund 90 % der Verkehrsunfälle auf menschliches Versagen zurückzuführen. Siehe Bericht der Kommission zur Rettung von Menschenleben: Mehr Fahrzeugsicherheit in der EU (COM(2016) 0787 final).

[13] So kann beispielsweise der Fahrer eines Fahrzeugs gewarnt und zur Verringerung seiner Geschwindigkeit aufgefordert werden, wenn sich vor ihm ein Unfall ereignet hat.

[14] OECD (2018), „Measuring and maximising the impact of product recalls globally: OECD workshop report“, *OECD Science, Technology and Industry Policy Papers*, Nr. 56, OECD Publishing, Paris, https://doi.org/10.1787/ab757416-en

[15] OECD (2018), „Enhancing product recall effectiveness globally: OECD background report“, *OECD Science, Technology and Industry Policy Papers*, Nr. 58, OECD Publishing, Paris, https://doi.org/10.1787/ef71935c-en

Neben den Chancen, die sich aufgrund von künstlicher Intelligenz, Internet der Dinge und Robotik für die Wirtschaft und unsere Gesellschaften ergeben können, besteht jedoch auch die Gefahr, dass durch diese Technologien rechtlich geschützte Interessen, sowohl materieller als auch immaterieller Art, Schaden nehmen könnten. Diese Gefahr erhöht sich mit zunehmenden Anwendungsmöglichkeiten. In diesem Zusammenhang muss geprüft werden, ob und inwieweit der derzeitige Rechtsrahmen für Sicherheit und Haftung noch geeignet ist, die Nutzer zu schützen.

## 2. Sicherheit

In der Mitteilung der Kommission „Schaffung von Vertrauen in eine auf den Menschen ausgerichtete künstliche Intelligenz" heißt es, dass ***KI-Systeme konzeptuell integrierte Schutz- und Sicherheitsvorkehrungen aufweisen sollten, damit sie in jeder Phase nachprüfbar sicher sind, wobei es auf die körperliche und geistige Sicherheit aller Beteiligten ankommt***[16].

Bei der Bewertung der Produktsicherheitsvorschriften der Union in diesem Abschnitt wird analysiert, ob der derzeitige Rechtsrahmen der Union die relevanten Elemente enthält, um sicherzustellen, dass neue Technologien und insbesondere KI-Systeme konzeptuell integrierte Schutz- und Sicherheitsvorkehrungen aufweisen.

Dieser Bericht befasst sich hauptsächlich mit der Richtlinie über die allgemeine Produktsicherheit[17] und den harmonisierten Produktvorschriften, die sich an den horizontalen Bestimmungen der „neuen Konzeption"[18] und/oder am „neuen Rechtsrahmen" (im Folgenden „Produktsicherheitsvorschriften der Union" oder „Rechtsrahmen der Union zur Produktsicherheit")[19] orientieren. Die horizontalen Bestimmungen gewährleisten die Kohärenz zwischen den sektorspezifischen Vorschriften über die Produktsicherheit.

Mit den Produktsicherheitsvorschriften der Union soll sichergestellt werden, dass Produkte, die in der Union in Verkehr gebracht werden, hohen Gesundheits-, Sicherheits- und Umweltanforderungen genügen und dass solche Produkte in der gesamten Union frei zirkulieren können. Die sektorspezifischen Rechtsvorschriften[20] werden durch die Richtlinie über die allgemeine Produktsicherheit[21] ergänzt, nach der alle Konsumgüter sicher sein müssen, auch wenn sie nicht unter die sektorspezifischen Rechtsvorschriften der Union fallen. Die Sicherheitsvorschriften werden durch Marktüberwachung und die Befugnisse ergänzt, die den nationalen Behörden im Rahmen der Marktüberwachungsverordnung[22] und

---

[16] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen — Schaffung von Vertrauen in eine auf den Menschen ausgerichtete künstliche Intelligenz (COM(2019) 168 final vom 8.4.2019).

[17] Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates vom 3. Dezember 2001 über die allgemeine Produktsicherheit (ABl. L 11 vom 15.1.2002, S. 4).

[18] ABl. C 136 vom 4.6.1985, S. 1.

[19] Verordnung (EG) Nr. 765/2008 und Beschluss Nr. 768/2008/EG.

[20] Dieses Schema umfasst nicht die Rechtsvorschriften der Union im Bereich Verkehr und Kraftfahrzeuge.

[21] Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates vom 3. Dezember 2001 über die allgemeine Produktsicherheit (ABl. L 11 vom 15.1.2002, S. 4).

[22] Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates (ABl. L 218 vom 13.8.2008, S. 30), ELI: http://data.europa.eu/eli/reg/2008/765/oj, und ab 2021 Verordnung (EU) 2019/1020 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über Marktüberwachung und die Konformität

der Richtlinie über die allgemeine Produktsicherheit[23] übertragen werden. Im Verkehrssektor gibt es auf Unionsebene und auf nationaler Ebene zusätzliche Vorschriften für die Inbetriebnahme von Kraftfahrzeugen[24],Luftfahrzeugen und Schiffen sowie eindeutige Vorschriften für die Sicherheit während des Betriebs, darunter die Aufgaben der Betreiber und die Überwachungsaufgaben der Behörden.

Die europäische Normung ist ebenfalls ein wesentliches Element der Produktsicherheitsvorschriften der Union. Angesichts des globalen Charakters der Digitalisierung und der neuen digitalen Technologien ist die internationale Zusammenarbeit bei der Normung von besonderer Bedeutung für die Wettbewerbsfähigkeit der europäischen Industrie.

Ein großer Teil des Rechtsrahmens der Union zur Produktsicherheit wurde vor dem Aufkommen neuer digitaler Technologien wie künstliche Intelligenz, Internet der Dinge oder Robotik verfasst. Daher enthält er nicht immer Bestimmungen, die ausdrücklich auf die neuen Herausforderungen und Risiken dieser neuen Technologien eingehen. Dass der bestehende Rechtsrahmen zur Produktsicherheit technologieneutral ist, heißt nicht, dass er nicht für Produkte gilt, die diese Technologien enthalten. Darüber hinaus wurden in späteren Rechtsakten dieses Rechtsrahmens, z. B. in den Bereichen Medizinprodukte oder Kraftfahrzeuge, bereits einige Aspekte im Zusammenhang mit dem Aufkommen neuer digitaler Technologien wie automatisierte Entscheidungen, Software als eigenständiges Produkt und Konnektivität ausdrücklich berücksichtigt.

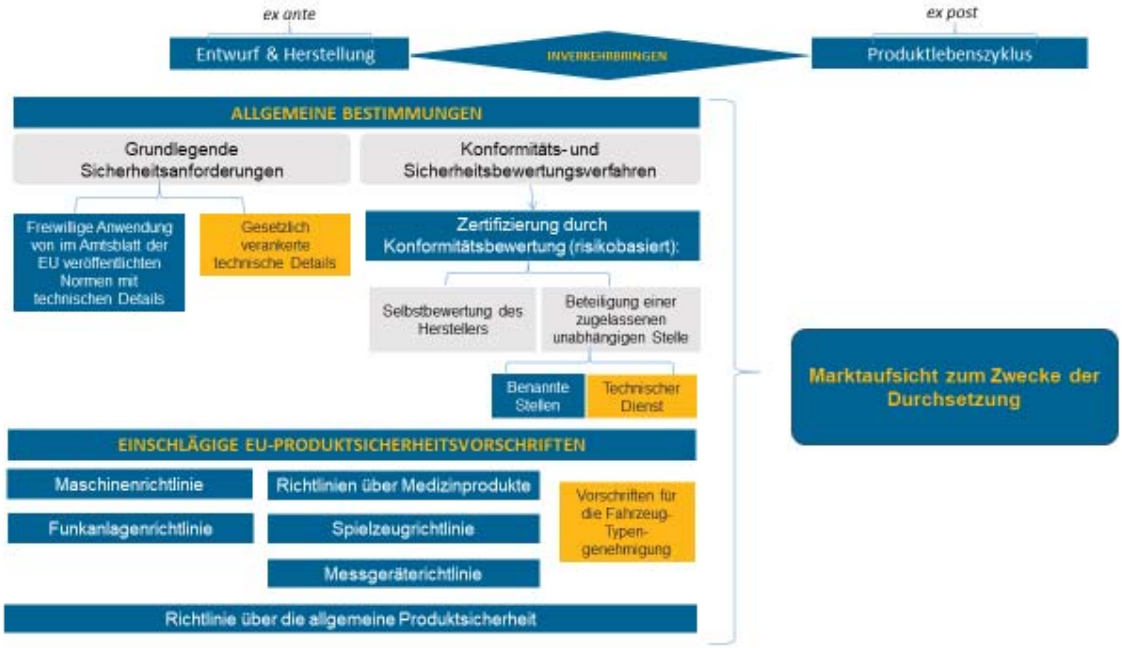
---

von Produkten sowie zur Änderung der Richtlinie 2004/42/EG und der Verordnungen (EG) Nr. 765/2008 und (EU) Nr. 305/2011 (ABl. L 169 vom 25.6.2019, S. 1), ELI: http://data.europa.eu/eli/reg/2019/1020/oj

[23] Artikel 8 Absatz 1 Buchstabe b und Absatz 3 der Richtlinie über die allgemeine Produktsicherheit.

[24] Z. B. Richtlinie 2007/46/EG zur Schaffung eines Rahmens für die Genehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge und Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates vom 30. Mai 2018 über die Genehmigung und Marktüberwachung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge, zur Änderung der Verordnungen (EG) Nr. 715/2007 und (EG) Nr. 595/2009 und zur Aufhebung der Richtlinie 2007/46/EG.

**Die den derzeitigen Produktsicherheitsvorschriften der Union zugrunde liegende Logik**[25]




Im Folgenden werden die Herausforderungen erläutert, die sich durch die neuen digitalen Technologien für den Produktsicherheitsrahmen der Union ergeben.

Ein Kernmerkmal einer stetig zunehmenden Zahl von Produkten und Dienstleistungen ist die **Konnektivität**. Konnektivität ist eine große Herausforderung für das traditionelle Sicherheitskonzept, da sie die Sicherheit des Produkts direkt beeinträchtigen und, sofern das Produkt gehackt werden kann, indirekt zu Sicherheitsbedrohungen führen und sich auf die Sicherheit der Nutzer auswirken kann.

Als Beispiel hierfür kann eine Meldung Islands[26] dienen, die über das EU-Schnellwarnsystem einging und eine intelligente Armbanduhr für Kinder betraf. Dieses Produkt würde dem Kind, das es trägt, zwar keinen direkten Schaden zufügen, da jedoch kein Mindestsicherheitsniveau gewährleistet ist, kann die Uhr leicht von Dritten dazu verwendet werden, Kontakt zu dem Kind aufzunehmen. Da eine der beabsichtigten Funktionen des Produkts darin besteht, die Sicherheit von Kindern durch Mitteilung ihres Aufenthaltsorts zu gewährleisten, würde der Verbraucher erwarten, dass das Produkt keine Sicherheitsbedrohung für Kinder darstellt, indem Dritte möglicherweise ihren Aufenthaltsort ermitteln und/oder Kontakt zu ihnen aufnehmen können.

Ein weiteres Beispiel findet sich in einer Meldung Deutschlands[27] bezüglich eines Personenkraftwagens. Es bestand der Verdacht, dass das im Fahrzeug eingebaute Radio bestimmte Software-Sicherheitslücken aufweist, die unbefugten Dritten Zugang zu den miteinander vernetzten Steuersystemen im Fahrzeug ermöglichen könnten. Würden diese Software-Sicherheitslücken von Dritten für böswillige Zwecke genutzt, könnte dies zu einem Verkehrsunfall führen.

---

[25] In diesem Schaubild sind die rechtlichen Anforderungen in Bezug auf den Lebenszyklus von Produkten (d. h. an Nutzung und Wartung) nicht berücksichtigt; es dient lediglich der allgemeinen Veranschaulichung.

[26] RAPEX-Meldung Islands (A12/0157/19) veröffentlicht auf der EU-Website „Safety Gate“.

[27] RAPEX-Meldung Deutschlands (A12/1671/15) veröffentlicht auf der EU-Website „Safety Gate“.

Auch industrielle Anwendungen, die nicht über das erforderliche Sicherheitsniveau verfügen, können Cyberbedrohungen ausgesetzt sein, die die Sicherheit von Personen in größerem Umfang beeinträchtigen. Hier wären als Beispiel Cyberangriffe auf ein wichtiges Steuersystem einer Industrieanlage zu nennen, mit denen eine Explosion ausgelöst werden soll, die Menschenleben kosten könnte.

Die Produktsicherheitsvorschriften der Union enthalten in der Regel keine spezifischen verbindlichen Grundanforderungen zur Bekämpfung von Cyberbedrohungen, die die Sicherheit der Nutzer beeinträchtigen. Allerdings gibt es Bestimmungen zu Sicherheitsaspekten in der Verordnung über Medizinprodukte[28], der Richtlinie über Messgeräte[29], der Funkanlagenrichtlinie[30] und der Richtlinie über die Genehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern[31]. Mit dem Rechtsakt zur Cybersicherheit[32] wird ein freiwilliger Rahmen für die Cybersicherheitszertifizierung von Produkten, Dienstleistungen und Verfahren der Informations- und Kommunikationstechnologie (IKT) geschaffen, während die einschlägigen Produktsicherheitsvorschriften der Union verbindliche Anforderungen enthalten.

Darüber hinaus könnte das Risiko eines Verlusts der Konnektivität bei neuen digitalen Technologien auch Sicherheitsrisiken mit sich bringen. So könnte zum Beispiel der Verlust der Konnektivität bei einem vernetzten Feuermelder dazu führen, dass der Nutzer bei einem Brand nicht alarmiert wird.

Sicherheit ist in den derzeitigen Produktsicherheitsvorschriften der Union ein Ziel im Interesse des Gemeinwohls. Das Sicherheitskonzept hängt mit der Verwendung des Produkts und den (mechanischen, elektrischen u. a.) Risiken zusammen, die bewältigt werden müssen, um das Produkt sicher zu machen. Es sei darauf hingewiesen, dass sich die Verwendung des Produkts in Abhängigkeit von der jeweiligen Produktsicherheitsvorschrift der Union nicht nur auf die bestimmungsgemäße Verwendung bezieht, sondern auch auf die vorhersehbare Verwendung und in einigen Fällen, wie in der Maschinenrichtlinie[33], auch auf die vernünftigerweise vorhersehbare Fehlanwendung.

Das mit den derzeitigen Produktsicherheitsvorschriften der Union festgelegte Sicherheitskonzept steht mit einem erweiterten Sicherheitskonzept zum Schutz von Verbrauchern und Nutzern im Einklang. Das Produktsicherheitskonzept umfasst also den Schutz vor jeglichen Risiken, die von dem Produkt ausgehen; dazu zählen nicht nur mechanische, chemische und elektrische Risiken, sondern auch Cyberrisiken und Risiken im Zusammenhang mit dem Verlust der Konnektivität von Produkten.

---

28 Verordnung (EU) 2017/745 über Medizinprodukte.
29 Richtlinie 2014/32/EU über die Bereitstellung von Messgeräten auf dem Markt.
30 Richtlinie 2014/53/EU über die Bereitstellung von Funkanlagen auf dem Markt.
31 Richtlinie 2007/46/EG zur Schaffung eines Rahmens für die Genehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge. Die Richtlinie wird mit Wirkung vom 1. September 2020 durch die Verordnung (EU) 2018/858 über die Genehmigung und die Marktüberwachung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge, zur Änderung der Verordnungen (EG) Nr. 715/2007 und (EG) Nr. 595/2009 und zur Aufhebung der Richtlinie 2007/46/EG aufgehoben und ersetzt.
32 Verordnung (EU) 2019/881.
33 Richtlinie 2006/42/EG über Maschinen.

In diesem Zusammenhang könnten für den Anwendungsbereich der einschlägigen Rechtsakte der Union explizite Bestimmungen in Betracht gezogen werden, um einen besseren Schutz der Nutzer und mehr Rechtssicherheit zu gewährleisten.

**Autonomie**[34] ist eines der Hauptmerkmale künstlicher Intelligenz. Auf künstlicher Intelligenz beruhende unbeabsichtigte Ergebnisse könnten den Nutzern und gefährdeten Personen Schaden zufügen.

Soweit das künftige „Verhalten" von KI-Produkten im Voraus durch die vom Hersteller vor dem Inverkehrbringen der Produkte durchzuführende Risikobewertung bestimmt werden kann, sind die Hersteller gemäß dem Produktsicherheitsrahmen der Union bereits jetzt verpflichtet, bei der Risikobewertung die „Verwendung"[35] der Produkte während ihrer gesamten Lebensdauer zu berücksichtigen. Ferner müssen die Hersteller Gebrauchsanleitungen und Sicherheitsinformationen für die Nutzer oder Warnhinweise bereitstellen.[36] In diesem Zusammenhang schreibt beispielsweise die Funkanlagenrichtlinie[37] vor, dass der Hersteller eine Gebrauchsanleitung mit den für die bestimmungsgemäße Verwendung der Funkanlage erforderlichen Informationen beifügen muss.

In Zukunft kann es auch Situationen geben, in denen die Ergebnisse der KI-Systeme nicht vollständig im Voraus bestimmt werden können. In solchen Situationen spiegelt die vor dem Inverkehrbringen des Produkts durchgeführte Risikobewertung möglicherweise nicht mehr die Verwendung, die Funktionsweise oder das Verhalten des Produkts wider. Wird die vom Hersteller ursprünglich vorgesehene bestimmungsgemäße Verwendung aufgrund des autonomen Verhaltens geändert und ist die Einhaltung der Sicherheitsanforderungen beeinträchtigt, so kann in diesen Fällen davon ausgegangen werden, dass eine erneute Bewertung des selbstlernenden Produkts[38] erforderlich ist.[39]

Erlangen Hersteller davon Kenntnis, dass ein Produkt während seines gesamten Lebenszyklus Risiken mit Auswirkungen auf die Sicherheit birgt, müssen sie bereits im

---

[34] KI-gestützte Produkte können zwar autonom handeln, indem sie ihre Umgebung wahrnehmen und keine vorab festgelegten Anweisungen befolgen, ihr Verhalten wird jedoch durch das ihnen vorgegebene Ziel und andere relevante konzeptionelle Entscheidungen ihrer Entwickler eingeschränkt.

[35] Gemäß den Produktsicherheitsvorschriften der Union nehmen die Hersteller die Risikobewertung auf der Grundlage der bestimmungsgemäßen Verwendung, der vorhersehbaren Verwendung und/oder der vernünftigerweise vorhersehbaren Fehlanwendung des Produkts vor.

[36] Beschluss Nr. 768/2008/EG des Europäischen Parlaments und des Rates vom 9. Juli 2008 über einen gemeinsamen Rechtsrahmen für die Vermarktung von Produkten und zur Aufhebung des Beschlusses 93/465/EWG des Rates (ABl. L 218 vom 13.8.2008, S. 82). Anhang I Artikel R2 Absatz 7 lautet: *„Die Hersteller gewährleisten, dass dem Produkt die Gebrauchsanleitung und die Sicherheitsinformationen beigefügt sind, die in einer Sprache, die von den Verbrauchern und sonstigen Endbenutzern leicht verstanden werden kann, gemäß der Entscheidung des betreffenden Mitgliedstaats zur Verfügung gestellt wird."*

[37] Artikel 10 Absatz 8 zur Gebrauchsanleitung für den Endnutzer und Anhang VI in Bezug auf die EU-Konformitätserklärung.

[38] Bisher wird der Begriff „selbstlernend" im Zusammenhang mit künstlicher Intelligenz hauptsächlich verwendet, um darauf hinzuweisen, dass Maschinen in der Lage sind, während ihres Trainings zu lernen, d. h. es wird bislang nicht vorausgesetzt, dass KI-Maschinen nach ihrer Einführung weiterlernen. Im Gegenteil werden insbesondere im Gesundheitswesen KI-Maschinen eingesetzt, die in der Regel nach erfolgreichem Abschluss des Trainings das Lernen einstellen. Daher bedeutet das autonome Verhalten von KI-Systemen zum gegenwärtigen Zeitpunkt nicht, dass das Produkt Aufgaben ausführt, die von den Entwicklern nicht vorgesehen sind.

[39] Dies steht im Einklang mit Abschnitt 2.1 des Leitfadens für die Umsetzung der Produktvorschriften der EU 2016 („Blue Guide").

Rahmen der derzeitigen Rechtsvorschriften unverzüglich die zuständigen Behörden darüber informieren und Maßnahmen ergreifen, um Risiken für die Nutzer zu vermeiden.[40]

Neben der Risikobewertung, die vor dem Inverkehrbringen eines Produkts durchgeführt wird, könnte ein neues Risikobewertungsverfahren für Produkte eingeführt werden, bei denen es während ihrer Lebensdauer zu erheblichen Änderungen kommt, z. B. zu einer Änderung der Produktfunktion, die der Hersteller in der ursprünglichen Risikobewertung nicht vorhersehen konnte. Diese Risikobewertung sollte sich auf die Auswirkungen des autonomen Verhaltens auf die Sicherheit während der gesamten Lebensdauer des Produkts konzentrieren. Sie sollte von dem betreffenden Wirtschaftsakteur durchgeführt werden. Darüber hinaus könnten die einschlägigen Rechtsvorschriften der Union strengere Anforderungen für Hersteller in Bezug auf Gebrauchsanleitungen und Warnhinweise für die Nutzer enthalten.

In den Rechtsvorschriften im Verkehrssektor[41] wurden bereits ähnliche Risikobewertungen verankert. So sehen beispielsweise die Rechtsvorschriften im Bereich des Schienenverkehrs für Änderungen an Schienenfahrzeugen nach ihrer Zertifizierung ein spezielles Verfahren vor, das vom Urheber der Änderung (dem Vorschlagenden) zu befolgen ist, sowie klare Kriterien, auf deren Grundlage festgestellt werden kann, ob ein Eingreifen der Behörde erforderlich ist.

Durch die Selbstlernfunktion von KI-Produkten und -Systemen könnte eine Maschine unter Umständen Entscheidungen treffen, die von denen abweichen, die von den Herstellern ursprünglich beabsichtigt waren und folglich von den Nutzern erwartet werden. Dies wirft Fragen hinsichtlich der menschlichen Kontrolle auf, da der Mensch entscheiden können sollte, wie und ob er Entscheidungen an KI-Produkte und -Systeme delegiert, um die von ihm gewählten Ziele zu erreichen.[42] In den bestehenden Produktsicherheitsvorschriften der Union wird auf die menschliche Aufsicht im Zusammenhang mit selbstlernenden KI-Produkten und -Systemen nicht ausdrücklich eingegangen.[43]

Als Schutzmaßnahmen können die einschlägigen Rechtsvorschriften der Union spezifische Anforderungen an die menschliche Aufsicht vorsehen, die sich von der Produktgestaltung über den gesamten Lebenszyklus der KI-Produkte und -Systeme erstrecken.

---

[40] Artikel 5 der Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates vom 3. Dezember 2001 über die allgemeine Produktsicherheit.

[41] Im Falle einer Änderung am Eisenbahnsystem, die sich auf die Sicherheit auswirken könnte (d. h. technische oder betriebliche Änderungen oder aber organisatorische Änderungen, die sich auf die Betriebs- oder Instandhaltungsprozesse auswirken können), ist das in Anhang I der Durchführungsverordnung (EU) 2015/1136 der Kommission (ABl. L 185 vom 14.7.2015, S. 6) beschriebene Verfahren anzuwenden.
Handelt es sich um eine „signifikante Änderung“ sollte dem Vorschlagenden von einer unabhängigen „Bewertungsstelle“ (der nationalen Sicherheitsbehörde oder einer anderen technisch kompetenten Stelle) ein Sicherheitsbewertungsbericht vorgelegt werden.
Im Anschluss an die Risikoanalyse wird der Vorschlagende geeignete Maßnahmen zur Risikobeherrschung ergreifen (handelt es sich bei dem Vorschlagenden um ein Eisenbahnunternehmen oder einen Infrastrukturbetreiber, so ist die Anwendung der Verordnung Teil seines Sicherheitsmanagementsystems, dessen Anwendung von der nationalen Sicherheitsbehörde überwacht wird).

[42] Policy and Investment Recommendations for Trustworthy AI (Politik- und Investitionsempfehlungen für vertrauenswürdige KI), hochrangigen Expertengruppe für künstliche Intelligenz, Juni 2019.

[43] Dies schließt jedoch nicht aus, dass aufgrund allgemeinerer Verpflichtungen in Bezug auf das Inverkehrbringen eines Produkts in bestimmten Situationen eine Aufsicht erforderlich sein kann.

Das künftige „Verhalten“ von KI-Anwendungen könnte zu **psychischen Gesundheitsrisiken**[44] für die Nutzer führen, die sich beispielsweise aus ihrer Zusammenarbeit mit humanoiden KI-Robotern und -Systemen zu Hause oder im Arbeitsumfeld ergeben. Im Allgemeinen bezieht sich der Begriff Sicherheit in diesem Zusammenhang heute auf die vom Nutzer empfundene Gefahr physischer Schäden, die von der neuen digitalen Technologie ausgehen könnte. Gleichzeitig werden sichere Produkte im Rechtsrahmen der Union als Produkte definiert, die keine oder nur geringste Risiken für die Sicherheit und Gesundheit von Personen darstellen. Es herrscht Einigkeit darüber, dass der in der Definition genannte Begriff der Gesundheit sowohl das körperliche als auch das geistige Wohlbefinden umfasst. Das Konzept der Produktsicherheit des Rechtsrahmens sollte jedoch ausdrücklich die psychischen Gesundheitsrisiken erfassen.

So sollte beispielsweise die Autonomie nicht über längere Zeiträume zu übermäßigem Stress und Unbehagen führen und die psychische Gesundheit nicht schädigen. In diesem Zusammenhang zählen zu den Faktoren, die das Sicherheitsgefühl älterer Menschen[45] positiv beeinflussen: sichere Beziehungen zum medizinischen Pflegepersonal, Kontrolle über die täglichen Routinen und Informationen darüber. Hersteller von Robotern, die mit älteren Menschen interagieren, sollten diese Faktoren berücksichtigen, um psychische Gesundheitsrisiken zu vermeiden.

Für den Anwendungsbereich der einschlägigen EU-Rechtsvorschriften könnte in Betracht gezogen werden, dass Hersteller, unter anderem von KI-gestützten humanoiden Robotern, verpflichtet werden, insbesondere den immateriellen Schaden zu berücksichtigen, den ihre Produkte vor allem bei schutzbedürftigen Nutzern wie älteren, in Pflege befindlichen Menschen verursachen könnten.

Ein weiteres wesentliches Merkmal KI-gestützter Produkte und Systeme ist ihre **Datenabhängigkeit**. Die Genauigkeit und die Relevanz der Daten sind von wesentlicher Bedeutung, um sicherzustellen, dass KI-gestützte Systeme und Produkte die vom Hersteller beabsichtigten Entscheidungen treffen.

In den Produktsicherheitsvorschriften der Union wird nicht ausdrücklich auf die Sicherheitsrisiken eingegangen, die sich aus fehlerhaften Daten ergeben. Je nach beabsichtigter Verwendung des Produkts sollten die Hersteller jedoch bereits in der Entwurfs- und in der Testphase der Datengenauigkeit und ihrer Relevanz für die Sicherheitsfunktionen Rechnung tragen.

So kann beispielsweise ein KI-gestütztes System zum Aufspüren bestimmter Gegenstände Schwierigkeiten haben, diese Gegenstände bei schlechten Lichtverhältnissen zu erkennen, sodass die Konstrukteure Daten aus Produktprüfungen berücksichtigen sollten, die sowohl in typischen als auch in schlecht beleuchteten Umgebungen durchgeführt wurden.

Ein weiteres Beispiel sind landwirtschaftliche Roboter wie Roboter für die Obsternte, die reife Früchte auf Bäumen oder am Boden entdecken und lokalisieren sollen. Während die entsprechenden Algorithmen bei der Klassifizierung bereits Erfolgsquoten von über 90 % aufweisen, kann die Verwendung mangelhafter Datensätze in diesen Algorithmen zu

---

[44] Verfassung der Weltgesundheitsorganisation (WHO), erster Aufzählungspunkt: „Gesundheit ist ein Zustand des vollständigen körperlichen, geistigen und sozialen Wohlbefindens und nicht nur das Freisein von Krankheit oder Gebrechen.“ (https://www.who.int/about/who-we-are/constitution).

[45] Social Robots: Technological, Societal and Ethical Aspects of Human-Robot Interaction (Sozialroboter: Technologische, gesellschaftliche und ethische Aspekte der Interaktion Mensch-Roboter), S. 237, Research, Neziha Akalin, Annica Kristoff ersson und Amy Loutfi, Juli 2019.

Fehlentscheidungen der Roboter und dadurch zu einer Schädigung von Mensch oder Tier führen.

Es stellt sich die Frage, ob die Produktsicherheitsvorschriften der Union spezifische Anforderungen enthalten sollten, um Sicherheitsrisiken aufgrund fehlerhafter Daten in der Entwurfsphase Rechnung zu tragen, sowie Mechanismen, um während der gesamten Nutzungsdauer der KI-Produkte und -Systeme die Aufrechterhaltung der Datenqualität zu gewährleisten.

**Opazität** ist ein weiteres wesentliches Merkmal einiger KI-gestützter Produkte und Systeme und kann dadurch entstehen, dass diese Produkte und Systeme ihre Leistung durch Lernen aus Erfahrung verbessern können. Je nach methodischem Ansatz können KI-gestützte Produkte und Systeme durch unterschiedliche Opazitätsgrade charakterisiert werden. Dies kann dazu führen, dass der Entscheidungsprozess des Systems schwer nachvollziehbar ist („Blackboxeffekt"). Der Mensch muss sicherlich nicht jeden einzelnen Schritt des Entscheidungsprozesses verstehen, doch mit der Weiterentwicklung der KI-Algorithmen und deren Einsatz in kritischen Bereichen ist es entscheidend, dass er nachvollziehen kann, wie die algorithmischen Entscheidungen des Systems getroffen wurden. Dies wäre besonders für den Ex-post-Durchsetzungsmechanismus wichtig, da die Durchsetzungsbehörden damit die Möglichkeit hätten, die Verantwortlichkeit für das Verhalten und die Entscheidungen von KI-Systemen nachzuverfolgen. Dies wird auch in der Mitteilung der Kommission über die Schaffung von Vertrauen in eine auf den Menschen ausgerichtete künstliche Intelligenz[46] anerkannt.

In den Produktsicherheitsvorschriften der Union wird nicht ausdrücklich auf die zunehmenden Risiken eingegangen, die sich aus der Opazität von auf Algorithmen beruhenden Systemen ergeben. Daher ist es notwendig, Anforderungen an die Transparenz von Algorithmen sowie an die Robustheit, die Rechenschaftspflicht und, falls erforderlich die menschliche Aufsicht sowie unverzerrte Ergebnisse[47] zu prüfen, die besonders für den Ex-post-Durchsetzungsmechanismus und für die Schaffung von Vertrauen in die Nutzung dieser Technologien wichtig sind. Eine Möglichkeit zur Bewältigung dieser Herausforderung könnte darin bestehen, die Entwickler der Algorithmen dazu zu verpflichten, bei Unfällen die Konstruktionsparameter und die Metadaten von Datensätzen offenzulegen.

Darüber hinaus kann die Sicherheit auch durch Risiken aufgrund der **Komplexität der Produkte und Systeme** beeinträchtigt werden, da sich die Funktionen verschiedener integrierbarer Komponenten, Geräte und Produkte wechselseitig beeinflussen können (z. B. Produkte, die Teil eines Smart-Home-Ökosystems sind).

Dieser Komplexität wird bereits durch den am Anfang dieses Abschnitts genannten Rechtsrahmen der Union zur Produktsicherheit[48] Rechnung getragen. Bei der Risikobewertung eines Produkts muss der Hersteller insbesondere der bestimmungsgemäßen Verwendung, der vorhersehbaren Verwendung und gegebenenfalls der vernünftigerweise vorhersehbaren Fehlanwendung Rechnung tragen.

---

46 https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top

47 Auf der Grundlage der von der hochrangigen Expertengruppe in den Ethik-Leitlinien für eine vertrauenswürdige KI vorgeschlagenen zentralen Anforderungen: https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines

48 Verordnung (EG) Nr. 2008/765 und Beschluss Nr. 768/2008/EG sowie harmonisierte sektorspezifische Produktsicherheitsvorschriften wie die Maschinenrichtlinie 2006/42/EG.

**Beabsichtigt der Hersteller also die Zusammenschaltung und Interaktion seines Geräts mit anderen Geräten, sollte dies bereits bei der Risikobewertung berücksichtigt werden.** Bei der Ermittlung von Verwendungen und Fehlanwendungen werden beispielsweise frühere Erfahrungen bei der Verwendung gleichartiger Produkte, Unfalluntersuchungen oder menschliches Verhalten herangezogen.

Auf die Komplexität der Systeme wird außerdem in sektorspezifischen Sicherheitsvorschriften wie der Verordnung über Medizinprodukte und in gewissem Umfang auch in den Rechtsvorschriften über die allgemeine Produktsicherheit[49] genauer eingegangen. So sollte beispielsweise der Hersteller eines vernetzten Geräts, das Teil eines Smart-Home-Ökosystems sein soll, vernünftigerweise vorhersehen können, dass seine Produkte Auswirkungen auf die Sicherheit anderer Produkte haben werden.

In den Rechtsvorschriften im Verkehrsbereich wird diese Komplexität darüber hinaus auf Systemebene behandelt. Bei Pkw, Zügen und Flugzeugen erfolgt die Typgenehmigung und Zertifizierung sowohl für jedes Bauteil als auch für das gesamte Fahrzeug oder Luftfahrzeug. Verkehrstauglichkeit, Lufttüchtigkeit und Eisenbahninteroperabilität sind Teil der Sicherheitsbewertung. Im Verkehrsbereich müssen „Systeme“ von einer Behörde „zugelassen“ werden, und zwar entweder auf der Grundlage einer Konformitätsbewertung durch eine unabhängige Stelle anhand eindeutiger technischer Anforderungen oder nachdem nachgewiesen wurde, wie mit Risiken umgegangen wird. Die Lösung liegt in der Regel in der Verknüpfung von Produkt- und Systemebene.

Um den Risiken zu begegnen, die sich auf die Sicherheit der Nutzer auswirken können, tragen die Produktsicherheitsvorschriften der Union, einschließlich der Rechtsvorschriften im Verkehrsbereich, in gewissen Umfang bereits der Komplexität von Produkten und Systemen Rechnung.

Komplexe Systeme arbeiten häufig mit **Software**, die ein wesentlicher Bestandteil KI-gestützter Systeme ist. Generell ist der Hersteller des Endprodukts dazu verpflichtet, im Rahmen der ersten Risikobewertung die Risiken der zum Zeitpunkt des Inverkehrbringens in dieses Produkt integrierten Software vorherzusehen.

Bestimmte Teile der Produktsicherheitsvorschriften der Union beziehen sich ausdrücklich auf die in das Produkt integrierte Software. So darf beispielsweise gemäß der Maschinenrichtlinie ein Defekt der Software der Steuerung nicht zu Gefährdungssituationen führen[50].

In den Produktsicherheitsvorschriften der Union könnten Software-Aktualisierungen mit aus Sicherheitsgründen erfolgenden Wartungsarbeiten verglichen werden, sofern mit ihnen ein bereits in Verkehr gebrachtes Produkt nicht erheblich verändert wird und keine neuen Risiken entstehen, die in der ersten Risikobewertung nicht vorhergesehen wurden. Wird jedoch mit der Software-Aktualisierung das Produkt, in dem die Software aktualisiert wird, erheblich verändert, könnte das gesamte Produkt als neues Produkt angesehen werden, und die Einhaltung der einschlägigen Sicherheitsvorschriften für das Produkt muss zu dem Zeitpunkt, zu dem die Veränderung des Produkts erfolgt, erneut geprüft werden.[51]

---

[49] Gemäß Artikel 2 der Richtlinie über die allgemeine Produktsicherheit ist bei einem sicheren Produkt „seine Einwirkung auf andere Produkte, wenn eine gemeinsame Verwendung mit anderen Produkten vernünftigerweise vorhersehbar ist“ zu berücksichtigen.

[50] Anhang I Abschnitt 1.2.1 der Maschinenrichtlinie.

[51] Leitfaden für die Umsetzung der Produktvorschriften der EU 2016 („Blue Guide“)

Für eigenständige Software, die als solche in Verkehr gebracht oder nach dem Inverkehrbringen des Produkts hochgeladen wird, enthalten die sektorspezifischen harmonisierten Produktsicherheitsvorschriften der Union im Allgemeinen keine spezifischen Bestimmungen. In einigen Rechtsvorschriften der Union, z. B. in der Verordnung über Medizinprodukte, wird jedoch auf eigenständige Software eingegangen. Darüber hinaus kann eigenständige Software, die in vernetzte, über bestimmte Funkmodule[52] kommunizierende Produkte geladen wird, mittels delegierter Rechtsakte durch die Funkanlagenrichtlinie geregelt werden. Gemäß dieser Richtlinie müssen bestimmte Klassen oder Kategorien von Funkanlagen Funktionen unterstützen, mit denen sichergestellt wird, dass die Konformität der Anlagen beim Laden von Software nicht beeinträchtigt wird.[53]

Während in den Produktsicherheitsvorschriften der Union die Sicherheitsrisiken berücksichtigt sind, die von zum Zeitpunkt des Inverkehrbringens in ein Produkt integrierter Software und möglicherweise vom Hersteller später vorgesehenen Aktualisierungen ausgehen, könnten spezifische und/oder explizite Anforderungen an eigenständige Software (z. B. eine herunterzuladende „App“) erforderlich sein. Besondere Aufmerksamkeit sollte der eigenständigen Software gewidmet werden, die in den KI-Produkten und -Systemen Sicherheitsfunktionen gewährleistet.

Außerdem könnten zusätzliche Verpflichtungen für Hersteller erforderlich sein, um sicherzustellen, dass sie Funktionen bereitstellen, mit denen während der Lebensdauer von KI-Produkten das Laden von Software verhindert wird, die die Sicherheit beeinträchtigt.

Neue digitale Technologien sind auch mit **komplexen Wertschöpfungsketten** verbunden. Diese Komplexität ist jedoch weder neu noch ausschließlich ein Aspekt, der neue digitale Technologien wie künstliche Intelligenz oder das Internet der Dinge betrifft. Sie tritt beispielsweise auch bei Produkten wie Computern, Servicerobotern oder Verkehrssystemen auf.

Unabhängig von der Komplexität der Wertschöpfungskette liegt die Verantwortlichkeit für die Sicherheit des Produkts nach dem Rechtsrahmen der Union für die Produktsicherheit bei dem Hersteller, der das Produkt in Verkehr bringt. Die Hersteller sind für die Sicherheit des Endprodukts einschließlich der in das Produkt integrierten Teile, z. B. der Software eines Computers, verantwortlich.

Einige Rechtsakte der Union zur Produktsicherheit enthalten bereits Bestimmungen, die ausdrücklich auf Situationen Bezug nehmen, in denen mehrere Wirtschaftsakteure vor dem Inverkehrbringen eines bestimmten Produkts auf dieses Einfluss nehmen. Nach der Aufzugsrichtlinie[54] muss beispielsweise der Wirtschaftsakteur, der den Aufzug entwirft und herstellt, dem Montagebetrieb[55] „*alle Unterlagen zur Verfügung stellen und alle erforderlichen Angaben machen, damit der Einbau und die Prüfung des Aufzugs ordnungsgemäß und sicher durchgeführt werden können*“. Gemäß der Maschinenrichtlinie sind die Hersteller von Geräten verpflichtet, dem Bediener Informationen darüber zur

[52] Funkmodule sind elektronische Geräte, die Funksignale (WIFI, Bluetooth) zwischen zwei Geräten übertragen und/oder empfangen.

[53] Artikel 3 Absatz 3 Buchstabe i der Funkanlagenrichtlinie.

[54] Gemäß Artikel 16 Absatz 2 der Richtlinie 2014/33/EU.

[55] In der Aufzugsrichtlinie 2014/33/EU ist der Montagebetrieb dem Hersteller gleichgestellt und muss die Verantwortung für den Entwurf, die Herstellung, den Einbau und das Inverkehrbringen des Aufzugs übernehmen.

Verfügung zu stellen, wie das jeweilige Gerät an oder auf ein anderes Gerät montiert werden kann.[56]

Die Produktsicherheitsvorschriften der Union tragen der Komplexität der Wertschöpfungsketten Rechnung, indem sie nach dem Grundsatz der „geteilten Verantwortung" mehreren Wirtschaftsakteuren Verpflichtungen auferlegen.

Während sich bei den derzeitigen komplexen Wertschöpfungsketten die Verantwortlichkeit des Herstellers für die Sicherheit des Endprodukts als angemessen erwiesen hat, könnten explizite Bestimmungen, mit denen ausdrücklich eine Zusammenarbeit zwischen den Wirtschaftsakteuren in der Lieferkette und den Nutzern gefordert wird, Rechtssicherheit in möglicherweise noch komplexeren Wertschöpfungsketten schaffen. Insbesondere würden alle Akteure innerhalb der Wertschöpfungskette, die Einfluss auf die Produktsicherheit nehmen (z. B. Softwarehersteller) und die Nutzer (durch Änderung von Produkten) ihrer Verantwortung nachkommen und dem nächsten Akteur in der Wertschöpfungskette die erforderlichen Informationen und Maßnahmen zur Verfügung stellen.

## 3. Haftung

Auf Unionsebene sind die Produktsicherheits- und die Produkthaftungsbestimmungen zwei einander ergänzende Mechanismen, mit denen dasselbe politische Ziel verfolgt wird: ein funktionierender Binnenmarkt für Waren, in dem ein hohes Sicherheitsniveau gewährleistet wird, d. h. das Risiko eines Schadens für die Nutzer minimiert und für durch fehlerhafte Waren verursachte Schäden eine Entschädigung vorgesehen ist.

Auf nationaler Ebene werden diese Unionsvorschriften durch nicht harmonisierte Rechtsrahmen zur zivilrechtlichen Haftung ergänzt, die für Schäden unterschiedlicher Ursachen (z. B. durch Produkte und Dienstleistungen) einen Schadenersatz gewährleisten und sich an verschiedene haftbare Personen (z. B. Eigentümer, Betreiber oder Dienstleistungserbringer) richten.

Auch wenn die Optimierung der Sicherheitsvorschriften der Union für künstliche Intelligenz dazu beitragen kann, Unfälle zu vermeiden, können diese dennoch eintreten. In genau diesem Fall greift die zivilrechtliche Haftung. Vorschriften zur zivilrechtlichen Haftung haben in unserer Gesellschaft eine doppelte Funktion: zum einen stellen sie sicher, dass Opfer eines von anderen verursachten Schadens eine Entschädigung erhalten, und zum anderen schaffen sie wirtschaftliche Anreize für die haftende Partei, die Verursachung eines solchen Schadens zu vermeiden. Bei Haftungsvorschriften muss stets ein ausgewogenes Verhältnis zwischen dem Schutz der Bevölkerung vor Schäden und der Ermöglichung von Innovationen für Unternehmen gefunden werden.

Die Haftungsrahmen in der Union funktionieren bisher gut. Sie stützen sich auf die parallele Anwendung der Produkthaftungsrichtlinie (Richtlinie 85/374/EWG), mit der die Haftung der Hersteller fehlerhafter Produkte harmonisiert wurde, und anderer nicht harmonisierter nationaler Haftungsregelungen.

[56] In Anhang I Abschnitt 1.7.4.2 der Maschinenrichtlinie heißt es: *„Jede Betriebsanleitung muss erforderlichenfalls folgende Mindestangaben enthalten: … i) Anleitungen zur Montage, zum Aufbau und zum Anschluss der Maschine, einschließlich der Zeichnungen, Schaltpläne und der Befestigungen, sowie Angabe des Maschinengestells oder der Anlage, auf das bzw. in die die Maschine montiert werden soll"*.

Die Produkthaftungsrichtlinie bietet Schutz auf einer Ebene, die von der nationalen verschuldensabhängigen Haftung allein nicht abgedeckt ist. Mit ihr wird ein System der verschuldensunabhängigen Haftung des Herstellers für Schäden eingeführt, die durch einen Fehler seiner Produkte verursacht wurden. Im Falle eines physischen oder materiellen Schadens hat der Geschädigte Anspruch auf Schadenersatz, wenn er den Schaden, den Fehler des Produkts (d. h. den Mangel an Sicherheit, die von der Allgemeinheit berechtigterweise erwartet werden darf) und den ursächlichen Zusammenhang zwischen dem fehlerhaften Produkt und dem Schaden nachweist.

Die nationalen, nicht harmonisierten Regelungen enthalten Vorschriften für die verschuldensabhängige Haftung, nach denen Opfer von Schäden das Verschulden der haftbaren Person, den Schaden und den ursächlichen Zusammenhang zwischen dem Verschulden und dem Schaden nachweisen müssen, um einen Haftungsanspruch erfolgreich geltend zu machen. Sie enthalten auch Regelungen für die verschuldensunabhängige Haftung, bei denen der nationale Gesetzgeber eine bestimmte Person für ein Risiko haftbar gemacht hat, ohne dass das Opfer ein Verschulden/einen Fehler oder einen ursächlichen Zusammenhang zwischen Verschulden/Fehler und dem Schaden nachweisen muss.

Nach nationalen Haftungsregelungen haben Opfer von Schäden, die durch Produkte und Dienstleistungen verursacht wurden, mehrere parallele Schadenersatzansprüche auf der Grundlage einer verschuldensabhängigen oder einer verschuldensunabhängigen Haftung. Diese Ansprüche richten sich häufig gegen verschiedene haftbare Personen und bestehen unter unterschiedlichen Voraussetzungen.

So hat ein Opfer eines Autounfalls in der Regel nach nationalen Zivilrecht einen verschuldensunabhängigen Haftungsanspruch gegen den Fahrzeughalter (d. h. die Person, die die Kraftfahrzeug-Haftpflichtversicherung abgeschlossen hat) und einen verschuldensabhängigen Haftungsanspruch gegen den Fahrer sowie außerdem, sofern das Fahrzeug einen Fehler aufweist, nach der Produkthaftungsrichtlinie einen Anspruch gegen den Hersteller.

Gemäß den harmonisierten Vorschriften für die Kraftfahrzeugversicherung muss die Nutzung des Fahrzeugs versichert sein[57], und der Versicherer ist in der Praxis immer die erste Anlaufstelle für Schadenersatzansprüche bei Personen- oder Sachschäden. Nach diesen Vorschriften leistet die Pflichtversicherung dem Geschädigten Schadenersatz und schützt den Versicherten, der nach nationalen zivilrechtlichen Vorschriften[58] dazu verpflichtet ist, für finanzielle Schäden aus einem Unfall mit dem Kraftfahrzeug aufzukommen. Für Hersteller besteht nach der Produkthaftungsrichtlinie keine Versicherungspflicht. Autonome Fahrzeuge werden im Unionsrecht in Bezug auf die Kraftfahrzeugversicherung nicht anders behandelt als nicht autonome Fahrzeuge. Für diese Fahrzeuge muss wie für alle Fahrzeuge eine Kraftfahrzeug-Haftpflichtversicherung abgeschlossen werden, die für den Geschädigten die einfachste Möglichkeit darstellt, Schadenersatz zu erhalten.

Der Abschluss einer angemessenen Versicherung kann die negativen Folgen von Unfällen mildern, da so für eine reibungslose Entschädigung des Opfers gesorgt wird. Klare Haftungsregeln helfen den Versicherungsunternehmen, ihre Risiken zu berechnen und von der letztlich für den Schaden haftenden Partei eine Erstattung zu verlangen. Wird

[57] Für Kraftfahrzeuge mit der Richtlinie 2009/103/EG über die Kraftfahrzeug-Haftpflichtversicherung und die Kontrolle der entsprechenden Versicherungspflicht harmonisiert.

[58] In den meisten Mitgliedstaaten gilt eine verschuldensunabhängige Haftung der Person, auf deren Namen das Kraftfahrzeug zugelassen ist.

beispielsweise ein Unfall durch einen Fehler verursacht, kann der Kraftfahrzeugversicherer nach Entschädigung des Opfers vom Hersteller eine Erstattung fordern.

Neue digitale Technologien wie künstliche Intelligenz, Internet der Dinge und Robotik stellen jedoch aufgrund ihrer Merkmale einige Aspekte der Haftungsrahmen der Union und der Mitgliedstaaten infrage und könnten deren Wirksamkeit verringern. Aufgrund einiger dieser Merkmale könnte es schwierig werden, einen Schaden auf menschliches Verhalten zurückzuführen, womit nach nationalen Vorschriften ein verschuldensabhängiger Haftungsanspruch begründet wäre. Das bedeutet, dass es möglicherweise zu schwierig oder zu kostspielig sein könnte, Haftungsansprüche auf der Grundlage des nationalen Deliktsrechts zu beweisen, und dass die Opfer daher unter Umständen nicht angemessen entschädigt würden. Wichtig ist, dass Opfer von Unfällen, die auf Produkte und Dienstleistungen zurückzuführen sind, an denen neue digitale Technologien wie künstliche Intelligenz beteiligt sind, keinen geringeren Schutz genießen als Opfer von Unfällen aufgrund vergleichbarer anderer Produkte und Dienstleistungen, die nach nationalem Deliktsrecht entschädigt würden. Dies könnte die gesellschaftliche Akzeptanz dieser neuen Technologien verringern und dazu führen, dass sie nur zögerlich eingesetzt werden.

Es muss geprüft werden, ob die Herausforderungen, die sich aufgrund der neuen Technologien für die bestehenden Rechtsrahmen ergeben, auch zu Rechtsunsicherheit in Bezug auf die Anwendung der bestehenden Rechtsvorschriften führen könnten (z. B. wie das Konzept des Verschuldens auf durch künstliche Intelligenz verursachte Schäden anzuwenden wäre). Dadurch könnten wiederum Investitionen behindert und die Informations- und Versicherungskosten für Hersteller und andere Unternehmen in der Lieferkette, insbesondere europäische KMU, erhöht werden. Sollten die Mitgliedstaaten schließlich die Herausforderungen für die nationalen Haftungsrahmen in Angriff nehmen, könnte dies zudem zu einer weiteren Fragmentierung führen und dadurch die Kosten für die Einführung innovativer KI-Lösungen erhöhen und den grenzüberschreitenden Handel im Binnenmarkt verringern. Es ist wichtig, dass die Unternehmen ihre Haftungsrisiken in der gesamten Wertschöpfungskette kennen, sie verringern oder verhindern können und sich wirksam gegen diese Risiken versichern.

In diesem Kapitel wird erläutert, wie die bestehenden Rechtsrahmen durch neue Technologien infrage gestellt werden und wie diese Herausforderungen angegangen werden könnten. Darüber hinaus sollte möglicherweise auch den Besonderheiten einiger Sektoren, beispielsweise des Gesundheitswesens, Aufmerksamkeit gewidmet werden.

**Komplexität von Produkten, Dienstleistungen und der Wertschöpfungskette**: Technologie und Industrie haben sich in den letzten Jahrzehnten spürbar weiterentwickelt. Insbesondere die Trennlinie zwischen Produkten und Dienstleistungen ist möglicherweise nicht mehr so klar wie bisher. Produkte und Dienstleistungen sind zunehmend miteinander verflochten. Während komplexe Produkte und Wertschöpfungsketten für die europäische Industrie und ihr Regulierungsmodell nicht neu sind, verdienen Software und auch künstliche Intelligenz im Hinblick auf die Produkthaftung besondere Aufmerksamkeit. Software ist für das Funktionieren einer Vielzahl von Produkten von wesentlicher Bedeutung und kann deren Sicherheit beeinträchtigen. Sie ist in Produkte integriert, kann aber auch getrennt bereitgestellt werden, um die bestimmungsgemäße Verwendung des Produkts zu ermöglichen. Weder Computer noch Smartphones wären ohne Software besonders nützlich. Software kann also zu einem fehlerhaften materiellen Produkt und physischen Schäden führen (siehe Kasten zur Software im Abschnitt Sicherheit). Dies könnte wiederum die Haftung des Produktherstellers im Rahmen der Produkthaftungsrichtlinie zur Folge haben.

Da Software jedoch in vielen Arten und Formen angeboten wird, ist die Einstufung von Software als Dienstleistung oder als Produkt möglicherweise nicht immer einfach. So könnte Software zur Steuerung des Betriebs eines materiellen Produkts zwar als Teil oder Bestandteil dieses Produkts angesehen werden, einige Formen eigenständiger Software könnten jedoch schwieriger einzustufen sein.

Obwohl die Begriffsbestimmung für „Produkt“ in der Produkthaftungsrichtlinie weit gefasst ist, könnte ihr Anwendungsbereich weiter präzisiert werden, um der Komplexität neuer Technologien besser Rechnung zu tragen und sicherzustellen, dass für durch fehlerhafte Produkte verursachte Schäden, die auf Software oder andere digitale Merkmale zurückzuführen sind, stets Schadenersatz gewährt wird. Dadurch könnten Wirtschaftsakteure wie Softwareentwickler besser beurteilen, ob sie als Hersteller im Sinne der Produkthaftungsrichtlinie angesehen werden können.

KI-Anwendungen sind häufig in **komplexe IoT-Umgebungen** integriert, in denen viele verschiedene vernetzte Geräte und Dienste interagieren. Die Kombination verschiedener digitaler Komponenten in einem komplexen Ökosystem und die Vielfalt der beteiligten Akteure kann es schwierig machen zu beurteilen, in welchem Fall ein potenzieller Schaden verursacht wird und wer dafür haftet. Aufgrund der Komplexität dieser Technologien kann es für die Opfer sehr schwer sein, die haftbare Person zu ermitteln und alle nach nationalem Recht erforderlichen Voraussetzungen für einen erfolgreichen Anspruch nachzuweisen. Die Kosten des Nachweises können wirtschaftlich untragbar sein und die Opfer davon abhalten, eine Entschädigung zu verlangen.

Darüber hinaus werden Produkte und Dienstleistungen auf der Grundlage von künstlicher Intelligenz mit traditionellen Technologien interagieren, was auch in Bezug auf die Haftung zu einer größeren Komplexität führt. Autonome Fahrzeuge beispielsweise werden sich eine bestimmte Zeit lang die Straße mit herkömmlichen Fahrzeugen teilen. Eine ähnliche Komplexität interagierender Akteure wird sich in einigen Dienstleistungssektoren (z. B. Verkehrsmanagement und Gesundheitswesen) ergeben, in denen teilweise automatisierte KI-Systeme die menschliche Entscheidungsfindung unterstützen werden.

Dem von der Untergruppe für neue Technologien der Expertengruppe für Haftung und neue Technologien erstellten Bericht[59] zufolge könnten Anpassungen der nationalen Rechtsvorschriften in Betracht gezogen werden, um den Opfern von Schäden im Zusammenhang mit künstlicher Intelligenz die Beweislast zu erleichtern. So könnte die Beweislast beispielsweise an die Einhaltung spezifischer rechtlicher Verpflichtungen im Hinblick auf die Cybersicherheit oder anderer Sicherheitspflichten (durch einen relevanten Betreiber) geknüpft sein. Eine Nichteinhaltung dieser Vorschriften könnte eine Änderung der Beweislast in Bezug auf Verschulden und ursächlichen Zusammenhang zur Folge haben.

Im Rahmen einer geeigneten EU-Initiative möchte die Kommission Meinungsäußerungen zu der Frage einholen, ob und in welchem Umfang es erforderlich sein könnte, die Folgen der Komplexität abzumildern, indem für Schäden, die durch den Betrieb von KI-Anwendungen verursacht werden, die in den nationalen Haftungsvorschriften vorgesehene Beweislast erleichtert oder umgekehrt wird.

[59] Liability for Artificial Intelligence and other emerging technologies' Report (Bericht über die Haftung für künstliche Intelligenz und andere neue Technologien), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

Was die Rechtsvorschriften der Union betrifft, so gilt gemäß der Produkthaftungsrichtlinie ein Produkt, das die verbindlichen Sicherheitsvorschriften nicht erfüllt, unabhängig vom Verschulden des Herstellers als fehlerhaft. Es kann jedoch auch Gründe geben, um über Möglichkeiten nachzudenken, wie die Beweislast für Opfer im Rahmen der Richtlinie erleichtert werden kann, da sich die Richtlinie auf nationale Vorschriften zur Beweislast und zur Feststellung des ursächlichen Zusammenhangs stützt.

**Konnektivität und Offenheit**: Derzeit ist nicht ganz klar, welche Sicherheitserwartungen in Bezug auf Schäden aufgrund von Cybersicherheitsverletzungen im Produkt möglicherweise bestehen und ob solche Schäden im Rahmen der Produkthaftungsrichtlinie angemessen entschädigt würden.

Schwachstellen in Bezug auf die Cybersicherheit können von Beginn an, d. h. ab dem Zeitpunkt des Inverkehrbringens eines Produkts, bestehen, oder aber zu einem späteren Zeitpunkt, also lange nach dem Inverkehrbringen des Produkts, auftreten.

Bei verschuldensabhängigen Haftungsrahmen mit eindeutigen Verpflichtungen im Hinblick auf die Cybersicherheit haben die Betreiber die Möglichkeit zu bestimmen, was sie tun müssen, um die sich aus der Haftung ergebenden Folgen zu vermeiden.

Im Rahmen der Produkthaftungsrichtlinie könnte die Frage, ob ein Hersteller unter Berücksichtigung der vernünftigerweise vorhersehbaren Verwendung des Produkts bestimmte Änderungen hätte vorhersehen können, an Bedeutung gewinnen. So könnte beispielsweise verstärkt der Rechtfertigungsgrund des später aufgetretenen Fehlers geltend gemacht werden, wonach ein Hersteller nicht haftbar ist, wenn der Fehler beim Inverkehrbringen des Produkts noch nicht vorlag, oder der Rechtfertigungsgrund des Entwicklungsrisikos, d. h., dass der Fehler nach dem damaligen Wissensstand nicht vorherzusehen war. Darüber hinaus könnte die Haftung gemindert werden, wenn der Geschädigte keine sicherheitsrelevanten Aktualisierungen vornimmt. Dies könnte potenziell als Mitverschulden des Geschädigten angesehen werden und damit die Haftung des Herstellers verringern. Da das Konzept der vernünftigerweise vorhersehbaren Verwendung und Fragen des Mitverschuldens, z. B. bei unterlassenem Herunterladen einer Sicherheitsaktualisierung, möglicherweise an Bedeutung gewinnen, könnte es für Geschädigte schwieriger werden, Schadenersatz zu erhalten, wenn die Schäden durch einen Fehler in einem Produkt verursacht wurden.

**Autonomie und Opazität:** Autonom handelnde KI-Anwendungen führen eine Aufgabe aus, ohne dass jeder Schritt im Voraus festgelegt wird, und werden in geringerem Maße oder schließlich gar nicht mehr unmittelbar durch den Menschen gesteuert oder beaufsichtigt. Algorithmen, die auf maschinellem Lernen beruhen, können schwer oder gar nicht zu verstehen sein (der sogenannte Blackboxeffekt).

Zusätzlich zu der oben erörterten Komplexität könnte es daher aufgrund des bei einigen KI-Systemen bestehenden Blackboxeffekts schwierig werden, für Schäden, die durch autonome KI-Anwendungen verursacht wurden, Schadenersatz zu erhalten. Die Notwendigkeit, den Algorithmus und die von der künstlicher Intelligenz verwendeten Daten zu verstehen, erfordert Analysekapazitäten und Fachwissen, die für die Geschädigten übermäßig teuer sein könnten. Darüber hinaus ist unter Umständen der Zugang zum Algorithmus und zu den Daten nicht ohne die Mitwirkung der potenziell haftbaren Partei möglich. In der Praxis sind die Geschädigten daher möglicherweise nicht in der Lage, einen Haftungsanspruch geltend zu machen. Zudem wäre nicht klar, wie das Verschulden einer autonom handelnden künstlichen Intelligenz nachgewiesen werden kann oder was als Verschulden einer Person anzusehen wäre, die sich auf die Verwendung von künstlicher Intelligenz verlässt.

In den nationalen Rechtsvorschriften wurde bereits eine Reihe von Lösungen entwickelt, um in ähnlichen Situationen die Beweislast der Geschädigten zu verringern.

Ein Leitprinzip der Produktsicherheit und Produkthaftung in der Union ist nach wie vor, dass die Hersteller dafür sorgen müssen, dass alle in Verkehr gebrachten Produkte während ihres gesamten Lebenszyklus sowie für ihre vernünftigerweise zu erwartende Verwendung sicher sind. Die Hersteller müssen somit gewährleisten, dass bei Produkten, in denen künstliche Intelligenz zum Einsatz kommt, bestimmte Sicherheitsparameter eingehalten werden. Die Besonderheiten künstlicher Intelligenz schließen jedoch einen Anspruch auf Sicherheitserwartungen an Produkte nicht aus, unabhängig davon, ob es sich dabei um automatische Rasenmäher oder Chirurgieroboter handelt.

Autonomie kann die Sicherheit eines Produkts beeinträchtigen, da sie die Eigenschaften des Produkts – auch seine Sicherheitseigenschaften – erheblich verändern kann. Es stellt sich die Frage, unter welchen Bedingungen sich die Haftung des Herstellers durch die Selbstlerneigenschaften verlängert und in welchem Umfang der Hersteller bestimmte Änderungen hätte voraussehen müssen.

Um zu berücksichtigen, dass sich Produkte ändern und verändert werden können, könnte der derzeit in der Produkthaftungsrichtlinie verwendete Begriff des „Inverkehrbringens“ in enger Abstimmung hinsichtlich entsprechender Änderungen im Produktsicherheitsrahmen der Union überarbeitet werden. Dies könnte auch dazu beitragen zu klären, wer für Änderungen an einem Produkt haftbar ist.

Dem von der Untergruppe für neue Technologien der Expertengruppe für Haftung und neue Technologien erstellten Bericht[60] zufolge könnte für den Betrieb einiger autonomer KI-Geräte und -Dienste in Bezug auf die Haftung ein spezifisches Risikoprofil gelten, da sie wichtige rechtliche Interessen wie Leben, Gesundheit und Eigentum erheblich schädigen und die breite Öffentlichkeit Risiken aussetzen könnten. Dies könnte vor allem KI-Geräte betreffen, die sich in öffentlichen Räumen bewegen (z. B. vollständig autonome Fahrzeuge, Drohnen[61] und Paketzustellroboter), oder KI-gestützte Dienstleistungen mit ähnlichen Risiken (z. B. Verkehrsmanagementdienste, mit denen Fahrzeuge geleitet oder gesteuert werden, oder Stromverteilungsmanagement). Die Herausforderungen, die sich durch Autonomie und Opazität für das nationale Deliktsrecht ergeben, könnten mit einem risikobasierten Ansatz in Angriff genommen werden. Mit verschuldensunabhängigen Haftungsregelungen könnte gewährleistet werden, dass Geschädigte bei Eintreten des Risikos unabhängig vom Verschulden entschädigt werden. Unter Erwägung eines risikobasierten Ansatzes muss sorgsam bewertet werden, wie sich die Entscheidung darüber, wer in solchen Fällen verschuldensunabhängig haftbar sein sollte, auf die Entwicklung und Einführung von künstlicher Intelligenz auswirkt.

Die Kommission möchte im Zusammenhang mit dem Betrieb von KI-Anwendungen mit einem spezifischen Risikoprofil Meinungsäußerungen dazu einholen, ob und inwieweit eine verschuldensunabhängige Haftung, wie sie in den nationalen Rechtsvorschriften für ähnliche für die Öffentlichkeit bestehende Risiken (z. B. für den Betrieb von Kraftfahrzeugen, Flugzeugen oder Kernkraftwerken) vorgesehen ist, erforderlich sein könnte, um mögliche

[60] Liability for Artificial Intelligence and other emerging technologies' Report (Bericht über die Haftung für künstliche Intelligenz und andere neue Technologien), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

[61] Unbemannte Luftfahrzeugsysteme gemäß der Durchführungsverordnung (EU) 2019/947 der Kommission vom 24. Mai 2019 über die Vorschriften und Verfahren für den Betrieb unbemannter Luftfahrzeuge.

Opfer wirksam zu entschädigen. Darüber hinaus möchte die Kommission Meinungsäußerungen dazu einholen, ob nach dem Beispiel der Kraftfahrzeughaftpflicht-Richtlinie eine verschuldensunabhängige Haftung mit einer Verpflichtung zum Abschluss einer verfügbaren Versicherung verbunden werden sollte, mit der unabhängig von der Zahlungsfähigkeit der haftbaren Person eine Entschädigung gewährleistet und zur Verringerung der Schadenskosten beigetragen würde.

Für den Betrieb aller anderen KI-Anwendungen, die die überwiegende Mehrheit der KI-Anwendungen ausmachen dürften, prüft die Kommission, ob die Beweislast in Bezug auf ursächlichen Zusammenhang und Verschulden angepasst werden muss. In diesem Zusammenhang wird im Bericht[62] der Untergruppe für neue Technologien der Expertengruppe für Haftung und neue Technologien unter anderem auf die Situation hingewiesen, die entsteht, wenn die potenziell haftbare Partei die für die Beurteilung der Haftung relevanten Daten nicht aufgezeichnet hat oder nicht bereit ist, sie dem Geschädigten zur Verfügung zu stellen.

## 4. Schlussfolgerung

Das Aufkommen neuer digitaler Technologien wie künstlicher Intelligenz, Internet der Dinge und Robotik birgt in Bezug auf Produktsicherheit und -haftung neue Herausforderungen wie Konnektivität, Autonomie, Datenabhängigkeit, Opazität, Komplexität von Produkten und Systemen, Softwareaktualisierungen sowie ein komplexeres Sicherheitsmanagement und komplexere Wertschöpfungsketten.

Die geltenden Produktsicherheitsvorschriften, insbesondere die Richtlinie über die allgemeine Produktsicherheit, die Maschinenrichtlinie, die Funkanlagenrichtlinie und der neue Rechtsrahmen, enthalten eine Reihe von Lücken, die geschlossen werden müssen. Die künftigen Arbeiten zur Anpassung der verschiedenen Rechtsvorschriften innerhalb dieses Rahmens werden in kohärenter und harmonisierter Weise erfolgen.

Durch die neuen Herausforderungen in Bezug auf die Sicherheit entstehen auch neue Herausforderungen im Zusammenhang mit der Haftung. Diese haftungsbezogenen Herausforderungen müssen bewältigt werden, um das gleiche Schutzniveau zu gewährleisten wie für die Opfer von Schäden durch traditionelle Technologien und dabei gleichzeitig ein ausgewogenes Verhältnis zwischen Schutz und dem Erfordernis technologischer Innovation zu wahren. Dies wird dazu beitragen, Vertrauen in diese neuen digitalen Technologien und Investitionsstabilität zu schaffen.

Grundsätzlich sind die bestehenden Haftungsvorschriften der Union und der Mitgliedstaaten auch für neue Technologien geeignet, doch könnte es aufgrund des Umfangs und der kombinierten Auswirkungen der sich durch künstliche Intelligenz ergebenden Herausforderungen schwieriger werden, Opfer von Schäden in allen Fällen, in denen dies gerechtfertigt wäre, zu entschädigen.[63] Daher kann die Verteilung der Kosten im Schadensfall nach den geltenden Vorschriften ungerecht oder ineffizient sein. Um hier Abhilfe zu schaffen und mögliche Unsicherheiten im bestehenden Rechtsrahmen zu beseitigen, könnten

[62] Liability for Artificial Intelligence and other emerging technologies' Report (Bericht über die Haftung für künstliche Intelligenz und andere neue Technologien), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

[63] Siehe den Bericht der Untergruppe für neue Technologien, S. 3, und die politische Empfehlung 27.2. der hochrangigen Expertengruppe für künstliche Intelligenz.

bestimmte Anpassungen der Produkthaftungsrichtlinie und der nationalen Haftungsregelungen durch geeignete EU-Initiativen auf der Grundlage eines gezielten, risikobasierten Ansatzes, d. h. unter Berücksichtigung der Tatsache, dass unterschiedliche KI-Anwendungen unterschiedliche Risiken bergen, in Erwägung gezogen werden.