C. Smarte Produkte im Anwendungsbereich der Produktbeobachtungspflicht

Nachdem die Grundlagen der Produktbeobachtungspflicht dargestellt wurden, soll nun der Anwendungsbereich geklärt werden, um sich der Bedeutung der Produktbeobachtungspflicht für smarte Produkte anzunähern.

I. Technikneutrale Ausgestaltung der deliktischen Produzentenhaftung

Zunächst stellt sich die Frage nach der grundsätzlichen Anwendbarkeit der deliktischen Produzentenhaftung nach § 823 Abs. 1 BGB auf Software und digitale Techniken im Allgemeinen und smarte Produkte im Besonderen. Diese ist aufgrund der technikneutralen Ausgestaltung des nationalen Deliktsrechts in den §§ 823 ff. BGB eindeutig zu bejahen.[270] Im Rahmen der Produzentenhaftung liegt dies daran, dass die Verantwortlichkeit des Herstellers nicht an eine wie auch immer geartete Produktqualität, sondern allgemein an Verkehrssicherungspflichten und die geschaffene Gefahrenlage anknüpft.[271] Welche schädigende Handlung ein nach § 823 Abs. 1 BGB geschütztes Rechtsgut konkret verletzt hat, ist nicht relevant. Insbesondere muss der Schaden nicht durch ein fehlerhaftes „Produkt" entstanden sein.[272] Aufgrund dieser handlungsbezogenen Betrachtungsweise spielt der im Rahmen des ProdHaftG relevante Streit um die Sacheigenschaft von Software keine Rolle.[273] Dort knüpft die gegenständliche Betrachtungsweise die Haftung nach § 1 ProdHaftG explizit an den Fehler eines Produkts an, das nach § 2 ProdHaftG als bewegliche Sache definiert ist. Am Wortlaut

270 *Wagner*, VersR 2020, 717 (717); *Wagner*, JZ 2023, 1 (2); *Schmid*, CR 2019, 141 (143); i.E. in Bezug auf Software schon *Reese*, DStR 1994, 1121 (1122); *Lehmann*, NJW 1992, 1721 (1723).

271 *Förster*, in: BeckOK, BGB, § 823, Rn. 687; *Spindler*, MMR 1998, 23 (24); *Wittbrodt*, InTer 2020, 74 (78); *Wagner,* in: MüKo, BGB, § 823, Rn. 1040 spricht davon, dass „der Sachbegriff [auf] den Anwendungsbereich produkthaftungsrechtlicher Prinzipien" keinen Einfluss hat und dem Produktbegriff damit keine diesbezügliche „Determinationskraft" zukommt.

272 *Schmid*, CR 2019, 141 (146).

273 Vgl. nur *Spindler*, NJW 2004, 3145 (3145); *Marly*, Praxishandbuch Softwarerecht, Rn. 1828; *Droste*, CCZ 2015, 105 (107).

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

anhaftend wäre demnach eine Verkörperung der Software zwingende Voraussetzung für die Anwendbarkeit des ProdHaftG. Vor diesem Hintergrund stellen Kombinationsprodukte aus physischem Gegenstand und embedded software aber ohne weiteres ein Produkt i.S.d § 2 ProdHaftG dar.[274] Streitig ist dies nur dort, wo Software – weil bspw. heruntergeladen – nicht verkörpert ist. Aus teleologischen Gründen wird teilweise auch hier eine Anwendung des ProdHaftG gefordert.[275] Zukünftig stellt Art. 4 Nr. 1 ProdHaftRL dagegen klar, dass auch Software unter den Produktbegriff fällt.[276] Da das ProdHaftG de lege lata eine Verantwortung des Herstellers im für diese Arbeit relevanten Zeitraum nach Inverkehrgabe aber gerade nicht kennt und de lege ferenda Software in den Produktbegriff miteinbezogen wird, soll auf diese Frage nicht weiter eingegangen werden. Für die verschuldensabhängige Haftung nach § 823 Abs. 1 BGB und das Maß an gebotenen Sicherungsvorkehrungen kommt es jedenfalls auf die Verkörperung nicht an. Entscheidend ist die begründete Gefahr für die deliktsrechtlich geschützten Rechtsgüter.[277] Auf diese von § 823 Abs. 1 BGB geschützten Rechtsgüter können reine Softwarefehler aber ebenfalls Einfluss nehmen. Denn durch die Integration von Software in physische Produkte sind zunehmend auch physische Schädigungen möglich. Vor diesem Hintergrund kann auch die Unterscheidung, ob es sich um Standardsoftware oder eine Individualsoftware handelt, keine Rolle spielen.[278] Zusammenfassend lässt sich festhalten, dass die deliktische Produzentenhaftung – und damit freilich auch die Produktbeobachtungspflicht –[279] unterschiedslos für herkömmliche (analoge) Produkte, aber auch für digitale Produkte und autonome Systeme gilt.[280]

---

274 *Wagner,* in: MüKo, BGB, § 2 ProdHaftG, Rn. 7; m.w.N. *Oechsler*, in: Staudinger, BGB, § 2 ProdHaftG, Rn. 64; mittlerweile aber skeptisch mit Blick auf die Krone-Entscheidung des EuGH (EuGH, NJW 2021, 2015), *Wagner*, NJW 2023, 1313 (1317).

275 Vgl. zum Ganzen statt aller *Wagner,* in: MüKo, BGB, § 2 ProdHaftG, Rn. 21 ff. und *Reusch*, BB 2019, 904 (905 f.); zum ProdSG *Wiebe*, NJW 2019, 625 (626).

276 Vgl. dazu *Brenner*, RDi 2024, 345 (346).

277 *Spindler*, MMR 1998, 23 (24); *Meier/Wehlau,* CR 1990, 95 (95).

278 *Voigt,* in: BeckOGK, BGB, § 823, Rn. 751; *Droste*, CCZ 2015, 105 (107); i.E. zustimmend *Lehmann*, NJW 1992, 1721 (1722 f.); auch *Wagner,* in: MüKo, BGB, § 823, Rn. 1040, der darauf hinweist, dass die Grundsätze der Produkthaftung ihre Domäne im Bereich der Güterproduktion haben und die Verkehrssicherungspflichten selbstverständlich – ggf. mit anderem Inhalt – überall dort gelten, wo Schwierigkeiten des Nachweises pflichtwidrigen Verhaltens aufgrund arbeitsteiliger Produktion bestehen; in diese Richtung auch *Foerste*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 171.

279 Speziell hierzu *Chibanguza*, in: Buck-Heeb/Oppermann (Hg.), Automatisierte Systeme, S. 407 (408 f.).

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

II. Die Bedeutung technischen Fortschritts für die Produktbeobachtungspflicht

Wurde in einem ersten Schritt festgestellt, dass die Produktbeobachtungspflicht auf smarte Produkte grundsätzlich anwendbar ist, muss in einem nächsten Schritt die Reichweite der Produktbeobachtungspflicht untersucht werden. Dabei liegt der Fokus darauf, welche nach dem Inverkehrbringen bekanntwerdenden Faktoren die Produktbeobachtungspflicht im Allgemeinen überhaupt auslösen. Konkret geht es um die Bedeutung des technischen Fortschritts bzw. von Produktverbesserungen für die Produktbeobachtungspflicht und damit für bereits vermarktete Produkte.

Praktische Bedeutung erlangt die Reichweite der Produktbeobachtungspflicht allerdings erst im Rahmen der Reaktionspflichten. Denn hinsichtlich der Produktbeobachtung i.e.S. wird stets das Produkt als Ganzes auf nach der Inverkehrgabe auftretende Produktgefahren zu beobachten sein, da der Hersteller ex ante nicht wissen kann, um welche Gefahren es sich hierbei handeln wird. Indes wird der Hersteller womöglich nicht auf alle Gefahren, die sich nach dem Inverkehrbringen im Zusammenhang mit dem Produkt zeigen, auch tatsächlich reagieren müssen.

1. Fehlerhaftigkeit bei Inverkehrgabe

Ist das Produkt bereits zum Zeitpunkt des Inverkehrbringens fehlerhaft, kann die Gefahrenquelle dem Produktionsprozess und damit der Sphäre des Herstellers zugerechnet werden, der damit eine andauernde Gefahrenquelle geschaffen hat, auch wenn sich diese erst nach dem Inverkehrbringen beim Benutzer zeigt. Als Inhaber der Bestimmungsgewalt während des Produktionsvorgangs fällt die Fehlerhaftigkeit in den Verantwortungsbereich des Herstellers, sodass sich zur Begründung der Produktbeobachtungspflicht in diesem Fall – unabhängig von der konkreten Fehlerkategorie – auf die Grundsätze der Bereichshaftung als Zurechnungsgrund abheben lässt.[281]

280 *Wagner,* in: MüKo, BGB, § 823, Rn. 1040; *Sommer*, Haftung für autonome Systeme, S. 268 f; *Littbarski*, in: Taeger/Pohle (Hg.), Computerrechts-Handbuch, Teil 18, Rn. 24; speziell in Bezug auf Roboter *Spindler*, in: *Hilgendorf* (Hg.), Robotik im Kontext von Recht und Moral, S. 63 (72); *Wiesner*, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 10.6, Rn. 49.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

Gleiches gilt für Entwicklungsfehler und Ausreißer.[282] Zwar kann dem Hersteller in beiden Fällen keine Pflichtwidrigkeit angelastet werden, allerdings entsprach das Produkt schon bei Inverkehrgabe nicht den berechtigten Sicherheitserwartungen. Aufgrund der – wenn auch zunächst nicht erkennbaren – objektiven Fehlerhaftigkeit des Produkts, geht von dem Produkt eine Gefahr aus, die wiederum auf den Herstellungsprozess zurückzuführen ist.[283] Die Verantwortlichkeit des Herstellers rührt aus der von ihm geschaffenen andauernden Gefahrenquelle, auch wenn das Sicherheitsdefizit erst in der Nutzungsphase erkennbar wird. Da im Rahmen der Bereichshaftung an die Verantwortung für die eigene Sphäre angeknüpft wird, spielt die fehlende Pflichtwidrigkeit des Verhaltens keine Rolle. Mit der herstellerseitigen Reaktion soll dem Produktnutzer dann vor Augen geführt werden, dass entgegen der ursprünglichen Erwartung das Produkt Gefahren aufweist. Weiter soll der Nutzer erstmalig in die Lage versetzt werden, eine eigene Gefahrensteuerung vornehmen zu können.[284]

2. Verschleiß

Unstreitig nicht von der Produktbeobachtungspflicht erfasst ist dagegen der gewöhnliche Verschleiß eines Produkts.[285] Gemeint sind Abnutzungserscheinungen, die sich bei längerem Gebrauch stets zeigen und daher unvermeidlich zu gefährlichen Eigenschaften der Produkte im Feld führen. Da die Beanspruchung und die damit verbundene Abnutzung der Produkte

281 Vgl. *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 177 f; allgemein schon unter B.I.3.b).

282 Zwar betreffen Ausreißer nur Einzelstücke, allerdings ist es auch hier möglich, einen Fehler noch vor Eintritt der Rechtsgutsverletzung und des Schadens zu erkennen und diese zu vermeiden. Daneben kann ein Ausreißer auch eine spezielle Charge betreffen; i.Ü. allg. Meinung, vgl. *Hager*, in: Staudinger, BGB, § 823, Rn. F 20; *Lenz*, in: Hamm (Hg.): Beck'sches Rechtsanwaltshandbuch, § 27, Rn. 101; prägnant zum Entwicklungsfehler OLG Düsseldorf, NJW-RR 1992, 284 (284); *Krause*, in: Viehweg (Hg.), Risiko – Recht – Verantwortung, S. 451 (457) sieht die Funktion der Produktbeobachtungspflicht gerade darin, die Schutzlücke bei Entwicklungsrisiken zu schließen; ähnlich *Krause*, in: Soergel, BGB, § 823 Anh. III, Rn. 25; *Pieper*, BB 1991, 985 (987) sieht bei Entwicklungsrisiken mit Blick auf die Haftungsbegründung den Hauptanwendungsbereich.

283 Vgl. *Ulmer*, ZHR 152 (1988), 564 (575).

284 Hierzu *Helte*, Anforderungen an die Produktsicherheit, S. 262.

285 *Hager*, in: Staudinger, BGB, § 823, Rn. F 20; *Voigt,* in: BeckOGK, BGB, § 823, Rn. 674.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

klassischerweise in die Nutzungsphase fallen und der Hersteller darauf keinen Einfluss hat, ist die nur begrenzte Haltbarkeit der Verantwortungssphäre des Nutzers zuzuordnen.[286] Anders ist dies nur dann, wenn der Verschleiß und die daraus resultierende Gefährlichkeit des Produkts den berechtigten Sicherheitserwartungen des Verkehrs widerspricht, sodass die Beschaffenheit des Produkts von Anfang an unzureichend war, mithin schon ein Fehler bei Inverkehrgabe vorlag.[287]

3. Entwicklungslücken und „Produktalterung"

Neben diesen unproblematischen Fällen gibt es Grenzfälle, die noch wenig Beachtung gefunden haben.[288] Hierzu zählen sowohl Entwicklungslücken als auch die „Produktalterung". Beiden Fällen ist gemein, dass das Produkt – im Gegensatz zum Entwicklungsfehler und dem Ausreißer – den historischen Sicherheitserwartungen entsprach, sodass dem Hersteller weder ein pflichtwidriges Verhalten vorgeworfen werden kann noch ein Produktfehler bei Inverkehrgabe vorlag. Die Produkte haben folglich bei Inverkehrbringen den historischen Sicherheitserwartungen entsprochen, werden nun aber aufgrund der Weiterentwicklung von Wissenschaft und Technik den gehobeneren Sicherheitsstandards nicht mehr gerecht. Lediglich in der aktuellen sicherheitstechnischen Bewertung fallen die Produkte damit durch, da sich mittlerweile aufgrund der Weiterentwicklung des Standes von Wissenschaft und Technik die Sicherheitsanforderungen verschärft haben.[289] Damit kann aber zur Begründung einer Verkehrspflicht nach Inverkehrgabe nicht auf den Zurechnungsgrund der Bereichshaftung abgestellt werden. Die Gefahr geht gerade nicht auf den Produktionsvorgang und damit auf die Sphäre des Herstellers zurück. Folglich kommt die Verantwortung des Herstellers in beiden Fällen nur unter dem Gesichtspunkt des vorangegangenen gefährlichen Tuns in Betracht.

---

286 *Lenz*, in: Lenz, Produkthaftung, § 3, Rn. 213; vgl. auch BGH, NJW 1975, 1827 (1829).

287 Zu dem dann vorliegenden Fehler bei Inverkehrgabe *Wagner,* in: MüKo, BGB, § 1 ProdHaftG, Rn. 36; *Graf v. Westphalen*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 46, Rn. 42; *Oechsler*, in: Staudinger, BGB, § 1 ProdHaftG, Rn. 84; speziell zur Produktbeobachtung *Hager*, in: Staudinger, BGB, § 823, Rn. F 20.

288 *Bachmeier*, Rechtshandbuch Autokauf, Rn. 1856 stellt die Frage nach einer Pflicht zur „Nachinformation" vor dem Hintergrund der schnellen Entwicklungszyklen bei der Fahrzeugherstellung speziell in Bezug auf den Automotive-Sektor, ohne diese allerdings zu beantworten.

289 Instruktiv mit Beispielen nochmals *Taschner*, NJW 1986, 611 (615).

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

a) Abgrenzung

Schon eine klare Abgrenzung[290] zwischen Entwicklungslücken und „bloßer Produktalterung" ist schwierig.[291] Gleichwohl soll ein Versuch in diese Richtung gewagt werden, um eine Systematisierung zu erleichtern. Entwicklungslücken liegen vor, wenn die Produktgefahr bei Inverkehrgabe schon erkennbar, aber technisch nicht vermeidbar war, das Produkt aber trotzdem aufgrund einer positiven Risiko-Nutzen-Abwägung in den Verkehr gebracht werden durfte.[292] Ein nachträglicher Erkenntnisgewinn ermöglicht dann erstmalig dieser dem Produkt inhärenten und bereits konkret ausgemachten Gefahr durch nun mögliche oder zumutbare Sicherungsmaßnahmen zu begegnen. Folglich geht es um die nachträgliche Generierung erstmaligen Gefahrenvermeidungswissens bei bekannter Gefahrenlage. Von Entwicklungslücken dürften daher primär Neuentwicklungen betroffen sein, bei denen sich Sicherungsmaßnahmen noch nicht herausentwickelt haben. Dagegen soll unter Produktalterung die aufgrund neuer Erkenntnisse mögliche Optimierung bereits bestehender Sicherheitsmaßnahmen verstanden werden, die nicht zwangsläufig an eine bereits bekannte Gefahr geknüpft ist. Es geht damit um die Anpassung an ein nunmehr verschärftes Sicherheitsniveau, welches sich aus dem Prozess kontinuierlicher Produktentwicklung und -verbesserung sowie aus der nachträglichen Anhebung technischer Normen ergeben kann.[293] Beispielhaft unterliegen Fahrerassistenzsysteme einer stetigen technischen Entwicklung, durch welche die Funktionen und Einsatzbereiche kontinuierlich zunehmen.[294]

b) Keine Fehlerhaftigkeit durch spätere Produktverbesserung

Speziell § 3 Abs. 2 ProdHaftG stellt klar, dass eine Produktverbesserung, also technischer Fortschritt und die dadurch erhöhten Sicherheitsanforderungen, nicht dazu führen, dass ein einmal fehlerfrei in den Verkehr

290 Begrifflich scheint eine solche Abgrenzung *Lenz*, in: Lenz, Produkthaftung, § 3, Rn. 332 vorzunehmen.

291 Krit. bzgl. der Praxistauglichkeit daher *Tamme*, Rückrufkosten, S. 174 f., vgl. dann aber S. 176.

292 Vgl. bereits unter B.II.6.

293 *Riehm/Leithäuser/Brenner*, in: Raue (Hg.), Digitale Resilienz, S. 5 (20) sprechen von „evolvierende[n] Sicherheitsanforderungen".

294 Beispiel nach *Hammel*, Haftung und Versicherung bei Pkw, S. 453 f.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

gebrachtes Produkt nachträglich fehlerhaft werden kann. Daneben lässt sich auch aus § 1 Abs. 2 Nr. 5 und § 3 Abs. 1 lit. c ProdHaftG ein haftungsbegrenzendes Prinzip entnehmen, dass sich eine nachträgliche Verschärfung des einzuhaltenden Sicherheitsniveaus nicht auf bereits in den Verkehr gebrachte Produkte auswirkt.[295] Über die ex ante vorzunehmende Statuierung der Verkehrssicherungspflichten gilt dies auch im Rahmen der deliktischen Produzentenhaftung. Fraglich ist allerdings, ob sich aus diesen Feststellungen bereits eine Aussage über möglicherweise zu treffende Reaktionsmaßnahmen des Herstellers hinsichtlich der schon vermarkteten Produkte treffen lässt.

Zum Teil wird angeführt, dass die Wertung des § 3 Abs. 2 ProdHaftG auch nicht über die Produktbeobachtungspflicht nach § 823 Abs. 1 BGB konterkariert werden dürfe, indem dem Hersteller die Pflicht aufgegeben wird, Produktnutzer über spätere Verbesserungen der Sicherheitstechnik zu informieren und eine Umrüstung anzuregen.[296] Ein solches Verständnis greift allerdings schon im Ausgangspunkt zu kurz. Denn nach dem ausdrücklichen Willen des nationalen Gesetzgebers bei der Umsetzung der Produkthaftungsrichtlinie sollte § 3 Abs. 2 ProdHaftG die Grundsätze zur Produktbeobachtungspflicht unbeeinflusst lassen.[297] Damit ist der Anwendungsbereich der Produktbeobachtungspflicht autonom zu bestimmen. Bereits deswegen kann aus § 3 Abs. 2 ProdHaftG nicht gefolgert werden, dass der Hersteller bei nachträglich eingetretenen Sicherheitsverbesserungen gleich welcher Art nicht reagieren muss.[298] Hinzu kommt, dass es sich bei § 3 Abs. 2 ProdHaftG um eine Vorschrift handelt, welche im Rahmen der Beweiswürdigung Bedeutung erhält.[299] Sie soll bewirken, dass allein aus dem Nachweis eines verbesserten Produkts auf dem Markt nicht der Schluss gezogen werden kann, dass das Produkt ursprünglich fehlerhaft war. Bei der Bestimmung der historischen Sicherheitserwartungen zum Zeitpunkt des Inverkehrbringens gilt es allgemein solche Rückschaufehler zu vermeiden.[300] Indes ist die Produktbeobachtungspflicht zukunftsgerichtet. Es geht darum, den Eintritt von Schäden zu verhindern. Damit

295 *Wagner,* in: MüKo, BGB, § 3 ProdHaftG, Rn. 38; *Lenz*, in: Lenz, Produkthaftung, § 3, Rn. 320.
296 So *Wagner,* in: MüKo, BGB, § 3 ProdHaftG, Rn. 38.
297 Vgl. BT-Drs. 11/2447, S. 18.
298 So auch *Oechsler*, in: Staudinger, BGB, § 3 ProdHaftG, Rn. 82.
299 Vgl. *Graf v. Westphalen*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 48, Rn. 76.
300 Hierzu allgemein *Wagner,* in: MüKo, BGB, § 823, Rn. 963.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

können aber aus der Tatsache, dass eine Produktverbesserung die historischen Sicherheitserwartungen unberührt lässt, keine Schlüsse hinsichtlich einer zukunftsgerichteten Pflicht gezogen werden. Insoweit sind die Anknüpfungspunkte schlicht andere.[301]

c) Abgrenzung der Verantwortungsbereiche

Möglicherweise kann obigem Argument aber auch unter autonomer Bestimmung des Anwendungsbereichs der Produktbeobachtungspflicht zugestimmt werden. Dies wäre dann der Fall, wenn andernfalls die allgemeine Abgrenzung der Verantwortungsbereiche konterkariert würde. Immerhin handelt es sich um Fälle, bei denen der Hersteller zum Zeitpunkt der Inverkehrgabe alles Erforderliche und Zumutbare getan hat und das Produkt den damaligen Sicherheitserwartungen entsprach. Da dem Hersteller weder ein Sorgfaltspflichtenverstoß angelastet werden kann noch das Produkt in einer Ex-post-Perspektive als fehlerhaft einzustufen ist (im Unterschied zum Entwicklungsfehler),[302] spricht zunächst viel dafür, die in der Nutzungsphase eintretenden verschärften Sicherheitsanforderungen auch dem Verantwortungsbereich des Produktnutzers zuzuordnen.

aa) Vergleichsüberlegung: Kombinationsgefahren

Allerdings kann die Produktbeobachtungspflicht auch Fälle umfassen, in denen ein (auch ex post betrachtet) fehlerfreies Produkt in den Verkehr gebracht wurde. Dies betrifft die vom BGH vorgenommene Erstreckung der Produktbeobachtungspflicht auf Kombinationsgefahren in der Honda-Entscheidung.[303]

Unter Kombinationsgefahren sind solche Risiken und Fehler zu verstehen, die sich erst aus der Kombination des eigenen Produkts mit einem fremden Zubehörteil ergeben, das ohne Wissen und Wollen des Herstellers des Hauptprodukts in den Verkehr gebracht wurde. Hier treffen zwei für sich genommen ungefährliche Produkte aufeinander, die erst in ihrer

301 Wohl auch *Graf v. Westphalen*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 48, Rn. 77.
302 *Pieper*, BB 1991, 985 (987) spricht vom „ex post-Mangel".
303 BGH, NJW 1987, 1009.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

Kombination eine Gefahr begründen.[304] Auch wenn in diesem Fall die Gefahr nicht durch den Hersteller des Hauptprodukts, sondern durch die Kombination mit dem Produkt eines Dritten verursacht wird, soll der Verantwortungsbereich des Herstellers des Hauptprodukts eröffnet sein.[305] Die Produktbeobachtungspflicht erstreckt sich somit auch auf Gefahren, die sich aus der Kombination des eigenen Produkts mit Produkten anderer Hersteller ergeben können. Diese Haftungserstreckung soll für Zubehör gelten, das für die Funktionsfähigkeit des Hauptprodukts notwendig ist oder vom Hersteller empfohlen wurde und daneben auch für Zubehör, dessen Verwendung durch Vorrichtungen vom Hersteller vorgesehen ist. Ferner sah es der BGH für die Haftungserstreckung als ausreichend an, dass das Zubehör allgemein gebräuchlich ist.[306]

Diese Ausdehnung aber allein damit zu begründen, dass der Hersteller ohnehin dazu angehalten ist, all seine Produkte zu beobachten, würde einer sorgfältigen Abgrenzung der Verantwortungsbereiche nicht gerecht.[307] Denn Erwägungen der Zumutbarkeit können die Gefahrschaffung als unumstößliches Abwägungskriterium bei der Begründung von Verkehrspflichten nicht ersetzen.[308] Daher wird der Grund für die Haftungserstreckung darin gesehen, dass der Hersteller durch die Inverkehrgabe seines eigenen Produkts den Anlass zu einer Kombination mit dem Zubehör gesetzt hat.[309] Betrachtet man die Rechtsprechung zu den Kombinationsgefahren, so lässt sich eine Verantwortung des Herstellers jedenfalls dort ableiten, wo er das Zubehör eigens empfohlen hat oder Vorrichtungen für das Zubehör am eigenen Produkt vorgehalten hat. Denn dadurch hat er die Geeignetheit für Komplementärprodukte signalisiert und einen eigenen nennenswerten Beitrag zur Gefahrenschaffung geleistet. Handelt es sich um notwendiges

304 Vgl. auch *Hartmann*, Der Warenhersteller im Spannungsfeld, S. 46, 63 f.

305 *Klinger*, Die Produktbeobachtungspflicht bezüglich Fremdzubehörteilen, S. 18 sieht darin eine Entfernung von dem ursprünglich die Produktbeobachtungspflicht auslösenden Faktor der Gefahrerhöhung. Denn der Hersteller habe keinerlei Einfluss auf die Inverkehrgabe eines gänzlich fremden Zubehörs; hieran angelehnt wird die Produktbeobachtungspflicht auch bei Produktfälschungen diskutiert, vgl. *Hornung/Fuchs*, PharmR 2012, 501 (508 f.); *Hager*, in: Staudinger, BGB, § 823, Rn. F 21; *Voigt,* in: BeckOGK, BGB, § 823, Rn. 641.

306 Hierzu BGH, NJW 1987, 1009 (1010 f.); *Wagner,* in: MüKo, BGB, § 823, Rn. 1099.

307 *Voigt,* in: BeckOGK, BGB, § 823, Rn. 678.

308 *Ulmer*, ZHR 152 (1988), 564 (579).

309 *Hartmann*, BB 2012, 267 (268); *Hornung/Fuchs*, PharmR 2012, 501 (509): „Das Ersatzteil wird aber nur deshalb produziert – und entfaltet seine Gefährlichkeit nur deshalb –, weil das Originalprodukt angeboten wird." *Ulmer*, ZHR 152 (1988), 564 (576 f.) unter Zugrundelegung der Herausforderungsdogmatik.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

Zubehör, kann argumentiert werden, dass das Produkt nur sinnvoll im Zusammenspiel mit anderen Produkten eingesetzt werden kann und der Hersteller daher mit Blick auf die zwingende Vervollständigung in erhöhtem Maße verantwortlich ist. In beiden Fällen lässt sich die Gefahr damit wieder auf den Produktionsprozess und die Sphäre des Herstellers zurückführen, sodass die Bereichshaftung als Zurechnungsgrund betroffen ist.

Schwierig wird es allerdings dort, wo das Zubehör lediglich aufgrund entsprechender Verbrauchergewohnheiten allgemein gebräuchlich ist, ohne dass der Hersteller irgendeinen konkreten Anlass zum Einsatz des Zubehörteils gegeben hätte.[310] Damit lässt sich die Gefahr aber nicht auf einen Umstand zurückführen, der der Bestimmungsgewalt des Herstellers unterliegt. Der Zurechnungsgrund der Bereichshaftung greift folglich nicht. Zur Begründung der Produktbeobachtungspflicht des Herstellers in diesem Fall kann auch nicht auf das allgemeine Vertrauen abgestellt werden, das der Nutzer dem Hersteller auch nach der Inverkehrgabe entgegenbringt.[311] Denn außerhalb der Bereichshaftung muss sich ein vorangegangenes Tun als gefährlich darstellen, um einen Zurechnungsgrund darstellen zu können. Andernfalls würde das Kriterium an Konturschärfe verlieren. Würde man allein das Inverkehrbringen eines Produkts für sich schon als in diesem Zusammenhang relevante Gefahrschaffung ansehen, würde letztlich auf das Kriterium der Gefahrenschaffung verzichtet,[312] da diese Gefahr nicht über das allgemeine Lebensrisiko hinausgeht. Zwischen dem Inverkehrbringen des Hauptprodukts und der Beobachtung des Zubehörs fehlt es damit aber an einem inneren, pflichtenbegründenden Zusammenhang.[313] Als Kriterium scheint unter Vernachlässigung der Gefahrenschaffung vordergründig auf die Vorhersehbarkeit abgestellt zu werden.[314] Richtig ist, dass der Hersteller – ähnlich wie im Rahmen der Konstruktions- und Instruktionspflichten zum Ausschluss naheliegenden Fehlgebrauchs – aufgrund der eigenständigen Produktgestaltung über

310 Zum Ganzen *Foerste*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 25, Rn. 179 ff.; *Hartmann*, Der Warenhersteller im Spannungsfeld, S. 55 f.

311 So aber *Klinger*, Die Produktbeobachtungspflicht bezüglich Fremdzubehörteilen, S. 69.

312 So zu Recht *Hartmann*, Der Warenhersteller im Spannungsfeld, S. 59; vgl. auch *Voigt*, in: BeckOGK, BGB, § 823, Rn. 678.

313 So *Foerste*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 25, Rn. 222; *Kunz*, BB 1994, 450 (451) lässt es dagegen ausreichen, dass das Hauptprodukt zumindest auch die Gefahrenquelle bildet und der Hersteller diese durch Inverkehrgabe geschaffen hat.

314 Zur Vorhersehbarkeit als Kriterium auch *Hauke/Kremer*, PharmR 2013, 213 (218).

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

die umfassendsten Erkenntnisse verfügt, die es ermöglichen, allgemein gebräuchliche Kombinationen zu antizipieren. Eine so verstandene Ausdehnung der Produktbeobachtungspflicht stellt gleichwohl eine Friktion mit der tradierten, an der Gefahrenschaffung orientierten Abgrenzung der Verantwortungsbereiche dar.[315] Trotz der existierenden und hinsichtlich der Produktbeobachtungspflicht bzgl. Zubehörteilen auch zu beachtenden Rechtsprechung, lassen sich hieraus keine verallgemeinerungsfähigen Grundsätze ableiten.

bb) Vergleichsüberlegung: Fehlgebrauch

Ähnlich schwierig beurteilt sich die Erstreckung der Verantwortung des Herstellers auf einen etwaigen Fehlgebrauch im Feld.[316] Dabei sind nicht solche Fälle gemeint, bei denen der Hersteller die Nutzer in einer bestimmten Art über die Gefahren einer Verwendung nicht instruierte, weil die mit dieser Verwendungsart verbundenen Produktgefahren nach dem Stand von Wissenschaft und Forschung zum Zeitpunkt des Inverkehrbringens noch nicht erkennbar waren. Hier liegt ein einfacher Entwicklungsfehler vor. Vielmehr geht es um Fälle, bei denen sich das tatsächliche Nutzerverhalten anders darstellt als damit zu rechnen war; wenn es also trotz pflichtgemäßer Instruktion aufgrund bestimmungswidrigen Gebrauchs oder aufgrund veränderter Vorstellungen der Nutzer über den Verwendungszweck zu Gefahren kommt, die in Häufigkeit oder Ausmaß nicht vorherzusehen waren.

Aus dem Gesagten ergibt sich zunächst, dass der Fehlgebrauch nicht dem Verantwortungsbereich des Herstellers unterfällt. Die Herstellerverantwortung wird gleichwohl mit der Entwicklungsfähigkeit der Nutzer begründet. Je mehr Nutzer ein Produkt missbräuchlich verwenden und dabei davon ausgehen, dieses Verhalten sei gerechtfertigt, desto eher wandelt sich der Missbrauch in eine dem Hersteller zuzurechnende vorhersehbare Verwendung.[317] Sollte der Fehlgebrauch bei Inverkehrgabe tatsächlich nicht als der-

315 Dies erkennt auch *Klinger*, Die Produktbeobachtungspflicht bezüglich Fremdzubehörteilen, S. 27 an.

316 Bereits angedeutet BGH, NJW 1981, 1606 (1607 f.) und BGH, NJW 1981, 1603 (1604); *Veltins*, in: Moosmayer/Lösler (Hg.), Corporate Compliance, § 35, Rn. 14; *Reusch*, BB 2017, 2248 (2250); *Hornung/Fuchs*, PharmR 2012, 501 (508); BGH, NJW 1992, 560 (562).

317 So explizit *Reusch*, BB 2017, 2248 (2250); ähnlich *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 248; i.E. wohl auch *Foerste*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 309.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

art naheliegend erkennbar gewesen sein, lässt sich aber eine argumentative Nähe zum Entwicklungsfehler herstellen und daher die Verantwortlichkeit des Herstellers nach dem Inverkehrbringen begründen. Denn die herstellerseitige Instruktion bei Inverkehrgabe erweist sich in der Rückschau als nicht ausreichend. Damit aber wurden die berechtigten Sicherheitserwartungen bereits bei Inverkehrgabe unterschritten und es lassen sich keine Vergleichsüberlegungen zu den hier interessierenden Konstellationen ziehen.

cc) Verantwortungsbereich und eigene Verkehrssicherungspflichten des Nutzers

Mit dem Verweis darauf, dass die Fehlerkategorie zwar keine Rolle spiele, solange der Fehler nur aus dem Bereich des Herstellers stamme,[318] wird jedenfalls insinuiert, dass nur das Unterschreiten der berechtigten Sicherheitserwartung bei Inverkehrgabe als Ursache aus dem Bereich des Herstellers angesehen werden könne und Voraussetzung für eine nachgelagerte Produktbeobachtungspflicht sein könne.[319] Umgekehrt und in der Konsequenz lägen damit Änderungen der Sicherheitserwartung oder die Verschärfung technischer Normen aufgrund von Produktverbesserungen gerade außerhalb des Bereichs des Herstellers und wären diesem nicht zuzurechnen. In diese Richtung geht auch die amtliche Begründung zum Vorschlag der (alten) Produkthaftungsrichtlinie. Demnach bestehe in Fällen, in denen Sicherheitsvorschriften nachträglich verschärft worden sind, die Produkte bei Inverkehrgabe aber den bestehenden Normen entsprochen haben, „grundsätzlich keine Verpflichtung des Herstellers, alle älteren Produkte zurückzuziehen. Wer Produkte verwendet, die neueren Sicherheitsvorschriften nicht mehr genügen, handel[e] auf eigene Gefahr".[320] Wiederum ist die Regelung des § 3 Abs. 2 ProdHaftG angesprochen. Sofern allerdings auf die unterschiedlichen Verantwortungsbereiche abgestellt wird, lässt sich die Argumentation übertragen.

In diesem Zusammenhang darf nicht vergessen werden, dass der Produktnutzer mit der Verwendung des Produkts ebenfalls eine Gefahrenquel-

318 So *Hager*, in: Staudinger, BGB, § 823, Rn. F 20; ähnlich *Voigt,* in: BeckOGK, BGB, § 823, Rn. 674.

319 Explizit anderer Meinung in Bezug auf die Produktbeobachtungspflicht in Österreich *Sessa-Jahn*, Automatisiertes Fahren, S. 144.

320 Siehe unter BT-Drs. 7/5812, S. 8.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

le schafft bzw. andauern lässt und ihn daher gegenüber Dritten oder der Allgemeinheit auch die allgemeinen und Jedermann obliegenden Verkehrssicherungspflichten treffen können.[321] In diesem Rahmen hatte die Rechtsprechung bereits mehrfach Gelegenheit, sich zur Frage der Nachrüstung durch den Betreiber oder Nutzer aufgrund im Laufe der Zeit verschärfter Sicherheitsanforderungen zu äußern.[322] Im Ausgangspunkt hat der Nutzer jedenfalls diejenige Sicherheit zu gewährleisten, die der historischen Sicherheitserwartung zum Zeitpunkt der Herstellung entsprach.[323] Darüber hinaus kann es aber gemessen an den aktuellen Sorgfaltsanforderungen zu Absenkungen des Sorgfaltsmaßstabs kommen. Dies wird damit begründet, dass zum einen Nachrüstungen im Vergleich zur konstruktiven Berücksichtigung bereits im Herstellungsprozess deutlich teurer seien. Zum anderen damit, dass der Verkehr – jedenfalls dann, wenn das ältere Produkt ersichtlich als solches erkennbar ist – vernünftigerweise nicht erwarten könne, den aktuellen Sicherheitsstandard geboten zu bekommen und daher eigens erweiterte Selbstschutzmaßnahmen ergreifen müsse.[324] Andererseits kann eine Anpassung an die aktuellen Sicherheitsanforderungen geboten sein, um naheliegende Gefahren für die Rechtsgüter anderer abzuwenden.[325] Gleiches gilt, wenn die nunmehr geltenden technischen Normen eine Nachrüstung oder Stilllegung vorsehen.[326] Maßgebend ist – und das machen diese Entscheidungen deutlich – erneut die Zumutbarkeit der Maßnahmen, die von den Kosten und dem Umfang des dadurch erzielten Sicherheitsgewinns abhängt.

Nutzer und Betreiber können folglich in der Pflicht sein, Sicherungsvorkehrungen an neueste Erkenntnisse anzupassen.[327] Die Tatsache, dass der Nutzer zu solchen Anpassungsmaßnahmen verpflichtet sein kann, lässt aber noch nicht den Schluss zu, dass der Hersteller völlig aus der

321 Instruktiv *Foerste*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 27, Rn. 1, 17.
322 Vgl. nur LG Bonn, VersR 1988, 1268; OLG Hamm, VersR 1997, 200; OLG, Frankfurt, MDR 2013, 592 (593); BGH, NJW 2010, 1967 (1968).
323 OLG, Frankfurt, MDR 2013, 592 (593).
324 Dazu *Wagner,* in: MüKo, BGB, § 823, Rn. 549 ff. und OLG Hamm, VersR 1997, 200; vgl. auch LG Bonn, VersR 1988, 1268.
325 Vgl. BGH, NJW 2010, 1967 (1968).
326 OLG, Frankfurt, MDR 2013, 592 (593).
327 Vgl. auch *Spindler*, in: *Hilgendorf* (Hg.), Robotik im Kontext von Recht und Moral, S. 63 (71).

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

Verantwortung genommen ist.[328] In diesem Kontext scheint es angezeigt, zwischen der Frage des „Ob" der Reaktion und des „Wie" der Reaktion zu unterscheiden und die Frage nach dem „Ob" nicht vorschnell zu verneinen. Denn Verantwortungsbereiche können sich auch überschneiden. Möglicherweise ist der Hersteller daher zumindest gehalten, den Produktnutzer auf eine nunmehr vorhandene serienreife sicherheitstechnisch überlegene Alternative hinzuweisen.[329]

d) OLG München zur Produktverbesserung

Interessant ist in diesem Zusammenhang eine Entscheidung des OLG München, welche sich ausdrücklich mit den Verkehrspflichten des Herstellers bei nachträglicher Produktverbesserung auseinandersetzt.[330]

Konkret ging es um eine manuelle Zentralverriegelung eines Autos, welche bei Inverkehrgabe dem Stand der Wissenschaft und Technik entsprach, sich mittlerweile aufgrund der Möglichkeit der Verriegelungsautomatik aber als überholt darstellte. Das Gericht lehnte eine auf die Produktbeobachtungspflicht gestützte Hinweispflicht des Herstellers auf die nunmehr mögliche Umprogrammierung der Verriegelungssystematik ab. Begründet wurde dies damit, dass es sich bei der Möglichkeit der Optimierung lediglich um eine Funktionsänderung mit in erster Linie einhergehendem Komfortgewinn handelte. Weiter wurde ausgeführt, dass ein Hersteller schlicht überfordert wäre, müsste er das gesamte Kundenverhalten analysieren, um zu ermitteln, in welchen einzelnen unbedeutenden Punkten eine Aufrüstung des Fahrzeugs für den Kunden infrage kommt. Auch hätte der Kunde bereits bei Erwerb auf eine automatische Verriegelung eines Konkurrenzmodells zurückgreifen können.

Mit Referenz auf diese Entscheidung eine Reaktionspflicht des Herstellers bei Produktverbesserungen pauschal abzulehnen, greift indes zu

328 Ähnlich *Huber*, Rechtsfragen des Produktrückrufs, S. 169; anders wohl *Molitoris/Klindt*, NJW 2012, 1489 (1495), die die Entscheidung BGH, NJW 2010, 1967 dahingehend verallgemeinern, dass „Gefahren, die von Produkten allein wegen „Veraltung" ausgehen […] deshalb gerade nicht mehr vom Pflichtenkreis des Herstellers umfasst werden".

329 So *Huber*, Rechtsfragen des Produktrückrufs, S. 169.

330 OLG München, VersR 2004, 866.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

kurz.[331] Denn lehrreich ist diese Entscheidung weniger mit dem, was sie sagt, als mit dem, was sie nicht sagt. Bei genauerer Betrachtung – und darauf wird die Begründung auch zu Recht gestützt – geht es nämlich nicht um eine Produktverbesserung im Rahmen der Produktsicherheit, sondern lediglich um eine Komfortsteigerung. Denn der Schutz vor unberechtigtem Zugriff von außen war auch bei der manuellen Technik gewährleistet. Im Ergebnis kann der Entscheidung daher nur beigepflichtet werden. Alles andere hätte zur Folge, dass die Hersteller über jeden einzelnen Innovationsschritt informieren müssten.[332] Dass die Frage des Einschreitens des Herstellers auch anders ausfallen kann, wird in der Entscheidung selbst angemerkt. So könne beim Hinzutreten weiterer Umstände die Produktbeobachtungspflicht verletzt sein.[333] Dabei braucht es wenig Fantasie, sich diese weiteren Umstände vorzustellen. Man denke daran, dass es sich nicht um eine bloße Komfortsteigerung handele, sondern um eine echte Sicherheitsbereicherung, noch dazu bzgl. einer Produktgefahr hinsichtlich derer der Nutzer keine andere Erwerbsentscheidung hatte, derer er also zwangsläufig – wenn auch aufgrund eigener Risikoentscheidung – ausgesetzt war.

e) Anwendung auf die Entwicklungslücke

Unter Berücksichtigung der eben dargestellten Herleitungen, könnte bei Entwicklungslücken allein der Verantwortungsbereich des Nutzers eröffnet sein. Denn hinsichtlich der bekannten, aber nicht zu vermeidenden Restgefahren musste der Hersteller bereits bei Inverkehrgabe warnen. Damit aber waren die Gefahren dem Nutzer bekannt und er erwarb das Produkt im Bewusstsein einer Nutzen-Risiko-Abwägung. Vor diesem Hintergrund wird vertreten, dass die eigene Risikoabwägung des Nutzers, welche durch die Instruktion bei Inverkehrgabe ermöglicht wurde, auch zu einer Verantwortungszuweisung an den Nutzer führe.[334] Daher sei es auch allein an diesem,

331 So aber *Wagner,* in: MüKo, BGB, § 3 ProdHaftG, Rn. 38, wobei aber zweifelhaft ist, ob er nicht nur die Produktalterung meint; als Teil der Argumentation auch *Helte*, Anforderungen an die Produktsicherheit, S. 263.

332 So zu Recht auch *Helte*, Anforderungen an die Produktsicherheit, S. 263.

333 OLG München, VersR 2004, 866 (Ls.).

334 *Helte*, Anforderungen an die Produktsicherheit, S. 262; in der Folgerung unklar *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 289, der allenfalls eine Warnpflicht bei gravierenden Gefahren für Leib und Leben annimmt und die Gefahrenabwehr-

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

sich Informationen über die weitere technische Entwicklung einzuholen und anhand dieser erneut zu entscheiden, ob weiter das gefahrbehaftete Produkt benutzt oder auf die überlegene Sicherheitstechnik umgestiegen werden soll.[335] Das Argument der Verantwortungszuweisung ist dabei gerade im Vergleich zu den Entwicklungsfehlern nicht von der Hand zu weisen. Das Gefahrenlevel wurde bei der Entwicklungslücke vom Nutzer beim Erwerb des Produkts als vertretbar eingestuft. Diese Abwägung wird nicht durch neue bekannt gewordene Gefahren erschüttert, durch die das Produkt nun aufgrund neuer Erkenntnisse als gefährlicher einzustufen wäre. Vielmehr lassen sich die ursprünglich in die Abwägung eingepreisten Gefahren nun eben vermeiden.[336] Wie im Falle der Produktalterung stellt sich das Produkt nicht als gefährlicher heraus, sondern kann lediglich sicherer gemacht werden.

Indes greift diese Überwälzung der Verantwortung auf den Nutzer im Falle einer Entwicklungslücke zu kurz. Zentraler Punkt ist nämlich, dass die Gefahr bereits bei Inverkehrbringen in dem Produkt angelegt war. Zwar ist die Gefahr damit nicht unmittelbar auf den Herstellungsprozess oder die Sphäre des Herstellers zurückzuführen,[337] wohl aber handelt es sich um eine dem Produkt inhärente Gefahr. Damit lässt sich als Zurechnungsgrund für die Begründung der Verkehrspflicht auf ein vorangegangenes gefährliches Tun abstellen. Das Produkt durfte lediglich aufgrund einer positiven Nutzen-Risiko-Abwägung überhaupt in den Verkehr gebracht werden. Den Hersteller aber, der einer Gefahr ursprünglich nicht abhelfen konnte, das Produkt aber trotz des Wissens um die unvermeidbare Gefährlichkeit in den Verkehr bringen durfte, müssen nach Inverkehrgabe auch latente Pflichten treffen.[338] Damit knüpft die Fortschreibung der Verantwortung für das Produkt in

---

pflicht jedenfalls beim Angebot der neuen Schutzmechanismen gegen Bezahlung als erfüllt ansieht.

335 *Helte*, Anforderungen an die Produktsicherheit, S. 262; wohl auch *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 289.

336 Zur insoweit unterschiedlichen Ausgangslage *Tamme*, Rückrufkosten, S. 175 f.

337 Vgl. *Tamme*, Rückrufkosten, S. 176, der eine von außen dem Produkt zugeordnete Gefahr ausmacht, die ihren Ursprung nicht in der Einflusssphäre des Herstellers hat, dann aber Verkehrspflichten des Herstellers gänzlich ablehnt. Anders aber *Krause*, in: Soergel, BGB, § 823 Anh. III, Rn. 25, wenn er ein Produkt, das im Laufe der Zeit aus Gründen, die der Sphäre des Herstellers zuzurechnen sind, gefährliche Eigenschaft entwickelt, von der Produktbeobachtungspflicht erfasst sieht.

338 Vgl. *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 170 f.; so auch *Sommer*, Haftung für autonome Systeme, S. 277; *Spindler*, in: Hilgendorf (Hg.), Robotik im Kontext von Recht und Moral, S. 63 (73) folgert aus dem Wissen um die Unvermeidbarkeit eine Pflicht zur besonders sorgfältigen Beobachtung; ebenso *Chibanguza*, in:

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

diesem Fall losgelöst von einem pflichtwidrigen Verhalten des Herstellers oder einer Unterschreitung der Sicherheitserwartungen zum Zeitpunkt des Inverkehrbringens als Kehrseite an das Inverkehrbringen einer unbeherrschbaren Gefahrenquelle an.[339] Insoweit geht bei wertender Betrachtung die Gefahr auch über das allgemeine Lebensrisiko hinaus.

Die Tatsache, dass die Gefahren auch den Nutzern aufgrund der herstellerseitigen Instruktion bekannt waren, darf auch aufgrund des Wissensvorsprungs, über welchen der Hersteller verfügt, nicht zu einer völligen Übertragung der Verantwortung führen. Zwar wird mit der Instruktion über die Restgefahren die Verantwortung für deren Realisierung und den Schadenseintritt auf den Nutzer verlagert. Mit dem bei Entwicklungslücken zwangsläufig erst im Nachhinein anfallenden Wissen um die Gefahrvermeidung trifft die Verantwortung dann aber wieder den Hersteller. Denn bei ihm fällt das Gefahrenvermeidungswissen an.[340] Dies liegt daran, dass den Hersteller schon im Rahmen von Neuentwicklungen im Allgemeinen aufgrund des ihnen anhaftenden diffusen Gefahrenverdachts eine besonders intensive Produktbeobachtungspflicht trifft.[341] Erst recht muss dies bei bereits bekannten latenten Gefahren gelten. Hier ist der Hersteller schon im Vorfeld der Inverkehrgabe gehalten, im Rahmen eigener Forschungsanstrengungen eine Gefahrenminimierung zu erreichen, um das Produkt aufgrund der dann positiven Nutzen-Risiko-Bilanz vermarkten zu dürfen.[342] Trotz dieser positiven Bilanz ist der Hersteller auch nach Inverkehrbringen noch in der Pflicht, aktiv nach Möglichkeiten zu suchen, die bestehenden Sicherheitslücken zu schließen.[343] Die Tatsache, dass die Gefährlichkeit bei Inverkehrgabe erkennbar ist, der Hersteller also um die Unvermeidbarkeit der Gefahr weiß, führt nämlich dazu, dass der Hersteller in der Lage ist, Ge-

---

Chibanguza/Kuß/Steege (Hg.), Künstliche Intelligenz, § 5, K., Rn. 26; *Redeker*, in: Redeker, IT-Recht, Rn. 901 und *Meier/Wehlau,* CR 1990, 95 (97).

339 In diese Richtung auch *Wittig*, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 219: „das Wissen über eine erhöhte Fehlerwahrscheinlichkeit eines Produktes spricht für die Anwendbarkeit von haftungsrechtlichen Vorschriften. Wer Kenntnis von einer hohen Fehlerwahrscheinlichkeit hat, diese aber dennoch in Kauf nimmt, muss zumindest sicherstellen, dass die Fehler so wenig Gefahrenpotential wie möglich entwickeln"; beiläufig auch *Dötsch*, Außervertragliche Haftung für KI, S. 254: „War die Gefahr für den Hersteller […] nicht verhinderbar, […] war er derjenige, der diese Gefahr verursacht hat".

340 In diese Richtung auch *Sommer*, Haftung für autonome Systeme, S. 277.

341 Vgl. BGH, NJW 1992, 560 (562); in diese Richtung auch OLG Karlsruhe, VersR 1978, 550.

342 Vgl. *Wagner,* in: MüKo, BGB, § 823, Rn. 1081.

343 *Thöne*, Autonome Systeme, S. 209; wohl auch *Sosnitza*, CR 2016, 764 (769).

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

fahrensteuerung zu betreiben und die Lücke hinsichtlich der zukünftigen Produktion zu schließen. Denn schon aufgrund des Herstellungsprozesses und der Kenntnis der Produkteigenschaften verfügt der Hersteller über das größtmögliche Wissen um die Produktgefahren und die potenziellen Möglichkeiten der Risikominimierung.[344] Die durch die Nachmarktforschung gewonnenen Erkenntnisse führen dazu, dass sich der Hersteller hinsichtlich der Gefahrenvermeidung in der vordersten Position befindet.[345] Dem Nutzer dagegen wird es gerade bei technisch komplexen Zusammenhängen schwerfallen, selbst Informationen über neue Sicherungsmaßnahmen einzuholen und deren tatsächliche Überlegenheit beurteilen zu können.[346] Aus Sicht des Nutzers besteht jedenfalls hinsichtlich seines Informationsbedürfnisses wenig Unterschied, ob eine Gefahr gänzlich neu entdeckt wird oder neue Sicherungsmaßnahmen für eine bekannte Gefahr zu Tage treten. Unabhängig davon, ob der Nutzer sich auf die Gefahr bereits eingestellt hat oder dies aufgrund der Neuentdeckung der Gefahr nicht möglich war, ist nunmehr ein Sicherheitsgewinn am Produkt möglich.

Für den Fall, dass Sicherungsmaßnahmen unterblieben sind, weil sie für den Hersteller mit einem unzumutbaren Aufwand verbunden waren und aus diesem Grund bereits bei Inverkehrgabe eine erkennbare Gefahr bestand, muss diese Argumentation erst recht greifen. Denn hier steht nicht das fehlende Wissen oder die fehlende Technik hinsichtlich der Gefahrenvermeidung in Rede, sondern (berechtigte) wirtschaftliche Erwägungen.

f) Anwendung auf die „Produktalterung"

Anders könnte die Lage bei der bloßen Produktalterung zu bewerten sein. Hier erscheint fraglich, ob mit der Inverkehrgabe des Produkts ein gefährliches Tun des Herstellers vorliegt, das als Zurechnungsgrund herangezogen werden kann und eine Verantwortungszuweisung an den Hersteller rechtfertigt. Während bei der Entwicklungslücke bereits bei Inverkehrgabe eine inhärente Produktgefahr vorlag, fehlt es hieran nämlich im Rahmen der Produktalterung. Gemessen am Zeitpunkt der Inverkehrgabe ergibt

344 Dazu *Zech*, JZ 2013, 21 (24 f.).
345 Ähnlich *Sommer*, Haftung für autonome Systeme, S. 277.
346 Zu diesem Argument, wenn auch allgemein im Rahmen der Beweislastverteilung *Hager*, in: Staudinger, BGB, § 823, Rn. F 44.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

sich damit kein erhöhtes vom Produkt ausgehendes Gefahrenlevel.[347] Erst in der zeitlichen Entwicklung stellt sich heraus, dass Sicherheitsgewinne am Produkt möglich sind. Erst in der Rückschau mit den derzeitigen Erkenntnissen ergibt sich, dass das Produkt die nunmehr an es gestellten Anforderungen nicht mehr erfüllen kann. Dies ändert aber nichts daran, dass es zum maßgeblichen Zeitpunkt seiner Inverkehrgabe die objektiven Sicherheitserwartung erfüllt hat und das Gefahrenlevel zum Zeitpunkt der Inverkehrgabe nicht erhöht war. Damit aber kann in der Inverkehrgabe kein gefährliches Tun des Herstellers gesehen werden. Vielmehr handelt es sich um eine durch die technische Weiterentwicklung von außen herangetragene Gefahr, die keinen Zurechnungsgrund begründen kann.[348]

Zwar wird auch in dieser Fallgruppe das Wissen um die Sicherheitssteigerung aufgrund der kontinuierlichen Produktentwicklung beim Hersteller generiert. Mit diesem Wissen soll aber gerade keine von Anfang an bestehende Sicherheitslücke geschlossen werden. Insoweit ist auch die Erwartungshaltung des Nutzers eine andere. Dieser wird gerade nicht mit einer inhärenten und handgreiflichen Gefahr bei der Nutzung konfrontiert. Eine solche konkrete Gefahr rechtfertigt aber erst das Vertrauen des Nutzers, dass der Hersteller die Verantwortung für die ursprüngliche Sicherheitslücke übernimmt. Dagegen gehört es zum Allgemeinwissen, dass sich die Produktsicherheit mit der Zeit erhöht und ältere Produkte hinter neuen Standards zurückbleiben. Hier kann es nicht die Aufgabe des Herstellers sein, den Produktnutzer daran zu erinnern.[349] Auch wenn gerade im Bereich smarter Produkte Hersteller häufig Anpassungen über Updates vornehmen und sich Nutzer aufgrund dieser Praxis darauf eingestellt haben, dass ihr Produkt aktiv an den Stand von Wissenschaft und Technik ange-

347 Zum Gefahrenlevel bei Inverkehrgabe als maßgeblichem Kriterium *Sommer*, Haftung für autonome Systeme, S. 277.

348 Auch *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 227 steht daher beispielhaft einer nachträglichen Schutzpflicht des Herstellers im Falle der Entwicklung von Sicherheitsgurten oder ABS im Automobilbereich zweifelnd gegenüber; *Tamme*, Rückrufkosten, S. 177 nimmt wie schon bei der Entwicklungslücke an, es handle sich um die Zuordnung einer Gefahr von außen.

349 *Helte*, Anforderungen an die Produktsicherheit, S. 263; in diese Richtung auch *Hess*, in: Martinek/Semler/Flohr (Hg.), Handbuch des Vertriebsrechts, § 12, Rn. 71a: „[…] Gefahren, die von Produkten allein wegen „Veralterung" ausgehen und deshalb gerade nicht mehr vom Pflichtenkreis des Herstellers umfasst werden"; *Sessa-Jahn*, Automatisiertes Fahren, S. 177 spricht von einem allgemeinen Lebensrisiko und dem gewöhnlichen Lauf der Dinge.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

passt wird,[350] griffe es zu kurz hieraus eine Pflicht des Herstellers abzuleiten. Denn allein daran anzuknüpfen, dass der Hersteller ein Produkt in den Verkehr gibt, von dem er weiß, dass es noch nicht „ausentwickelt" ist, kann diese Verantwortung auch im Vergleich zu der Entwicklungslücke nicht begründen. Hier erfolgt die weitere Forschung zur Verbesserung des Produkts durch den Hersteller nicht aufgrund einer sich aus der ursprünglichen Sicherheitslücke ergebenden Pflicht, sondern aufgrund einer freien unternehmerischen Entscheidung, um auch künftig konkurrenzfähig zu sein. Der Umstand, dass die technische Entwicklung mit hoher Wahrscheinlichkeit dazu führen wird, dass ein einmal entwickeltes Produkt in Zukunft den an es zu stellenden Anforderungen nicht mehr genügen wird und dass dies für den Hersteller bei Inverkehrbringen bereits abstrakt vorhersehbar ist, kann bei Inverkehrbringen eines fehlerfreien Produkts nicht zu einer nachträglichen Haftung des Herstellers führen.[351]

Bei einem fehlerfreien Produkt aus dem bloßen Inverkehrbringen eine Verkehrspflicht unabhängig von einer konkreten Gefährlichkeit abzuleiten, würde die Sorgfaltsanforderungen überspannen.[352] Zwar geht hier das Mehr an Sicherheit über den in der Entscheidung des OLG München angesprochenen Komfortgedanken einer bloßen Funktionsänderung hinaus. Allerdings ist zu bezweifeln, dass dies – ohne zurechenbare Anknüpfung in der Sphäre des Herstellers – als weitere Umstände aufzufassen ist, die eine Reaktionspflicht des Herstellers begründen.[353] Denn andernfalls würde

350 Dazu *Riehm*, in: Schmidt-Kessel/Kramme (Hg.), Geschäftsmodelle in der digitalen Welt, S. 201 (204).

351 So *Kipker/Walkusz*, DuD 2019, 513 (514 f.) in Bezug auf das Kaufrecht und die Frage, ob ein bei Übergabe zukünftig zu erwartender Mangel einen gegenwärtigen Mangel darstellen kann; im Ausgangspunkt ebenso *Marly*, Praxishandbuch Softwarerecht, Rn. 1496 und *Riehm*, in: Schmidt-Kessel/Kramme (Hg.), Geschäftsmodelle in der digitalen Welt, S. 201 (213); in diesem Zusammenhang lehnte das OLG Koblenz, BeckRS 2006, 1012 eine vorauseilende Aufklärungspflicht im Rahmen der Produktbeobachtungspflicht für ein wenige Tage nach der Inverkehrgabe in Kraft tretendes Verwendungsverbot ab (zustimmend Förster, in: BeckOK, BGB, § 823, Rn. 738: Keine „in die Zukunft gerichtete Produktbeobachtung"; einschränkend *Hager*, in: Staudinger, BGB, § 823, Rn. F 20: Nur bei fehlender Kenntnis vom Verbot). Offen ließ das Gericht allerdings, ob nach Inkrafttreten des Verbots unter Beachtung der Produktbeobachtungspflicht eine Aufklärung geschuldet ist.

352 Allgemein *Larenz/Canaris*, Lehrbuch des Schuldrechts II/2, S. 410 f.

353 Vgl. *Hager*, in: Staudinger, BGB, § 823, Rn. F 26: „Autos müssen nicht etwa kostenlos mit ABS nachgerüstet werden, wenn dieses System bei der Auslieferung noch nicht oder nicht hinreichend entwickelt war". Gerichtsentscheidungen, die sich mit späteren sicherheitsrelevanten Produktverbesserungen auseinandersetzen gehen lediglich auf den Gedanken des § 3 Abs. 2 ProdHaftG ein, nicht aber auf

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

es zu einem Auseinanderfallen der Vorteile der Nutzung und der damit verbundenen zu tragenden Lasten in Form der Alterung kommen, wenn Letztere ohne hinreichenden Zurechnungsgrund auf den Hersteller abgewälzt würden.[354]

g) Fazit

Hinsichtlich der Bedeutung des technischen Fortschritts für die Produktbeobachtungspflicht lässt sich damit festhalten, dass der Hersteller jedenfalls bei inhärenten Produktgefahren im Rahmen von Entwicklungslücken zum Einschreiten verpflichtet sein kann.[355] Dies ergibt sich daraus, dass dem Produkt die Gefahr bereits bei Verlassen der Herstellersphäre anhaftet, der Hersteller um die Unvermeidbarkeit der Gefährdung weiß und er im Folgenden über die besten Erkenntnismöglichkeiten bzgl. der überlegenen Sicherheitstechniken verfügt. Daher wird er die Produktnutzer zumindest zur eigenständigen Gefahrenminimierung befähigen müssen. Ob er darüber hinaus zu weitergehenden Maßnahmen verpflichtet ist, wird noch zu untersuchen sein. Stellt sich dagegen ein Produkt aufgrund der kontinuierlichen Produktentwicklung lediglich als sicherheitstechnisch „veraltet" dar, löst dies noch keine Reaktionspflicht des Herstellers aus.[356] Da die Argumentation hinsichtlich der Entwicklungslücke und der Produktalterung letztendlich am „Gefahrenlevel bei Inverkehrbringen"[357] ausgerichtet ist, wird sie auch den Kenngrößen der Erforderlichkeit und Zumutbarkeit gerecht.

---

eine diesbezügliche Produktbeobachtungspflicht, vgl. OLG Saarbrücken NJW 2014, 1600; OLG Düsseldorf, BeckRS 2010, 5734.

354 Ähnlich für das Kaufrecht *Kipker/Walkusz*, DuD 2019, 513 (515).

355 I.E. ohne nähere Begründung auch *Wagner,* in: MüKo, BGB, § 823, Rn. 1083: „[E]rweitern sich die Möglichkeiten der Technik, kann der Hersteller allerdings gehalten sein, […] vor nunmehr […] vermeidbaren Gefahren zu warnen"; ebenso *Foerste*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 309.

356 Es wundert daher nicht, dass die Produktalterung bei der Fallgruppenauflistung bzgl. der nachträglichen Aufklärungspflichten bei *Foerste*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 309 fehlt.

357 Hierauf hebt *Sommer*, Haftung für autonome Systeme, S. 277 in diesem Zusammenhang ab.

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

III. Haftungsrechtliche Relevanz der kritischen Eigenschaften smarter Produkte für die Produktbeobachtungspflicht

Anknüpfend an diese Ausführungen soll nun analysiert werden, inwieweit die von smarten Produkten nach der Inverkehrgabe ausgehenden Gefahren in den Anwendungsbereich der Produktbeobachtungspflicht fallen. Hierzu müssen die kritischen Eigenschaften smarter Produkte im Hinblick auf mögliche Unsicherheiten nach dem Inverkehrbringen ausgemacht und ihre haftungsrechtliche Relevanz für die Produktbeobachtungspflicht herausgearbeitet werden.

1. (Un)vermeidbarkeit von Softwarefehlern

a) Tatsächliche Herausforderung

Die Kombination von Hardware und Software führt dazu, dass auch ein spezifisch die Software betreffendes Risiko in die Produkte implementiert wird. So haftet Software der grundsätzlich anerkannte Makel der erhöhten Fehleranfälligkeit an.[358] Mit dieser ist ein jeder in seinem täglichen Leben konfrontiert. Augenfällig werden Softwarefehler dann, wenn sie zu Computerabstürzen oder Sicherheitslecks führen und entsprechende Updates nach sich ziehen.[359] Betrachtet man Softwarefehler, lassen sich im Wesentlichen zwei Arten ausmachen: So existieren Softwarefehler, die bereits im Bauplan der Software angelegt sind, also auf ein defizitäres Software-Design zurückgehen; man spricht dabei von architekturellen Softwarefehlern. Davon zu unterscheiden sind Programmierfehler, die mal mehr oder weniger banal sind, wie kleine Zählabweichungen um ein Byte oder die fehlende Prüfung der Größe eines Zielspeicherbereichs (sog. „buffer overflow").[360]

358 Vgl. *Oechsler*, in: Staudinger, BGB, § 3 ProdHaftG, Rn. 126; *Wende*, in: Sassenberg/Faber (Hg.), Industrie 4.0 und Internet of Things, § 4, Rn. 59.

359 *Hoffmann*, Software-Qualität, S. V.

360 Zu dieser vereinfachten Unterscheidung von Softwarefehlern speziell in Bezug auf Sicherheitslücken *Sohr/Kemmerich*, in: Kipker (Hg.), Cybersecurity, Kap. 3, Rn. 155 ff.; *Eichelberger*, in: Ebers et al., (Hg.), Künstliche Intelligenz und Robotik, S. 181; *Ritter*, in: Raue (Hg.), Digitale Resilienz, S. 79 (79 ff.); ähnlich *Taeger*, CR 1996, 257 (268): „Die besonderen Gefahren von Computerprogrammen resultieren vornehmlich aus Mängeln bei ihrem Entwurf und bei der Codierung"; anschaulich zu den Programmierfehlern *Deusch/Eggendorfer*, DSRITB 2015, 833 (834 ff.).

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

Fast mantraartig wird in diesem Zusammenhang wiederholt, dass Software nie gänzlich fehlerfrei programmiert werden könne.[361] Als Grund ist schnell der Aspekt der Komplexität ausgemacht.[362] Denn die abstrakte Materie und die begrenzte Fähigkeit des menschlichen Denkens, diese Befehlsfolgen und Programmschritte nachzuvollziehen und einzuordnen, machen die Softwareprogrammierung zu einem fehleranfälligen Prozess.[363] Hinzu kommt, dass aufgrund ihrer Leistungsstärke gängig genutzte „Low-Level-Programmiersprachen" wie C/C++ Fehler beim Programmieren geradezu herausfordern.[364] Zwar variieren die Angaben zu den durchschnittlich enthaltenen Fehlern pro 1000 Zeilen Code.[365] Vor dem Hintergrund der explodierenden Programmgrößen kommt dieser relativen Zahl gleichwohl nur eine untergeordnete Bedeutung zu.[366] Hinzu kommt, dass es selbst bei kleineren Programmen aufgrund der Anzahl an entstehenden Ausführungspfaden praktisch kaum mehr möglich ist, das korrekte Verhalten für alle möglichen Eingaben zu überprüfen.[367] Bei einer manuellen Fehlersuche wird sich daher auf eine kleine Auswahl an Testfällen beschränkt. Auch Software-Verifikationen kommen aufgrund der benötigten Rechenleistung ihrer Algorithmen an Grenzen und der Einsatz von Künstlicher Intelligenz scheint zwar vielversprechend, steckt aber noch in den Kinderschuhen.[368] Das Auffinden und Beheben von Softwarefehlern ist daher limitierenden Faktoren ausgesetzt. Umgekehrt lässt sich aus den vorhandenen Testmetho-

361 So ausdrücklich *Raue*, NJW 2017, 1841 (1841); *Bundesamt für Sicherheit in der Informationstechnik (BSI)*, Sicherheitsbericht 2015, S. 10; *Engel*, CR 1986, 702 (708); *Marly*, Praxishandbuch Softwarerecht, Rn. 1438, welcher dies aber krit. hinterfragt; krit. auch *Lenhard*, Datensicherheit, S. 27 f., der diese Aussage dem Kalkül von Software-Unternehmen zuschreibt.

362 Dazu *Hoffmann*, Software-Qualität, S. 13; *Hohler* in: Pfeifer/Schmitt (Hg.), Masing Handbuch Qualitätsmanagement, S. 430.

363 *Meier/Wehlau*, CR 1990, 95 (96); *Taeger*, CR 1996, 257 (268) spricht daher davon, dass sich der Produktionsvorgang von Software grundlegend von der Herstellung eines traditionellen körperlichen Gegenstandes unterscheide.

364 In diese Richtung *Sohr/Kemmerich*, in: Kipker (Hg.), Cybersecurity, Kap. 3, Rn. 158.

365 *Söbbing*, ITRB 2020, 12 (13) spricht von drei bis zehn Fehlern pro 1.000 Zeilen; *Rockstroh/Peschel*, NJW 2020, 3345 (3345) von zwei bis fünf Fehlern; vgl. auch *Hohler*, in: Pfeifer/Schmitt (Hg.), Masing Handbuch Qualitätsmanagement, S. 430.

366 Mit Beispielen *Hoffmann*, Software-Qualität, S. 13 f.; *Heussen*, CR 2004, 1 (Fn. 1) führt bei Windows 95 bei 20 Mio. Zeilen 200.000 Fehler an.

367 *Hoffmann*, Software-Qualität, S. 13, 22; *Hohler*, in: Pfeifer/Schmitt (Hg.), Masing Handbuch Qualitätsmanagement, S. 430; anschaulich zum Ganzen *Ritter*, in: Raue (Hg.), Digitale Resilienz, S. 79 (80 f.).

368 *Hoffmann*, Software-Qualität, S. 24; *Fox*, DuD 2016, 701 (701); *Yamaguchi/Rieck*, DuD 2016, 713 (passim).

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

den aber auch der Schluss ziehen, dass – würde man nur alle erdenklichen Testfälle durchspielen – Softwarefehler in einem technischen Sinne nicht unvermeidbar sind und eine fehlerfreie Programmierung theoretisch möglich ist.[369] Gleichwohl ist sie jedenfalls ab einem bestimmten Komplexitätsgrad schlicht utopisch, weil mit unverhältnismäßigem Aufwand verbunden.[370] Herstellerseits wird damit aus wirtschaftlichen Gründen bewusst darauf verzichtet, eine vollends fehlerfreie Software zu entwickeln.[371] Dabei drängt sich der Verdacht auf, dass die Sichtweise „Software ist nie fehlerfrei" zu einer selbsterfüllenden Prophezeiung wird und Hersteller schon deshalb Qualitätsanforderungen unterschreiten.[372] Dies hat zur Folge, dass sich der Verkehr mit Produkten auseinanderzusetzen hat, die bereits bei Eigentumsübergang mit Programmierfehlern im technischen Sinne behaftetet sind.[373]

b) Softwarefehler als rechtliche Kategorie

Dass Software im Tatsächlichen nie gänzlich fehlerfrei ist, stellt somit eine Binse dar. Gleichwohl handelt es sich hierbei zunächst um eine technische Kategorie.[374] Zudem ist nur ein kleiner Bruchteil dieser möglichen Fehler auch sicherheitsrelevant.[375] So können Softwarefehler sowohl das Äquivalenz- als auch das Integritätsinteresse der Nutzer betreffen. Beeinträchtigen Softwarefehler allein die Funktionalität, etwa weil ein genutztes Programm

369 *Deusch/Eggendorfer*, DSRITB 2015, 833 (836) nennen das OpenSource-Betriebssystem „OpenBSD" und die verwendeten Gegenmaßnahmen zur Verhinderung von Softwarefehlern als leuchtendes Gegenbeispiel. Hier traten in rund 20 Jahren nur zwei entfernt ausnutzbare Sicherheitslücken auf.

370 *Wiebe*, NJW 2019, 625 (625); *Oechsler*, in: Staudinger, BGB, § 3 ProdHaftG, Rn. 126; *Taeger*, CR 1996, 257 (268); *Foerste*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 173; ähnlich wohl auch *Spindler*, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, Rn. 168; einschränkend *Wagner,* in: MüKo, BGB, § 3 ProdHaftG, Rn. 20.

371 Näher zu den Gründen *Wittig*, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 165 ff.

372 In diese Richtung auch *Deusch/Eggendorfer*, in: Taeger/Pohle (Hg.), Computerrechts-Handbuch, Teil 5, Rn. 457.

373 *Reusch*, BB 2019, 904 (908). Ohne dass mit dieser Feststellung zwangsläufig der Vorwurf der Verletzung einer Verkehrssicherungspflicht bzw. eines Konstruktionsfehlers einhergeht; *Heckmann/Paschke*, in: Bräutigam/Kraul (Hg.), Internet of Things, § 10, Rn. 126 sprechen von „latenter IT-Unsicherheit".

374 *Riehm/Leithäuser/Brenner*, in: Raue (Hg.), Digitale Resilienz, S. 5 (17).

375 *Riehm/Leithäuser/Brenner*, in: Raue (Hg.), Digitale Resilienz, S. 5 (17).

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

langsam abläuft oder andauernd abstürzt, ist das Äquivalenzinteresse angesprochen.[376] Diese Fehler mögen für den Nutzer zwar störend sein, bilden aber keine Frage der deliktischen Produkthaftung.[377]

aa) Softwarefehler als produkthaftungsrechtlich relevanter Fehler

Im Rahmen der Produkthaftung können die zwei als wesentlich ausgemachten Fehlerarten im Bereich der Software, nämlich architekturelle Fehler und Programmierfehler, beide dem Konstruktionsbereich zugerechnet werden. Dieser umfasst bei der Softwareherstellung die gesamte Phase von der Programmerstellung (= notwendige Entwurfsarbeiten und konkreter Programmablaufplan) über die Programmierung, Codierung und Kompilierung bis hin zu den Kontrollen und Testläufen.[378] Gerade architekturelle Fehler – häufig ist hier eine nicht angelegte Authentifizierung[379] – sind herkömmlichen Konstruktionsfehlern sehr ähnlich.

Die Frage, wann nun ein Softwarefehler im Einzelfall auch einen produkthaftungsrechtlich relevanten Fehler darstellt, wird nach den allgemeinen Grundsätzen beurteilt. Juristisch übersetzt,[380] kann damit die Fehleranfälligkeit von Software nicht dazu führen, dass Software deliktsrechtlich stets oder auch nie als fehlerhaft zu qualifizieren wäre. Insoweit kann auch von Software keine absolute Sicherheit verlangt werden.[381] Denn die Obergrenze des Pflichtenprogramms bildet der Stand der Wissenschaft und Technik.[382] Andererseits wurde bereits festgestellt, dass Programmierfehler

376 Anders kann dies freilich sein, wenn ein Programmabsturz gleichzeitig zu einer Schädigung der von § 823 Abs. 1 BGB geschützten Rechtsgütern oder Rechten führt.

377 Vgl. auch *Spindler*, in Hornung/Schallbruch (Hg.), IT-Sicherheitsrecht, § 11, Rn. 2; *Spindler*, CR 2015, 766 (768).

378 *Lehmann*, NJW 1992, 1721 (1723); *Reese*, DStR 1994, 1121 (1123); *Taeger*, CR 1996, 257 (268). Es wird darauf hingewiesen, dass für den Fabrikationsbereich damit lediglich ein etwaiges Aufbringen des Programms auf einen Datenträger und damit ein Übertragungsfehler verbleibt; vgl. auch *Dötsch*, Außervertragliche Haftung für KI, S. 242; weiter dagegen *Mayrhofer,* Außervertragliche Haftung für fremde Autonomie, S. 253 f.

379 Beispiele bei *Sohr/Kemmerich*, in: Kipker (Hg.), Cybersecurity, Kap. 3, Rn. 163.

380 In seiner Bedeutung im Hinblick auf den Sachmangelbegriff vom BGH noch offengelassen, vgl. BGH, NJW 1988, 406 (408); vgl. zum Fehlerbegriff in der Informatik und Juristerei bspw. *Marly*, Praxishandbuch Softwarerecht, Rn. 1437.

381 Hierzu *Wagner*, AcP 217 (2017), 707 (727 f.).

382 Vgl. explizit in Bezug auf Softwarefehler *Schaub*, JZ 2017, 342 (344).

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

mit dem entsprechenden Aufwand sehr wohl vermeidbar sind.[383] Damit kann der Einwand der Komplexität bei der Entwicklung von Software nicht zu einer pauschalen Entlastung des Herstellers führen,[384] sondern lediglich im Rahmen der Zumutbarkeit die haftungsrechtliche Verantwortlichkeit begrenzen. Gleichwohl ist stets die Basissicherheit zu gewährleisten.[385] Wie diese Basissicherheit aber zu bestimmen ist und welche Risiken noch zumutbar und welche nicht mehr tragbar sind, ist bislang offengeblieben.[386]

bb) Ableitungen aus dem vertraglichen Mangelbegriff

Bisher kam es nach der Rechtsprechung im Vertragsrecht maßgeblich darauf an, ob der Programmierfehler den alltäglichen Gebrauch der Software negativ beeinträchtigt, er also zu Funktionseinschränkungen führt, die für den Anwender wahrnehmbar sind.[387] Der so verstandene Mangelbegriff kann sicherheitsrelevante Softwarefehler allerdings kaum abbilden. Denn nicht selten kann ein Softwarefehler auch ohne augenscheinliche Beeinträchtigung der Funktionalität ein erhebliches Schadensrisiko nach sich ziehen.[388] Jedenfalls im auf den Integritätsschutz angelegten Produkthaftungsrecht kann die Funktionsbeeinträchtigung damit nicht entscheidend für das Vorliegen eines Produktfehlers sein. Hier kommt es allein auf die

383 Freilich kann es Einzelfälle geben, wo dies mangels Gefahren- oder Gefahrenabwehrwissens anders zu beurteilen ist; dazu *Heussen*, CR 2004, 1 (3); *Riehm*, in: Schmidt-Kessel/Kramme (Hg.), Geschäftsmodelle in der digitalen Welt, S. 201 (211) nennt die Heartbleed-Sicherheitslücke als solchen Fall.

384 *Engel*, CR 1986, 702 (708); *Spindler*, in: Hilgendorf (Hg.), Robotik im Kontext von Recht und Moral, S. 63 (72); *Voigt,* in: BeckOGK, BGB, § 823, Rn. 751; *Oster*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 57, Rn. 21; *Thöne*, Autonome Systeme, S. 203; *Wende*, in: Sassenberg/Faber (Hg.), Industrie 4.0 und Internet of Things, § 4, Rn. 76; *Wittig*, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 178 f.

385 Vgl. in Bezug auf Softwarefehler *Wiesner*, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 10.6, Rn. 18; *Oster*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 57, Rn. 21.

386 So *Söbbing*, ITRB 2020, 12 (14); ebenso *Deusch/Eggendorfer*, DSRITB 2015, 833 (842) welche dieses Vakuum konkreter Sicherheitsvorgaben als möglichen Grund für unzureichende Qualitätssicherung bei den Softwareherstellern sehen.

387 Vgl. m.w.N. zur Rechtsprechung *Deusch/Eggendorfer*, in: Taeger/Pohle (Hg.), Computerrechts-Handbuch, Teil 5, Rn. 455; dazu auch *Söbbing*, ITRB 2020, 12 (14 f.).

388 *Söbbing*, ITRB 2020, 12 (13); krit. daher auch *Deusch/Eggendorfer*, in: Taeger/Pohle (Hg.), Computerrechts-Handbuch, Teil 5, Rn. 456 und *Deusch/Eggendorfer*, DSRITB 2015, 833 (841, 843): „[G]efährliche[] Verengung des Sachmangelbegriffs".

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

Schadensrisiken an, die sich verwirklichen können. Mit der Umsetzung der Warenkaufrichtlinie[389] und der Richtlinie über digitale Inhalte und digitale Dienstleistungen[390] hat der Gesetzgeber nun auch im Vertragsrecht in § 434 Abs. 3 S. 2 BGB sowie in § 327e Abs. 3 S. 1 Nr. 2 BGB den Begriff der „Sicherheit" als Bezugspunkt für die übliche und erwartbare Beschaffenheit in den Gesetzestext aufgenommen. Vor diesem Hintergrund wird sich die Rechtsprechung von ihrer bisherigen Linie abwenden und einen sicherheitsrelevanten Softwarefehler unabhängig von einer Funktionsbeeinträchtigung als Mangel ansehen müssen.[391]

cc) Maßgeblichkeit der berechtigten Verkehrserwartung

Da der vertragsrechtliche Mangelbegriff in seiner objektiven Komponente und der produkthaftungsrechtliche Fehlerbegriff letztlich auf den „Schutz der berechtigten Verkehrserwartungen" zurückgehen,[392] sollten sie auch gleichen Erwägungen folgen.[393] Allerdings wurde der im Vertragsrecht implementierte Begriff der „Sicherheit" nicht weiter definiert,[394] sodass sich aus ihm keine Kriterien zur Bestimmung der Basissicherheit ableiten lassen.[395] In diesem Zusammenhang darf auch in Zweifel gezogen werden, ob das nutzerseits aus dem Alltag im Umgang mit Software vorhandene Wissen um die Fehleranfälligkeit von Software zu herabgesetzten Sicherheitserwartungen führt.[396] Ein Nutzer, dem zwar allgemein bekannt ist, dass Software Programmierfehler aufweisen kann, wird gleichwohl erwarten, dass der Betrieb der Software sicher ist und diese keine Fehler aufweist,

389 Richtlinie (EU) 2019/771.
390 Richtlinie (EU) 2019/770.
391 *Klett/Gehrmann*, MMR 2022, 435 (437); *Söbbing*, ITRB 2020, 12 (16).
392 So *Riehm*, in: Schmidt-Kessel/Kramme (Hg.), Geschäftsmodelle in der digitalen Welt, S. 201 (204).
393 I.E. auch *Deusch/Eggendorfer*, in: Taeger/Pohle (Hg.), Computerrechts-Handbuch, Teil 5, Rn. 457; ausführlich *Sommer*, Haftung für autonome Systeme, S. 90 f.
394 Vgl. näher *Schmidt-Kessel*, ZfPC 2022, 117 (118).
395 Ausführlich zum vertragsrechtlichen Mangelbegriff bei Softwarefehlern *Riehm/Leithäuser/Brenner*, in: Raue (Hg.), Digitale Resilienz, S. 5 (13 ff.).
396 So aber *Lehmann*, NJW 1992, 1721 (1725); wohl auch *Wittig*, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 179 f.; zu Recht zurückhaltend *Wende*, in: Sassenberg/Faber (Hg.), Industrie 4.0 und Internet of Things, § 4, Rn. 76 und *Wiesner*, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 10.6, Rn. 41.

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

die zu Schäden an seinen Rechtsgütern führen können.[397] Die Erwartung des Nutzers wird vielmehr dahin gehen, dass der Hersteller diejenigen Qualitätssicherungsmaßnahmen ergreift, die dem Stand von Wissenschaft und Technik entsprechen,[398] ihm zumutbar sind und dass gleichzeitig die Basissicherheit erreicht wird.[399] Da die Erwägungen der Zumutbarkeit maßgeblich vom Kriterium der Gefährlichkeit getragen sind, wird dies dazu führen, dass herstellerseits eine möglichst geringe und zu den jeweiligen Anwendungsbereichen der Software passende Fehlerrate anzustreben ist.[400] Bleibt der Hersteller hinter diesem im Einzelfall bereichsabhängig zu bestimmendem Mindeststandard zurück, weil auch solche Sicherungsmaßnahmen nicht zumutbar oder technisch nicht möglich sind (Entwicklungslücke), hat die Inverkehrgabe zu unterbleiben.

397 So *Riehm/Meier*, MMR 2020, 250; *Fida*, Updates, Patches & Co, S. 142; *Marly*, Praxishandbuch Softwarerecht, Rn. 1823; *Taeger*, CR 1996, 257 (265, 268); *Sessa-Jahn*, Automatisiertes Fahren, S. 152 merkt an, dass von bekannten Gefahren nicht darauf geschlossen werden kann, dass diese auch in Kauf genommen werden; anders OLG Köln, MMR 2020, 248 (249) zum Vertragsrecht, sehr krit. hierzu *Deusch/Eggendorfer*, in: Taeger/Pohle (Hg.), Computerrechts-Handbuch, Teil 5, Rn. 457 f.

398 *Wittig*, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 165 ff. beschäftigt sich näher mit dieser Frage; *Riehm/Leithäuser/Brenner*, in: Raue (Hg.), Digitale Resilienz, S. 5 (16 f.) sehen vertragsrechtlich darüber hinaus in jeder anfänglichen Sicherheitslücke einen Mangel, um in diesen Fällen dem Verbraucher einen gewährleistungsrechtlichen Anspruch auf die Bereitstellung einer Sicherheitsaktualisierung einräumen zu können.

399 In diese Richtung *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 107 f.

400 *Rockstroh/Kunkel*, MMR 2017, 77 (79); ähnlich *Taeger*, CR 1996, 257 (265 f.); *Foerste*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 173; *Reusch*, BB 2019, 904 (908) spricht von „Produkte[n], die nicht mehr als akzeptabel im Bereich Software angesehen werden können"; ähnlich *Söbbing*, ITRB 2020, 12 (13); *Deusch/Eggendorfer*, DSRITB 2015, 833 (844 f.) merken gleichwohl an, dass künftig die zunehmende Vernetzung der Produkte auch vermeintlich risikolosen Bereichen das Potential verleiht, weitere Risikodimensionen zu eröffnen; *Klett/Gehrmann*, MMR 2022, 435 (437) nennen die Fehlerdichte, die Anzahl und Schwere der vorhandenen Sicherheitslücken, das Einhalten bestimmter Sicherheitsstandards bei vergleichbaren Produkten sowie das Risiko eines Cyberangriffs in dem Nutzungsbereich der Software und den Gegenstand der Software als mögliche Kriterien zur Bestimmung der Mangelhaftigkeit im Vertragsrecht.

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

dd) Entwicklungsfehler

Gleichwohl ändert die Tatsache, dass ein Softwarefehler bei der Inverkehrgabe nicht entdeckt wurde, nichts an dem Vorliegen eines Fehlers.[401] Denn für die Beurteilung der Verantwortlichkeit kommt es nicht darauf an, ob ein Fehler zum Zeitpunkt des Inverkehrbringens nicht erkannt wurde, sondern darauf, ob er nach dem Stand von Wissenschaft und Technik zumutbar hätte erkannt werden können.[402] Anders könnte sich die Lage darstellen, sollte es sich um objektiv nicht erkennbare Fehler handeln. Dann steht ein die Haftung bei Inverkehrgabe ausschließender Entwicklungsfehler im Raum.

Problematisch bei der Einordnung eines Softwarefehlers als Entwicklungsfehler sind aber ein tatsächlicher und ein rechtlicher Gesichtspunkt. Zum einen ist in tatsächlicher Hinsicht schon die Frage nach der objektiven Erkennbarkeit nicht einfach zu beantworten. Denn ein allgemeingültiger Maßstab mit Blick auf das entsprechend verfügbare Risikowissen lässt sich kaum bilden. Dies liegt daran, dass aufgrund der Individualität von Software Fehler regelmäßig nur durch spezifische Testläufe aufgefunden werden. Zum anderen kommt es für die Annahme eines Entwicklungsfehlers nach der Rechtsprechung darauf an, ob die potenzielle Gefährlichkeit des Produkts im Zeitpunkt seiner Inverkehrgabe nach dem damaligen Stand von Wissenschaft und Technik nicht erkannt werden konnte, weil die Erkenntnismöglichkeiten (noch) nicht weit genug fortgeschritten waren. Maßgeblich ist damit nicht die Erkennbarkeit des spezifischen Fehlers des konkreten schadensstiftenden Produkts, sondern die Erkennbarkeit des zu Grunde liegenden allgemeinen, mit der gewählten Konzeption verbundenen Fehlerrisikos.[403] Entsprechend obiger Feststellung haftet aber jeder Programmierung eine abstrakte und bekannte Fehleranfälligkeit an. Das Fehlerrisiko ist der Softwareentwicklung inhärent und wird von den Herstellern erkannt. Jedenfalls in Bezug auf den Programmierfehler sollte dies aber noch nicht zur vorschnellen Ablehnung eines Entwicklungsfehlers führen.[404] Denn die allgemeine Fehleranfälligkeit von Programmierun-

401 So zum Mangelbegriff in Bezug auf Sicherheitslücken *Riehm/Meier*, MMR 2020, 250; ebenso *Lapp*, in: Kipker (Hg.), Cybersecurity, Kap. 10, Rn. 119.

402 *Horner/Kaulartz*, CR 2016, 7 (11); *Grützmacher*, CR 2016, 695 (696); *Raue*, NJW 2017, 1841 (1843).

403 Diese stehende Formulierung verwendet BGH, NJW 2009, 2952 (2955).

404 So aber, wenn auch verengt auf die IT-Sicherheitslücke *Wende*, in: Sassenberg/Faber (Hg.), Industrie 4.0 und Internet of Things, § 4, Rn. 71; *Wagner*, AcP 217 (2017),

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

gen zieht eine Vielgestaltigkeit unterschiedlichster Programmierfehler nach sich. Damit ist die Bandbreite dessen, was sich aus dem abstrakten Fehlerrisiko der unzureichenden Programmierung konkret schadensstiftend auswirken kann, groß. Hierin liegt aber der Unterschied zu der grundsätzlichen Erkennbarkeit von Haarrissen in Mineralwasserflaschen oder von Fehlauslösungen von Airbags.[405] In diesen Fällen besteht ein hinsichtlich der gewählten Konstruktion sehr konkretes Fehlerrisiko, das auch hinsichtlich der schadensstiftenden Auswirkung genau lokalisiert werden kann. Bei Programmierfehlern dagegen besteht aufgrund der allgemeinen Fehleranfälligkeit mehr ein abstraktes Risikowissen vergleichbar dem diffusen Gefahrenverdacht bei Neuentwicklungen. Dem Hersteller fehlt es damit aber gerade an einer bestimmten Vorstellung vom konkreten Fehler, wodurch er nicht einschätzen kann, welches schadenstiftende Risiko sich verwirklichen wird.[406] Hinsichtlich des mit der gewählten Konzeption verbundenen Fehlerrisikos kann damit nicht auf das allgemeine Fehlerrisiko bei der Programmierung abgestellt werden, sondern muss auf das mit der konkret gewählten Programmierung verbundene Fehlerrisiko abgestellt werden.[407] Anders verstanden würde bei Programmierfehlern nie der Haftungsausschluss des Entwicklungsfehlers greifen und immer nur die Frage der Entwicklungslücke thematisiert werden können; nämlich ob der so verstandene erkennbare Programmierfehler (zumutbar) vermeidbar gewesen ist und die Mindestsicherheit gewährleistet. Dagegen kann eine – im Vergleich zur gewählten Programmierung – fehlerfreie Programmierung aber

---

707 (750) merkt in Bezug auf das Autonomierisiko an, dass Entwicklungsfehler keine typischen das Produkt betreffende Gefahren sein dürften. Vielmehr könne heute definitionsgemäß noch nicht gesagt werden, was Entwicklungsfehler sind, da diese noch nicht bekannt sein können; dagegen geht *Spindler*, in Hornung/Schallbruch (Hg.), IT-Sicherheitsrecht, § 11, Rn. 28 beiläufig und ganz selbstverständlich von der Möglichkeit eines Entwicklungsfehlers aus; ebenso *Rockstroh/Kunkel*, MMR 2017, 77 (80).

405 In beiden Fällen lehnte der BGH mit obiger Argumentation einen die Haftung ausschließenden Entwicklungsfehler ab, vgl. BGH, NJW 1995, 2162 und BGH, NJW 2009, 2952; ähnlich *Graf v. Westphalen*, ZIP 2019, 889 (892) „spezielles, produktbezogenes Entwicklungsrisiko"; anders sieht *Wende*, in: Sassenberg/Faber (Hg.), Industrie 4.0 und Internet of Things, § 4, Rn. 71 im Ausschluss des Entwicklungsfehlers für Programmierfehler eine „konsequente Fortführung der ständigen Rechtsprechung".

406 So zu Recht *Leupold/Wiesner*, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 9.6.4, Rn. 64.

407 Vgl. mit Beispiel auch *Mayrhofer,* Außervertragliche Haftung für fremde Autonomie, S. 309.

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

durchaus nach dem Stand von Wissenschaft und Technik zum Zeitpunkt des Inverkehrbringens noch nicht erkennbar sein.[408]

c) Bedeutung für die Produktbeobachtung

Nach dieser Übersetzung der technisch erhöhten Fehleranfälligkeit bei der Softwareentwicklung in rechtliche Kategorien, zeichnet sich für die Phase nach dem Inverkehrbringen folgendes Bild: Die erhöhte Fehleranfälligkeit von Software hat zum einen zur Folge, dass eine hohe Dunkelziffer an produkthaftungsrechtlich fehlerhaften Produkten im Verkehr sein dürfte, die aufgrund ihrer Programmierfehler die Basissicherheit nicht gewährleisten, ohne dass dies aber erkannt wurde.[409] Andere Produkte gewährleisten zwar die Basissicherheit und sind im produkthaftungsrechtlichen Sinne nicht fehlerhaft, weisen aber gleichwohl Programmierfehler auf, deren Behebung aufgrund der kostenintensiven Testläufe zum Aufsuchen von Fehlern bei Inverkehrgabe nicht zumutbar war. Solche als Entwicklungslücken verstandene Programmierfehler werden regelmäßig erst nach Inverkehrgabe aufgedeckt. Zum anderen sind nach der hier vertretenen Ansicht auch haftungsausschließende Entwicklungsfehler denkbar, bei denen das Gefahrenwissen erst nach Inverkehrgabe greifbar wird.[410] Vor diesem Hintergrund nimmt es daher nicht Wunder, dass in der juristischen Literatur eine besonders intensive Pflicht zur Produktbeobachtung konstatiert wird.[411] Denn die gerade beschriebenen Szenarien als Hauptanwendungsfälle der tatsächlichen Unsicherheiten der Softwareentwicklung – rechtlich übersetzt in anfänglich

408 Vgl. *Wurm*, Automotive Cybersecurity, S. 72; *Rosenberger*, Die außervertragliche Haftung für automatisierte Fahrzeuge, S. 393.

409 *Deusch/Eggendorfer*, in: Taeger/Pohle (Hg.), Computerrechts-Handbuch, Teil 5, Rn. 452 weisen darauf hin, dass „es zahlreiche – auch neuartige – Malware-Programme [gibt], die keine neuen Sicherheitslücken schaffen oder entdecken, sondern lediglich längst bekannte, aber nicht beseitigte Unzulänglichkeiten bei der Softwareherstellung ausnutzen"; ebenso *Sessa-Jahn*, Automatisiertes Fahren, S. 174; erschreckende Beispiele geben *Deusch/Eggendorfer*, DSRITB 2015, 833 (837); *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 77.

410 Ebenso *Sessa-Jahn*, Automatisiertes Fahren, S. 175.

411 Einhellige Meinung, vgl. nur *Raue*, NJW 2017, 1841 (1844); *Spindler*, NJW 2004, 3145 (3147); *Spindler*, in: Hilgendorf (Hg.), Robotik im Kontext von Recht und Moral, S. 63 (73); *Oster*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 57, Rn. 21; *Chibanguza*, in: Chibanguza/Kuß/Steege (Hg.), Künstliche Intelligenz, § 5, K., Rn. 26; *Redeker*, in: Redeker, IT-Recht, Rn. 901; *Meier/Wehlau,* CR 1990, 95 (97); *Ebert* et al., ZfPC 2023, 16 (21); *Ebers*, in: Oppermann/Stender-Vorwachs (Hg.), Autonomes Fahren, 1. Aufl., S. 93 (107).

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

fehlerhafte Produkte, Entwicklungsfehler und Entwicklungslücken – fallen nach den gefundenen Ergebnissen allesamt in den Anwendungsbereich der Produktbeobachtungspflicht.

2. Digitale Resilienz

a) Tatsächliche Herausforderung

Ein weiterer Aspekt, der sich aus der Verzahnung von Hardware- und Softwareprodukten ergibt, ist der Bedeutungsgewinn der IT-Sicherheit.[412] So sind Cyberangriffe längst kein auf den staatlichen oder unternehmerischen Bereich beschränktes Phänomen mehr. Die zunehmende Vernetzung aller Lebensbereiche im Zuge des IoT und die daraus resultierenden Abhängigkeiten führen dazu, dass auch die private Sphäre ein attraktives Ziel für Angreifer wird.[413]

Ein System kann dabei auf mehreren Wegen kompromittiert werden.[414] Zum einen können aus Softwarefehlern – das betrifft sowohl Programmierfehler als auch architekturelle Fehler – Sicherheitslücken resultieren. Solche Sicherheitslücken stellen die wichtigste Ursache für Cyberangriffe dar.[415] Denn durch die Ausnutzung von Sicherheitslücken können sich Dritte gegen den Willen des Berechtigten Zugang zu informationstechnischen Systemen verschaffen oder diese beeinflussen (vgl. § 2 Abs. 6 BSIG). Zum anderen können die Angreifer eine „soziale" Komponente nutzen. Beim Social-Engineering-Angriff erreichen die Angreifer den Zugang zum System nicht über eine in der Software vorhandene Sicherheitslücke, sondern sie verleiten den Geschädigten bspw. durch eine Phishing-Mail, eine Handlung wie das Klicken auf einen Link vorzunehmen, um so eine Schadsoftware auf dem System zu installieren.[416] Durch Sicherheitslücken oder mittels Social Engineerings infizierte Systeme können dann zur Ausübung von Distributed Denial of Service (DDoS)-Attacken missbraucht werden. Die

412 Vgl. *Wiebe*, InTer 2020, 66 (66).
413 Dazu *Zech*, ZfPW 2019, 198 (205); *Thöne*, Autonome Systeme, S. 222 f.; *Schallbruch*, CR 2018, 215 (221 f.); Angriffsszenarien bei *Schmon*, IWRZ 2018, 254 (256).
414 Prägnante Übersicht bei *Roos/Schumacher*, MMR 2014, 377 (378).
415 So *Sohr/Kemmerich*, in: Kipker (Hg.), Cybersecurity, Kap. 3, Rn. 155.
416 Dazu *Sohr/Kemmerich*, in: Kipker (Hg.), Cybersecurity, Kap. 3, Rn. 178 ff; vgl. auch zur wachsenden Bedeutung des Social Engineering *Bundesamt für Sicherheit in der Informationstechnik (BSI)*, Sicherheitsbericht 2022, S. 12.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

übernommenen Systeme werden dann dazu genutzt, andere Server gezielt mit wiederkehrenden Anfragen zu überlasten, bis diese abstürzen und nicht mehr erreichbar sind.[417]

Hacker nutzen damit gerade die Fehleranfälligkeit von Software und die zunehmende Vernetzung aus. Dadurch werden sowohl Hersteller als auch Nutzer mit von außen kommenden Gefahren durch IT-Angriffe konfrontiert, deren Abwehr sich schwieriger darstellen könnte als die Gewährleistung der Produktsicherheit von innen.[418] So führen neben den klassischen IT-Schnittstellen weitere Hardware-Schnittstellen wie Sensoren oder Signalempfänger zu einer großen Angriffsfläche.[419] Auch die Vielzahl an unterschiedlichen Komponenten solcher Systeme führt zu einer hohen Komplexität und damit zu einer Zunahme der Fehleranfälligkeit und der Möglichkeit diese auszunutzen. Hinzu kommt, dass gerade im Bereich Smart-Home die Produkte in weniger sicheren Netzwerkumgebungen eingesetzt werden. Außerdem macht es die bereits angesprochene Vernetzung der Produkte möglich, einen Angriff von einem unsicheren System auf ein anderes System überspringen zu lassen.[420] Dies hat zur Folge, dass ein unsicheres Produkt nicht nur Auswirkungen für den Nutzer, sondern auch für Dritte und die digitale Infrastruktur in Gänze hat und somit die gesamte digitale Umgebung Gefahren ausgesetzt wird.[421]

b) IT-Sicherheit als Element des produkthaftungsrechtlichen Fehlerbegriffs

In welcher Weise Anforderungen an die IT-Sicherheit vom produkthaftungsrechtlichen Fehlerbegriff umfasst sind und der Hersteller daher die „digitale Resilienz" seiner Softwareprodukte gewährleisten muss, ist jedoch unklar und umstritten. Insbesondere gilt das für die Frage, inwieweit Soft-

417 *Sohr/Kemmerich*, in: Kipker (Hg.), Cybersecurity, Kap. 3, Rn. 181 ff; anschaulich *Ritter*, in: Raue (Hg.), Digitale Resilienz, S. 79 (88 f.).

418 In diese Richtung *Bräutigam/Klindt*, NJW 2015, 1137 (1142); ähnlich *Hartmann*, DAR 2015, 122 (123). Dieser geht am Beispiel der Automobilbranche davon aus, dass die Produktsicherheit teilweise eher an den Maßstäben der IT-Branche zu messen sein wird als an denen der „klassischen" Automobilbranche; vergleichbar *Seufert*, CR 2023, 73 (74).

419 *Krauß/Waidner*, DuD 2015, 383 (385 f.) geben einen Überblick über mögliche Angriffspunkte bei vernetzten Fahrzeugen.

420 Zum Ganzen mit der Auflistung von Angriffsszenarien *Fedler*, in: Ebers/Steinrötter (Hg.), Künstliche Intelligenz und smarte Robotik, S. 91 (103 ff.).

421 Vgl. *Riehm/Meier*, MMR 2020, 250.

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

warehersteller auch für Cyberangriffe Dritter verantwortlich im Sinne des Produkthaftungsrechts sind, die auf Sicherheitslücken der im Produkt verwendeten Software zurückzuführen sind. Erst hieran anschließend lässt sich die Frage klären, ob den Hersteller auch Produktbeobachtungspflichten hinsichtlich Gefahren für die IT-Sicherheit treffen. Freilich ließe sich fragen, wer, wenn nicht der Hersteller, die Cybersicherheit smarter Produkte gewährleisten solle. Indes greift eine aus diesem Gedanken folgende reflexartige Zuweisung der Verantwortung an den Hersteller zu kurz.[422] Denn es darf nicht übersehen werden, dass der Schaden erst durch das bewusste Ausnutzen der Sicherheitslücke und damit durch einen vorsätzlichen und rechtswidrigen Angriff eines Dritten, nämlich des Hackers herbeigeführt wird.[423]

c) Status Quo der gesetzlichen Lage in Deutschland

Betrachtet man die aktuelle gesetzliche Lage hinsichtlich der Gewährleistung der IT-Sicherheit, ergibt sich eine fragmentarische Gemengelage, die durch mehrere unterschiedliche Rechtsmaterien gekennzeichnet ist.[424] Auch das IT-Sicherheitsgesetz 2.0[425] hat entgegen anders lautender Ankün-

422 So aber häufig in der Literatur, vgl. nur *Hartmann*, DAR 2015, 122 (123); *Ebers*, in: Oppermann/Stender-Vorwachs (Hg.), Autonomes Fahren, 1. Aufl., S. 93 (106); *Droste*, CCZ 2015, 105 (109).

423 Dazu *Geistfeld*, Cal. L. Rev. 105 (2017), 1611 (1660 ff.); *Wende*, in: Sassenberg/Faber (Hg.), Industrie 4.0 und Internet of Things, § 4, Rn. 68 fordert daher „noch eine intensive rechtsdogmatische Diskussion"; ähnlich *Hartmann/Klindt*, ZfPC 2022, 73 (73 f.), die es als „in der Rechtswissenschaft noch nicht annähernd ausreichend erforscht [ansehen], inwieweit das etablierte Regelungsregime rund um Safety nolens volens auf Herausforderungen der Security angewendet werden kann"; speziell in Bezug auf die Produktbeobachtung *Schmid*, IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme, S. 193 „[es] bleibt im juristischen Schrifttum bislang weitestgehend unbeantwortet, ob Produktbeobachtungspflichten auch zur Gewährleistung der Informationssicherheit bestehen können".

424 Vgl. *Bräutigam/Klindt*, NJW 2015, 1137 (1141).

425 Die maßgeblichen Regelungen finden sich im BSIG. Das erste Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 1.0) trat bereits 2015 in Kraft und wurde 2017 durch das Gesetz zur Umsetzung der NIS-Richtlinie der EU noch einmal erweitert. Das Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme trat am 28.05.2021 in Kraft. Es erweiterte insbesondere den Anwendungsbereich des BSIG und ergänzt die dortigen Pflichten. Am 16.01.2023 trat die NIS2-Richtlinie der EU in Kraft. Vgl. zur nationalen Umsetzung den Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Umsetzung

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

digungen hieran nichts geändert.[426] Es nimmt weiterhin lediglich die Betreiber bestimmter kritischer Systeme und digitale Online-Dienste in die Pflicht, Sicherheitsvorkehrungen zu schaffen, um die Sicherheit ihrer eigenen informationstechnischen Systeme zu gewährleisten (vgl. §§ 8a und 8c BSIG).[427] Herstellern von IT-Produkten erlegt das BSIG aber grundsätzlich keine eigenen Pflichten auf.[428]

Daneben sind auch die Produktsicherheitsvorschriften der Union hinsichtlich verbindlicher Anforderungen für die Hersteller zur Gewährleistung der Cybersicherheit ihrer Produkte (noch) äußerst zurückhaltend. Zwar setzt sich der bereits im Juni 2019 in Kraft getretene Cybersecurity Act (im Folgenden „CSA")[429] zum Ziel, digitale Produkte besser vor Cyberbedrohungen zu schützen, vgl. Erwägungsgrund (3) CSA. In diesem Zusammenhang sollen Hersteller dazu angehalten werden, die Sicherheit gegen Cyberangriffe bereits im Produktdesign und während des gesamten Produktlebenszyklus zu berücksichtigen, vgl. Erwägungsgrund (12) CSA. In diesem Zusammenhang gilt ab dem 27.02.2025 die Durchführungsverordnung (EU) 2024/482 der Kommission, die einen einheitlichen Zertifizierungsrahmen für Cybersicherheit auf europäischer Ebene einführt und damit die Grundlage eines transparenten und einheitlichen Systems der IT-Sicherheitszertifizierung (vgl. Art. 46 CSA) bildet. Allerdings ist die eigentliche Zertifizierung von Produkten unter einem noch zu erarbeitenden Schema für die Hersteller der Produkte freiwillig (Art. 56 Abs. 2 CSA).[430]

---

der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung.

426 Vgl. *Schallbruch*, CR 2021, 450 (455).

427 Für Unternehmen im besonderen öffentlichen Interesse ist eine weniger aufwendige Regulierung vorgesehen, die deutlich hinter den Pflichten für KRITIS-Unternehmen zurückbleibt; eingehend *Beucher/Ehlen/Utzerath*, in: Kipker (Hg.), Cybersecurity, Kap. 14, Rn. 78 ff.

428 Zum Sicherheitsgesetz 1.0 schon *Spindler*, CR 2016, 297 (309) und *Schallbruch*, CR 2018, 215 (222); nunmehr *Schallbruch*, CR 2021, 450 (455) mit dem Hinweis, dass das Sicherheitsgesetz 2.0 den Gedanken der Erhöhung der IT-Sicherheit von IT-Produkten außerhalb der zivilrechtlichen Haftung insoweit aufnimmt, als die Möglichkeit des BSI zur sicherheitstechnischen Untersuchung von IT-Produkten ausgeweitet wird, bestimmte IT-Produkte als Komponenten kritischer Infrastrukturen verboten werden können und eine freiwillige IT-Sicherheitskennzeichnung möglich ist; *Zech*, DJT 2020 Gutachten, A S. 47 f.

429 Verordnung (EU) 2019/881.

430 Krit. zur Zukunftsträchtigkeit dieser freiwilligen Zertifizierung *Hessel/Callewaert*, DB 2022, 2589 (2590); *Kipker*, DuD 2020, 263 (263) erwartet mittelfristig im Rahmen der Evaluierung und Überarbeitung des CSA gem. Art. 67 CSA jedenfalls für bestimmte Stufen, insbesondere den KRITIS-Sektor, die Aufhebung der Freiwillig-

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

Eine gewichtige Ausnahme stellt indes die Verordnung über Medizinprodukte (im Folgenden „MDR")[431] dar.[432] So fordert die MDR in Anhang I, 17.2. explizit eine Softwareentwicklung nach dem Stand der Technik auch in Bezug auf die IT-Sicherheit. Nach Anhang I, 18.8. haben die Hersteller die Produkte dabei so herzustellen, dass sie so weit wie möglich vor einem unbefugten Zugriff geschützt sind.

d) IT- Sicherheit im Rahmen der Produzentenhaftung

Eine allgemeine und gesetzlich verankerte verbindliche Herstellerpflicht zur Gewährleistung von IT-Sicherheit in Bezug auf smarte Produkte besteht aktuell nicht. Ebenso fehlt es an eigenständigen Haftungsregelungen für Cyberrisiken.[433] Allerdings könnten sich die haftungsrechtliche Generalklausel des § 823 Abs. 1 BGB und die entwickelten Grundsätze zur Produzentenhaftung auf Grund ihres hohen Abstraktionsniveaus zur Durchsetzung von IT-Sicherheitsvorgaben eignen, auch wenn sie keine konkreten inhaltlichen Anforderungen an die IT-Sicherheit stellen.[434] Um die IT-Sicherheit aber im Haftungstatbestand des § 823 Abs. 1 BGB verankern zu können, muss zunächst geklärt werden, inwieweit die IT-Sicherheit von der Schutzrichtung des Haftungsrechts umfasst ist und wo die Grenzen der Herstellerverantwortung für Cyberangriffe erreicht sind.[435] Denn im Gegensatz zur klassischen Produkthaftung sind bei smarten Produkten und im Rahmen der IT-Sicherheit gerade Einflüsse Dritter im Spiel.[436]

---

keit; auch zuvor bereits veröffentlichte Standards für den Bereich der IT-Sicherheit wie der am 30.06.2020 veröffentlichte europäische Standard ETSI EN 303 6458 für die Sicherheit von IoT-Verbraucherprodukten haben lediglich Empfehlungscharakter und bauen auf eine freiwillige Zertifizierung.

431 Verordnung (EU) 2017/745.

432 Vgl. den Bericht der EU-Kommission über die Auswirkungen Künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung, COM (2020) 64 final, S. 7.

433 Vgl. *Wiebe*, InTer 2020, 66 (66, 67); *Böck/Theurer*, BB 2021, 520 (522).

434 Vgl. *Riehm/Meier*, MMR 2020, 571 (573); *Thöne*, Autonome Systeme, S. 223.

435 Saubere Herausarbeitung bei *Wiebe*, InTer 2020, 66 (67).

436 Prägnant *Spindler*, in Hornung/Schallbruch (Hg.), IT-Sicherheitsrecht, § 11, Rn. 24.

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

aa) Schutzumfang des Haftungsrechts bei Cyberangriffen

Hinsichtlich der Frage des Schutzumfangs des Haftungsrechts geht es darum, dass der Begriff der Sicherheit in der IT im Ausgangspunkt nicht mit dem Begriff der Produktsicherheit des Produkthaftungsrechts gleichzusetzen ist.[437] Dies führt im Ausgangspunkt zu der Unterscheidung zwischen safety und security: Traditionell beziehen sich Anforderungen an die Produktsicherheit auf den Schutz des Nutzers oder Dritten gegenüber von dem Produkt ausgehenden Gefahren (safety). Dem steht die IT-Sicherheit gegenüber, also die Sicherheit des Softwareprodukts selbst gegenüber inneren und äußeren Einflüssen (security).[438] Security betrifft die Einhaltung von Sicherheitsstandards zur Gewährleistung der Integrität, Verfügbarkeit und Vertraulichkeit von Informationen (vgl. § 2 Abs. 2 S. 4 BSIG). Dadurch soll der Schutz des Produkts vor Eingriffen oder Manipulationen Dritter sichergestellt werden (Resilienz).[439]

Indes kennt § 823 Abs. 1 BGB diese Unterscheidung selbst nicht. Vielmehr schützt die Haftungsnorm das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum und sonstige Rechte unabhängig davon, wodurch der Sorgfaltspflichtenverstoß ausgelöst wurde. Ansprüche aus § 823 Abs. 1 BGB bestehen damit immer erst dann, wenn ein Fehler – unabhängig davon, ob es sich um einen herkömmlichen Produktfehler oder eine IT-Schwachstelle handelt – eine Rechtsgutsverletzung der genannten Schutzgüter herbeiführt.[440] Diese genannten Rechtsgüter haben ihre Relevanz bisher aber ausschließlich im Bereich der safety entfaltet.[441] Denn hinsichtlich des Schutzes vor Gefahren, die von einem herkömmlichen Produkten ausgingen, führten Produktfehler regelmäßig zu Beeinträchtigungen

437 Vgl. *Bräutigam/Klindt*, NJW 2015, 1137 (1141 f.); *Rockstroh*, DSRITB 2016, 279 (281); *Rockstroh/Kunkel*, MMR 2017, 77 (78); *Wiebe*, InTer 2020, 66 (66); *Wittig*, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 34.

438 Zu den Begriffen von safety und security: *Kipker*, in: Kipker (Hg.), Cybersecurity, Kap.1, Rn. 6; *Fedler*, in: Ebers/Steinrötter (Hg.), Künstliche Intelligenz und smarte Robotik, S. 91 (99); plakativ und bewusst zur vereinfachten Gegenüberstellung von safety als „Schutz der Umwelt vor Systemen" und security als „Schutz der Systeme vor der Umwelt": *Grimm/Waidner*, in: Hornung/Schallbruch (Hg.), IT-Sicherheitsrecht, § 2, Rn. 4.

439 Dazu *Bräutigam/Klindt*, NJW 2015, 1137 (1141).

440 Speziell in Bezug auf IT-Schwachstellen erinnert hieran *Rockstroh*, DSRITB 2016, 279 (285).

441 Ähnlich wohl auch *Schmid*, IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme, S. 193 und *Schucht*, NVwZ 2021, 532 (532 f.).

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

dieser Schutzgüter. Die Produkthaftung konnte damit als Sonderform der Verletzung der körperlichen Integrität und des Sacheigentums aufgefasst werden.[442] Der Aspekt der safety wird daher seit jeher vom Schutzumfang des § 823 Abs. 1 BGB erfasst. Dagegen musste die Produktsicherheit den Aspekt der security herkömmlich nicht abbilden.[443] Ein Produkt galt als sicher, wenn seine safety sichergestellt war. Ein im Rahmen der security relevanter unberechtigter Zugriff eines Dritten betrifft nämlich im Ausgangspunkt die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen.[444] Spätestens mit der Implementierung von Software in physische Produkte beschränken sich die IT-Gefährdungen aber längst nicht mehr hierauf.[445] Vielmehr kann ein solcher Zugriff auch wieder safety-relevante Gefahren nach sich ziehen.[446] Man denke an das eingangs erwähnte Beispiel, in dem Hacker einen Jeep Cherokee ferngesteuert haben.[447] Obwohl ein solcher unbefugter Zugriff auf ein IT-System zunächst der security zuzuordnen wäre, unterfallen dessen Auswirkungen – nämlich die Gefahr für die Insassen und allgemein die Umgebung des ferngesteuerten Autos – der safety.[448]

Damit kann aber auch bei der Frage des haftungsrechtlichen Schutzumfangs an dieser Stelle nicht stehengeblieben werden. Denn wo eine Gefahr für die Schutzgüter der security in eine Gefahr für die Schutzgüter der safety umschlagen kann, wo security und safety also verschmelzen, entstehen Gefährdungen, die klassischerweise dem Rechtsgüterschutz des § 823 Abs. 1 BGB unterfallen.[449] Da diese Gefährdungen auch von einer ausnutz-

442 So *Bartsch*, CR 2008, 613 (615).

443 In diese Richtung *Schucht*, NVwZ 2021, 532 (532 f.); *Hartmann*, in: Knappertsbusch/Gondlach (Hg.), Arbeitswelt und KI 2030, S. 63 (66).

444 *Klindt*, Robotik und Produktion 2022, S. 38 weist daher darauf hin, dass „[die] durch Cyberunsicherheit betroffenen Rechtsgüter […] vielfach ganz andere [sind] als diejenigen, die Produktsicherheit schützen möchte." Er plädiert daher dafür Safety und Security nicht „allzu leichtfertig" gleichzusetzen.

445 *Schucht*, NVwZ 2021, 532 (532 f.); *Fedler*, in: Ebers/Steinrötter (Hg.), Künstliche Intelligenz und smarte Robotik, S. 91 (103).

446 *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 89 sprechen davon, dass die IT-Sicherheit mittelbar der Produktsicherheit dient und sich als Teilaspekt des Produktsicherheitsrechts entpuppt.

447 Vgl. Fn. 1.

448 Vgl. dazu *Schmid*, IT- und Rechtssicherheit automatisierter und vernetzter cyberphysischer Systeme, S. 183; *Koch*, NJW 2004, 801 (802) spricht von mittelbaren Beeinträchtigungen.

449 So auch *Schmid*, IT- und Rechtssicherheit automatisierter und vernetzter cyberphysischer Systeme, S. 193 und *Wiebe*, InTer 2020, 66 (67); ferner *Ackermann*, in:

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

baren Sicherheitslücke ausgehen können, lassen sich security und safety im Bereich smarter Produkte gar nicht mehr voneinander trennen. Das eine ist nicht mehr ohne das andere denkbar.[450] Sie treffen sich zu einem einheitlichen Begriff von IT-Sicherheit als Anforderung des Produktsicherheits- und des Produkthaftungsrechts.[451] Inwieweit einer IT-Schwachstelle ohne Auswirkungen auf die safety eine eigenständige haftungsrechtliche Bedeutung zukommt, hängt dagegen davon ab, ob bereits der unberechtigte Zugriff eines Dritten bzw. die bloße Einsicht, Manipulation oder Löschung von Daten dem Rechtsgüterschutz des § 823 Abs. 1 BGB unterfallen. Mit Blick auf das vom BVerfG als Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG abgeleitete neue Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme scheint dies zumindest nicht ausgeschlossen.[452] Inwieweit dieses „IT-Grundrecht" im Rahmen der mittelbaren Drittwirkung aber eigenständig als sonstiges Recht im Sinne von § 823 Abs. 1 BGB anzuerkennen ist, ist noch nicht abschließend geklärt.[453]

Der Einwand, dass die Produkthaftung den Ausgleich für versehentlich provozierte Schäden durch das Produkt betreffe, während Cyberangriffe vorsätzliche und rechtswidrige Angriffe Dritter und damit gerade keine versehentlichen Fehlerbilder seien, verfängt in diesem Zusammenhang nicht.[454] Eine solche Verengung der Produkthaftung auf die safety verkennt, dass im Rahmen von § 823 Abs. 1 BGB dem Schutzgut maßgebliche Be-

NK-ProdR, § 823 BGB, Rn. 22 und *Raue*, NJW 2017, 1841 (1843); im Ansatz auch *Hartmann*, in: Knappertsbusch/Gondlach (Hg.), Arbeitswelt und KI 2030, S. 63 (66).

450 So *Kipker*, MMR-Aktuell 2022, 452009 anlässlich des Entwurfs der EU-Kommission zu einem Cyber-Resilience-Act (COM (2022) 454 final).

451 Im Englischen "safety-relevant cybersecurity", dazu *Kapoor/Klindt*, BB 2023, 67 (68); *Wiebe*, BB 2022, 899 (900); *Wiesner*, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 10.6, Rn. 244; vgl. auch *Ortner/Daubenbüchel*, NJW 2016, 2918 (2923). Diese weisen speziell im Bereich von mhealth daraufhin, dass andernfalls dort, wo die Beeinflussung einer IT-Funktion spürbare Auswirkungen auf den Gesundheitszustand des Patienten haben kann, der nach Stand von Wissenschaft und Technik geschuldete höchste Sicherheitsstand in Zeiten zunehmender Cyber-Kriminalität gar nicht gewährleistet werden könne.

452 BVerfG NJW 2008, 822.

453 Vgl. *Kannowski*, in: Staudinger, BGB, Vor § 1, Rn. 26; für eine Anerkennung *Sprau*, in: Grüneberg, BGB, § 823, Rn. 132; als naheliegend wird dies von *Roßnagel/Schnabel*, NJW 2008, 3534 (3537) und *Heydn* in: Schuster/Grützmacher (Hg.), IT-Recht, § 823 BGB, Rn. 44 bezeichnet; ausführlich *Riehm*, VersR 2019, 714 (720 ff.).

454 Diese Bedenken formulieren *Hartmann/Klindt*, ZfPC 2022, 73 (73 f.).

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

deutung zukommt, nicht aber der Modalität der Begehung.[455] Daneben ist auch der Anknüpfungspunkt des dem Hersteller vorzuwerfenden Verhaltens falsch gewählt. Dieser liegt nämlich nicht im eigentlichen Cyberangriff, sondern – wie stets im Rahmen der Produzentenhaftung – in dem zum Fehler und damit hier zur Sicherheitslücke führenden Sorgfaltspflichtenverstoß.[456] Damit handelt es sich im Ausgangspunkt aber sehr wohl um ein für die Produkthaftung charakteristisches Fehlerbild.[457]

bb) Reichweite der Herstellerverantwortung bei Cyberangriffen

Wird das vorsätzliche und rechtswidrige Ausnutzen der Sicherheitslücke in den Vordergrund gestellt, ist gleichwohl die zentrale zweite Frage angesprochen, nämlich inwieweit die Herstellerverantwortung bei Cyberangriffen reicht. Letztlich lässt sich dies auf die Frage herunterbrechen, inwieweit der Hersteller nach Inverkehrgabe auch für das Fehlverhalten anderer im Zusammenhang mit seinem Produkt einzustehen hat. Angesichts der tatsächlichen Schwierigkeiten, die unmittelbar für den Cyberangriff Verantwortlichen zur Rechenschaft zu ziehen, liegt der rechtliche Fokus nämlich auf der Schadensprävention und dem Rückgriff auf den Hersteller als den mittelbaren Verursacher.[458]

Um sich dieser Thematik zu nähern, soll eine vergleichende Betrachtungsweise mit den zu herkömmlichen Produkten entwickelten Grundsätzen vorgenommen werden.[459] Hier ist anerkannt, dass dem Hersteller, nur weil er mit der Inverkehrgabe des Produkts die Möglichkeit des Schadenseintritts überhaupt erst geschaffen hat, nicht jeder Fehlgebrauch, durch den sich eine im Produkt angelegte Gefahr verwirklicht, auch zuzurechnen ist.[460] Vielmehr ist eine an den Verantwortungssphären anknüpfende Betrachtung vorzunehmen.

455 Prägnant *Bartsch*, CR 2008, 613 (615).
456 So im Zusammenhang mit der ProdHaftRL auch *Wagner/Ruttloff/Römer*, CCZ 2023, 109 (109).
457 *Klindt*, DAR 2023, 7 (9) spricht dagegen von einer völlig unterschiedlichen „Genetik".
458 *Raue*, NJW 2017, 1841 (1842).
459 Hierfür plädiert auch *Steege*, SVR 2023, 9 (14).
460 Vgl. *v. Bar*, in: Lieb (Hg.), Produktverantwortung und Risikoakzeptanz, S. 29 (31).

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

(1) Sicherungsmaßnahmen bei Produktfehlgebrauch und Produktmissbrauch

In diesem Zusammenhang sei zunächst auf eine Selbstverständlichkeit hingewiesen. Nimmt ein Produkt einen schadensstiftenden Fehler erst nach dem Zeitpunkt des Inverkehrbringens an, etwa aufgrund einer unsachgemäßen Behandlung innerhalb der Vertriebskette oder durch den Geschädigten selbst, ist der Hersteller für diesen nicht verantwortlich.[461] Die Verantwortlichkeit des Herstellers endet grundsätzlich mit der Inverkehrgabe seines Produkts. Dies entspricht der Zäsurwirkung des Inverkehrbringens für die haftungsrechtliche Zuweisung der Risikosphären. Klargestellt wird dieser Gedanke dann explizit in § 1 Abs. 2 Nr. 2 ProdHaftG.

Diese Abgrenzung der Verantwortungsbereiche fortgeführt, kann aber auch ein nach der Inverkehrgabe stattfindendes Fehlerverhalten in den Verantwortungsbereich des Herstellers fallen. Dann nämlich, wenn der Hersteller dieses Fehlverhalten bereits vor dem Inverkehrbringen berücksichtigen muss. Angesprochen ist damit der vorhersehbare Fehlgebrauch des Nutzers in der Verwendungsphase, dem der Hersteller in Ausdehnung des Vertrauensgrundsatzes bereits durch konstruktive Maßnahmen vorzubeugen hat. Hier ist die Grenze der Herstellerverantwortung erst dort erreicht, wo sich das Fehlverhalten des Nutzers als Missbrauch darstellt.[462] Maßgeblich für die Einordnung als Missbrauch ist die Frage, ob die Nutzung noch innerhalb des allgemeinen Verwendungszwecks des Produkts liegt und vom Hersteller vorherzusehen ist.[463] Für diese Abgrenzung können die vom LASI entwickelten Leitlinien unterstützend herangezogen werden.[464] Hiernach fallen insbesondere die vorsätzliche Gesundheitsverletzung unter Zuhilfenahme des Produkts, die vorsätzliche Zerstörung des Produkts (Vandalismus) und das vorsätzliche Zerstören von Schutzeinrichtungen mit hohem Aufwand nicht mehr unter die vorhersehbare Verwendung.[465] Eine derartige Pervertierung des Produkts bei der Verwendung durch den Nutzer ist nicht mehr vom allgemeinen Verwendungszweck gedeckt und fällt daher nicht in den Verantwortungsbereich des Herstellers. Dieser muss folglich auch keine diesbezüglichen Sicherungsmaßnahmen ergreifen.

461 Vgl. BT-Drs. 11/2447, S. 14.
462 Allgemeine Meinung, vgl. nur *Ackermann*, in: NK-ProdR, § 823 BGB, Rn. 81; *Oechsler*, in: Staudinger, BGB, § 3 ProdHaftG, Rn. 60.
463 Vgl. B.II.2.a); BGH, NJW 1989, 707 (708).
464 Vgl. in Bezug auf das ProdSG die Leitlinien des Länderausschusses für Arbeitsschutz und Sicherheitstechnik (LASI) LV 46, S. 16 f.
465 Vgl. hierzu auch *Reusch* BB 2017, 2248 (2249).

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

Bei einer Übertragung dieser Erkenntnisse auf von Dritten durchgeführte Cyberangriffe, lässt sich ein Spannungsfeld ausmachen.[466] Stellt man die Vorhersehbarkeit des Fehlverhaltens in den Vordergrund, sind Cyberangriffe vor dem Hintergrund der Allgegenwärtigkeit von Schadsoftware und der rasanten Verbreitung smarter Produkte ohne Weiteres für den Hersteller vorhersehbar.[467] Anderseits handelt es sich bei einem Cyberangriff gerade um eine vorsätzliche Pervertierung des Produkts und damit um einen Missbrauch.[468] Damit ist die Frage aufgeworfen, inwieweit ein voraussehbarer Missbrauch eine Herstellerverantwortlichkeit auslösen kann.[469] Aber auch für Fallkonstellation, in denen der Hersteller um das allgemeine Missbrauchspotential seiner Produktgattung weiß (bspw. „sniffing" gefährlicher Chemikalien), wurde eine weitergehende Verkehrspflicht abgelehnt.[470] Die Grenze der Verantwortung des Herstellers bildet der Verwendungszweck des Produkts. Wenn die Verwendung des Produkts nichts mehr mit der Zweckbestimmung des Produkts zu tun hat, wie sie bei der Herstellung vorgesehen war, endet die Haftung des Herstellers.[471]

Indes darf bei der hier zu betrachtenden Situation eines Cyberangriffs nicht übersehen werden, dass es sich gerade um einen von außen kommenden vorsätzlichen und rechtswidrigen Eingriff handelt. Es geht nicht um eine missbräuchliche Verwendung des Produkts durch den Nutzer. Vielmehr gefährdet ein Dritter den Nutzer und unbeteiligte Dritte. Anders als bei der Eigengefährdung durch eine völlig zweckwidrige Verwendung des Produkts gibt der Produktnutzer damit keinen Anlass, ihm seine Schutzwürdigkeit im Hinblick auf von dem Produkt ausgehende Gefahren zu versagen.[472]

466 In diese Richtung auch *Schucht*, NVwZ 2021, 532 (534).
467 Ähnlich *Wagner*, AcP 217 (2017), 707 (727); *Eichelberger*, in: Ebers et al., (Hg.), Künstliche Intelligenz und Robotik, S. 181; *Schucht*, NVwZ 2021, 532 (534).
468 *Klindt*, DAR 2023, 7 (9) und *Hartmann/Klindt*, ZfPC 2022, 73 (74) sprechen daher von „IT-Vandalismus" und sprechen sich gegen eine Verantwortung des Herstellers aus.
469 Dazu auch *Bräutigam/Klindt*, NJW 2015, 1137 (1142).
470 BGH, NJW 1981, 2514 (2516); instruktiv OLG Karlsruhe, NJW-RR 2001, 1174.
471 *Arndt/Wende*, ZfPC 2023, 110 (114).
472 Hierauf weist in produktsicherheitsrechtlicher Hinsicht *Schucht*, NVwZ 2021, 532 (534) hin.

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

(2) Sicherungsmaßnahmen bei Fehlverhalten Dritter

Vor diesem Hintergrund ist zu untersuchen, ob Sicherungsmaßnahmen des Herstellers auch bei einem Fehlverhalten Dritter zu ergreifen sind. Es geht dabei um die Frage, ob der Hersteller als mittelbarer Verursacher aufgrund eigener Verkehrssicherungspflichten für die Rechtsgutsverletzungen Dritter einzustehen hat.[473]

α) Allgemeines Deliktsrecht

Betrachtet man den dogmatischen Hintergrund solcher Sicherungsmaßnahmen, dienen diese dazu, der Zurechnung des schädigenden Verhaltens eines anderen gegen die Verwirklichung der eigens geschaffenen Gefahr vorzubeugen.[474] Wenn dem Sicherungspflichtigen dabei überlegene Möglichkeiten zur Verfügung stehen, solche Schäden zu vermeiden, kann es für die Ausdehnung des Vertrauensgrundsatzes keinen Unterschied machen, durch wessen sorgfaltswidriges Verhalten die Schadensverwirklichung seinen Lauf genommen hat. Daher muss auch in Bezug auf das Fehlverhalten Dritter der Grundsatz gelten, dass der eigene Sorgfaltsaufwand bis zu derjenigen Grenze auszudehnen ist, bis zu der ein anderer die Gefahr mit weniger Aufwand steuern kann.[475] Nach den allgemeinen Grundsätzen des Haftungs- und Schadensrechts schließt damit das Dazwischentreten eines Dritten die Verantwortlichkeit des Erstschädigers nicht grundsätzlich aus.[476] Vor diesem Hintergrund ist im allgemeinen Deliktsrecht anerkannt, dass der Sicherungspflichtige neben dem Fehlverhalten des gefährdeten Opfers auch das Fehlverhalten Dritter zu berücksichtigen hat, welches die von ihm gesetzte Gefahr im Zusammenwirken erhöht.[477]

Fraglich ist allerdings, ob damit jegliches Fehlverhalten eines Dritten zu berücksichtigen ist. Möglicherweise ist die Grenze wiederum zwischen einem naheliegenden Fehlverhalten des Dritten und einem vorsätzlichen und damit missbräuchlichen Verhalten des Dritten zu ziehen. Allerdings

473 Zu Recht *Raue*, NJW 2017, 1841 (1843).
474 *Flume*, in: BeckOK, BGB, § 249, Rn. 313; *Brand,* in: BeckOGK, BGB, § 249, Rn. 274.
475 Hierzu *Förster*, in: BeckOK, BGB, § 823, Rn. 333; *Wagner,* in: MüKo, BGB, § 823, Rn. 484.
476 Vgl. nur *Oetker,* in: MüKo, BGB, § 249, Rn. 157; *Flume*, in: BeckOK, BGB, § 249, Rn. 31.
477 Allgemeine Meinung, vgl. *Förster*, in: BeckOK, BGB, § 823, Rn. 333; *Wagner,* in: MüKo, BGB, § 823, Rn. 485; *Voigt,* in: BeckOGK, BGB, § 823, Rn. 425.

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

dienen die Sicherungspflichten gegen vorsätzliches Drittverhalten gerade dem Geschädigten und dieser ist in doppelter Hinsicht schutzwürdig. Zum einen hat der Geschädigte kaum Möglichkeiten den Eingriff des Dritten abzuwehren, während dies dem Pflichtigen mit geringem Aufwand möglich ist. Zum anderen ist der Geschädigte anders als bei einem eigenen Fehlverhalten nicht weniger schutzwürdig.[478] Anders gewendet darf sich ein Hersteller nach dem Vertrauensgrundsatz grundsätzlich darauf verlassen, dass die Nutzer ordnungsgemäß mit dem Produkt umgehen, während es ein solches Vertrauen dahingehend, dass auch Dritte die Grenzen des Normalgebrauchs einhalten, nicht gibt.[479] Die Anforderungen an die Sicherungspflichten im Verhältnis zu einem unbefugten Dritten fallen folglich strenger aus als gegenüber einer sich selbst schädigenden Person. Während hier Sicherungsmaßnahmen nur zur Abwendung eines vorhersehbaren und nahe liegenden Fehlverhaltens geboten sind, ist gegenüber einem unbefugten Dritten grundsätzlich auch vorsätzlich-missbräuchliches Fehlverhalten zu berücksichtigen.[480]

Damit das schädigende Verhalten des Dritten aber nicht zu einer Unterbrechung des Kausalzusammenhangs führt und eine Zurechnung erfolgen kann, muss eine besondere Gefahrenlage begründet worden sein, die das Einwirken des Dritten erst ermöglicht oder zumindest wesentlich erleichtert hat.[481] Insoweit ist wieder darauf abzustellen, dass die geschaffene Gefahrenlage über das allgemeine Lebensrisiko hinausgeht.[482] Umgekehrt ist eine Zurechnung ausgeschlossen, wenn zwischen den Schadensbeiträgen lediglich ein äußerer Zusammenhang besteht. Das ist aber insbesondere der Fall, wenn mit dem Einwirken des Dritten nach der allgemeinen Lebenserfahrung nicht zu rechnen war oder das Verhalten des Dritten so stark in den Vordergrund tritt, dass er als Herr des Geschehens[483] ausge-

478 Vgl. *Förster*, in: BeckOK, BGB, § 823, Rn. 333; *Wagner,* in: MüKo, BGB, § 823, Rn. 485.

479 *Mayrhofer,* Außervertragliche Haftung für fremde Autonomie, S. 256.

480 BGH, NJW 1990, 1236 (1237); BGH, NJW-RR 1990, 789 (790); m.w.N. zur Rechtsprechung *Förster*, in: BeckOK, BGB, § 823, Rn. 333.1 und *Hager*, in: Staudinger, BGB, § 823, Rn. E 33.

481 Vgl. BGH, NJW 1965, 1177 (1178); *Oetker,* in: MüKo, BGB, § 249, Rn. 158; *Flume*, in: BeckOK, BGB, § 249, Rn. 31.

482 *Oetker,* in: MüKo, BGB, § 249, Rn. 158.

483 So lehnte der BGH in seinem berühmten Grünstreifenfall (BGH, NJW 1972, 904 (906)) eine Haftung des unfallverursachenden Pkw-Fahrers für Schäden ab, die andere Fahrer durch die Umgehung der Unfallstelle unter Befahren des Grünstreifens verursachten. Hier seien die Fahrer aus freien Stücken auf den Grünstreifen

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

macht werden kann.[484] Gerade mit Blick auf das unbefugte Eingreifen eines Dritten sind der Haftung des Verkehrssicherungspflichtigen damit Grenzen gesetzt,[485] die bei einem nur hypothetisch möglichen, praktisch aber fernliegenden Kausalverlauf erreicht sind.[486]

Bei der Bestimmung der konkreten Sicherungsmaßnahmen spielt sodann die Üblichkeit von Sicherungsvorkehrungen eine entscheidende Rolle. Denn im Rahmen des Vertrauensgrundsatzes wird dadurch zum einen die Sicherheitserwartung und zum anderen der Grad des Selbstschutzes des potenziell Geschädigten beeinflusst.[487] Neben Fällen, in denen die Übernahme der Aufgabe des Verkehrssicherungspflichtigen gerade dazu dient, die Gefahr auch vorsätzlichen Drittverhaltens zu bannen, sind Sicherungspflichten gegen vorsätzliches Drittverhalten insbesondere im Rahmen der Bereichshaftung anzufinden.[488] So muss ein Grundstückseigentümer Abdeckroste dagegen sichern, dass sie mutwillig herausgehoben werden können, da ansonsten eine Sturzgefahr begründet wird.[489] Auch muss ein Pferdestall, der nahe an einer Autobahn liegt, durch ein Schloss gesichert werden, um ein absichtliches Befreien der Pferde und ein Entlaufen auf die Autobahn zu verhindern.[490]

β) Übertragung auf die Produkthaftung am Beispiel der Produktsabotage

Es stellt sich die Frage, ob diese im allgemeinen Deliktsrecht geltenden Grundsätze auch auf die Produkthaftung des Herstellers übertragen werden können.[491] Einen ersten Anhaltspunkt könnte § 6 Abs. 2 S. 1 ProdHaftG geben. Hiernach wird die Haftung des Herstellers nicht gemindert, wenn

---

gefahren und die unfallbedingte Sperrung sei nicht mehr als ein äußerer Umstand, der lediglich die Motivation für das eigenmächtige Verhalten schuf, gewesen.

484 Vgl. *Oetker,* in: MüKo, BGB, § 249, Rn. 158.; *Flume*, in: BeckOK, BGB, § 249, Rn. 311.

485 Zur grundsätzlichen Anwendbarkeit dieser Kriterien auch bei einer vorsätzlichen Schadensverursachung durch Dritte *Flume*, in: BeckOK, BGB, § 249, Rn. 314; *Grüneberg*, in: Grüneberg, BGB, Vor § 249, Rn. 49; *Larenz/Canaris*, Lehrbuch des Schuldrechts II/2, S. 415.

486 *Förster*, in: BeckOK, BGB, § 823, Rn. 334.

487 Hierzu *Larenz/Canaris*, Lehrbuch des Schuldrechts II/2, S. 416.

488 *Hager*, in: Staudinger, BGB, § 823, Rn. E 33.

489 BGH, NJW 1990, 1236 (1237).

490 BGH, NJW-RR 1990, 789 (790).

491 Diese Frage wirft *Wende*, in: Sassenberg/Faber (Hg.), Industrie 4.0 und Internet of Things, § 4, Rn. 54 auf, ohne sie allerdings zu beantworten; ohne nähere Betrachtung *Spindler*, NJW 2004, 3145 (3146).

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

der Schaden durch einen Fehler des Produkts und zugleich durch die Handlung eines Dritten verursacht worden ist. Allerdings regelt die Norm lediglich die Rechtsfolgen für den Fall, dass eine kumulative Kausalität vorliegt.[492] Ist der Hersteller dagegen aufgrund eines überholenden Drittverhaltens schon gar nicht verantwortlich, greift die Norm nicht.[493] Vor diesem Hintergrund soll eine produkthaftungsrechtliche Konstellation betrachtet werden, in der kein Fehlverhalten des Produktnutzers, sondern das eines Dritten in Rede steht.[494] Der Blick soll dabei auf die Produktsabotage gerichtet werden. Darunter sind Fälle zu verstehen, in denen ein ursprünglich sicheres Produkt durch die vorsätzliche Handlung eines Dritten gefahrbringende Eigenschaften erhält.[495]

Da das Produkt erst nach Inverkehrgabe fehlerbehaftet wurde, wird unter Bezugnahme auf den Rechtsgedanken des § 1 Abs. 2 Nr. 2 ProdHaftG jedenfalls im Ausgangspunkt eine Verantwortlichkeit des Herstellers abgelehnt.[496] Für die Frage der Fehlerhaftigkeit des Produkts bei Inverkehrgabe kann es in der Tat keinen Unterschied machen, ob der Fehler durch den Nutzer oder einen Dritten verursacht wurde, sofern die Einwirkung nur nach dem Inverkehrbringen stattfand. Denn ebenso wenig wie bei einem missbräuchlichen Verhalten des Nutzers kann der Hersteller hier als eigentlicher Gefahrenverursacher ausgemacht werden. Indes darf die Bedeutung der Vorschrift im Zusammenhang mit der Produktsabotage nicht überschätzt werden. Denn eine Entlastung ist dem Hersteller lediglich bei nach der Inverkehrgabe entstehenden Fehlern möglich. Haftet dem Produkt dagegen bereits zum Zeitpunkt des Inverkehrbringens ein Fehler – zumindest im Keim – an, greift der Haftungsausschluss nicht ein.[497] Insoweit entspringt der Fehler nämlich der Verantwortungssphäre des Herstellers. Daher kommt der Vorschrift bei Konstruktionsfehlern, die dem Produkt

492 Vgl. *Graf v. Westphalen*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 51, Rn. 10.

493 *Oechsler*, in: Staudinger, BGB, § 6 ProdHaftG, Rn. 19; *Graf v. Westphalen*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 51, Rn. 10, 12; *Ehring*, in: NK-ProdR, § 6 ProdHaftG, Rn. 15; vgl. auch *Stöhr*, in: FS Müller, S. 173 (185).

494 Entscheidungen der Rechtsprechung hierzu sind – soweit ersichtlich – noch nicht vorhanden.

495 Vgl. dazu *v. Bar*, in: Lieb (Hg.), Produktverantwortung und Risikoakzeptanz, S. 29 (44).

496 *Ehring*, in: NK-ProdR, § 1 ProdHaftG, Rn. 71; *Wagner,* in: MüKo, BGB, § 1 ProdHaftG, Rn. 34; *Oechsler*, in: Staudinger, BGB, § 1 ProdHaftG, Rn. 85; *Lenz*, in: Lenz, Produkthaftung, § 3, Rn. 372.

497 Vgl. *Lenz*, in: Lenz, Produkthaftung, § 3, Rn. 372.

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

begriffsnotwendig bereits vor der Inverkehrgabe auf Dauer anhaften, nicht zur Anwendung.[498] Unterlässt der Hersteller damit aber Vorkehrungen auf konstruktiver Ebene, um einer späteren Sabotage entgegenzuwirken und besteht diesbezüglich eine entsprechende Verkehrserwartung, ist sehr wohl sein Verantwortungsbereich eröffnet.[499] Dann fällt zwar der eigentliche Akt der Sabotage in den Zeitraum nach dem Inverkehrbringen, eine konstruktive Sabotageanfälligkeit haftete dem Produkt allerdings bereits bei Inverkehrgabe an, sodass nicht von einem späteren Entstehen des Fehlers gesprochen werden kann. Fehlt es an den erforderlichen und zumutbaren Sicherungsmaßnahmen, hat der Hersteller dadurch erst eine Gefahrenlage für nachträgliche Manipulationshandlungen Dritter geschaffen.[500]

Nach den eben dargelegten Grundsätzen im allgemeinen Deliktsrecht kommt eine Zurechnung der auch vorsätzlichen Dritthandlung aber erst dann in Betracht, wenn eine besondere Gefahrenlage geschaffen wurde, die über das allgemeine Lebensrisiko hinausgeht und bei der folglich nicht lediglich ein äußerer Zusammenhang zwischen der Handlung des Pflichtigen und des schädigenden Dritten besteht. Diese Kriterien sollen anhand der Lebensmittelbranche, in der Sabotagehandlungen ein leidliches Problem darstellen, beleuchtet werden.

Produkthaftungsrechtlich wird hier von den Herstellern gefordert, dass Verpackungen so gestaltet sind, dass ein spurenloses Öffnen und Schließen nicht möglich ist.[501] Freilich kann damit eine gewisse Basissicherheit jedenfalls vor plumpen Manipulationshandlungen gewährleistet werden. Die bloße Möglichkeit einer Manipulation nach Inverkehrgabe führt indes noch nicht zu einer Verantwortung des Herstellers, Sicherungsmaßnahmen zu ergreifen. Insofern muss konstatiert werden, dass vorsätzliche Produktmanipulationen nicht immer verhinderbar sind.[502] Betrachtet man perfide Produktmanipulation wie bspw. eine Vergiftung mittels Injektion durch die Verpackung, dürfte die fehlende Vermeidbarkeit gar der Regelfall sein.[503] Gerade im Lebensmittelbereich wird eine Zurechnung der

498 *Sprau*, in: Grüneberg, BGB, § 1 ProdHaftG, Rn. 17; *Ehring*, in: NK-ProdR, § 1 ProdHaftG, Rn. 70; *Förster*, in: BeckOK, BGB, § 1 ProdHaftG, Rn. 43.

499 *Wagner,* in: MüKo, BGB, § 1 ProdHaftG, Rn. 34; *Krause*, in: Soergel, BGB, § 823 Anh. III, Rn. 17; *Foerste*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 413.

500 So *Moseschus*, Risknews 2005, 69 (71).

501 *Wagner,* in: MüKo, BGB, § 1 ProdHaftG, Rn. 34.

502 Vgl. *Oechsler*, in: Staudinger, BGB, § 1 ProdHaftG, Rn. 85.

503 Ähnlich *Moseschus*, Risknews 2005, 69 (71).

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

Produktmanipulation nach dem Inverkehrbringen[504] bei Einhaltung der Basissicherheitsvorkehrungen regelmäßig scheitern. Daher kommt der Hersteller seiner Sicherungspflicht schon dann nach, wenn seine Maßnahmen wenigstens zu einer geringeren Manipulationsanfälligkeit beitragen und einen gewissen Schutz für Verbraucher bieten. In diesem Fall kann nicht davon gesprochen werden, dass dem Produkt die Sabotageanfälligkeit bereits bei Inverkehrgabe anhaftet. Da Täter mit entsprechender krimineller Energie jedes Produkt manipulieren können, liegt keine durch den Hersteller geschaffene besondere Gefahrenlage vor. Unter Zurechnungsgesichtspunkten knüpft das Handeln des Dritten nicht an eine unterlassene Sicherungsmaßnahme an, sondern stellt sich als den inneren Zusammenhang durchbrechendes eigenes Handeln dar. Vergegenwärtigt man sich, dass es die eine, ein solches Drittverhalten ausschließende Maßnahme gar nicht gibt, kommt eine Haftung nur ausnahmsweise dann in Betracht, wenn das gewählte Verpackungsdesign besonders sabotageanfällig und damit unverhältnismäßig gefährlich ist und vor diesem Hintergrund zur Opferauswahl beiträgt.[505] Dann kann tatsächlich von der Begründung einer besonderen Gefahrenlage gesprochen werden. In der analogen Produktwelt müssen die Hersteller folglich lediglich in speziellen Branchen rudimentären Sabotageschutz gewährleisten.[506]

(3) Übertragung auf Cyberangriffe

Bei der Übertragung der gewonnen Erkenntnisse auf die Frage der Herstellerverantwortung bei Cyberangriffen muss zwischen den einzelnen Angriffsszenarien differenziert werden.[507] Denn ein IT-System begründet aus sich heraus noch nicht zwangsläufig eine Gefahrenlage.[508] Es greift daher zu kurz, die Inverkehrgabe als relevante Schaffung einer Gefahrenquelle zu sehen und damit allein die Herstellerverantwortlichkeit zu begründen.[509]

504 Anders sieht dies freilich bei einer Manipulationshandlung vor dem Inverkehrbringen und damit in der Risikosphäre des Herstellers aus, vgl. *Schäfer*, in: BeckOGK, BGB, § 6 ProdHaftG, Rn. 24.
505 Vgl. *Moseschus*, Risknews 2005, 69 (72).
506 In diese Richtung auch *Foerste*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 413.
507 Hierfür plädiert auch *Wende*, in: Sassenberg/Faber (Hg.), Industrie 4.0 und Internet of Things, § 4, Rn. 46.
508 *Koch*, CR 2009, 485 (486).
509 So aber *Droste*, CCZ 2015, 105 (109).

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

α) Ausnutzen einer Sicherheitslücke

Zunächst soll ein Cyberangriff betrachtet werden, der eine in der Software vorhandene Sicherheitslücke ausnutzt.

i) Besondere Gefahrenlage und nicht lediglich äußerer Zusammenhang

Nun könnte man argumentieren, dass in der analogen Welt niemand auf die Idee gekommen wäre, „den Hersteller eines zerstörten Produkts dafür verantwortlich zu machen, dass ein Angreifer das Produkt zerstören konnte: Denn es ist nicht das Problem eines Reifenherstellers, wenn ein Täter den Reifen zersticht."[510]

Indes hinkt beim Programmierfehler der Vergleich zur Sabotage in der analogen Welt bereits im Ausgangspunkt. Denn ein Produkt, das einen Programmierfehler aufweist, ist bereits aus sich heraus besonders sabotageanfällig. Es ist gerade nicht so dass, ein Täter wie bei der herkömmlichen Produktsabotage jedes beliebige andere Produkt manipulieren könnte und die Gefahr daher einzig von ihm ausginge.[511] Im Vergleich zur Produktsabotage im Lebensmittelbereich ist es so, als ob die Produktverpackung bereits bei Inverkehrbringen eine Öffnung aufweist, durch die ein Täter Gift in das Produkt einbringen kann. Dies bedeutet jedoch, dass das betreffende Produkt bzw. sein Nutzer im Vergleich zu anderen Produkten gefahrenexponiert ist, ohne dass es auf das Ergreifen zusätzlicher Sicherungsmaßnahmen ankäme. Um bei dem Beispiel des zerstochenen Reifens zu bleiben: Es stehen keine Sicherungsmaßnahmen des Herstellers in Rede, den Reifen durch die Verwendung stichfester Materialien zu schützen. Vielmehr stellt ein bei Inverkehrbringen bestehender Programmierfehler schon ein offenes Einfallstor für Hacker dar.[512] Denn die Angriffsmethoden der Cyberkriminellen nutzen gerade diese Sicherheitslücke aus, um ihre Schadsoftware in das System einzuschleusen. Daher schafft der Hersteller mit einem

510 So *Klindt*, Hilft das Produkthaftungsgesetz gegen IT-Vandalismus?, Tagesspiegel Background, 21.11.2018: „Denn hinter englischen Umschreibungen wie Cyber-Attack oder Cyber-Resilience steckt doch nichts anderes als ein absichtlicher IT-Vandalismus. Der Angriff, die Störung oder gar die Übernahme der integrierten Software fällt ja nicht vom Himmel, sondern ist (koordinierte) Tat eines Angreifers"; zurückhaltend auch *Steege*, SVR 2023, 9 (14).

511 So zur herkömmlichen Produktsabotage *v. Bar*, in: Lieb (Hg.), Produktverantwortung und Risikoakzeptanz, S. 29 (45).

512 So auch *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 90.

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

Programmierfehler eine besondere und – in Anbetracht der tatsächlichen Fehleranfälligkeit von Software – softwaretypische Gefahrenlage. Erst die durch den Programmierfehler ausgelöste Sicherheitslücke gibt den Hackern die spezifische Gelegenheit zur Vornahme der schädigenden Handlung. Damit ist bei einer Sicherheitslücke, die auf einem Programmierfehler beruht, zwar auch das Dazwischentreten eines Dritten angesprochen, es geht aber weniger um das Gegensteuern mittels entsprechender Sicherungsmaßnahmen als vielmehr um das originäre fehlerfreie Programmieren und die entsprechende berechtigte Verkehrserwartung hieran. Hinzu kommt, dass sich der Nutzer anders als gegenüber herkömmlichen Vandalismustaten kaum schützen kann. Um das Reifenbeispiel erneut aufzugreifen: Ein Nutzer kann sein Fahrzeug vor dem Zerstechen der Reifen schützen, indem er es nachts in einer Garage abstellt oder bestimmte Orte meidet. Hinsichtlich einer vorhandenen Sicherheitslücke fehlt es dem Nutzer an der Kenntnis und Fähigkeit, diese zu schließen. Da der Zugriff auf smarte Produkte einfache und vor allem anonym und unbemerkt aus der Distanz erfolgen kann, hat der Nutzer hier auch nur geringe Möglichkeiten, sich selbst zu schützen.[513] Anders als für den Hersteller ist das aus einer Sicherheitslücke resultierende Risiko für den Nutzer somit nicht beherrschbar.

Dagegen betrifft eine durch einen architekturellen Fehler ausgelöste Sicherheitslücke das konzeptionelle Unterlassen von Schutzmechanismen. Für Hacker macht es indes keinen Unterschied, ob sie einen Programmierfehler oder einen architekturellen Fehler ausnutzen. In jedem Fall sind solche Produkte für Cyberkriminelle besonders interessant, die über eine Sicherheitslücke verfügen. Fehlen daher konzeptionelle Sicherungsmaßnahmen gänzlich, käme dies auch einem „Einladen" zur Vornahme von Cyberangriffen gleich.[514] Damit lässt aber der Hersteller den Nutzer ebenso gefahrexponiert zurück wie bei einem sicherheitsrelevanten Programmierfehler. Hinzu kommt, dass architekturelle Probleme häufig schwer zu beheben sind[515] und die Beherrschbarkeit der Gefahr daher maßgeblich von den vom Hersteller ergriffenen Schutzmaßnahmen abhängt. Letztendlich ist es allein der Hersteller, der durch sein Wissen und seinen Einfluss auf das Produktdesign in der Lage ist, einen effektiven Schutz vor Hackerangriffen

513 *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 90.

514 So *Wiebe*, InTer 2020, 66 (68) und *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 90 f.; ähnlich *Reusch*, in: Kaulartz/Braegelmann (Hg.), Artificial Intelligence und Machine Learning, S. 101.

515 *Sohr/Kemmerich*, in: Kipker (Hg.), Cybersecurity, Kap. 3, Rn. 164.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

zu ermöglichen.[516] Erneut kann auf die fehlende Selbstschutzmöglichkeit des Nutzers und die daraus resultierende fehlende Beherrschbarkeit des Risikos für ihn verwiesen werden. Insoweit ist der Hersteller nicht von seiner Haftung befreit, wenn es gerade ein Merkmal des Produkts ist, gegen derartige Eingriffe gesichert zu sein.[517] Vor dem Hintergrund der fehlenden Selbstschutzmaßnahmen ergibt sich aber eine Erwartung der Nutzer, dass der Hersteller die erforderlichen und zumutbaren Sicherungsvorkehrungen trifft, die eine Schädigung durch vorsätzliches Drittverhalten ausschließen.[518] In diesem Punkt ähneln sich Cyberattacken und Sabotagen in der Lebensmittelbranche; auch wenn in der Lebensmittelbranche eher als Ausnahme Sicherheitsvorkehrungen gegen Manipulationshandlungen geboten sind.

Mit einer Sicherheitslücke – unabhängig davon, worauf diese nun konkret beruht – haftet der Software damit bereits ab Inverkehrgabe eine latente Gefahr an, die nach dem Inverkehrbringen jederzeit von Hackern ausgenutzt werden kann.[519] Damit liegt aber auch ein nicht lediglich äußerer Zusammenhang zwischen der Inverkehrgabe eines Produkts mit Sicherheitslücken und dem Angriff des Hackers vor. Folglich kann auch nicht mehr von einem allgemeinen Lebensrisiko beim Einsatz vernetzter IoT-Geräte gesprochen werden. Angesichts der Häufigkeit von Cyberangriffen mag zwar ein allgegenwärtiges Gefährdungspotential vorhanden sein,[520] dies darf aber nicht darüber hinwegtäuschen, dass die Sicherheitslücke aus

516 *Wiebe*, ZRP 2023, 73 (74).

517 *Klindt* et al., in: Bräutigam/Klindt (Hg.), Digitalisierte Wirtschaft/Industrie 4.0, S. 76 (87); *Rockstroh/Kunkel*, MMR 2017, 77 (81).

518 *Gomille*, JZ 2016, 76 (78); *Martin/Uhl*, RAW 2020, 7 (11); *Haftenberger*, Die Produkthaftung für künstlich intelligente Medizinprodukte, S. 175; *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 103; i.E. auch *Zech*, DJT 2020 Gutachten, A S. 72.

519 *Spindler*, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, Rn. 119; *Spindler*, in Hornung/Schallbruch (Hg.), IT-Sicherheitsrecht, § 11, Rn. 24; *Wittig*, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 76; *Mehrbrey/Schreibauer*, MMR 2016, 75 (78).

520 *Libertus*, MMR 2005, 507 (509) folgert wohl allein hieraus das Bestehen eines allgemeinen Lebensrisikos beim Versenden virenverseuchter E-Mails; dagegen *Koch*, NJW 2004, 801 (803) und *Spindler*, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, Rn. 293, wonach mit der Einstufung als „übliche[m] Risiko" noch keine rechtliche Wertung verbunden sei. *Hossenfelder*, Pflichten von Internetnutzern zur Abwehr von Malware und Phishing, S. 153 weist darauf hin, dass die Infizierung mit Malware „in der Bevölkerung gerade nicht als erlaubtes Risiko hingenommen wird".

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

dem Verantwortungsbereich des Herstellers stammt und daher die Wahrscheinlichkeit der Rechtsgutsverletzung erhöht wurde. Da bei der aktuellen Bedrohungslage[521] jederzeit mit der Ausnutzung einer Sicherheitslücke zu rechnen ist, liegt auch ein innerer Zusammenhang zwischen den schadensursächlichen Handlungen vor. Diese Erkenntnis verschärft sich dadurch, dass es keine schlechthin für Cyberangriffe unbedeutenden Produkte mehr gibt. Durch die Vernetzung kann jedes Produkt Ausgangspunkt für einen weitergehenden Cyberangriff sein.[522] Mithin handelt es sich dabei um eine naheliegende Gefahr.

ii) Umfang der zu gewährleistenden IT-Sicherheit

Die Tatsache, dass ein Cyberangriff unter Ausnutzung von Sicherheitslücken die Verantwortlichkeit des Herstellers nicht ausschließt und folglich eigene Verkehrssicherungspflichten bestehen, sagt allerdings noch nichts über deren Inhalt und Umfang aus. Maßgeblich ist auch hier wieder die berechtigte Verkehrserwartung.[523] Da es sich bei der Sicherheitslücke um einen Unterfall des Softwarefehlers handelt, kann unter Berücksichtigung einiger Besonderheiten auf obige Ausführungen zurückgegriffen werden. Normative Aufladung findet die berechtigte Verkehrserwartung im Bereich der IT-Sicherheit zudem durch das bereits erwähnte IT-Grundrecht.[524] Dessen mittelbare Wirkung im Privatrechtsverkehr schlägt sich in der Konkretisierung von Sorgfaltsanforderungen nieder und fordert insbesondere von den Herstellern die Beachtung von Sicherheitsmaßnahmen, um die Vertraulichkeit und Integrität von IT-Systemen Dritter nicht zu gefährden.[525] Diese grundrechtliche Verankerung führt aber weder dazu, dass die konkrete Haftungsverteilung bzw. die Intensität der zu ergreifenden Sicherungsmaßnahmen bereits determiniert wären[526] noch dazu, dass die

521 Vgl. *Bundesamt für Sicherheit in der Informationstechnik (BSI)*, Sicherheitsbericht 2022, S. 11.

522 Hierzu *Roos/Schumacher*, MMR 2014, 377 (378).

523 Vgl. auch *Koch*, NJW 2004, 801 (804); *Wiebe*, InTer 2020, 66 (68).

524 *Roßnagel/Schnabel*, NJW 2008, 3534 (3536): „Was in diesem [„Informationsverkehr"] Sicherheit bedeutet, wird künftig auch durch das neue Grundrecht bestimmt".

525 *Roßnagel/Schnabel*, NJW 2008, 3534 (3536); *Wiesemann/Mattheis/Wende*, MMR 2020, 139 (143) „Mitwirkung an der Integrität von IT-Produkten".

526 Zu Recht *Hossenfelder*, Pflichten von Internetnutzern zur Abwehr von Malware und Phishing, S. 179.

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

berechtigte Verkehrserwartung soweit geht, dass sicherheitsrelevante IT-Schwachstellen absolut vermieden werden müssten.[527] So wie man zur Absicherung des eigenen Hauses zwar verschiedene Schutzmaßnahmen wie eine stabile Haustür, eine Alarmanlage, vergitterte Fenster usw. ergreifen kann, es aber dennoch kein vollkommen einbruchssicheres Haus gibt, verhält es sich auch mit sicherheitsrelevanten Schwachstellen in der IT.[528] Eine absolute Haftung für Schäden, die durch Angriffe von Hackern verursacht werden, besteht daher nicht. Geschuldet ist nach allgemeinen Grundsätzen die Sorgfalt im Rahmen des Möglichen und Zumutbaren.[529]

Es geht vielmehr darum, solche Sicherheitsvorkehrungen zu treffen, dass ein möglicher Angriff aufgrund des verbundenen Aufwands nicht mehr rentabel ist. Dabei ist im Rahmen der Softwareentwicklung auch einer in der Praxis eingerissenen Nachlässigkeit entgegenzuwirken. Denn gerade bei IoT-Geräten ist die IT-Sicherheit lange Zeit als aufschiebbar betrachtet worden. Um Verzögerungen bei der Markteinführung zu vermeiden, wurde die bewusste Entscheidung getroffen, Sicherheitslücken erst im Nachhinein mittels Updates zu schließen. Dies hat aber zur Konsequenz, dass Schadensfälle bereits eintreten konnten.[530] Ein solches Vorgehen wird der berechtigten Verkehrserwartung nicht gerecht. Vielmehr ist zu verlangen, dass nach dem Konzept „security by design" die IT-Sicherheit als Anforderung in den gesamten Entwicklungsprozess einbezogen wird.[531]

527 Speziell in Bezug auf Hacker-Angriffe *Wagner*, AcP 217 (2017), 707 (727); *Wagner*, in: MüKo, BGB, § 3 ProdHaftG, Rn. 35; *Steege*, in: Buck-Heeb/Oppermann (Hg.), Automatisierte Systeme, S. 367 (385); *Haagen*, Verantwortung für Künstliche Intelligenz, S. 266.

528 Diesen Vergleich zieht *Siglmüller*, ZfPC 2023, 221 (222).

529 Vgl. nur *Oster*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 57, Rn. 21; *Wagner*, AcP 217 (2017), 707 (727 f.); *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 105; *Thöne*, Autonome Systeme, S. 223, 226; *Hinze*, Haftungsrisiken des automatisierten und autonomen Fahrens, S. 131 f.

530 Vgl. hierzu *Schlotthauer/Schmitz*, Security und Privacy by Design und Default, Security Insider, 11.02.2019; vgl. auch *Riehm*, in: Schmidt-Kessel/Kramme (Hg.), Geschäftsmodelle in der digitalen Welt, S. 201 (204) „Bananen-Software", „reift beim Kunden".

531 *Heckmann/Paschke*, in: Bräutigam/Kraul (Hg.), Internet of Things, § 10, Rn. 116; *Wiebe*, InTer 2020, 66 (68); wohl auch *Böck/Theurer*, BB 2021, 520 (522).

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

iii) Haftungsrelevante Konstellationen

Für die Haftung des Herstellers für Schäden, die durch die Ausnutzung von Sicherheitslücken im Zuge von Cyberangriffen entstehen, ergibt sich damit folgendes Bild:

Lag bereits bei Inverkehrgabe eine Sicherheitslücke vor, die dann durch eine bekannte Schadsoftware ausgenutzt wurde, kann von einem produkthaftungsrechtlich relevanten Fehler gesprochen werden, es sei denn die Vermeidung der Sicherheitslücke war mit unverhältnismäßigem Aufwand verbunden und die Basissicherheit ist gleichwohl gewährleistet.[532] Erfolgt die sabotageähnliche Einwirkung eines Dritten trotz Einhaltung des „security by design"-Ansatzes und damit trotz Inverkehrbringens eines unter security Gesichtspunkten fehlerfreien Produkts, trifft den Hersteller keine Haftung (vgl. auch § 1 Abs. 2 Nr. 2 ProdHaftG).[533] Daher wird eine scharfe Abgrenzung vorzunehmen sein, ob das Produkt bzw. die Software zum Zeitpunkt des Inverkehrbringens dem verfügbaren Stand von Wissenschaft und Technik entsprach und der Angriff dennoch erfolgen konnte oder ob ein Angriff durch das Unterlassen möglicher Schutzmaßnahmen erst ermöglicht wurde.[534]

Hiervon sind Fälle abzugrenzen, bei denen zwar auch bei Inverkehrgabe eine Sicherheitslücke vorlag, zu der aber noch keine Schadsoftware existierte. Entdeckt ein Angreifer diese Sicherheitslücke und entwickelt einen neuen Schadcode, spricht man von einem Zero-Day-Exploit.[535] Für die rechtliche Einordnung muss differenziert werden: War die Sicherheitslücke erkennbar, hätten also gängige Qualitätssicherungsmaßnahmen bei der Programmierung den Angriff durch den Schadcode verhindern können, liegt grundsätzlich ein relevanter Fehler vor. Dies muss auch dann gelten, wenn der Schadcode erst nach der Inverkehrgabe bekannt wurde. Denn eine Sicherheitslücke kann nicht erst dann als Fehler gelten, wenn ein dafür

532 Beispiele bei *Deusch/Eggendorfer*, DSRITB 2015, 833 (837); a.A. *Sessa-Jahn*, Automatisiertes Fahren, S. 173 f., welche zwar statuiert, dass die Sicherheitslücken nach Stand von Wissenschaft und Technik hätten erkannt werden können, ein Auffinden der Sicherheitslücke aber undifferenziert für zu aufwendig hält. Sie setzt sich damit dem Verdacht aus, der Sichtweise „Software könne nie fehlerfrei sein" zu folgen.

533 So *Reusch*, in: Kaulartz/Braegelmann (Hg.), Artificial Intelligence und Machine Learning, S. 134.

534 *Reusch*, RDi 2023, 152 (158).

535 Vgl. *Lapp*, in: Kipker (Hg.), Cybersecurity, Kap. 10, Rn. 119.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

passender Schadcode verfügbar ist.[536] Eine solche Sichtweise würde verkennen, dass das dem Hersteller vorwerfbare Verhalten in der unzureichenden Programmierung liegt und die so hervorgebrachte Sicherheitslücke erst die besondere Gefahrenlage für den Cyberangriff mittels Schadsoftware schafft.[537] War es dagegen schon nicht möglich die Sicherheitslücke als solche zu erkennen, liegt ein die Haftung ausschließender Entwicklungsfehler vor.[538] Maßgeblich dabei ist nicht, ob die konkrete Schwachstelle als solche schon bekannt ist. Denn auch erstmals programmierte, aber durch Qualitätssicherungsmaßnahmen aufdeckbare Sicherheitslücken stellen relevante Fehler dar.

Eine dritte Fallgruppe bilden neu entwickelte Angriffstechniken, welche keine bereits bei der Inverkehrgabe in der Software bestehende Sicherheitslücke ausnutzen, sondern eine solche erst nachträglich schaffen. Bietet die Software gegen diese neuen Angriffstechniken, die zum Zeitpunkt des Inverkehrbringens noch nicht denkbar waren – z.B. neue kryptographische Verfahren, die eine ursprünglich sichere Verschlüsselung nun angreifbar machen – keine ausreichende Sicherheit, kann grundsätzlich keine Fehlerhaftigkeit angenommen werden.[539] Denn das Produkt entsprach bei Inverkehrgabe den historischen Sicherheitserwartungen. Etwas anderes könnte nur dann angenommen werden, wenn die technische Entwicklung neuer Angriffsmethoden bei dem Inverkehrbringen derart vorhersehbar gewesen wäre, dass deren konstruktive Berücksichtigung schon im Vorfeld erwarten werden konnte.[540] Bloße Vermutungen, dass ein Produkt späteren Anforderungen nicht mehr genügen könnte, reichen freilich nicht. Zumal auch in

536 Zum Sachmangel *Deusch/Eggendorfer*, in: Taeger/Pohle (Hg.), Computerrechts-Handbuch, Teil 5, Rn. 452; ebenso *Lapp*, in: Kipker (Hg.), Cybersecurity, Kap. 10, Rn. 119.

537 Anders aber *Sessa-Jahn*, Automatisiertes Fahren, S. 175, welche die Bekanntheit der Schadsoftware als maßgeblich ansieht.

538 *Spindler*, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, Rn. 123; *Spindler*, NJW 2004, 3145 (3146); *Rockstroh*, DSRITB 2016, 279 (289).

539 *Wiesner*, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 10.6, Rn. 45; *Sessa-Jahn*, Automatisiertes Fahren, S. 175 f., welche aber in Fn. 1099 eine Instruktionspflicht anspricht; zum Vertragsrecht *Raue*, NJW 2017, 1841 (1843); ebenso *Marly*, Praxishandbuch Softwarerecht, Rn. 1528 und *Lapp*, in: Kipker (Hg.), Cybersecurity, Kap. 8, Rn. 119; implizit auch *Riehm/Leithäuser/Brenner*, in: Raue (Hg.), Digitale Resilienz, S. 5 (19 f.).

540 So zum Kaufrecht *Riehm*, in: Schmidt-Kessel/Kramme (Hg.), Geschäftsmodelle in der digitalen Welt, S. 201 (213); *Marly*, Praxishandbuch Softwarerecht, Rn. 1496 nimmt dies an, wenn mit der Innovation in einem deutlich kürzeren Zeitraum zu rechnen ist als dem zu erwartende Nutzungszeitraum.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

technischer Hinsicht eine solch künftige Sicherheitslücke nicht hinreichend konkret wäre, um bereits bei Inverkehrgabe eine antizipierende Produktentwicklung zu begründen.[541]

β) Social Engineering-Angriff

Von der Ausnutzung einer Sicherheitslücke muss ein Cyberangriff unterschieden werden, der sich des Social-Engineerings bedient.

i) Besondere Gefahrenlage

Hier bringt der Hersteller ein grundsätzlich sicheres Produkt in den Verkehr, bei dem der Hackerangriff erst durch eine Mitwirkungshandlung des Nutzers ermöglicht wird. Es ist daher fraglich, ob von einer besonderen Gefahr gesprochen werden kann, die der Hersteller mit der Inverkehrgabe des Produkts geschaffen hat. Denn es wird eben kein der unmittelbaren Sphäre des Herstellers zuzuordnender Programmierfehler ausgenutzt, sondern eine Unachtsamkeit des Nutzers. Allerdings handelt es sich beim Social Engineering um eine allgegenwärtige Gefahr, sodass die Inverkehrgabe eines Produkts ohne Mindestschutzmaßnahmen durch den Hersteller den Nutzer wiederum gefahrenexponiert zurücklässt. Fehlen Maßnahmen gänzlich, die dem Social Engineering entgegenwirken, werden Cyberkriminelle auch hier zu Angriffshandlungen eingeladen. In diesem Fall kann – vergleichbar zur Produktmanipulation bei einem besonders sabotageanfälligen Verpackungsdesign – von einem Beitrag zur Opferauswahl gesprochen werden. Unterlässt der Hersteller daher solche Basisschutzmaßnahmen, begründet er eine besondere Gefahrenlage für den Nutzer, die sich aus der unverhältnismäßigen Exposition gegenüber den Cyberkriminellen ergibt.

ii) Umfang der zu gewährleistenden IT-Sicherheit

Wiederum schließt sich die Frage des Umfangs und der Intensität der Sicherungspflicht an. Spätestens beim Phänomen des Social Engineerings zeigt sich, dass das erforderliche Maß an IT-Sicherheit nur durch das Zu-

541 *Kipker/Walkusz*, DuD 2019, 513 (514 f.).

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

sammenwirken aller Beteiligten erreicht werden kann.[542] Dass es sich bei der Gewährleistung der IT-Sicherheit um eine gemeinsam zu bewältigende Aufgabe handelt, muss sich daher auch bei der Bestimmung der Verkehrssicherungspflichten niederschlagen.[543] Daher ist dem allgemeinen Grundsatz, dass eigene Sorgfaltsmaßnahmen nur bis zu dem Punkt zu ergreifen sind, bis ein anderer die Gefahr mit weniger Aufwand steuern kann, besondere Beachtung zu schenken. Vor diesem Hintergrund ist es klar, dass der Nutzer mit hinreichender Sensibilisierung und sorgfältiger Prüfung Social-Engineering-Angriffe eigens erkennen und abwenden kann.[544] Es ist daher der Nutzer, der die vom Hersteller geschaffene Gefahrenlage nochmals erhöht und den Cyberangriff erst ermöglicht. Vor dem Hintergrund der breiten Gefährdungslage muss aber stets mit dem „Faktor Mensch" gerechnet werden und einkalkuliert werden, dass Angriffe von Nutzern übersehen werden. Hinzu kommt, dass sich zwar ein Wandel in der Beziehung der Nutzer zur Technik ergibt und auch diese IT-spezifische Gefahren besser abschätzen können,[545] aber ein immer noch sehr heterogener Nutzerkreis auf einen schnelllebigen IT-Sektor mit sich wandelenden Gefahrenpotentialen trifft.[546] Es ist daher Aufgabe des Herstellers, durch Voreinstellungen eine gewisse Sicherheit in dem Produkt zu integrieren („security by default").[547] Zum einen sollen dadurch Angriffe bereits im Vorfeld, also bevor der Nutzer damit überhaupt in Berührung kommt, abgewendet werden. Dazu können Blocklisten bei Webbrowsern oder Spamschutz-Einstellungen implementiert werden. Zum anderen soll es dem Nutzer erleichtert werden, relevante Selbstschutzmaßnahmen zu ergreifen.[548] Hierzu kann die Aufforderung gehören, ein ausreichend sicheres Passwort zu wählen und auch nur ein solches zu akzeptieren. Bei den Maßnahmen kann es entsprechend den Verantwortungssphären nicht darum gehen, Social-Engineering-Angriffe

542 So *Rockstroh/Kunkel*, MMR 2017, 77 (78) in Anlehnung an den Gesetzentwurf zum BSIG, vgl. BR-Drs. 134/90, S. 1; ebenso *Wende*, in: Sassenberg/Faber (Hg.), Industrie 4.0 und Internet of Things, § 4, Rn. 54; *Roos/Schumacher*, MMR 2014, 377 (383) sehen die Einbeziehung des Nutzers als wichtigen Baustein an; *Riehm/Meier*, MMR 2020, 571 (573 f.) plädieren dafür, auch dem Nutzer mehr Maßnahmen zuzumuten.

543 *Rockstroh*, DSRITB 2016, 279 (288).

544 *Sohr/Kemmerich*, in: Kipker (Hg.), Cybersecurity, Kap. 3, Rn. 180.

545 Hierauf weisen *Riehm/Meier*, MMR 2020, 571 (574) hin.

546 Hierzu *Spindler*, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, Rn. 284.

547 *Heckmann/Paschke*, in: Bräutigam/Kraul (Hg.), Internet of Things, § 10, Rn. 117; in diese Richtung auch *Böck/Theurer*, BB 2021, 520 (522).

548 *Thöne*, Autonome Systeme, S. 227.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

gänzlich zu verhindern, sondern lediglich darum, diese zu erschweren und durch eine geringere Anfälligkeit nicht zur Opferauswahl beizutragen.

γ) DDoS-Angriff

Eine weitere Fallgruppe bilden DDoS-Angriffe. Die Besonderheit dieser Angriffe liegt darin, dass smarte Produkt nicht unmittelbar selbst attackiert werden, sondern es sich um einen Angriff unter Zuhilfenahme infizierter Systeme auf die Verfügbarkeit eines Webservers, eines Webdienstes oder eines Netzwerkes handelt. Ist das smarte Produkt aber auf die digitale Infrastruktur, die nunmehr durch den Angriff lahmgelegt worden ist, angewiesen, führt dies mittelbar zu negativen Auswirkungen. Auch in dieser Konstellation bringt der Hersteller ein grundsätzlich sicheres Produkt in den Verkehr, das aber aufgrund der durch die Vernetzung geschaffenen Abhängigkeiten anfällig bei Störungen der digitalen Infrastruktur ist. Fraglich ist daher, ob und welche Sicherungsmaßnahmen der Hersteller an seinem Produkt für den Fall treffen muss, dass die digitale Infrastruktur, auf die sein Produkt zurückgreift, nicht erreichbar ist. Angesprochen ist damit schon das Vernetzungsrisiko. Hierauf ist sogleich einzugehen.

e) Künftige normative Berücksichtigung der Cybersicherheit

Da sich im Bereich von Software security und safety gar nicht mehr voneinander trennen lassen, treffen sie sich zu einem einheitlichen Begriff von Informationssicherheit als Anforderung des Produkthaftungsrechts. Auch die Zurechnung eines schädigenden Verhaltens Dritter in Form eines Cyberangriffs wird regelmäßig erfolgen, so dass es eine sicherheitsrelevante Produkteigenschaft darstellt, Schutz gegen solche Eingriffe zu bieten. Dieses Verständnis wird künftig ohnehin nicht mehr in Zweifel zu ziehen sein, da diverse gesetzliche Regelungen der Cybersicherheit größere Bedeutung beimessen werden.[549]

Als sektorale Rechtsvorschrift ist zunächst die Funkanlagenrichtlinie (im Folgenden „RED“)[550] und eine von der EU-Kommission am 29.10.2021

549 Zu den Tendenzen, Cybersecurity in den Kanon der berechtigten Sicherheitserwartungen aufzunehmen auch *Klindt*, DAR 2023, 7 (9).

550 Richtlinie 2014/53/EU.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

erlassene delegierte Verordnung zur RED[551] hinsichtlich bestimmter Funkanlagen zu nennen, die ab dem 01.08.2025 in den Verkehr gebracht werden. Danach dürfen mit dem Internet verbundene Funkanlagen weder schädliche Auswirkungen auf das Netz oder seinen Betrieb haben noch eine missbräuchliche Nutzung von Netzressourcen bewirken (gemäß Art. 3 Abs. 3 lit. d RED). Aufgrund des weit gefassten Anwendungsbereichs ist die Bedeutsamkeit und Tragweite der delegierten Verordnung in der Praxis nicht zu unterschätzen.[552] In diesem Zusammenhang darf künftig die Erarbeitung harmonisierter Normen erwartet werden, mithilfe derer die Hersteller die Einhaltung der neu vorgeschriebenen Produktanforderungen nachweisen und von der Konformitätsvermutung gem. Art. 16 und Art. 17 Abs. 3 RED profitieren können.[553] Damit würden erstmals die IT-Sicherheit betreffende Standards verbindliche Grundlage und Voraussetzung einer CE-Kennzeichnung.

Vom Schutzbereich auf die Gesundheit und Sicherheit von Verbrauchern zielt die neue und bereits am 12.06.2023 in Kraft getretene Produktsicherheitsverordnung (im Folgenden „GPSR")[554] ab, die ab dem 13.12.2024 gilt. Nach Art. 5 GPSR dürfen nur sichere Produkte in den Verkehr gebracht werden. Bei der entsprechenden Beurteilung sind nach Art. 6 Abs. 1 lit. g GPSR nunmehr explizit auch angemessene Cybersicherheitsmerkmale zu berücksichtigen, die erforderlich sind, um das Produkt vor äußeren Einflüssen, einschließlich böswilliger Dritter, zu schützen, sofern sich ein solcher Einfluss auf die Sicherheit des Produkts auswirken kann.[555] Mit dieser horizontalen Regelung soll sichergestellt werden, dass auch außerhalb sektorspezifischer Rechtsvorschriften die Gesundheit und Sicherheit von Verbrauchern nicht durch Cybersicherheitsrisiken beeinträchtigt wird, vgl. Erwägungsgrund (26) GPSR. Allerdings werden Produktrisiken für die Datensicherheit oder die Privatsphäre der Nutzer nicht adressiert.[556]

Daneben soll auch der Cyber Resilience Act (im Folgenden „CRA")[557] produkt- und branchenübergreifend gewährleisten, dass die Rahmenbedin-

551 Delegierte Verordnung (EU) 2022/30.
552 So *Böck/Reinsberg*, ZfPC 2022, 126 (129); ähnlich *Hessel/Callewaert*, DB 2022, 2589 (2590).
553 Hierauf weisen *Böck/Reinsberg*, ZfPC 2022, 126 (129) hin.
554 Verordnung (EU) 2023/988.
555 Vgl. auch Erwägungsgrund (25) GPSR.
556 Vgl. auch *Ackermann/Golling*, ZfPC 2022, 67 (68).
557 Die Arbeit basiert auf dem Standpunkt des Europäischen Parlaments festgelegt in erster Lesung am 12.3.2024 im Hinblick auf den Erlass der Verordnung (EU) 2024/... des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsan-

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

gungen für die Entwicklung sicherer Produkte mit digitalen Elementen geschaffen werden, damit Hardware- und Softwareprodukte mit weniger Schwachstellen in Verkehr gebracht werden und damit sich die Hersteller während des gesamten Lebenszyklus eines Produkts konsequent um die Sicherheit kümmern, vgl. Erwägungsgrund (2) CRA.[558] So darf ein Produkt nach Art. 13 Abs. 1 CRA nur in Verkehr gebracht werden, wenn es die grundlegenden Cybersicherheitsanforderungen nach Anhang I Teil 1 CRA erfüllt. In seiner Konkretisierung geht der CRA dabei weit über die neue GPSR hinaus. Sowohl der Ansatz security by design als auch security by default werden aufgegriffen. Weiter muss ein Produkt ohne bekannte ausnutzbare Schwachstellen ausgeliefert werden und durch geeignete Kontrollmechanismen Schutz vor unbefugtem Zugriff bieten. Daneben ist explizit auch die Vertraulichkeit und Integrität von Daten zu schützen.

Speziell für Hochrisiko-KI-Systeme[559] sieht die am 01.08.2024 in Kraft und nach Art. 113 KI-VO ab dem 02.08.2026 geltende KI-Verordnung (im Folgenden „KI-VO)[560] vor, dass diese gem. Art. 15 Abs. 1, Abs. 5 KI-VO so entwickelt und konzipiert werden müssen, dass ein angemessenes Maß an Cybersicherheit erreicht wird und die Systeme diesbezüglich auch während ihres gesamten Lebenszyklus beständig funktionieren.[561] Insoweit sieht Art. 12 CRA eine Verzahnung der Cybersicherheitsanforderungen vor. Denn gem. Art. 12 Abs. 1 CRA gilt ein Hochrisiko-KI-System hinsichtlich der Cybersicherheitsanforderungen nach Art. 15 KI-VO konform, wenn es die grundlegenden Anforderungen des CRA erfüllt (vgl. auch Erwägungsgrund (77) KI-VO).

Kfz sind indes gem. Art. 2 Abs. 2 lit. c CRA (vgl. auch Erwägungsgrund (27) CRA) vom Anwendungsbereich des CRA ausgenommen. Nach Art. 4 Abs. 5 i.V.m. Anhang II, D4 VO (EU) 2019/2144 zur Kfz-Typgenehmigung müssen neue Fahrzeugtypen aber bereits seit Juli 2022 und seit Juli 2024

---

forderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2019/1020 (Cyberresilienz-Verordnung). Da sich das Europäische Parlament und der Rat bereits im Vorfeld vorläufig auf die finale Fassung des Verordnungstextes geeinigt hatten, ist von einer Zustimmung des Rats noch im Jahr 2024 auszugehen. Geltung beanspruchen die Vorschriften dann gem. Art. 71 Abs. 2 CRA grundsätzlich 36 Monate nach dem Inkrafttreten.

558 Dazu auch Art. 2 lit. b, lit. c CRA; ferner *Kipker*, MMR-Aktuell 2022, 452009; *Kipker*, in: Kipker (Hg.), Cybersecurity, Kap. 1, Rn. 30.

559 Vgl. zur entsprechenden Einstufung Art. 6 KI-VO.

560 Verordnung (EU) 2024/1689.

561 Vgl. auch Erwägungsgründe (74) und (76) KI-VO.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

sämtliche Neufahrzeuge[562] gegen Cyberangriffe geschützt sein. Hinsichtlich der bestimmten Anforderungen wird auf die UN-Regelung Nr. 155 verwiesen.[563] Dabei ist gem. Ziff. 7.3.1 UN-Regelung Nr. 155 für die Erteilung der Typengenehmigung eine Konformitätsbescheinigung über ein zu implementierendes Cybersicherheitsmanagementsystems („CSMS") erforderlich. Anhang 5 der UN-Regelung Nr. 155 listet exemplarisch Risiken (Bedrohungen, Schwachstellen und Angriffsmethoden) sowie mögliche zu ergreifende Minderungsmaßnahmen auf, die bei der Ausgestaltung des CSMS berücksichtigt werden sollten, vgl. Ziff. 7.2.2.2 UN-Regelung Nr. 155. Gegen die ermittelten Risiken ist das Fahrzeug gem. Ziff. 7.3.4 zu schützen. Die Implementierung der geeigneten Cybersicherheitsmaßnahmen bei der Konzeption des Fahrzeugtyps wird von der Genehmigungsbehörde geprüft, vgl. Ziff. 5.1.1 lit. c, Ziff. 5.1.2 UN-Regelung Nr. 155.

In haftungsrechtlicher Hinsicht sieht Art. 7 Abs. 2 lit. f ProdHaftRL vor, dass bei der Bestimmung der Fehlerhaftigkeit eines Produkts auch die sicherheitsrelevanten Cybersicherheitsanforderungen zu berücksichtigen sind. Auch hier erfolgt eine Verzahnung mit den grundlegenden Sicherheitsanforderungen des CRA, welche bei der Bestimmung der Fehlerhaftigkeit eines Produkts heranzuziehen sind. Denn gem. Art. 10 Abs. 2 lit. b ProdHaftRL wird bei einem Verstoß gegen verbindliche Anforderungen der Produktsicherheit die Fehlerhaftigkeit des Produkts vermutet. In diesem Sinne ist auch die Einhaltung harmonisierter Standards oder die Erlangung eines Cybersicherheitszertifikats nach dem CSA zu berücksichtigen, da diese eine Konformitätsvermutung nach Art. 27 Abs. 1, Abs. 8 CRA begründen.[564] Weiter stellt Erwägungsgrund (55) ProdHaftRL explizit klar, dass im Interesse des Verbraucherschutzes bei einer ausnutzbaren Schwachstelle, die das Produkt weniger sicher macht als von der breiten Öffentlichkeit berechtigterweise erwartet, die Haftung des Herstellers nicht aufgrund solcher Handlungen oder Unterlassungen Dritter gemindert werden oder entfallen soll. Daneben bezieht Art. 6 Abs. 1 lit. c ProdHaftRL auch den Verlust oder

562 Dies zwingt deutsche Autobauer zur Einstellung diverser Produktreihen, VW-Markenchef Thomas Schäfer: „Wir müssten da sonst noch einmal eine komplett neue Elektronik-Architektur integrieren" […] Das wäre schlichtweg zu teuer.", vgl. https://www.faz.net/aktuell/wirtschaft/neue-eu-huerde-fuer-neuwagen-laesst-modellpalette-schrumpfen-19596698.html (zuletzt abgerufen am 23.09.2024).

563 Ausführlich *Seufert*, CR 2023, 73 (75 ff.).

564 Zum Ganzen *Brenner*, RDi 2024, 345 (350 f.).

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

Verfälschung von Daten, die nicht ausschließlich für berufliche Zwecke verwendet werden, in den Schutzbereich der Haftung mit ein.[565]

f) Bedeutung für die Produktbeobachtung

Treffen den Hersteller auf der Ebene der Konstruktion entsprechende Pflichten zur Gewährleistung der IT-Sicherheit, muss auch eine Produktbeobachtungspflicht für smarte Produkte hinsichtlich dieser Gefahren bestehen.[566] Leidet ein Produkt bereits ab Inverkehrgabe an einem die IT-Sicherheit betreffenden Fehler, weil etwa die Konzepte security by design und security by default nicht umgesetzt wurden, liegt ohne Weiteres ein Fall der Produktbeobachtungspflicht vor. Gleiches gilt im Falle eines Entwicklungsfehlers bei einer nicht erkennbaren Zero-Day-Schwachstelle.[567] Betrachtet man dies vor dem Hintergrund der Allgegenwärtigkeit von Softwarefehlern auf der einen Seite und von Schadsoftware auf der anderen Seite, kann auch hier Rufen der Literatur nach einer intensiven Produktbeobachtung zugestimmt werden.[568] In diesem Zusammenhang fordert der CRA künftig in Anhang I Teil 2 Abs. 3, dass die Sicherheit des Produkts mit digitalen Elementen im Hinblick auf Schwachstellen regelmäßig und wirksam zu testen und zu überprüfen ist. Der Fokus des CRA liegt dann darauf, dass im Falle einer entdeckten Schwachstelle Korrekturmaßnahmen ergriffen werden können (vgl. Art. 13 Abs. 8, Abs. 6 CRA).

Schwieriger stellt sich dagegen die Lage hinsichtlich neu entwickelter Cyberangriffe dar.[569] Haben Hacker erstmalig Möglichkeiten gefunden, bestehende und bisher dem Stand von Wissenschaft und Technik entsprechende Schutzmechanismen zu umgehen, führt dies zu einer geänderten Bedrohungslage. So kann ein Produkt, das bei dem Inverkehrbringen den seinerzeit gängigen Verschlüsselungsstandards entsprach und daher sicher war, durch die Entwicklung neuer Decodierungsprogramme zu einem un-

565 Vgl. auch Erwägungsgrund (20) ProdHaftRL; auch *Brenner*, RDi 2024, 345 (349).
566 So auch *Hartmann*, in: Knappertsbusch/Gondlach (Hg.), Arbeitswelt und KI 2030, S. 63 (66).
567 Explizit auch *Sessa-Jahn*, Automatisiertes Fahren, S. 214.
568 So *Klindt* et al., in: Bräutigam/Klindt (Hg.), Digitalisierte Wirtschaft/Industrie 4.0, S. 76 (87 f.); *Droste*, CCZ 2015, 105 (106); *Spindler*, NJW 2004, 3145 (3147).
569 So auch *Wende*, in: Sassenberg/Faber (Hg.), Industrie 4.0 und Internet of Things, § 4, Rn. 48.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

sicheren Produkt werden.[570] Damit könnte aber die Fallkonstellation der „Produktalterung" angesprochen sein, für die den Hersteller nach der hier vertretenen Auffassung keine Verantwortlichkeit nach der Inverkehrgabe trifft.

Jedenfalls kann im Hinblick auf eine Gefahr, die bei Inverkehrgabe noch gar nicht bestand, nicht von einer Entwicklungslücke die Rede sein. Andererseits liegt auch keine klassische Fallkonstellation der „Produktalterung" vor. Diese betrifft nämlich die technische Weiterentwicklung im Sinne einer kontinuierlichen Verbesserung der Produktserie. Dadurch werden die bereits vermarkteten Produkte aber nicht unsicherer als bei ihrem Inverkehrbringen. Sie genügen lediglich den geänderten und nunmehr anzulegenden Sicherheitsanforderungen nicht mehr. Bei neuen Angriffstechniken handelt es sich um eine gegenläufige Entwicklung. Diese führen nämlich dazu, dass Sicherheitslücken nachträglich entstehen und das Produkt unsicherer als bei seiner Inverkehrgabe wird. Da in beiden Fällen die ursprünglichen Sicherheitserwartungen erfüllt wurden, die durch äußere Umstände geänderten Sicherheitserwartungen dagegen nicht mehr erreicht werden, ist gleichwohl eine einheitliche Betrachtung angezeigt. Entscheidend ist, dass es sich bei der Weiterentwicklung von Angriffstechniken nicht um immanente Produktgefahren, sondern um äußere Umstände handelt und der Hersteller daher nicht schon bei Inverkehrgabe ein Gefahrenlevel begründet hat, das eine nachträgliche Verantwortung rechtfertigen würde.[571]

570 Vgl. *Schrader/Engstler*, MMR 2018, 356 (357); *Kipker/Walkusz*, DuD 2019, 513 (514); *Wurm*, Automotive Cybersecurity, S. 72.

571 I.E. auch zurückhaltend *Steege*, SVR 2023, 9 (14): „gilt es zu beachten, dass nach Inverkehrgabe ein Zeitpunkt erreicht sein wird, an dem ein Produkt gehackt werden kann"; ähnlich *Klindt* et al., in: Bräutigam/Klindt (Hg.), Digitalisierte Wirtschaft/Industrie 4.0, S. 76 (86): Die kontinuierliche Fortentwicklung darf „nicht zu einer stetigen Nachbesserungs- und Nachlieferungspflicht der Softwarehersteller führen". Zwar wird damit schon die Reaktion angesprochen, *Spindler*, MMR 2008, 7 (12) weist in diesem Kontext aber darauf hin, dass man ansonsten über das allgemeine „Ziel einer effizienten Zuweisung von Risiken in erheblichem Maße hinausschießen würde"; tendenziell a.A. jedenfalls bei einer zu erwartenden Änderung des nach der Verkehrsanschauung erforderlichen Standards im Hinblick auf die IT-Sicherheit nach der Inverkehrgabe *Heckmann/Paschke*, in: Bräutigam/Kraul (Hg.), Internet of Things, § 10, Rn. 81.

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

3. Vernetzung

a) Tatsächliche Herausforderung

Durch die Zusammenführung von Hardware und Software wird es erst möglich, dass sich die Produkte über das Internet untereinander vernetzen. Die Tatsache, dass ein smartes Produkt selbst aus einer Vielzahl unterschiedlicher Hard- und Softwarekomponenten besteht und eine Vielzahl unterschiedlicher Akteure beteiligt sind, erhöht per se schon die Wahrscheinlichkeit vorhandener Produktfehler.[572] Ein hoher Vernetzungsgrad der Produkte führt dann zusätzlich zu systemischen Abhängigkeiten und Interdependenzen.[573] Dieses Phänomen, welches die Interaktion und den Datenaustausch der Systeme untereinander betrifft, wird unter dem Schlagwort des „Vernetzungsrisikos" diskutiert.[574] Der störungsfreie Betrieb eines Systems hängt dann aber nicht mehr lediglich von der eigenen Konstruktion ab, sondern auch von den zugelieferten Daten und Diensten anderer Systeme.[575] Ursächlich für eine vom Produkt ausgehende Rechtsgutsverletzung kann damit zusätzlich ein Fehler in den ausgetauschten Daten, ein Funktionsfehler eines beteiligten Systems oder auch eine Kombination aus beidem sein.[576] Daneben können an der Schnittstelle zweier miteinander agierender unterschiedlicher Produkte von verschiedenen Herstellern Kombinationsrisiken auftreten.[577] Der Komplexität und Vernetzung schei-

572 *Schmid*, IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme, S. 88; *Heckmann/Paschke*, in: Bräutigam/Kraul (Hg.), Internet of Things, § 10, Rn. 126; *Riehm*, DJT 2022 Referat, K S. 49.

573 *Spiecker gen. Döhmann*, CR 2016, 698 (701).

574 Vgl. *Riehm/Meier*, in: Fischer/Hoppen/Wimmers, DGRI Jahrbuch 2018, S. 1 (Rn. 28); *Zech*, DJT 2020 Gutachten, A S. 45 ff; *Zech*, in: Gless/Seelmann (Hg.), Intelligente Agenten und das Recht, S. 163 (169 f., 175); *Sommer*, Haftung für autonome Systeme, S. 45 f.; *Cornelius*, ZRP 2019, 8 (10); *Teubner*, AcP 218 (2018), 155 (201 ff.).

575 *Schrader*, NZV 2018, 489 (489 f.).

576 *Riehm/Meier*, in: Fischer/Hoppen/Wimmers, DGRI Jahrbuch 2018, S. 1 (Rn. 28); *Zech*, ZfPW 2019, 198 (208) nennt für das Beispiel des autonomen Fahrens, dass Verursachungsbeiträge nicht nur durch das Kfz selbst denkbar sind, sondern auch durch Daten von anderen Fahrzeugen, zentralen Plattformen oder durch von außen kommende Einflüsse wie Gegenstände am Fahrbahnrand, mit denen kommuniziert wird.

577 *Wende*, in: Sassenberg/Faber (Hg.), Industrie 4.0 und Internet of Things, § 4, Rn. 60; *Heckmann/Paschke*, in: Bräutigam/Kraul (Hg.), Internet of Things, § 10, Rn. 126.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

nen kaum Grenzen gesetzt zu sein. So ist es möglich, aus vernetzten Systemen ein zusammenhängendes Gesamtsystem zu bilden, wie es in einem industriellen Produktionsprozess denkbar ist.[578]

> Beispiel: Smarte Bewässerungsanlage. Damit die Bewässerungsanlage ordnungsgemäß funktioniert, müssen die Hardwarebauteile, die Steuerungssoftware, Daten und Dienste fehlerfrei zusammenwirken.

b) Haftungsrechtliche Einordnung eines zunehmenden „Unbundlings"

Damit bilden Cyberangriffe nicht die einzigen Gefahren, die von außen auf smarte Produkte einwirken. Durch die zunehmende Vernetzung sind IoT-Geräte nicht isoliert zu betrachten, sondern muss ihre Interaktion mit anderer Software, Diensten und Daten berücksichtigt werden. Gerade aus diesem Zusammenspiel können gefährliche Wechselwirkungen entstehen, ohne dass dem eigenen Produkt für sich genommen ein Fehler anhaftet. Vielmehr führen externe Einflüsse aus der Systemumgebung, in die das Produkt eingebettet ist, dazu, dass das Produkt zur Gefahrenquelle wird. Anders als bei Manipulationshandlungen Dritter ergibt sich dieses Gefahrenpotential jedoch spezifisch aus der auf Vernetzung angelegten Konstruktion der Produkte.[579]

Abgesehen von schwierigen Beweisproblemen hinsichtlich der Zuordnung einzelner Verantwortungsbeiträge,[580] die hier nicht Gegenstand sein sollen, bereitet schon die haftungsrechtliche Einordnung dieses Vernetzungsrisikos insbesondere aufgrund eines zunehmenden „Unbundlings" Schwierigkeiten. Darunter ist die getrennte Vermarktung einzelner Komponenten im Rahmen der digitalen Wertschöpfungskette bei IoT-Geräten sowie die damit zusammenhängende Aufspaltung der an der Wertschöpfung Beteiligten zu verstehen.[581] Bei der Defokussierung weg von einem einzigen Unternehmer handelt es sich freilich nicht um eine Besonderheit von IoT-Produkten. Auch bei herkömmlichen Waren sind eine Vielzahl

578 Vgl. *Hornung/Hofmann*, in: Hornung (Hg.), Rechtsfragen der Industrie 4.0, S. 9 (30).

579 Hierzu *Kreutz*, in: Oppermann/Stender-Vorwachs (Hg.), Autonomes Fahren, 2. Aufl., S. 177 (186 f.).

580 Hierzu *Zech*, DJT 2020 Gutachten, A S. 46.

581 *Wagner*, in: Lohsse/Schulze/Staudenmayer (Hg.), Liability for AI and the IoT, S. 27 (47 f.); *Voigt,* in: BeckOGK, BGB, § 823, Rn. 784 f.; *Sommer*, Haftung für autonome Systeme, S. 226.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

unterschiedlicher Akteure entlang der Distributionskette beteiligt.[582] Deren deliktsrechtliche Verantwortlichkeit im Rahmen der Produzentenhaftung hängt dabei nicht von der formalen Herstellereigenschaft ab, sondern allein von der Verletzung einer eigenen Verkehrssicherungspflicht.[583] Auch beim Phänomen des Unbundlings wird es daher darauf ankommen, welche Verkehrssicherungs- und Gefahrabwendungspflichten den einzelnen Beteiligten bei der Aufteilung der Herstellungstätigkeiten obliegen.[584] Maßgeblich für die Verantwortungsallokation ist, ob sich der Unternehmer derart mit der Ware identifiziert, dass ihm die besonderen Produzentenpflichten auferlegt werden können.[585] Dabei kommt es entscheidend auf die Kenntnis- und Einflussmöglichkeiten der jeweiligen Beteiligten im Hinblick auf den Herstellungsprozess an.[586]

Für eine den Verantwortungssphären entsprechende Einordnung des Vernetzungsrisikos kommt es daneben auf die Unterscheidung von „Kombinationsgefahren" und „fehlervermittelten Gefahren" an.[587] Unter Kombinationsgefahren sind dabei solche Risiken und Fehler zu verstehen, die sich erst aus der Kombination des eigenen Produkts mit einem fremden Zubehörteil ergeben.[588] So können Softwareprodukte isoliert genommen ungefährlich sein, aber im Zusammenspiel mit anderen Programmen (des Herstellers oder eines Drittanbieters) zu Konflikten führen.[589] Bei fehlervermittelten Gefahren hingegen beeinflusst ein Fehler aus der Systemumgebung das eigene Produkt. Hier treffen nicht zwei für sich betrachtet ungefährliche Produkte aufeinander, sondern die Fehlerhaftigkeit eines Produktes wirkt sich auf ein fehlerfreies Produkt aus. Im IoT-Kontext sind

582 So auch *Wagner*, VersR 2020, 717 (725).

583 Vgl. BGH, NJW 1980, 1219 (1219); BGH, NJW 1994, 517 (519); prägnant auch *Wende*, in: Sassenberg/Faber (Hg.), Industrie 4.0 und Internet of Things, § 4, Rn. 84.

584 *Wende*, in: Sassenberg/Faber (Hg.), Industrie 4.0 und Internet of Things, § 4, Rn. 85; *Klindt* et al., in: Bräutigam/Klindt (Hg.), Digitalisierte Wirtschaft/Industrie 4.0, S. 76 (83 f.).

585 So BGH, NJW 1980, 1219 (1219); *Klindt* et al., in: Bräutigam/Klindt (Hg.), Digitalisierte Wirtschaft/Industrie 4.0, S. 76 (84) sehen dies auch im Kontext des Unbundlings als zentrale Abgrenzungsfrage.

586 *Wende*, in: Sassenberg/Faber (Hg.), Industrie 4.0 und Internet of Things, § 4, Rn. 84.

587 Eine solche Differenzierung findet in der Literatur gegenwärtig kaum statt, vgl. nur *Schrader*, NZV 2018, 489 (492); ebenso wenig bei *Eichelberger*, in: Ebers et al., (Hg.), Künstliche Intelligenz und Robotik, S. 187 f.; ansatzweise bei *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 153 ff.

588 S. schon unter C.II.3.c)aa); grundlegend dazu BGH, NJW 1987, 1009 (1010); vgl. auch *Hartmann*, Der Warenhersteller im Spannungsfeld, S. 63 f.

589 *Thöne*, Autonome Systeme, S. 230 spricht von „systemische[n] Risiken".

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

hier insbesondere zwei Fallkonstellationen relevant. Zum einen die Fehlerhaftigkeit von externen Daten bzw. Informationen, auf deren Verarbeitung das Produkt angewiesen ist. Zum anderen die fehlende Erreichbarkeit eines anderen Systems, von dessen Verfügbarkeit das Produkt abhängig ist.

c) Kombinationsgefahren

Bei herkömmlichen Produkten im analogen Bereich hat der BGH bereits früh in seiner Honda-Entscheidung die Verantwortlichkeit des Herstellers auch auf Kombinationsgefahren erstreckt.[590] Bei notwendigem Zubehör bzw. bei Zubehör, das der Hersteller empfohlen hat oder Vorrichtungen hierfür am eigenen Produkt vorgehalten hat, fügt sich diese Haftungserweiterung als Ausfluss der Bereichshaftung in die Dogmatik der Verkehrspflichten ein. Ist das Zubehör allerdings lediglich aufgrund entsprechender Verbrauchergewohnheiten allgemein gebräuchlich, fehlt es an einer relevanten Gefahrschaffung durch den Hersteller jenseits des allgemeinen Lebensrisikos und bewegt sich die Haftungserstreckung außerhalb der dogmatischen Grundsätze.[591] Trotz dieser dogmatischen Unsauberkeiten gibt die Entscheidung doch die Stoßrichtung für die Haftung beim Zusammenwirken verschiedener Produkte vor und soll im Folgenden auf ihre Übertragbarkeit auf IoT-Produkte untersucht werden.

Das wichtigste Kombinationsprodukt im IoT-Kontext stellt Fremdsoftware dar. Smarte Produkte sind darauf angelegt, sich mit der Software anderer Produkte oder mit Apps unterschiedlichster Hersteller zu koppeln.[592] Schon im Ausgangspunkt nicht von der deliktischen Haftung umfasst ist die bloße mangelnde Kompatibilität mit jeder Art von Fremdprodukten, da hiervon allein das Äquivalenzinteresse des Nutzers betroffen ist.[593] Wird eine konstruktiv angelegte Kompatibilität, etwa über das Angebot eines App-Stores oder das Vorhalten einer Schnittstelle, aber tatsächlich genutzt, können sich daraus Gefahren ergeben, die geeignet sind, die deliktische Haftung auszulösen. Führen bislang unbekannte Funktionalitäten, etwa einzelner Apps oder die Kombination von Apps, zu einem Systemabsturz

590 BGH, NJW 1987, 1009.
591 Ausführlich bereits unter C.II.3.c)aa).
592 Vgl. nur *Spindler*, CR 2022, 689 (693).
593 *Spindler*, in Hornung/Schallbruch (Hg.), IT-Sicherheitsrecht, § 11, Rn. 35; *Voigt,* in: BeckOGK, BGB, § 823, Rn. 785.

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

des Hauptprodukts, bedarf es wenig Fantasie, sich die eingangs beschriebenen physischen Schädigungen vorzustellen.[594]

> Beispiel: Die Steuerungsapp der smarten Bewässerungsanlage ist mit dieser nicht kompatibel. Die preisgekrönten Rosen vertrocknen, weil die Bewässerung nicht ausgelöst wird.

Haftungsrechtlich dürfte der Fokus dabei auf der Produktbeobachtungspflicht liegen. Denn komplexe Wechselwirkungen treten häufig erst nach der Inverkehrgabe infolge der Veränderung des digitalen Umfelds auf.[595] So führt die Schnelllebigkeit des Softwaremarkts zu zahlreichen Neuentwicklungen und laufend neuen vernetzbaren Produkten.[596] Aufgrund der unzähligen Kombinationsmöglichkeiten sind auch Gefahren denkbar, die bei der Herstellung entweder mangels entsprechenden Erkenntniswissens oder aufgrund fehlender Zumutbarkeit der Überprüfung noch nicht vorhersehbar waren.[597] Auch vorsorgliche Konstruktionspflichten scheinen denkbar. Je nach Konstellation des Unbundlings können die Produzentenpflichten mit Blick auf die Kombinationsrisiken unterschiedlich ausgeprägt sein.

aa) Betrachtung des Zubehörbegriffs

Zunächst ist festzuhalten, dass der produkthaftungsrechtliche Zubehörbegriff – wie er auch vom BGH in der Honda-Entscheidung zur Erstreckung der Produktbeobachtungspflicht auf Fremdzubehörteile verwendet wird[598] – nicht auf die Sachqualität des Zubehörs oder das rechtliche Verhältnis zur Hauptsache i.S.d. § 97 Abs. 1 BGB abstellt, sondern allein eine haftungsrechtliche Zuordnung von Kombinationsrisiken ermöglichen soll.[599] Vor

---

594 Speziell zum vernetzten Fahren *Droste*, CCZ 2015, 105 (109) und *Hans*, GWR 2016, 393 (396).

595 So *Spindler*, in: Lohsse/Schulze/Staudenmayer (Hg.), Liability for AI and the IoT, S. 125 (129); ähnlich *Heckmann/Paschke*, in: Bräutigam/Kraul (Hg.), Internet of Things, § 10, Rn. 126, welche darauf hinweisen, dass aufgrund der Vielzahl unterschiedlicher Einsatzszenarien eine vollständige Wirkanalyse im Vorfeld kaum vorgenommen werden könne und auch Softwareupdates nachträglich neue Wirkungen entfalten können.

596 *Spindler*, in: Hilgendorf (Hg.), Robotik im Kontext von Recht und Moral, S. 63 (74); *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 156.

597 Vgl. *Schulz*, Verantwortlichkeit bei autonom agierenden Systemen, S. 172.

598 BGH, NJW 1987, 1009; vgl. dazu schon oben C.II.3.c)aa).

599 Vgl. *Hartmann*, Der Warenhersteller im Spannungsfeld, S. 40; *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 81 f.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

diesem Hintergrund stellt auch Software ohne Weiteres ein Zubehör im produkthaftungsrechtlichen Sinne dar (sog. digitales Zubehör).[600] Schwieriger ist diese Einordung indes bei isolierter Software. Denn hier befinden sich die Anwendungen in der Cloud und werden nicht auf dem Produkt installiert, sind also nicht Bestandteil des Produkts. Gleichwohl ist auch ohne Integration in das Hauptprodukt eine identische Gefährdungslage gegeben. Denn auch isolierte Software kann das System, die Funktionalität und damit die Sicherheitseigenschaften des Hauptprodukts beeinflussen (sog. digitales Quasi-Zubehör).[601] Unterschiedliche vertragliche Vertriebsformen, Geschäfts- und Liefermodelle rechtfertigen daher bei der risikobasierten Betrachtung der Produkthaftung keinen Unterschied, ganz gleich, ob es sich um die nachträgliche Integration von Software oder um die dauerhafte Erbringung einer Dienstleistung durch einen Dritten handelt.[602] Auch bei vernetzten Produkten ist keine abweichende Beurteilung angezeigt. Zwar stellen auch diese kein klassisches Zubehör dar, da sie im Vergleich zum Hauptprodukt nicht lediglich dienenden Charakter haben, sondern auf Augenhöhe operieren und über eine funktionale Eigenständigkeit verfügen.[603] Dennoch können sie angesichts der drahtlosen Verbindung als Kombinationsprodukte aufgefasst werden, für die produkthaftungsrechtlich dieselben Gesichtspunkte gelten wie für Zubehör.[604] Hier kann es keinen Unterschied machen, ob die Verbindung tatsächlich physisch oder digital erzeugt wird.[605] Ferner kann es keine Rolle spielen, dass vernetzte Produkte möglicherweise nur vorübergehend und nur für wenige Sekunden miteinander interagieren.[606]

bb) Einheitliche Herstellung

Für den Fall, dass die einzelnen Komponenten einheitlich aus der Hand des Herstellers stammen, liegt streng genommen begrifflich schon kein Unbundling vor. Die Identifikation mit einem Produkt könnte nicht größer

600 *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 81 f.
601 Zum Ganzen *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 84 f.
602 *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 85.
603 *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 87.
604 Vgl. BGH, NJW 1987, 1009 (1011), der allerdings eine Abgrenzung der Begrifflichkeiten in o.g. Sinne vermissen lässt.
605 *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 87.
606 *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 156.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

sein als bei der vollständigen Fertigung im eigenen Betrieb. Hinsichtlich der Produzentenpflichten ergeben sich keine Besonderheiten.[607]

> Beispiel: Der Hersteller stellt sowohl das Bewässerungsgerät als auch die zugehörige Steuerungsapp eigens her. Die App kann mittels beigefügten QR-Codes oder von der Homepage des Unternehmens heruntergeladen und installiert werden.

cc) Zulieferkomponenten

Werden zusätzliche Komponenten eines Produkts nicht vom Unternehmer selbst hergestellt, aber einheitlich von diesem in den Verkehr gebracht, handelt es sich um den klassischen Fall arbeitsteiligen Vorgehens, bei dem der Endhersteller Einzelteile von Zulieferern bezieht. In diesem Sinne präzisiert künftig auch Art. 4 Abs. 11 ProdHaftRL den Herstellerbegriff dahingehend, dass hierunter auch jede Person fällt, die ein Produkt entwickeln oder herstellen lässt oder dieses Produkt unter ihrem Namen oder ihrer eigenen Marke vermarktet. Dabei macht es im Ausgangspunkt keinen Unterschied, ob es sich um ein herkömmliches Zulieferprodukt, zugelieferte Betriebssoftware oder Software im Allgemeinen handelt.[608] Herkömmlicherweise werden die einzelnen Komponenten zwar vor der Inverkehrgabe vom Endhersteller selbst zusammengesetzt. Bei auf Vernetzung angelegten Produkten wird allerdings regelmäßig keine physische Verbindung der einzelnen Komponenten vorliegen und dieser letzte Fertigungsschritt durch den Endhersteller folglich fehlen.

> Beispiel: Lediglich das Bewässerungsgerät stammt vom Hersteller. Die via QR-Code oder über die Homepage des Herstellers heruntergeladene App stammt von einem externen Softwarehersteller.

Hier beschränkt sich die Tätigkeit des als Hersteller des Gesamtprodukts auftretenden Unternehmers hinsichtlich der zusätzlichen Komponente auf die gemeinsame Vermarktung.[609] Gleichwohl ändert dies nichts an der Zu-

607 Vgl. *Foerste*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 25, Rn. 170.
608 *Droste*, CCZ 2015, 105 (108); vgl. auch *Meyer/Harland*, CR 2007, 689 (692).
609 Vgl. auch *Foerste*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 25, Rn. 171.

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

lieferersituation.[610] Da allein der Endhersteller den Herstellungsprozess in seiner Gesamtheit überblickt und die notwendigen Einzelschritte steuert,[611] ergibt sich seine haftungsrechtliche Verantwortung für das Gesamtprodukt weniger aus dem Zusammenfügen der einzelnen Teile als mehr aus der Übernahme der gesamten konzeptionellen Planung.[612] Wer diese Planung für das Gesamtprodukt selbst vornimmt, zeichnet sich auch für das gefahrlose Zusammenwirken der von den Zulieferern bezogenen Einzelteile verantwortlich.[613] Die Kontrolle der Funktionalitäten im Zusammenspiel ist gerade nur dem Endhersteller möglich, bei dem vor der Inverkehrgabe des Gesamtprodukts alle Einzelteile zusammenlaufen.[614] Insoweit nimmt er auch das Vertrauen der Nutzer in Anspruch.[615] Diese Verantwortung betrifft freilich nicht nur den Konstruktion-, sondern auch den Produktbeobachtungsbereich.[616]

dd) Bereitstellung durch Drittanbieter

Eine grundlegende andere Situation liegt dagegen vor, wenn ein Hersteller das Zubehör zu seinem Produkt nicht selbst in den Verkehr bringt, sondern

610 Vgl. auch die Fallkonstellation in BGH, NJW 1994, 3349 (Atemüberwachungsgerät und mitgelieferte Elektrodenkabel eines Zulieferers, welche vom Nutzer selbst zu verbinden waren).

611 *Förster*, in: BeckOK, BGB, § 823, Rn. 759.

612 Wohl auch *Haftenberger*, Die Produkthaftung für künstlich intelligente Medizinprodukte, S. 225 f., die darauf abstellt, dass „der Hersteller als Entwickler seines Systems als best risk manager auftritt und daher keinesfalls aus der Verantwortung für die Vernetzung" genommen werden sollte.

613 *Krause*, in: Soergel, BGB, § 823 Anh. III, Rn. 31; *Wagner,* in: MüKo, BGB, § 823, Rn. 1044 m.w.N. zur Rechtsprechung; vgl. auch BGH, NJW 1988, 2611 (2612); BGH, NJW 1996, 2224 (2225); i.E. bzgl. zugelieferter Software in Fahrerassistenzsystemen *Meyer/Harland*, CR 2007, 689 (694); Da nach der neuen Produkthaftungsrichtlinie weiterhin jeder Hersteller einer fehlerhaften Komponente eines Produkts für den dadurch verursachten Schaden haftet (Art. 8 Abs. 1 UAbs. 1 lit. b ProdHaftRL), kann bei Fehlern der Software nicht nur der Endhersteller (Art. 8 Abs. 1 UAbs. 1 lit. a, Abs. I UAbs. 2 ProdHaftRL), sondern auch der Softwarehersteller in Anspruch genommen werden.

614 Hierauf weist *Hager*, in: Staudinger, BGB, § 823, Rn. F 27 hin; vgl. auch *Denga*, in: Bräutigam/Kraul (Hg.), Internet of Things, § 11, Rn. 78.

615 Hierauf stellt *Foerste*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 25, Rn. 171 maßgeblich ab.

616 *Droste*, CCZ 2015, 105 (108); *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 82.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

lediglich eine Bereitstellung durch Drittanbieter ermöglicht. Gerade im Automotivsektor ist eine Tendenz zu erkennen, dass Automobilhersteller ihre Fahrerinformationsdisplays für Apps Dritter öffnen.[617] Das Spektrum reicht hier von Zusatzfunktionen wie der Navigation des Autos hin zu reinen Unterhaltungsprogrammen wie Mediatheken oder sozialen Netzwerken. Dabei sind zwei Varianten möglich. Entweder kann direkt über das IoT-Gerät auf einen eigenen App-Store des Herstellers oder den eines großen Anbieters zugegriffen werden oder Schnittstellen ermöglichen es, dass sich ein mobiles Endgerät mit dem IoT-Gerät verbindet und Apps in Verbindung mit dem Endgerät auf dem System des IoT-Geräts genutzt werden können.[618] Anders als mit einem Zulieferer verbindet hier den Hersteller keine Geschäftsbeziehung mit dem Zubehörhersteller. Gerade bei nicht speziell als Zubehörprodukt für das jeweilige Hauptprodukt entwickelten Apps besteht regelmäßig keinerlei direkte Einflussnahme auf den Entwicklungsprozess. In diesem Zusammenhang ist aber danach zu differenzieren, ob ein Hersteller den Drittanbietern einen uneingeschränkten Zugang zu seinem Produkt öffnet oder dieser nur über einen eigenen App-Store geschieht.

(1) Eigener App-Store

α) Einflussnahmemöglichkeit und entgegengebrachtes Vertrauen

Bei dem Vorhalten eines eigenen App-Stores, bei dem es letztendlich um die Vermittlung fremder Apps geht, ist der Unternehmer seinem Wesen nach nicht an dem Entwicklungsprozess der entsprechenden Apps beteiligt.

> Beispiel: VW baut eine gemeinsame Online-Plattform für verschiedene Automarken des Konzerns auf. Zum Start gibt es aktuell rund 40 Apps. Darunter sind Musikdienste wie Spotify, Tidal und Amazon Music sowie die Video-Apps TikTok, ARD, ZDF und die Empfehlungs-App Yelp.[619]

Allerdings darf nicht verkannt werden, dass der Unternehmer durch das Betreiben des eigenen App-Stores selbst bestimmen kann, welche Drittanbieter ihre Apps bereitstellen dürfen. Damit behält er die Kontrolle über die verfügbaren Apps und ist in der Lage, über klare Vorgaben und ggf. im

617 *Hans*, GWR 2016, 393 (396).
618 *Droste*, CCZ 2015, 105 (109).
619 Vgl. https://www.computerbild.de/artikel/cb-News-Connected-Car-Volkswagen-Eigener-App-Store-angekuendigt-35296445.html (zuletzt abgerufen am 23.09.2024).

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

Wege einer vorgeschriebenen Zertifizierung Sicherheitsstandards durchzusetzen. Durch diese Einschränkung gibt der Unternehmer selbst die Kombinationsmöglichkeiten mit seinem Produkt vor.[620] Ob die Vorgabe solcher Sicherheitsstandards für sich allein genommen schon ausreichend ist, um aufgrund einer Identifikation mit dem Produkt als „eigenes" Träger von Gefahrenabwehrpflichten zu werden, kann hier offenbleiben.[621] Zwar wird mit den Vorgaben mittelbar Einfluss auf den Herstellungsprozess genommen, allerdings sind diese weit davon entfernt, Konstruktionspläne für die Fertigung des Produkts nach eigenen Vorstellungen zu sein.[622] Hinzu kommt aber, dass ein Nutzer dem Hersteller des Hauptprodukts aufgrund des von ihm eigens angebotenen App-Stores ein besonderes Vertrauen entgegenbringt und erwartet, dass nur Apps angeboten werden, die sich auch für eine Kombination mit dem von ihm hergestellten Produkt eignen und damit kein Sicherheitsrisiko darstellen.[623] Vor diesem Hintergrund wird der Nutzer eigene Prüfungen auf die Kompatibilität einer App mit dem IoT-Gerät unterlassen und sich auf die Kontrolle des Herstellers vor Bereitstellung in seinem App-Store verlassen.[624] Durch die mögliche Beschränkung der Kombinationsmöglichkeiten und das damit vom Nutzer entgegengebrachte Vertrauen rechtfertigen sich auch in dieser Fallkonstellation eigene Gefahrenabwendungspflichten hinsichtlich des gefahrlosen Zusammenwirkens.[625]

β) Keine Privilegierung nach TMG

Mit dem Bereitstellen eines eigenen App-Stores hält ein Unternehmer Telemedien bereit bzw. vermittelt entsprechenden Zugang zur Nutzung und ist daher als Dienstanbieter Verantwortlicher nach dem Telemediengesetz

620 Überzeugend zum Ganzen *Droste*, CCZ 2015, 105 (109); auch *Thöne*, Autonome Systeme, S. 231.

621 Zweifelnd aufgrund eines strengen anzulegenden Maßstabes *Förster*, in: BeckOK, BGB, § 823, Rn. 769.

622 Für diesen Fall hat das OLG München, VersR 1988, 635 (636) eine Identifikation mit dem Produkt als „eigenes" bejaht; dem folgend *Voigt,* in: BeckOGK, BGB, § 823, Rn. 717 und *Hager*, in: Staudinger, BGB, § 823, Rn. F 32.

623 *Hans*, GWR 2016, 393 (396); *Weisser/Färber*, MMR 2015, 506 (511); ähnlich *Wagner*, AcP 217 (2017), 707 (753 f.).

624 Allgemein zu der Möglichkeit eigener Gefahrenabwendungspflichten des Quasi-Herstellers in dieser Vertrauenskonstellation BGH, VersR 1977, 839.

625 Skeptisch indes *Kapoor/Sedlmaier*, RAW 2023, 8 (12).

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

(im Folgenden „TMG"), vgl. § 2 S. 1 Nr. 1 TMG. Als solcher könnte er aber von den Haftungsprivilegierungen der §§ 7 ff. TMG erfasst sein.[626] Ziel der Privilegierungen ist es im Wesentlichen, die Haftungsrisiken aus mittelbaren Rechts- bzw. Rechtsgutsverletzung für fremde Inhalte zu reduzieren, um keine Hemmnisse für Investitionen im Bereich der neuen Medien aufzubauen.[627] Maßgeblich für das Eingreifen eines Privilegierungstatbestands ist daher die Einordung als fremder Inhalt. Wann ein Inhalt fremd ist, wird allerdings nicht anhand einheitlicher Kriterien beurteilt. Zum Teil wird darauf abgestellt, dass auch solche Inhalte als eigene zu betrachten seien, die sich der Diensteanbieter nach Würdigung aller Umstände zu eigen macht.[628] Ein Zueigenmachen liege dabei immer dann vor, wenn sich für einen verständigen Durchschnittsnutzer, insbesondere aufgrund der äußeren Form der Darstellung, ergibt, dass der Dienstanbieter die Inhalte vorab auf Vollständigkeit und Richtigkeit überprüft hat.[629] Eine andere Ansicht stellt allein auf die Herrschaftsmacht des Dienstanbieters über den Inhalt bzw. seine Auswahlmöglichkeit bzgl. der Adressaten oder des Inhalts ab. Wie sich der Inhalt für einen Dritten darstellt, spiele dagegen keine Rolle. Dieses Verständnis geht auf die E-Commerce-Richtlinie (im Folgenden „ECRL")[630] zurück, die national im TMG umgesetzt wird und im Bereich der Verantwortlichkeiten auf Vollharmonisierung angelegt ist. Insoweit stellt Erwägungsgrund (42) ECRL klar, dass die Haftung des Dienstanbieters nur entfallen kann, wenn dessen Tätigkeit „rein technischer, automatischer und passiver Art [ist], was bedeutet, dass der Anbieter eines Dienstes der Informationsgesellschaft weder Kenntnis noch Kontrolle über die weitergeleitete oder gespeicherte Information besitzt." Damit liegt der ECRL ein auf technische Vorgänge und deren Kontrolle abzielendes Verständnis zugrunde, weshalb es keine Rolle spielen könne, wie sich ein Inhalt für einen Dritten darstellt.[631] Maßgeblich für das Eingreifen der Haftungsprivilegierung sei das Kriterium der Neutralität, während eine Privile-

626 Allgemein zur Haftung von IoT-Plattformbetreibern *Wende*, RDi 2021, 341 (345); speziell hinsichtlich Plattformbetreibern beim vernetzten autonomen Fahren *Kian/Tettenborn*, in: Hilgendorf/Hötitzsch/Lutz (Hg.), Rechtliche Aspekte automatisierter Fahrzeuge, S. 101 (111 ff.).

627 *Spindler*, in: Spindler/Schmitz, TMG, vor § 7, Rn. 1.

628 Vgl. Begr. RegE BT-Drs. 14/6098, S. 23; w.N. zur älteren nationalen Rspr. bei *Spindler*, in: Spindler/Schmitz, TMG, § 7, Rn. 7, Fn. 14.

629 Ohne diese Ansicht zu teilen *Spindler*, in: Spindler/Schmitz, TMG, § 7, Rn. 18.

630 Richtlinie 2000/31/EG.

631 H.M. im Schrifttum, vgl. zum Ganzen m.w.N. *Spindler*, in: Spindler/Schmitz, TMG, § 7, Rn. 8.

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

gierung ausscheide, wenn der Diensteanbieter die Position als Vermittler verlässt und durch Kenntnis oder Kontrolle der Daten oder der Unterstützung des Nutzers eine „aktive Rolle" einnimmt.[632] Für den hier zu beurteilenden Fall des Bereitstellen eines eigenen App-Stores mit fremden Inhalten kommen beide Ansichten gleichwohl zum gleichen Ergebnis. Durch die Vorgabe der Sicherheitsstandards wird für einen objektiven Dritten der Eindruck einer inhaltlichen Überprüfung durch den Anbieter erweckt. Gleichzeitig stellen diese vorgegebenen Standards eine Vorabauswahl der Inhalte dar, sodass der Anbieter seine neutrale Vermittlerrolle verlässt und ihm eine Funktionsherrschaft zukommt.[633] Eine Haftungsprivilegierung des Herstellers, der einen eignen App-Store anbietet, scheidet daher aus.

(2) Schnittstellenzugang

α) Fehlende Einflussnahmemöglichkeit

Anders dagegen stellt sich die Situation dar, wenn der Hersteller Dritten uneingeschränkten Zugang zu seinem Produkt eröffnet.

Beispiel: Android Auto und Apple CarPlay.

Ermöglicht der Hersteller konstruktiv die Verbindung mit anderen Geräten über eine Schnittstelle oder den Zugriff auf einen fremden App-Store, verliert er nämlich die Kontrolle über die vernetzten Geräte und bereitgestellten Apps und kann selbst keine Richtlinien zur Durchsetzung von Sicherheitsstandards vorgeben.[634] Damit hat er aber nicht einmal mittelbaren Einfluss auf den Herstellungsprozess der Zubehörprodukte. Daneben ist auch seine Kontrolle über die Kombinationsmöglichkeiten mit seinem Produkt deutlich zurückgefahren. Liegt die Kombination des eigenen Produktes mit fremdem Zubehör derart außerhalb der Einflusssphäre des Herstellers, betrifft dies die Konstellation der Honda-Rechtsprechung bzgl. Fremdzubehörteilen des BGH.[635]

632 Vgl. EuGH, GRUR 2011, 1025 (1032); zum Einzug des Kriteriums der Neutralität in die nationale Rspr. *Spindler*, in: Spindler/Schmitz, TMG, § 7, Rn. 10 m.w.N.
633 So auch *Schuster*, in: Hilgendorf (Hg.), Autonome Systeme und neue Mobilität, S. 49 (54 f.).
634 *Droste*, CCZ 2015, 105 (109).
635 BGH, NJW 1987, 1009.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

β) Übertragung der Honda-Rechtsprechung

Eine vorschnelle Übertragung der Grundsätze für die Überwachung von Fremdzubehörteilen auch auf IoT-Produkte setzt sich indes dem Vorwurf aus,[636] aufgrund der Vielzahl der Kombinationsmöglichkeiten einen uferlosen Pflichtenkatalog zu schaffen.[637]

Indes darf nicht übersehen werden, dass die Verantwortung für Zubehörteile bereits durch den BGH begrenzt wurde und keinesfalls die Verträglichkeit des Produkts mit jeglichem Zubehör umfasst.[638] So hat der Hersteller nur bei notwendigem Zubehör, das sein Produkt erst funktionstüchtig macht und bei Zubehör, dessen Verwendung er durch eigene Vorrichtungen vorgesehen hat sowie bei von ihm empfohlenem Zubehör, eine anlasslose Pflicht zur eigenen Überprüfung der Zubehörteile auf die Kompatibilität mit dem eigenen Produkt. Dabei sind aber selbst bei einer Gefahr für Leib und Leben lediglich die Erzeugnisse der Marktführer einer diesbezüglichen Prüfung zu unterziehen. Bei allgemein gebräuchlichem Zubehör dagegen steigert sich die Produktbeobachtungspflicht erst bei einem konkreten Anlass zu einer solchen Überprüfungspflicht des fremden Zubehörs. Im Übrigen ist eine reine passive Beobachtung ohne eigene Gefahrerforschung ausreichend. Daneben greift der BGH auch die Problematik auf, dass der Markt aufgrund einer Vielzahl an Zubehörteilen unübersichtlich werden kann. Dann darf sich der Hersteller auf die Überprüfung einzelner Zubehörteile zurückziehen.[639]

Diese abgestuften und an der Zumutbarkeit orientierten Beobachtungsmaßnahmen führen aber auch bei IoT-Produkten zu sachgerechten Ergebnissen.[640] Hinsichtlich notwendigem und empfohlenem Zubehör ergeben

636 Vgl. *Chibanguza/Schubmann*, GmbHR 2019, 313 (316); *Schrader*, NZV 2018, 489 (493).

637 *Spindler*, in: Hilgendorf (Hg.), Robotik im Kontext von Recht und Moral, S. 63 (73 f.); *Voigt*, in: BeckOGK, BGB, § 823, Rn. 779; krit. auch *Sosnitza*, CR 2016, 764 (769) und *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 82; offen gelassen von *Reusch*, in: Kaulartz/Braegelmann (Hg.), Artificial Intelligence und Machine Learning, S. 110.

638 Ausführlich hierzu *v. Bar*, in: Lieb (Hg.), Produktverantwortung und Risikoakzeptanz, S. 29 (34 f.).

639 Zum Ganzen BGH, NJW 1987, 1009 (1011).

640 So auch *Leupold/Wiesner*, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 9.6.4, Rn. 78; a.A. *Spindler*, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, Rn. 138, der die Haftung für fremde Software für weitgehend ausgeschlossen hält und eine Produktbeobachtungspflicht allenfalls bei spezifisch auf das Produkt zugeschnittener Software anerkennt.

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

sich keine Abweichungen zu herkömmlichen Produkten. Sofern die Vernetzung erst den Betrieb ermöglicht, hat der Nutzer gar keine andere Wahl, als darauf zurückzugreifen.[641] In diesem Kontext vertrauen die Nutzer auch bei IoT-Produkten bei einer bestimmungsgemäßen Verwendung in hohem Maße auf die fachliche Autorität des Herstellers und darauf, dass er vor Kombinationsrisiken warnt.[642] Um dieser Pflicht umfassend nachzukommen, sind neben der Beobachtung auch eigene Überprüfungen durchzuführen. Im Übrigen dürften Produkte, die mit dem IoT-Gerät vernetzt werden, allenfalls der Kategorie des allgemein gebräuchlichen Zubehörs zuzurechnen sein.[643] Zwar ermöglicht der Hersteller durch das Vorhalten einer Schnittstelle oder den Zugang zu einem App-Store erst die Kombination, sodass es sich auch um vorgesehenes Zubehör handeln könnte.[644] Indes eröffnet ein auf Vernetzung angelegtes Produkt eine unüberschaubare Möglichkeit an Kombinationen.[645] Aus dem bloßen Vorhalten der Schnittstelle lässt sich damit noch nicht auf konkret kombinierbare Produkte schließen. Hier liegt der qualitative Unterschied zu den in der Honda-Entscheidung angesprochenen Vorkehrungen wie Bohrlöchern, Ösen, Halterungen oder Aufhängevorrichtungen. Durch diese Vorrichtungen wird die Verwendung von bestimmtem Zubehör nahegelegt, sodass eine Konkretisierung auf bestimmte Zubehörarten erfolgt. Fehlt es aber an einer solchen Konkretisierung, erfolgt die Kombination des Nutzers nicht in Vertrauen auf die Autorität des Herstellers. Dieser fehlende Vertrauenstatbestand rechtfertigt daher bei lediglich allgemein gebräuchlichem[646] Zubehör eine abgeschwächte

641 Vgl. auch *Hinze*, Haftungsrisiken des automatisierten und autonomen Fahrens, S. 158 f.; i.E. auch *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 83.

642 Allgemein *Klinger*, Die Produktbeobachtungspflicht bezüglich Fremdzubehörteilen, S. 70 ff.

643 So auch *Leupold/Wiesner*, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 9.6.4, Rn. 78 „besteht eine Beobachtungspflicht jedenfalls für Zubehör und Software Dritter, deren Zugang zum autonomen System der Hersteller bewusst ermöglicht oder bewirbt. Dagegen dürfte die bloße Koppelungsmöglichkeit mit dem autonomen System nicht ausreichen, vielmehr […] müssen [die Zubehörteile] so allgemein gebräuchlich sein, dass der Hersteller mit ihrer Nutzung an seinem Produkt rechnen muss".

644 So wohl *Steege*, in: Buck-Heeb/Oppermann (Hg.), Automatisierte Systeme, S. 367 (396); *Steege*, NZV 2021, 6 (11).

645 *Droste*, CCZ 2015, 105 (109); *Burrer*, in: Bräutigam/Kraul (Hg.), Internet of Things, § 8, Rn. 102.

646 *Burrer*, in: Bräutigam/Kraul (Hg.), Internet of Things, § 8, Rn. 102 spricht von „gängigste[r] Hard- und Software".

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

Beobachtungspflicht, beschränkt auf die reine Beobachtung ohne eigene Gefahrerforschung.[647] Führt ein konkreter Anlass in diesem Fall zu eigenen Überprüfungspflichten, kann auch hinsichtlich der Zumutbarkeit auf die Einschränkungen der Honda-Entscheidung abgehoben werden.

Zieht man ins Kalkül, dass der Hersteller insbesondere zur Steigerung der Produktattraktivität die Kombinationsmöglichkeit und die Gefahrenquelle erst geschaffen hat,[648] überzeugt auch die dogmatische Begründung der Beobachtungspflicht in Bezug auf die Kombination mit allgemein gebräuchlichem Zubehör.[649] Die vielgestaltigen Kombinationsmöglichkeiten kommen zwar auch dem Verwender entgegen, indem geschlossenen Systemen entgegengewirkt wird und Technikoffenheit und Wettbewerb gefördert werden.[650] Dieser Nebeneffekt darf aber nicht darüber hinwegtäuschen, dass der Hersteller über einen höheren Produktpreis die ökomischen Vorteile daraus ziehen kann. Die Kehrseite dieses ökonomischen Vorteils liegt dann eben in der Produktbeobachtung.

Zwar betraf die Honda-Entscheidung des BGH lediglich die Produktbeobachtungspflicht des Herstellers, allerdings liegt der Entscheidung der allgemeine Gedanke der wirksamen Gefahrensteuerung im Hinblick auf Zubehörprodukte zugrunde. Daher ergeben sich auch Auswirkungen auf die übrigen Produzentenpflichten.[651] Gerade im Rahmen der Konstruktion sind bereits Sicherungsmaßnahmen zu treffen, um Kombinationsrisiken zu vermeiden. Allerdings kann dem Hersteller nicht zugemutet werden, sein Produkt konzeptionell auf alle möglichen Zubehörprodukte abzustimmen.[652] Insbesondere in gefahrenträchtigen Bereichen muss der Hersteller aber sicherstellen, dass sicherheitsrelevante Eigenschaften seines Produkts nicht durch Störungen aus der Kombination mit anderen Produkten beein-

647 So *Klinger*, Die Produktbeobachtungspflicht bezüglich Fremdzubehörteilen, S. 71 f.

648 Richtiger Hinweis bei *Thöne*, Autonome Systeme, S. 230.

649 A.A. *Spindler*, in: Hilgendorf (Hg.), Robotik im Kontext von Recht und Moral, S. 63 (74), welcher eine herstellerseitige Instruktion, „dass nur von ihm selbst freigegebene bzw. als unbedenklich eingestufte Zubehörteile gefahrlos benutzt werden können und dass die Benutzung nicht autorisierten Zubehörs auf Gefahr des Benutzers erfolgt" als ausreichend ansieht; ebenso *Spindler*, CR 2015, 766 (770).

650 *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 82 f. ziehen daraus aber den Schluss, dass die Produktbeobachtungspflicht lediglich „auf die besonders üblichen digitalen Zubehörprodukte der Marktführer" zu begrenzen sei.

651 Vgl. *Hartmann*, Der Warenhersteller im Spannungsfeld, S. 71 f.; *Wiesner*, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 10.6, Rn. 42.

652 Zum Ganzen *Foerste*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 25, Rn. 191.

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

flusst werden.[653] Hierfür kann die Abschirmung der Steuerungssoftware des eigenen Produkts erforderlich sein. Wo eine solche Resilienz technisch nicht umsetzbar ist, muss die Nutzung ungeprüfter Drittkomponenten konstruktiv ausgeschlossen werden.[654]

ee) Zwischenfazit Kombinationsgefahren

Betrachtet man die unterschiedlichen Konstellationen des Unbundlings, lässt sich hinsichtlich der Verantwortungsallokation danach differenzieren, ob der Hersteller bei der Konzeption eines IoT-Geräts einen geschlossenen oder offenen Ansatz verfolgt. Von einem geschlossenen System wird gesprochen, wenn ein Hersteller die Hard- und Software aus einer Hand anbietet, diese einen unauflösbaren Verbund darstellen und er auch den Zugang von Drittanbietern auf die Systemumgebung des eigenen IoT-Geräts kontrolliert. Bei offenen Systemen dagegen werden entweder die Hard- und Software des IoT-Geräts von vorneherein getrennt vertrieben oder nachträgliche Produktergänzungen bzw. -modifikationen durch Dritte oder den Nutzer selbst zugelassen.[655]

Dem geschlossenen System ist die einheitliche Fertigung durch den Hersteller, der Bezug von Zulieferteilen sowie das Vorhalten eines eigenen App-Stores zuzuordnen. Hier lässt sich die Systemkonzeption und die Sicherheitsarchitektur insgesamt auf den Hersteller zurückführen. Die Abstimmung und die Zuverlässigkeit der einzelnen Komponenten, insbesondere auch deren Wechselwirkungen unterliegen allein seiner Herrschaftssphäre.[656] Daher trifft ihn bereits die konstruktive Verantwortung, ein gefahrloses Zusammenwirken der Komponenten zu ermöglichen. Insoweit stellt auch die neue Produkthaftungsrichtlinie klar, dass sich die Haftung des Herstellers auch auf Schäden erstreckt, die durch eine fehlerhafte Komponente verursacht werden, wenn diese in ein Produkt integriert oder mit einem Produkt verbunden wurde, das unter der Kontrolle des Herstellers steht (vgl. Art. 8 Abs. 1 UAbs. 1 lit. a, Abs. I UAbs. 2 ProdHaftRL). Eine sol-

653 *Leupold/Wiesner*, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 9.6.4, Rn. 78; *Thöne*, Autonome Systeme, S. 231; *Wagner*, AcP 217 (2017), 707 (753).

654 *Thöne*, Autonome Systeme, S. 231; *Wagner*, AcP 217 (2017), 707 (753); zum Ganzen auch *Haftenberger*, Die Produkthaftung für künstlich intelligente Medizinprodukte, S. 180 ff.

655 Zu den Begrifflichkeiten und Abgrenzungen *Wagner*, AcP 217 (2017), 707 (753 f.); *Thöne*, Autonome Systeme, S. 229 f.

656 *Thöne*, Autonome Systeme, S. 229 f.

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

che Kontrolle des Herstellers liegt gem. Art. 4 Nr. 5 ProdHaftRL vor, wenn er die Integration oder Verbindung oder Lieferung der Komponente selbst vornimmt oder diese einem Dritten genehmigt bzw. ihr zustimmt. Auch im Rahmen der Produktbeobachtung ergeben sich keine Besonderheiten und die Interaktion ist auf bisher unbekannte Wechselwirkungen hin zu beobachten.

Ein offenes System betrifft insbesondere den Fall, dass der Hersteller lediglich die Schnittstelle oder den Zugang zu einem App-Store eines großen Anbieters vorhält und somit das System für Dritte öffnet. Dieses Weniger an Herstellerkontrolle in Bezug auf die Abstimmung und das Zusammenspiel der Produkte rechtfertigt es, den Nutzer, der die Geräte kombiniert, hinsichtlich der Systemkompatibilität verstärkt in die Pflicht zu nehmen.[657] Aufgrund der Schaffung einer Gefahrenquelle verbleibt allerdings eine konstruktive Restverantwortung beim Hersteller. Daneben trifft ihn die Produktbeobachtungspflicht nach den Grundsätzen der Honda-Entscheidung.

d) Fehlervermittelte Gefahren

IoT-Geräte können regelmäßig nicht alle für ihre Funktionen notwendigen Informationen selbst erzeugen, sondern sind auf externe Daten angewiesen. Greift ein IoT-Gerät dann auf solche externen Daten zurück, haben diese Inhalte direkten Einfluss auf die Funktionsweise des Produkts.[658] Werden fehlerhafte Inhalte von dem Produkt verarbeitet, können wiederum die bereits skizzierten physischen Schädigungen eintreten.

> Beispiel: Im Rahmen des smarten Bewässerungssystems erweisen sich die Wetterdaten des Wetterdienstes als unzutreffend, sodass der Garten nicht bewässert wird und vertrocknet.[659]

657 Vgl. *Thöne*, Autonome Systeme, S. 230; *Wagner*, AcP 217 (2017), 707 (753 f.); *Wiesner*, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 10.6, Rn. 42.

658 Dazu *Kian/Tettenborn*, in: Hilgendorf/Hötitzsch/Lutz (Hg.), Rechtliche Aspekte automatisierter Fahrzeuge, S. 101 (106); *Schulz*, Verantwortlichkeit bei autonom agierenden Systemen, S. 176; speziell zum autonomen Fahren *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 43 f.; Beispiele bei *Schuster*, in: Hilgendorf (Hg.), Autonome Systeme und neue Mobilität, S. 49 (51).

659 Für weitere Beispiele vgl. Erwägungsgrund (17) ProdHaftRL.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

aa) Konstellationen der fehlervermittelten Gefahren

Die Frage, inwieweit die Produzentenhaftung nach § 823 Abs. 1 BGB auch für informationsvermittelte Gefährdungen greift,[660] spielt bei der Frage der Verantwortlichkeit des Herstellers des Produkts aber keine Rolle. Denn mag zwar die fehlerhafte Information die Ursächlichkeit der Gefährdung darstellen, wird sie doch erst von dem Produkt umgesetzt und verarbeitet, sodass die Rechtsgutsverletzung insgesamt auf das Produkt zurückzuführen ist. Allerdings lag die Fehlerhaftigkeit des Produkts im Zeitpunkt seiner Inverkehrgabe regelmäßig noch nicht vor, sondern ergibt sich erst nachträglich durch die fortlaufende Versorgung mit externen Daten, welche auch fehlerhafte Informationen enthalten können.[661] Der Fokus der haftungsrechtlichen Verantwortlichkeit wird daher einmal mehr auf der Produktbeobachtungsphase liegen.

Eine gänzlich andere Konstellation liegt vor, wenn das smarte Produkt nicht mit Daten von Externen gespeist wird und fehlerhafte Daten selbständig an das Gerät gesendet werden („Push-Modell"), sondern sich das smarte Produkt selbstständig an sich fehlerfrei Daten, aber für den jeweiligen Zweck schlicht die falschen Daten zieht und hierauf basierend Entscheidungen trifft („Pull-Modell").[662] Werden hier bspw. aufgrund eines fehlerhaften Algorithmus falsche Daten gezogen, ist dies keine Frage der Fehlerhaftigkeit der Daten, sondern liegt vielmehr bereits bei Inverkehrgabe ein Fehler des Produkts vor, der nach den allgemeinen Grundsätzen die Produktbeobachtungspflicht auslöst. In diesem Fall scheint es angezeigt, bereits konstruktiv Routinen anzulegen, die potenziell fehlerhafte Daten im Zusammenspiel mit dem Produkt überprüfen und ggf. gar nicht verwenden.[663] Um eine fehlervermittelnde Gefahr handelt es sich indes nicht.

Die hinsichtlich der Haftungsallokation gefundenen Ergebnisse zu den Kombinationsgefahren können nun aber nicht unbenommen auf die fehlervermittelnden Gefahren übertragen werden. Denn zwischen beiden

660 Vgl. hierzu *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 45.

661 Vgl. *Oechsler*, in: Staudinger, BGB, § 3 ProdHaftG, Rn. 127, welcher im Rahmen des ProdHaftG über § 1 Abs. 2 Nr. 2 ProdHaftG zu einer Entlastung des Herstellers für fehlerhafte Daten Dritter gelangt; im Ansatz auch *Schrader*, in: Buck-Heeb/Oppermann (Hg.), Automatisierte Systeme, S. 333 (336).

662 Zu den Begrifflichkeiten *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 111 f.

663 *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 111.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

Konstellationen besteht ein grundlegender Unterschied. Bei Kombinationsgefahren geht es um die Neuzuordnung einer eigenständigen Gefahrenquelle, die nicht unmittelbar an das Hauptprodukt oder Zubehör anknüpft, sondern gerade durch deren Kombination entsteht.[664] Dagegen besteht bei fehlervermittelnden Gefahren bereits ein Fehler in den Daten oder dem Dienst eines Dritten, welcher durch die Vernetzung in das Produkt des Herstellers getragen wird und sich von diesem ausgehend schadensursächlich auswirkt. Diese unterschiedliche Ausgangslage muss sich in der Haftungsverteilung widerspiegeln. Entsprechend den obigen Ausarbeitungen soll auch hier wieder zwischen geschlossenen und offenen Systemen differenziert werden.

bb) Geschlossene Systeme

Verfolgt der Hersteller einen geschlossenen Ansatz, werden also Produkt und zugehöriger Dienst aus einer Hand angeboten oder kontrolliert der Hersteller den Zugang von Drittanbietern auf die Systemumgebung des eigenen IoT-Geräts, drängt sich eine Parallele zu der Zulieferkonstellation auf.

> Beispiel: Das smarte Bewässerungssystem wird mit einem Wetterdienst ausgestattet angeboten, auch wenn der Nutzer die Wetterapp nach dem Erwerb erst von der Website eines Dritten herunterladen muss.[665]

Dabei kann es keinen Unterschied machen, dass die bereitgestellten Daten kein Teil des Produkts werden, sondern nur vorübergehend in dessen Entscheidungsfindung einfließen.[666] Denn die Kategorisierungen entlang der Distributionskette sollen letztendlich nur zu einer gerechten Haftungsverteilung beim arbeitsteiligen Zusammenwirken unterschiedlicher Akteure führen. Damit kann es aber hinsichtlich der Haftungsallokation allein auf die konkrete Ausgestaltung des Zusammenwirkens und die jeweiligen originären Handlungszuständigkeiten ankommen.[667]

Im Ausgangspunkt ist dabei der Endhersteller deliktisch allein für seine eigene Sphäre verantwortlich, während er für Fehler im alleinigen Ver-

664 Prägnant *Hartmann*, Der Warenhersteller im Spannungsfeld, S. 46.
665 Angelehnt an Erwägungsgrund (50) ProdHaftRL.
666 A.A. *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 51.
667 In diese Richtung *Wagner,* in: MüKo, BGB, § 823, Rn. 1042 f.

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

antwortungsbereich des Zulieferers nicht einzustehen hat.[668] Gleichwohl wird der Hersteller aufgrund seiner Gesamtverantwortung für das Produkt nicht gänzlich von seinen Sorgfaltspflichten befreit. Bei zugelieferten Daten und Informationen handelt es sich immer um vom Informationsanbieter vorgefertigte Dienste. Deren Zustandekommen kann nicht durch Spezifikationen des Herstellers vorgegeben werden und entzieht sich damit seines Einflussbereichs. Bei dem Bezug solcher standardisierter Teilprodukte treffen den Hersteller aber Kontrollpflichten, denen regelmäßig mit der stichprobenhaften Überprüfung genüge getan ist. Hat der Hersteller dagegen den Zulieferer sorgfältig ausgewählt und sich von dessen Zuverlässigkeit überzeugt, kann auch die Kontrolldichte dieser nachgelagerten „Wareneingangskontrolle" zurückgefahren sein.[669] Insoweit stehen die Auswahl- bzw. Kontrollpflichten in einem wechselseitigen Verhältnis und begründen bei ordnungsgemäßer Wahrnehmung das Vertrauen des Herstellers in den Zulieferer.[670] In ähnlicher Weise findet eine Haftungsverteilung bei Druckerzeugnissen im Verhältnis der Arbeitsteilung zwischen Autor und Verleger statt.[671] Hier ist der Verleger zwar Hersteller des Druckerzeugnisses, entsprechend den Verantwortungssphären ist aber in erster Linie der Autor für die inhaltliche Fehlerhaftigkeit verantwortlich.[672] Auch die Korrektur kann der Verlag auf den Autor delegieren,[673] jedenfalls dann wenn er sich von dessen Fachkunde überzeugt hat.[674] Sofern von der inhaltlichen Fehlerhaftigkeit jedoch hochrangige Rechtsgüter gefährdet werden, ist eine stichprobenartige Kontrolle des Verlags zu verlangen.[675]

Entscheidender Unterschied zur herkömmlichen Zulieferersituation ist indes, dass ein IoT-Produkt fortlaufend mit Daten beliefert wird und diese selbständig und in Echtzeit vom Gerät verarbeitet und umgesetzt

668 *Krause*, in: Soergel, BGB, § 823 Anh. III, Rn. 32; *Voigt,* in: BeckOGK, BGB, § 823, Rn. 704; *Wagner,* in: MüKo, BGB, § 823, Rn. 1043 hebt auf den Vertrauensgrundsatz ab; speziell bzgl. zugelieferter Steuerungssoftware *Gless/Janal*, JR 2016, 561 (568).

669 Zum Ganzen *Krause*, in: Soergel, BGB, § 823 Anh. III, Rn. 32; *Förster*, in: BeckOK, BGB, § 823, Rn. 760; vgl. auch BGH, NJW 1975, 1827 (1828).

670 *Voigt,* in: BeckOGK, BGB, § 823, Rn. 706; *Foerste,* in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 25, Rn. 126.

671 Grundlegend BGH, NJW 1970, 1963.

672 *Voigt,* in: BeckOGK, BGB, § 823, Rn. 750; *Hager*, in: Staudinger, BGB, § 823, Rn. F 27.

673 BGH, NJW 1970, 1963 (1964).

674 *Foerste*, NJW 1991, 1433 (1437).

675 Ansatzweise BGH, NJW 1970, 1963 (1964); *Voigt,* in: BeckOGK, BGB, § 823, Rn. 750; *Hager*, in: Staudinger, BGB, § 823, Rn. F 27; *Foerste*, NJW 1991, 1433 (1437).

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

werden.[676] Es wurde bereits erläutert, dass das fehlende Zusammenfügen der „Produktkomponenten" insoweit keinen Unterschied machen kann. Allerdings ist es dem Hersteller sowohl aufgrund dieser zeitlichen Konstellation als auch aufgrund der schieren Flut an Daten aus tatsächlichen Gegebenheiten regelmäßig unmöglich, die Daten vor der Interaktion mit seinem Produkt einer Prüfung zu unterziehen. Daher wird es zu einer zeitlichen Verlagerung der Stichprobenkontrolle kommen.[677] Diese kann nur noch ex post erfolgen.[678] Sie kann dann aber ganz im Zeichen der Produktbeobachtungspflicht künftige Reaktionen nach sich ziehen. Dieses Defizit an Kontrollmöglichkeit der Daten im Vorfeld der Verarbeitung durch das Produkt muss durch eine sorgfältige Auswahl des Informationsanbieters im Rahmen der herstellerseitigen Organisations- und Kontrollpflichten hinsichtlich seiner Zuliefererkomponente ausgeglichen werden. Die konkreten Sorgfaltsanforderungen hängen maßgeblich davon ab, zu welchem Zweck die Daten genutzt werden.[679] So werden an die Richtigkeit und Genauigkeit von Wetterdaten für die intelligente Bewässerungen des Gartens geringere Anforderungen zu stellen sein als an Daten für steuerungsrelevante Funktionen eines autonomen Kfz.

cc) Offene Systeme

Werden dagegen bei einem offenen Ansatz lediglich Schnittstellen zur Integration oder Verbindung eines Dienstes bereitgestellt, ist fraglich, ob die

676 Ähnlich *Wagner*, VersR 2020, 717 (725): „Bei digitalen Produkten reicht die Kollaboration verschiedener Akteure über die Herstellungsphase hinaus und erfasst auch die Betriebsphase".

677 Eine stichprobenartige Prüfung übermittelter Daten fordern auch *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 157 und *Hey*, Die außervertragliche Haftung des Herstellers autonomer Fahrzeuge, S. 192 f.; *Wiesner*, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 10.6, Rn. 43 zieht eine Haftung in Betracht, „wenn der Hersteller auf die Richtigkeit der zugelieferten Daten nicht hätte vertrauen dürfen". Indes wird nicht auf eine Unterscheidung zwischen offenen oder geschlossenen Systemen eingegangen.

678 Vgl. auch *Grapentin*, JR 2019, 175 (179): „Hersteller werden, auch bedingt durch die Schnelllebigkeit, das hervorgebrachte Ergebnis nur noch bewerten und ihre Schlüsse für die Zukunft ziehen können".

679 In diese Richtung allerdings in Bezug auf das Inverkehrbringen der Daten durch die Informationsanbieter *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 100 und *Schulz*, Verantwortlichkeit bei autonom agierenden Systemen, S. 179.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

Grundsätze zur Verantwortung hinsichtlich Fremdzubehör auch hierauf übertragen werden können.

> Beispiel: Das smarte Bewässerungssystem hält die Möglichkeit vor, dass der Nutzer es mit einem beliebigen Wetterdienst seiner Wahl verbinden kann.

(1) Keine Übertragung der Honda-Rechtsprechung

Die Reichweite der Honda-Rechtsprechung ist in der juristischen Literatur nicht gänzlich unumstritten. Die wohl h.M. stellt darauf ab, dass sich die Verantwortung des Herstellers des Hauptprodukts lediglich auf Kombinationsgefahren erstreckt, nicht aber auf Fehler, die allein dem Zubehörteil anhaften.[680] Begründet wird dies damit, dass der Hersteller selbst bei notwendigem oder empfohlenem Zubehör allein einen Vertrauenstatbestand dahingehend schaffe, dass die Produkte bedenkenlos miteinander kombiniert werden können, nicht aber in Bezug auf die Steuerung selbständiger Gefahren des Zubehörteils. Eine solche würde auch der Nutzer entsprechend seiner Erwartungshaltung allein der Risikosphäre des Zubehörherstellers zuordnen.[681] Dem Hersteller des Hauptprodukts ist die entstandene Gefahrenquelle durch das fehlerhafte Zubehörteil nicht mehr zuzurechnen.[682] Dagegen wird angeführt, dass der Hersteller insgesamt für verwendetes Zubehör verantwortlich sei, das die Gesamtsache und damit auch sein eigenes Produkt unsicher machen kann, insbesondere wenn er zu dessen Verwendung angeregt hat.[683] Vor diesem Hintergrund wird gerade im Bereich des autonomen Fahrens eine Erstreckung der Beobachtungspflicht auf

680 Vgl. *Wagner,* in: MüKo, BGB, § 823, Rn. 1099; *Krause*, in: Soergel, BGB, § 823 Anh. III, Rn. 22; *Hartmann*, Der Warenhersteller im Spannungsfeld, S. 63 f.; *Leupold/Wiesner*, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 9.6.4, Rn. 78; *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 81; im IoT-Kontext *Burrer*, in: Bräutigam/Kraul (Hg.), Internet of Things, § 8, Rn. 102.

681 Ausführlich *Klinger*, Die Produktbeobachtungspflicht bezüglich Fremdzubehörteilen, S. 62 f.

682 *Kunz*, BB 1994, 450 (451); *Huber*, Rechtsfragen des Produktrückrufs, S. 188; *Ulmer*, ZHR 152 (1988), 564 (578).

683 So *Hager*, in: Staudinger, BGB, § 823, Rn. F 22; in diese Richtung auch *Foerste*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 25, Rn. 185.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

Dienste Dritter gefordert, die das autonome Fahren erst ermöglichen oder unterstützen.[684]

Indes darf nicht übersehen werden, dass es bei fehlervermittelten Gefahren nicht um die Zuordnung einer neuen und eigenständigen Gefahrenquelle geht, sondern um einen bestehenden Fehler, der entsprechend den Verantwortungssphären bereits dem Informationsanbieter zugeordnet ist. Damit ist die Gefahr aber durch einen Dritten verursacht, der auch zur Steuerung der Gefahr in der Lage ist, sodass ein Rückgriff auf den Hersteller nicht gerechtfertigt ist.[685] Auch bei zwingend für die ordnungsgemäße Nutzung erforderlichem Zubehör muss die Produktbeobachtungspflicht des Herstellers damit auf Kombinationsgefahren beschränkt sein.[686] Zieht man eine Parallele zu herkömmlichen Produktgefahren, hat der Hersteller eines Kfz auch nicht die Qualität des Treibstoffs zu beobachten, sondern nur, ob fehlerfreier Treibstoff zu keinen Gefahren in Verbindung mit seinem Kfz führt.[687] Weiter sollte daran gedacht werden, dass in Fällen, in denen fehlerhafte oder unvollständige Informationen eine Bedrohung für besonders schützenswerte Rechte und Rechtsgüter darstellen können, diese in Zukunft von staatlichen oder zumindest staatlich überwachten Einrichtungen bereitgestellt werden könnten.[688] Dadurch könnte das Vertrauen und die Akzeptanz der Nutzer in innovative Techniken gefördert werden.

684 *Schrader*, NZV 2018, 489 (492) nennt als Beispiel Baustelleninformationen für Fahrerassistenzsysteme; ähnlich *Eichelberger*, in: Ebers et al., (Hg.), Künstliche Intelligenz und Robotik, S. 187 f.; weitgehend *Ebers*, in: Oppermann/Stender-Vorwachs (Hg.), Autonomes Fahren, 1. Aufl., S. 93 (114), der die Beobachtung der Interaktion sämtlicher Fahrzeuge mit dem eigenen Kfz fordert; tendenziell zurückhaltender *Wagner*, AcP 217 (2017), 707 (752); auch *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 112 wollen fehlerhafte Daten wie Zubehör ansehen.

685 Hierzu auch *Spindler*, in: Hilgendorf (Hg.), Robotik im Kontext von Recht und Moral, S. 63 (73 f.); i.E. auch *Wiesner*, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 10.6, Rn. 43: „Im Übrigen wird eine Haftung des Systemherstellers für Schäden, die durch fehlerhafte Daten eines Dritten ausgelöst werden, in der Regel ausscheiden".

686 Vgl. *Ulmer*, ZHR 152 (1988), 564 (581).

687 Beispiel nach *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 157; vgl. auch *Ulmer*, ZHR 152 (1988), 564 (581).

688 Vgl. *Schulz*, Verantwortlichkeit bei autonom agierenden Systemen, S. 179 f. mit Verweis auf § 27e Abs. 1 LuftVG in Bezug auf Wetterinformationen zur meteorlogischen Sicherung des Luftverkehrs; ferner zur Verkehrsregelung mit entsprechenden Infrastrukturanlagen, S. 181 ff.

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

(2) Konstruktive Sicherheitsmaßnahmen bei Systemstörungen

Auch wenn den Hersteller keine Produktbeobachtungspflicht hinsichtlich fehlervermittelter Gefahren trifft, ist er diesbezüglich nicht gänzlich aus der Verantwortung entlassen.

Eine Haftung kommt dann in Betracht, wenn der Hersteller weitere Sicherheitsmaßnahmen hätte ergreifen können und müssen.[689] Dies betrifft weniger den Fall informationsvermittelter Schädigung als mehr den Fall der fehlenden Verfügbarkeit. Denn IoT-Geräte, die eine umfassende Vernetzung ermöglichen, sind regelmäßig auch auf eine kontinuierliche Vernetzung angewiesen. Nun können aber erforderliche Datenflüsse ausbleiben oder ganze Server nicht erreichbar sein.[690] Ein solches Szenario ist aufgrund allgemeiner Netzwerkprobleme, aber auch aufgrund eines gezielten DDoS-Angriffs auf die digitale Infrastruktur denkbar. Hersteller haben aber gerade bei offenen Systemen keinen Einfluss darauf, ob und welche Infrastruktur dem IoT-Produkt zur Verfügung steht und wie zuverlässig diese ist.[691] Mit den eben gewonnenen Erkenntnissen kann den Hersteller aber nicht die Verantwortung für die durchgängige Verfügbarkeit einer Verbindung treffen.[692] Ausdrücklich unberührt davon bleibt allerdings auch künftig nach der neuen Produkthaftungsrichtlinie die Frage, ob ein Produkt, das sich auf Internetzugangsdienste stützt und bei einer Verbindungsunterbrechung keine Sicherheit gewährleistet, fehlerhaft im Sinne der ProdHaftRL ist, vgl. Erwägungsgrund (17) ProdHaftRL. Hinsichtlich Hochrisiko-KI-Systemen ist eine entsprechende Robustheit, d.h. die Widerstandsfähigkeit in Bezug auf schädliches oder anderweitig unerwünschtes Verhalten, das sich aus der Umgebung, in der das System betrieben wird, ergeben kann (vgl. Erwägungsgrund (75) KI-VO), gem. Art. 15 Abs. 4 KI-VO gerade produktsicherheitsrechtliche Voraussetzung für die Inverkehrgabe. Hierzu können beispielsweise Mechanismen gehören, die es dem System ermöglichen, seinen Betrieb bei bestimmten Anomalien oder beim Betrieb außerhalb bestimmter vorab festgelegter Grenzen sicher zu unterbrechen, vgl. Erwägungsgrund (17) KI-VO. Wählt ein Hersteller aber bewusst eine Produktkonzeption, die auf eine Vernetzungsfähigkeit angelegt ist und zieht er daraus die entsprechenden (Absatz-)Vorteile, hat er auch außerhalb des

689 So *Wiesner*, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 10.6, Rn. 43.
690 Hierzu *Thöne*, Autonome Systeme, S. 228 f. „Risiken einer „digitalen Isolation".
691 *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 99.
692 So auch *Thöne*, Autonome Systeme, S. 228.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

Anwendungsbereichs der KI-VO entsprechende Sicherheitsvorkehrungen für den Fall des Verlusts der Konnektivität zu treffen und sicherzustellen, dass hieraus keine Gefährdungen entstehen.[693] Dabei wird dem Einbau von Redundanzmaßnahmen maßgebliche Bedeutung zukommen.[694] So können insbesondere Daten vorab heruntergeladen werden und vorgehalten werden.[695] Aber auch bei der Verarbeitung und Übertragung von Daten sind Redundanzen möglich. Steht in einer kritischen Situation noch ein Mensch als Rückfallebene zur Verfügung und ist mit dessen Eingreifen auch in zeitlicher Hinsicht rechtzeitig zu rechnen, kann bspw. durch ein akustisches Signal vor dem Ausfall gewarnt werden und der Nutzer über Handlungsmöglichkeiten informiert werden.[696] In den übrigen Fällen wird sich das System selbst in einen möglichst ungefährlichen Zustand bringen müssen.[697]

e) Bedeutung für die Produktbeobachtung

Im Bereich der Kombinationsgefahren unterliegen die Wechselwirkungen bei einem geschlossenen System allein der Herrschaftssphäre des Herstellers, sodass sich keine Besonderheiten hinsichtlich seiner Produktbeobachtungspflicht ergeben. Bei einem offenen System hat der Hersteller eine Produktbeobachtung nach den Grundsätzen der Honda-Entscheidung zu gewährleisten.

Auch im Produktsicherheitsrecht wird künftig klargestellt, dass die Verbindungen und Wechselwirkungen eines Produkts mit externen Gegenständen dessen Sicherheit nicht beeinträchtigen sollen, vgl. Erwägungsgrund (24) GPSR. Daher sind für die Bewertung der Sicherheit eines Produkts

693 I.E. auch *Thöne*, Autonome Systeme, S. 228 und *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 99 „infrastrukturunabhängig sicher nutzbar"; *Mayrhofer,* Außervertragliche Haftung für fremde Autonomie, S. 255 f. „Robustheit des Systems", daneben S. 312.

694 Vgl. auch *Schulz*, NZV 2017, 548 (552); vgl. hinsichtlich Hochrisiko-KI-Systemen Art. 15 Abs. 4 UAbs. 2 KI-VO.

695 *Arzt* et al., MMR 2022, 593 (610).

696 *Hey*, Die außervertragliche Haftung des Herstellers autonomer Fahrzeuge, S. 73 f.; *Oechsler*, in: Staudinger, BGB, § 3 ProdHaftG, Rn. 49.

697 *Hey*, Die außervertragliche Haftung des Herstellers autonomer Fahrzeuge, S. 73; *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 90 f. Beim autonomen Fahren etwa das Abbremsen und Einschalten der Warnblinklichtanlage auf dem Seitenstreifen.

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

nach Art. 6 Abs. 1 lit. c GPSR mögliche Einwirkung anderer Produkte zu berücksichtigen, wenn eine gemeinsame Verwendung vernünftigerweise vorhersehbar ist. Parallel wird diesem Umstand künftig auch haftungsrechtlich Rechnung getragen. Denn auch nach Art. 7 Abs. 2 lit. d ProdHaftRL sind bei der Bestimmung der Fehlerhaftigkeit eines Produkts Auswirkungen anderer Produkte zu berücksichtigen, die nach vernünftigem Ermessen vorhersehbar sind. Zur Bestimmung der Reichweite ließen sich die soeben dargelegten Grundsätze zu den Kombinationsrisiken in Parallele zur BGH-Rechtsprechung auf die Bereiche des öffentlich-rechtlichen Produktsicherheitsrechts und der verschuldensunabhängigen Produkthaftung übertragen.[698]

Hinsichtlich fehlervermittelnder Gefahren hat sich der Hersteller bei geschlossenen Systemen über stichprobenartige Kontrollen der Qualität der zugelieferten Daten und Dienste zu vergewissern. Da sich das Zusammenwirken nicht lediglich auf die Herstellungsphase bezieht, sondern gerade die Nutzungsphase betrifft, sind Stichproben als Teil der Produktbeobachtung zu gewährleisten. Bei offenen Systemen liegt in Bezug auf fehlervermittelnde Gefahren nicht die Konstellation der Honda-Entscheidung vor. Selbst bei notwendigen Daten oder Diensten ist die Gefahr allein durch einen Dritten verursacht und kann von diesem gesteuert werden, sodass den Hersteller des Hauptprodukts auch keine Beobachtungspflicht trifft.

Vor diesem Hintergrund wird die Produkthaftung auch auf digitale Dienste und damit in den Dienstleistungssektor hinein ausgeweitet.[699]

Auch die neue Produkthaftungsrichtlinie erkennt künftig an, dass digitale Dienste für die Sicherheit des Produkts genauso grundlegend sein können wie physische oder digitale Komponenten, vgl. Erwägungsgrund (15) ProdHaftRL. Vor diesem Hintergrund sieht Art. 11 Abs. 2 lit. a ProdHaftRL vor, dass sich ein Hersteller nicht von der Haftung befreien kann, wenn das Produkt im Zeitpunkt seines Inverkehrbringens fehlerfrei war, jedoch danach durch mit ihm verbundene und unter seiner Kontrolle stehende digitale Dienste fehlerhaft geworden ist. Ein solcher verbundener Dienst liegt nach Art. 4 Nr. 3 ProdHaftRL vor, wenn der digitale Dienst so in ein Produkt integriert oder so mit ihm verbunden ist, dass das Produkt ohne ihn eine oder mehrere seiner Funktionen, zum Beispiel die kontinuierliche Bereit-

698 *Kapoor/Sedlmaier*, RAW 2023, 8 (12).

699 Spindler CR 2022, 689 (690): „Fast schon revolutionär"; vgl. auch Wagner JZ 2023, 1 (5).

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

stellung von Verkehrsdaten in einem Navigationssystem,[700] nicht ausführen könnte. Eine die Haftung voraussetzende Kontrolle des Herstellers ist dabei nur dann gegeben, wenn er die Integration oder Verbindung des Dienstes selbst vornimmt oder diese einem Dritten genehmigt bzw. ihr zustimmt (Art. 4 Nr. 5 ProdHaftRL). Hierfür soll es ausweislich Erwägungsgrund (18) ProdHaftRL ausreichen, dass der verbundene Dienst als Teil des Produkts präsentiert wird. Im Kommissionsentwurf[701] wurde dagegen noch eine Empfehlung des Herstellers oder die Beeinflussung der Bereitstellung durch Dritte auf andere Weise als ausreichend erachtet.[702] Mit dieser Änderung im Gesetzgebungsprozess wird man eine Zustimmung des Herstellers immer nur als Autorisierung für die jeweilige Version des Dienstes ansehen können, nicht aber gleichzeitig für zukünftige Versionen.[703] Zumindest für geschlossene Systeme bedeutet dies eine Ausweitung der Herstellerhaftung, da der Hersteller aufgrund seiner Kontrolle verschuldensunabhängig für solche verbundenen digitalen Dienste haftet.[704] Nur am Rande sei darauf hingewiesen, dass künftig auch der Diensterbringer als Hersteller der Komponente nach Art. 8 Abs. 1 UAbs. 1 lit. b ProdHaftRL haftbar gemacht werden kann. Dagegen gelten nach Erwägungsgrund (18) ProdHaftRL die bloße Bereitstellung einer Schnittstelle zur Integration oder Verbindung des Dienstes oder die Empfehlung einer Marke oder auch die Tatsache, dass bestimmte Dienste nicht untersagt werden, nicht als Zustimmung des Herstellers. Vielmehr wird eine gewisse Identifikation mit dem verbundenen Dienst für eine Haftung vorausgesetzt. Damit kommt bei offenen Systemen auch weiterhin keine Haftung des Herstellers für die Fehlerhaftigkeit des Dienstes in Betracht.[705]

700 Dieses und weitere Beispiele nennt Erwägungsgrund (17) ProdHaftRL.
701 EU-Kommission, COM(2022) 495 final.
702 Vgl. Erwägungsrund (15) COM(2022) 495 final.
703 Nach dem Kommissionsentwurf noch offengelassen von Spindler CR 2022, 689 (691) und Kapoor/Sedlmaier RAW 2023, 8 (11).
704 Krit. auch *Kapoor*/*Sedlmaier*, RAW 2023, 8 (10 f.).
705 So auch *Lejeune*, ITRB 2024, 102 (104).

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

4. KI und Autonomie

a) Begriff und Bedeutungsgehalt

Künstliche Intelligenz (nachfolgend „KI") erhält zunehmend Einzug in Softwareprogramme und CPS.[706] KI greifbar zu machen, fällt deshalb so schwer, weil es an klaren Definitionen fehlt.[707] Damit gehen aber auch die Vorstellungen über den Bedeutungsgehalt der Begrifflichkeit weit auseinander.[708] Bei einer stark am Begriff und der Funktion orientierten Betrachtungsweise ließe sich unter KI der Versuch begreifen, abgrenzbare Bereiche des menschlichen Denkens nachzubilden oder zu übertreffen.[709] Gerade Nutzer meinen KI dann zu erkennen, wenn menschliches Verhalten imitiert wird (Bsp.: Sprachdienste), ein eigenes Handeln erkannt wird (Bsp.: Saugroboter) oder Daten nach menschlichem Vorbild klassifiziert werden (Bsp.: Erkennung von Verkehrszeichen).[710] Da ein Taschenrechner ein reines Rechenproblem schneller und präziser als ein Mensch lösen kann, könnte man diesen entsprechend dieser begrifflichen Einordnung bereits als künstlich intelligent bezeichnen.[711] Eine solche Betrachtungsweise ermöglicht aber keine Abgrenzung anhand der wesentlichen Eigenschaften und der sich daraus ergebenden Herausforderungen im Vergleich zu herkömmlichen Techniken. Der Kommissionsvorschlag[712] verfolgte in Art. 3 Nr. 1 KI-VO noch einen verfahrensbasierten Ansatz zur Definition von KI, indem darauf abgestellt wurde, ob bei der Entwicklung entsprechender Systeme Techniken oder Konzepte des maschinellen Lernens, logik-

706 *Riehm/Meier*, in: Fischer/Hoppen/Wimmers, DGRI Jahrbuch 2018, S. 1 (Rn. 4).

707 Vgl. die Nachweise der versch. Definitionsversuche von KI bei *Kaulartz/Braegelmann*, in: Kaulartz/Braegelmann (Hg.), Artificial Intelligence und Machine Learning, S. 2 ff; vgl. auch *Riehm/Meier*, in: Fischer/Hoppen/Wimmers, DGRI Jahrbuch 2018, S. 1 (Rn. 2).

708 Vgl. auch *Steege*, SVR 2023, 9 (9).

709 Vgl. *Riehm/Meier*, in: Fischer/Hoppen/Wimmers, DGRI Jahrbuch 2018, S. 1 (Rn. 2); *Stiemerling*, in: Kaulartz/Braegelmann (Hg.), Artificial Intelligence und Machine Learning, S. 15; *Linardatos*, ZIP 2019, 504 (504); bei „starke KI", die ein Bewusstsein oder Kreativität entwickelt und sich außerhalb der durch die Programmierung gesetzten Grenzen bewegt, handelt es sich dagegen um Zukunftsmusik, weshalb hier nicht näher darauf eingegangen werden soll.

710 *Schröder*, in: Kaulartz/Braegelmann (Hg.), Artificial Intelligence und Machine Learning, S. 52 f.

711 Vgl. *Dötsch*, Außervertragliche Haftung für KI, S. 5 f.; *Riehm/Meier*, in: Fischer/Hoppen/Wimmers, DGRI Jahrbuch 2018, S. 1 (Rn. 2).

712 EU-Kommission, COM(2021) 206 final.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

und wissensbasierte Konzepte oder bestimmte statistische Verfahren (vgl. Anhang I) verwendet wurden und die Systeme das Umfeld beeinflussen, mit dem sie interagieren.[713] Da die aufgelisteten Techniken aber auch bei herkömmlicher Programmierung zum Tragen kommen können, führte ein derart weitreichender verfahrensbasierter Ansatz dazu, dass nahezu jedes Computerprogramm auch als KI-System angesehen werden kann.[714] Um die kritischen Eigenschaften von KI-Systemen aber anhand ihrer wesentlichen Merkmale charakterisieren zu können, ist eine Abgrenzung von einfacheren herkömmlichen Softwaresystemen und Programmierungsansätzen erforderlich, welche auf ausschließlich von natürlichen Personen definierten Regeln für das automatische Ausführen von Operationen beruhen, vgl. nunmehr auch Erwägungsgrund (12) KI-VO.[715]

Der Ausführung vorgegebener Regeln kann die Ableitungsfähigkeit eines Systems gegenübergestellt werden. Diese Fähigkeit bezieht sich auf den Prozess des Erhalts von Ergebnissen sowie auf die Fähigkeit, Modelle oder Algorithmen aus Eingaben oder Daten abzuleiten, vgl. Erwägungsgrund (12) KI-VO. Bei genauerer Betrachtung der einzelnen Verfahren bzw. Techniken findet sich diese Fähigkeit insbesondere beim maschinellen Lernen und lässt sich daher eine Sonderstellung des maschinellen Lernens ausmachen.[716] So wird grundlegend von den klassischen Algorithmen-Strukturen abgewichen.[717] Das System beschränkt sich nicht darauf, vorprogrammierte Regeln auszuführen, sondern es besitzt die Fähigkeit unvollständige Strukturen durch selbst erlernte Erfahrungen und entsprechende Anpassung des

713 Der zweite Halbsatz der Definition, wonach das System im Hinblick auf von Menschen festgelegte Ziele Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, dürfte dagegen eine Leerformel dargestellt haben, da jegliche Software technisch so beschaffen ist, dass sie für definierte Zielvorgaben bestimmten Output erzeugt, so *Bomhard/Merkle*, RDi 2021, 276 (277). Gleichwohl findet sich dieser Satzteil auch im verabschiedeten Gesetzestext wieder.

714 Vgl. *Bomhard/Merkle*, RDi 2021, 276 (277); *Krüger/Wagner*, ZfPC 2023, 124 (125); *Haftenberger*, Die Produkthaftung für künstlich intelligente Medizinprodukte, S. 49 f.

715 Für ein hieran orientiertes Begriffsverständnis plädiert auch *Stiemerling*, in: Kaulartz/Braegelmann (Hg.), Artificial Intelligence und Machine Learning, S.23; *McGuire*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 58, Rn. 17 ff.; krit. daher auch *Steege*, SVR 2023, 9 (10).

716 Vgl. auch *McGuire*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 58, Rn. 20.

717 *Riehm/Meier*, in: Fischer/Hoppen/Wimmers, DGRI Jahrbuch 2018, S. 1 (Rn. 6).

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

Verhaltens zu erweitern.[718] Dazu wird dem System eine ausreichend große Menge an Beispiels- bzw. Trainingsdaten vorgegeben, anhand derer es Muster und Gesetzmäßigkeiten einer Problemstellung erfasst. Im Rahmen dieses Trainings[719] lernt das System eigenständig und generiert Wissen durch die eigene Erfahrung mit dem Ziel, seine Entscheidungsregeln zu verbessern und sich weiterzuentwickeln.[720] Das Wissen wird dabei in Modellen aufgebaut, wobei der zugrundeliegende Algorithmus geändert werden kann oder insbesondere bei leistungsstarken Systemen das Wissen in neuronale Netze eingebettet wird. Das erlernte Modell wird dann verwendet, um das erlernte Wissen auf neue Situationen und bisher nicht gekannte Daten anzuwenden.[721] Das System wird folglich nicht programmiert, sondern trainiert.[722] Anhand der gewonnenen Erfahrungen kann das System dann zukunftsrelevante, nicht explizit programmierte Entscheidungen treffen.[723] Dem System wird daher ein autonomes Verhalten attestiert.[724] Gerade die Fähigkeit des selbstlernenden Verhaltens und die damit verbundene eigenständige Weiterentwicklung ermöglichen eine Abgrenzung zu klassischer Software.[725] An die Kriterien der Autonomie und des Selbstlernens knüpft nunmehr auch die Definition in Art. 3 Nr. 1 KI-VO an, indem unter einem KI-System ein maschinengestütztes System verstanden wird, das so konzi-

718 *Dötsch*, Außervertragliche Haftung für KI, S. 13; *Riehm/Meier*, in: Fischer/Hoppen/Wimmers, DGRI Jahrbuch 2018, S. 1 (Rn. 6).

719 Zu den untersch. Arten des maschinellen Lernens *Niederée/Nejdl*, in: Ebers et al., (Hg.), Künstliche Intelligenz und Robotik, S. 49; *Sorge*, in: Hornung (Hg.), Rechtsfragen der Industrie 4.0, S. 139 (141). Beim überwachten Lernen enthalten die Trainingsdaten bereits das gewünschte Ergebnis. Das System lernt, anhand dieser Informationen Muster zu erkennen und zu verallgemeinern. Beim unüberwachten Lernen soll das System aus den Daten selbst Regeln ziehen und Cluster bilden, die vorher auch dem Entwickler nicht bekannt sind. Beim verstärkenden Lernen werden die Regeln, die das System findet und nicht vorgegeben sind, an eine Belohnung geknüpft.

720 *Specht/Herold*, MMR 2018, 40 (41); *Linardatos*, ZIP 2019, 504 (505); *Wagner*, VersR 2020, 717 (720); *Zech*, DJT 2020 Gutachten, A S. 31 f.

721 *Niederée/Nejdl*, in: Ebers et al., (Hg.), Künstliche Intelligenz und Robotik, S. 48; *Etzkorn*, MMR 2020, 360 (361).

722 *Zech*, DJT 2020 Gutachten, A S. 32; *Ebers*, in: Oppermann/Stender-Vorwachs (Hg.), Autonomes Fahren, 1. Aufl. S. 93 (94 f.).

723 *Linardatos*, ZIP 2019, 504 (505).

724 *Krüger/Wagner*, ZfPC 2023, 124 (124); zu den unterschiedlichen Ansätzen, Autonomie zu definieren, vgl. *Dötsch*, Außervertragliche Haftung für KI, S. 59 ff.

725 *Krüger/Wagner*, ZfPC 2023, 124 (125); *Hacker*, NJW 2020, 2142 (2142 f.); *Steege*, in: Buck-Heeb/Oppermann (Hg.), Automatisierte Systeme, S. 367 (371); *McGuire*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 58, Rn. 24.

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

piert ist, dass es in unterschiedlichem Maße autonom betrieben werden kann und nach seiner Inbetriebnahme anpassungsfähig sein kann.[726]

Indes zeigt auch ein Navigationssystem, das auf eine veränderte Umweltbedingung (wie einen Stau) selbständig mit einer Verhaltensänderung (Änderung der Route) reagiert, in gewissem Maße ein autonomes Verhalten, auch wenn der Algorithmus des Navigationssystems, nach dem die Route berechnet wird, unverändert bleibt.[727] Ein qualitativer Unterschied besteht aber, sobald die Grenzen herkömmlicher Programmierung erreicht werden.[728] Automatisierten Systemen, worunter allgemein die selbsttätige Steuerung durch einen Computer verstanden wird,[729] liegt nämlich klassischerweise eine „Wenn-dann"-Programmierung zugrunde. Dem System werden Voraussetzungen vorgegeben („Wenn"), unter welchen Aktionen („Dann") ausgeführt werden.[730] Diese Herangehensweise scheitert aber dort, wo dynamisch auf Umgebungen oder Problemstellungen reagiert werden muss und wo unvorhersehbare und komplexe Aufgaben flexibel gelöst werden müssen.[731] In diesen Fällen ist eine vollständige imperative Programmierung im Vorfeld aufgrund der unendlichen Möglichkeiten an Bedingungen gerade nicht möglich.[732] Um diesen qualitativen Unterschied autonomer Systeme abzubilden, sind darunter nur solche Systeme zu fassen, die nicht nach vordefinierten Bedingungen und Aktionen handeln, sondern ihr Verhalten selbständig festlegen oder dieses aufgrund selbständigen Lernens ändern und sich nicht ausschließlich in der vorprogrammierten Logik bewegen.[733] Die Grundlage hierfür bildet maschinelles Ler-

726 Auch der zweite Halbsatz der Definition wurde dahingehend angepasst, dass ein KI-System für explizite oder implizite Zwecke aus den Eingaben, die es erhält, Ergebnisse wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen ableitet, die die physische oder virtuelle Umgebung beeinflussen können.

727 Beispiel nach *Zech*, in: Gless/Seelemann (Hg.), Intelligente Agenten und das Recht, S. 163 (171).

728 Vgl. auch *Wagner*, JZ 2023, 1 (1 f.).

729 Vgl. *Zech*, in: *Gless/Seelemann* (Hg.), Intelligente Agenten und das Recht, S. 163 (168); der Übergang zu autonomen Systemen erfolgt allerdings graduell, vgl. *Sommer*, Haftung für autonome Systeme, S. 36.

730 *Fedler*, in: Ebers/Steinrötter (Hg.), Künstliche Intelligenz und smarte Robotik, S. 91 (95).

731 *Fedler*, in: Ebers/Steinrötter (Hg.), Künstliche Intelligenz und smarte Robotik, S. 91 (95); *Zech*, DJT 2020 Gutachten, A S. 31 f; *Zech*, in: Gless/Seelemann (Hg.), Intelligente Agenten und das Recht, S. 163 (171).

732 Vgl. *Zech*, DJT 2020 Gutachten, A S. 32 f.

733 *Fedler*, in: Ebers/Steinrötter (Hg.), Künstliche Intelligenz und smarte Robotik, S. 91 (95); *McGuire*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch,

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

nen.[734] Autonome Systeme können damit trotz unterschiedlicher Ausgangsstellungen komplexe Probleme anhand eines Handlungsplans eigenständig lösen.[735] Während es sich also bei Assistenzsystemen im Auto wie einem Spurhalteassistent oder einem Tempomat um automatisierte Systeme handelt, welche lediglich die zu einem früheren Zeitpunkt erfolgte und damit voreingestellte Anweisung eines Menschen (vereinfacht: Wenn sensorische Erkennung des Überfahrens des Fahrstreifens, dann Zurückziehen in Spur) ausführen, liegt vollständige Autonomie erst vor, wenn das Fahrzeug gänzlich ohne Zutun des Menschen am Straßenverkehr teilnimmt.[736] Die Gefahren so verstandener autonomer Entscheidungen, die mit dem Selbstlernen einhergehen, werden dann als „Autonomierisiko" bezeichnet.[737]

Bedeutsam ist in diesem Kontext noch die Unterscheidung zwischen der Trainingsphase, in der sich das System denklogisch weiterentwickelt, und der Nutzungsphase. Aktuell ist es nämlich noch die Regel, das System nach dem abgeschlossenen Training „einzufrieren", um sicherzustellen, dass es seinen bisherigen Lernzustand beibehält.[738] Gleichwohl können in der Nutzungsphase gesammelte und an den Hersteller geleitete Daten von diesem zu weiteren Trainingszwecken verwendet werden und das System später mittels eines Updates verbessert werden. Ebenso möglich ist es, dass das System weiter direkt aus der Interaktion mit der Umgebung lernt, sodass sich seine Entscheidungen und damit sein Verhalten auch im laufenden

§ 58, Rn. 24; *Haftenberger*, Die Produkthaftung für künstlich intelligente Medizinprodukte, S. 53; ähnlich *Teubner*, AcP 218 (2018), 155 (174).

734 *Wahlster*, Informatik Spektrum 2017, 409 (410).

735 *Wahlster*, Informatik Spektrum 2017, 409 (409).

736 Beispiele nach *Specht/Herold*, MMR 2018, 40 (40 f.). Diese nennen als weiteres Beispiel eines automatisierten Systems einen Drucker, der ohne Anweisung in der konkreten Situation Druckpatronen nachbestellt, wenn zuvor voreingestellt wurde, dass bei Eintritt der Bedingung „leere Druckpatrone" eine Bestellung erfolgen soll; in vergleichbarer Weise findet die Abgrenzung vom automatisierten und autonomen Vertragsschluss statt bei *Grützmacher/Heckmann*, CR 2019, 553 (553 f.).

737 Vgl. nur *Teubner*, AcP 218 (2018), 155 (164); *Zech*, in: Gless/Seelmann (Hg.), Intelligente Agenten und das Recht, S. 163 (175 f.); *Zech*, DJT 2020 Gutachten, A S. 31; *Sommer*, Haftung für autonome Systeme, S. 43; *Haftenberger*, Die Produkthaftung für künstlich intelligente Medizinprodukte, S. 55; *Eichelberger*, in: Ebers et al., (Hg.), Künstliche Intelligenz und Robotik, S. 175 spricht terminologisch vom Intelligenzrisiko; *Burchardi*, EuZW 2022, 685 (685); *Ebert* et al., ZfPC 2023, 16 (19).

738 *Zech*, DJT 2020 Gutachten, A S. 37; Vgl. *Handorn/Juknat*, MPR 2022, 77 (86) sprechen von „Design-Freeze" und als Folge von „statische[n] Systeme[n]".

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

Betrieb noch verändern. Damit gibt der Hersteller aber zugleich seinen Einfluss auf die Verhaltensänderungen auf.[739]

b) Eingeschränkte Vorhersehbarkeit

Die Lernfähigkeit führt dazu, dass – abhängig vom jeweiligen Lernzustand und im Unterschied zu deterministischen Systemen – gleiche Eingangsdaten in der Situation unterschiedliche Ergebnisse hervorbringen können,[740] die nicht im Vorfeld bereits festgelegt sind.[741] Das Verhalten bzw. die Ergebnisse lernfähiger Systeme sind damit nicht in jeder Situation berechenbar und nicht im Detail vorhersehbar und beeinflussbar.[742] Dadurch dass bei einem lernfähigen System die Regeln in geringerem Maße vom Programmierer vorgegeben werden als bei einem deterministischen System, nimmt auch die Kontrolle des Programmierers über das Verhalten des Systems ab.[743] Bei Lichte betrachtet findet ein Kontrollverlust aber bei entsprechender Komplexität und aufgrund des beschränkten menschlichen Verständnishorizonts zwar auch bei deterministischen Systemen statt.[744]

Die eingeschränkte Vorhersagbarkeit der Ergebnisse von KI-Systemen liegt jedoch in ihrer Funktionsweise begründet. Diese erkennen Muster und statistische Zusammenhänge (Korrelationen), suchen aber nicht nach den Ursachen der relevanten Parameter im Sinne einer eindeutigen, determinierten Kausalkette. Entscheidungen, die lediglich aufgrund von statischen Korrelationen und damit von Wahrscheinlichkeiten getroffen werden, mögen zwar immer sinnvoll erscheinende Resultate hervorbringen, diese müssen aber nicht zwangsläufig korrekt sein und weisen eine Feh-

739 Zum Ganzen *Stiemerling*, in: Kaulartz/Braegelmann (Hg.), Artificial Intelligence und Machine Learning, S. 27; *Haagen*, Verantwortung für künstliche Intelligenz, S. 281 ff. spricht von geschlossenen Systemen, welche sich aus einer abgeschlossenen über die Betriebsdauer gleichbleibenden Datenmenge zusammensetzen und offenen Systemen, welche sich selbst neue Verhaltensweisen antrainieren.

740 *Riehm/Meier*, in: Fischer/Hoppen/Wimmers, DGRI Jahrbuch 2018, S. 1 (Rn. 6).

741 *Haftenberger*, Die Produkthaftung für künstlich intelligente Medizinprodukte, S. 54.

742 *Zech*, DJT 2020 Gutachten, A S. 42; *Zech*, ZfPW 2019, 198 (205); *Riehm/Meier*, in: Fischer/Hoppen/Wimmers, DGRI Jahrbuch 2018, S. 1 (Rn. 5, 8); *Günther*, Roboter und rechtliche Verantwortung, S. 37 f.; *Lohmann*, AJP/PJA 2017, 152 (162) spricht daher von „Wundertüte".

743 *Zech*, DJT 2020 Gutachten, A S. 34; *Wagner*, JZ 2023, 1 (2).

744 Vgl. *Riehm*, DJT 2022 Referat, K S. 48 f.; *Riehm/Meier*, in: Fischer/Hoppen/Wimmers, DGRI Jahrbuch 2018, S. 1 (Rn. 7); *Zech*, DJT 2020 Gutachten, A S. 43 f.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

leranfälligkeit auf.[745] Hier spielt auch die Unvollständigkeit der Informationen, der sich KI-Systeme ausgesetzt sehen, hinein.[746] Denn das Training kann immer nur mit einer limitierten Datenmenge durchgeführt werden. Ebenso wenig wie ein Programmierer für eine unvorhersehbare, komplexe Situation alle Programmregeln definieren kann, kann ein System mit allen möglichen Daten trainiert werden. Dies führt aber zwangsläufig dazu, dass in der Praxis Situationen auftreten, in denen das System sich nicht wie gewünscht verhält, insbesondere beim Einsatz in komplexen Umgebungsszenarien.[747] Allen Fähigkeiten des Selbstlernens und der Weiterentwicklung zum Trotz können Situationen auftreten, in denen das System nicht nur die falsche Antwort gibt, sondern gar nicht eindeutig ist, worin die richtige Antwort eigentlich liegt oder nicht sicher ist, ob die Eingangsdaten aus der Situation die notwendigen Informationen für die notwendige Zuteilung enthalten.[748]

Da ein solches System seine eigenen Entscheidungsregeln entwickelt, stehen dem Programmierer zum Zeitpunkt der Entscheidung auch nicht alle Ausgangsdaten zur Verfügung. Vielmehr „entwächst es der Kontrolle durch seinen Programmierer".[749] So mag bei neuronalen Netzen für den Entwickler noch bekannt sein, welche Eingabewerte existierten, wie deren Gewichtung vorgesehen war und nach welchen Kriterien das System lernen sollte, wie die Entscheidung dann tatsächlich durch das Zusammenwirken dieser Faktoren ausfallen wird, ist im Einzelfall jedoch nicht mehr exakt vorhersehbar.[750] Ähnlich verhält es sich, wenn das System im Wege der

745 *Schröder*, in: Kaulartz/Braegelmann (Hg.), Artificial Intelligence und Machine Learning, S. 54; *Ebers*, in: Ebers et al., (Hg.), Künstliche Intelligenz und Robotik, S. 88 f.

746 *Riehm/Meier*, in: Fischer/Hoppen/Wimmers, DGRI Jahrbuch 2018, S. 1 (Rn. 6) sprechen von „inhärente[r] anfängliche[r] Unvollständigkeit" der KI-Systeme.

747 Hierzu *Horner/Kaulartz*, CR 2016, 7 (11), welche anmerken, dass gerade im öffentlichen Raum unvorhersehbare Umwelteinflüsse auftreten können; anschaulich *Staudenmayer*, NJW 2023, 894 (895) „Zwar kann man im Vorhinein testen, welche Entscheidung eine KI in einer bestimmten Situation treffen wird. Trifft etwa ein vollautonomes Fahrzeug dann auf dieselbe Verkehrssituation, wird es genau dieselbe Entscheidung treffen. Das Problem ist aber, dass es‚dieselbe Verkehrssituation' nicht gibt".

748 Zum Ganzen *Stiemerling*, in: Kaulartz/Braegelmann (Hg.), Artificial Intelligence und Machine Learning, S. 23 ff.

749 So *Wagner*, VersR 2020, 717 (720).

750 Vgl. *Riehm/Meier*, in: Fischer/Hoppen/Wimmers, DGRI Jahrbuch 2018, S. 1 (Rn. 5); *Linardatos*, ZIP 2019, 504 (505), welcher auch die Funktionsweise von neuronalen Netzen erklärt.

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

Weiterentwicklung seinen Algorithmus verändert. Die fehlende Nachvollziehbarkeit des Lernprozesses bzw. des Weges der Wissensgenerierung,[751] führt zur fehlenden Vorhersagbarkeit der Entscheidung.

c) Fehlende Nachvollziehbarkeit

Gleichzeitig führt die Lernfähigkeit auch zu der Schwierigkeit, das Verhalten ex post nachzuvollziehen.[752] Denn das System erklärt nicht, warum es eine Entscheidung in diese oder jene Richtung trifft, da es statistisch intuitiv aufgrund von Korrelationen und gerade nicht aufgrund von Kausalitäten vorgeht.[753] Um zu verstehen, warum ein autonomes System eine bestimmte Entscheidung getroffen hat, müsste man bei lernenden Algorithmen den entsprechenden Algorithmus unter gleichen Bedingungen wiederholen. Dies ist aber nur möglich, wenn alle Eingaben in das System seit dem Systemstart (Historie) gespeichert wurden. Eine solche Protokollierung der Historie kann aber mit Kapazitätsproblemen verbunden sein.[754] Bei neuronalen Netzen bleiben die entscheidungsrelevanten Kriterien gänzlich in den Tiefen des Netztes verborgen. Man spricht von „Black-Boxes". Unter explainable AI werden Ansätze verstanden, diese black-boxes wieder verständlich zu machen.[755]

d) Haftungsrechtliche Einordnung

Der besondere Wert autonomer Systeme liegt in ihrem Einsatz in unterschiedlichsten Umgebungsszenarien. Welche Entscheidung sie in diesen Umgebungsszenarien treffen ist allerdings weder für den Nutzer noch für den Hersteller ex ante exakt vorherzusagen. Aufgrund der denklogisch begrenzten Datenmenge in der Trainingsphase können nicht alle Einsatzsituationen in der Praxis abgebildet werden. Vielmehr muss sich der Hersteller darauf verlassen, dass das autonome System anhand der Trainingsda-

751 *Stiemerling*, CR 2015, 762 (764).
752 *Zech*, DJT 2020 Gutachten, A S. 42.
753 Vgl. *Körner*, in: Kaulartz/Braegelmann (Hg.), Artificial Intelligence und Machine Learning, S. 44 ff.; *Käde/von Maltzan*, CR 2020, 66 (71).
754 Vgl. *Reichwald/Pfisterer*, CR 2016, 208 (210 f.).
755 *Linardatos*, ZIP 2019, 504 (505); *Zech*, DJT 2020 Gutachten, A S. 33; zu den möglichen Ansätzen *Käde/von Maltzan*, CR 2020, 66 (69 ff.).

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

ten eigene Entscheidungsregeln entwickelt und sich in die Lage versetzt, möglichst alle individuell auftretenden Praxissituationen zu lösen. Die von solchen autonomen Entscheidungen ausgehenden Gefahren werfen in haftungsrechtlicher Hinsicht Fragen der Zuordnung der Verantwortlichkeit auf.[756] Bezogen auf den Hersteller erscheint fraglich, inwieweit ihm eine Rechtsgutsverletzung, die durch einen fehlerhaften Lernprozess des autonomen Systems verursacht wurde, überhaupt noch zugerechnet werden kann.[757]

aa) Keine Pflichtwidrigkeit durch Inverkehrgabe

Allein die Tatsache, dass das System auch für den Hersteller unvorhersehbar agiert, kann nicht zu dessen pauschaler Haftungsbefreiung führen.[758] Denn schon allgemein begründet das Schaffen einer unkontrollierbaren Gefahrenquelle keine Haftungserleichterung, sondern allenfalls eine Haftungsverschärfung.[759] Andererseits wird angeführt, dass die Unvorhersehbarkeit und damit die Unkontrollierbarkeit des Systems per se einen Pflichtenverstoß des Herstellers begründe.[760] Indes gehen die spezifischen Vorteile, die sich aus der Flexibilität und Anpassungsfähigkeit autonomer Systeme ergeben, auch mit der Möglichkeit sicherheitskritischer Entscheidungen einher und ziehen eben auch spezifische Nachteile nach sich. Das Inverkehrbringen autonomer Systeme stets als pflichtwidrig anzusehen würde bedeuten, dass es solchen Systemen von vorneherein verwehrt bliebe, die an sie gerichteten berechtigten Sicherheitserwartungen zu erfüllen. Dies ist mit den Prinzipien der Verschuldenshaftung nicht vereinbar und würde überdies den technischen Fortschritt ausbremsen.[761] Maßgeblich sind letztendlich die Sicherheitserwartungen der Nutzer und nicht die Ursachen für

756 Vgl. nur *Horner/Kaulartz*, CR 2016, 7 (7): „Kernfrage der Haftung 4.0".

757 So auch *Eichelberger*, in: Ebers et al., (Hg.), Künstliche Intelligenz und Robotik, S. 182 und *Taeger*, in: NK-ProdR, § 3 ProdHaftG, Rn. 55.

758 *Leupold/Wiesner*, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 9.6.4, Rn. 17; *v. Bodungen*, in: Chibanguza/Kuß/Steege (Hg.), Künstliche Intelligenz, § 3, I., Rn. 26.

759 *Wagner*, AcP 217 (2017), 707 (713); *Voigt,* in: BeckOGK, BGB, § 823, Rn. 763; *Haagen*, Verantwortung für Künstliche Intelligenz, S. 239.

760 So aber im Grundsatz, wenn auch mit der Anerkennung von Ausnahmen, *Zech*, in: Gless/Seelmann (Hg.), Intelligente Agenten und das Recht, S. 163 (192) und *Zech*, ZfPW 2019, 198 (213); dagegen *Steege*, in: Buck-Heeb/Oppermann (Hg.), Automatisierte Systeme, S. 367 (385) und *Voigt,* in: BeckOGK, BGB, § 823, Rn. 773.

761 *Dötsch*, Außervertragliche Haftung für KI, S. 207.

https://doi.org/10.5771/9783748964490-89 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

deren Durchbrechung.[762] Hiervon ausgehend ist ein Ausgleich zwischen den Interessen möglicher Geschädigter und denen des Herstellers an einer wirtschaftlichen Entwicklung und Vermarktung zu finden.[763] Eine absolute Sicherheit hat auch der Hersteller autonomer Systeme nicht zu gewährleisten, sondern nur die Schadensvermeidung im Rahmen des Möglichen und Zumutbaren.[764] Ein Pflichtenverstoß des Herstellers begründet die Inverkehrgabe einer unkontrollierbaren Gefahrenquelle demnach erst unter dem Gesichtspunkt der Außerachtlassung der erforderlichen und zumutbaren Sicherheitsvorkehrungen.[765]

Grundvoraussetzung hierfür wird die sorgfältige Programmierung und das hinreichende Training mit einer ausreichenden Datenmenge (vgl. zu den Qualitätskriterien für Hochrisiko-KI-Systeme Art. 10 KI-VO) des autonomen Systems sein.[766] Hierzu gehört auch die Durchführung von Tests (vgl. für Hochrisiko-KI-Systeme Art. 9 Abs. 6 KI-VO) und Wiederholungen bis die Fehlerrate der Entscheidungen unter einen für das Einsatzgebiet individuell zu bestimmenden Grenzwert gefallen ist.[767] Abhängig vom jeweiligen Einsatzzweck scheint auch eine räumliche Begrenzung oder eine Beschränkung auf Nutzer mit besonderer Sachkunde denkbar.[768] Soll das autonome System nicht lediglich in der Trainingsphase, sondern auch in der Nutzungsphase aus der Interaktion mit der Umgebung lernen und sich weiterentwickeln, ist an eine vorherige Verifizierung der Änderung der Verhaltensregeln durch den Hersteller zu denken und deren Implementie-

762 Hierzu *Oechsler*, in: Staudinger, BGB, § 3 ProdHaftG, Rn. 128.

763 *Dötsch*, Außervertragliche Haftung für KI, S. 207.

764 *Wagner*, VersR 2020, 717 (727); *Leupold/Wiesner*, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 9.6.4, Rn. 17; *Thöne*, Autonome Systeme, S. 208.

765 *v. Bodungen*, in: Chibanguza/Kuß/Steege (Hg.), Künstliche Intelligenz, § 3, I., Rn. 26; *Wagner*, VersR 2020, 717 (727); vgl. auch *Haftenberger*, Die Produkthaftung für künstlich intelligente Medizinprodukte, S. 158 ff.; *Dötsch*, Außervertragliche Haftung für KI, S. 207 und S. 217, daneben werden auf S. 219 f. maßgebliche Sicherungsmaßnahmen und Abwägungskriterien aufgelistet.

766 In diese Richtung auch *Thöne*, Autonome Systeme, S. 209; *Dötsch*, Außervertragliche Haftung für KI, S. 217.

767 *Ebers*, in: Oppermann/Stender-Vorwachs (Hg.), Autonomes Fahren, 1. Aufl., S. 93 (107); *Rosenberger*, Die außervertragliche Haftung für automatisierte Fahrzeuge, S. 317; ähnlich auch *McGuire*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 58, Rn. 33.

768 Hierzu *Zech*, in: Gless/Seelmann (Hg.), Intelligente Agenten und das Recht, S. 163 (192).

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

rung ggf. von einem Update abhängig zu machen.[769] In diesem Zusammenhang sind auch besondere Anforderungen bei der Programmierung des Lernalgorithmus zu berücksichtigen. Ein Selbstlernen darf nur innerhalb gesteckter Grenzen stattfinden und muss verhindern, dass aus vorhersehbarem Fehlgebrauch der Nutzer fehlerhafte Rückschlüsse gezogen werden und das System unerwünschte Entscheidungsregeln lernt.[770] In diesem Zusammenhang sieht auch Art. 7 Abs. 2 lit. c ProdHaftRL vor, dass bei der Beurteilung der Fehlerhaftigkeit eines Produkts die Auswirkungen einer etwaigen Fähigkeit des Produkts, nach Einsatzbeginn weiter zu lernen, zu berücksichtigen ist. KI-Systeme, die auch in der Nutzungsphase noch lernen, sind folglich derart zu konzipieren, dass ein gefährliches Verhalten verhindert wird (vgl. Erwägungsgrund (32) ProdHaftRL). Das Dazulernen wird indes gem. Art. 43 Abs. 4 UAbs. 2 KI-VO grundsätzlich nicht als wesentliche Änderung des KI-Systems angesehen, mit der Folge, dass ein neues Konformitätsbewertungsverfahren nicht erforderlich ist.

bb) Fehlerhaftigkeit bei Inverkehrgabe

Entwickeln autonome Systeme schädigende Verhaltensweisen erst nach deren Inverkehrbringen ist schon fraglich, ob überhaupt von einer Fehlerhaftigkeit bei Inverkehrgabe gesprochen werden kann oder der Haftungsausschluss des § 1 Abs. 2 Nr. 2 ProdHaftG greift.[771] So ergibt sich bei Systemen, deren Lernprozess sich auf die Trainingsphase beschränkt, zwar die konkret zur Rechtsgutsverletzung führende Entscheidung erst anhand der Eingabeparameter aus der Praxissituation und damit nach Inverkehrgabe, allerdings sind die entsprechenden Entscheidungsregeln schon vor dem Inverkehrbringen im Training entwickelt gewesen.[772] Die Entscheidung würde damit in einer Simulation in der Testphase bei gleichen Eingabepa-

769 Hierzu *Zech*, in: Gless/Seelmann (Hg.), Intelligente Agenten und das Recht, S. 163 (193).

770 *Eichelberger*, in: Ebers et al., (Hg.), Künstliche Intelligenz und Robotik, S. 182 nennt als Beispiel einen lernfähigen Autopiloten, der aggressives und gefährdendes Fahrverhalten lernt; *Reusch*, in: Kaulartz/Braegelmann (Hg.), Artificial Intelligence und Machine Learning, S. 89 f. spricht weitergehend von in einem „Supercode" verankerten absoluten Regeln, gegen die die KI niemals verstoßen darf; vgl. auch *Zech*, DJT 2020 Gutachten, A S. 35.

771 Diese Frage auch aufwerfend *Riehm/Meier*, in: Fischer/Hoppen/Wimmers, DGRI Jahrbuch 2018, S. 1 (Rn. 21).

772 *Seehafer/Kohler*, EuZW 2020, 213 (215).

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

rametern identisch ausfallen. Damit ist die autonome Fehlentscheidung aber bereits bei Inverkehrgabe angelegt.[773] Insofern hat sich das System gerade funktionsadäquat weiterentwickelt.[774] Ähnlich verhält es sich auch bei autonomen Systemen, die nicht in ihrem Zustand bei Inverkehrgabe verharren, sondern sich anhand der Interaktion mit ihrer Umgebung weiterentwickeln und auch in der Nutzungsphase lernen. Hier besteht die Bestimmung des Produkts bereits ab dem Inverkehrbringen darin, sich zu verändern, sodass auch hier die Veränderung bereits bei Inverkergabe im Produkt angelegt ist.[775]

Hat der Hersteller demnach konstruktiv nicht alle erforderlichen und zumutbaren Sicherungsmaßnahmen getroffen, liegt hierin bereits die Pflichtverletzung und der Konstruktionsfehler, der dann aber schon bei Inverkehrgabe bestand und lediglich später bei der konkreten Fehlentscheidung zu Tage tritt.[776] Nach Art. 7 Abs. 2 lit. c ProdHaftRL sind bei der Bestimmung der berechtigten Sicherheitserwartung eines Produkts auch die Auswirkungen einer etwaigen Fähigkeit, nach Einsatzbeginn weiter zu lernen, zu berücksichtigen. Dadurch wird klargestellt, dass die zugrundeliegenden Algorithmen so zu konzipieren sind, dass ein gefährliches Produktverhalten verhindert wird und auch durch selbstlernende Eigenschaften ausgelöste Effekte einen Produktfehler begründen können.[777] Daneben stellt auch Art. 7 Abs. 2 lit. e ProdHaftRL für die Bestimmung der berechtigten Sicherheitserwartungen und damit für die Fehlerhaftigkeit eines Produkts über den Zeitpunkt des Inverkehrbringens hinaus auf den gesamten Zeitraum ab, in dem das Produkt unter der Kontrolle des Herstellers steht. Da der Hersteller jedenfalls von Hochrisiko-KI-Systemen gem. Art. 72 KI-VO verpflichtet ist, diese nach dem Inverkehrbringen weiterhin zu überwachen,

773 Ähnlich auch *Pieper*, DSRITB 2016, 971 (983).

774 So *Taeger*, in: NK-ProdR, § 3 ProdHaftG, Rn. 53; *Reusch*, in: Kaulartz/Braegelmann (Hg.), Artificial Intelligence und Machine Learning, S. 85.

775 So *Taeger*, in: NK-ProdR, § 3 ProdHaftG, Rn. 53; *Essers*, Haftungsfragen automatisierter Systeme, S. 273 f.

776 *Reusch*, in: Kaulartz/Braegelmann (Hg.), Artificial Intelligence und Machine Learning, S. 85; *Leupold/Wiesner*, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 9.6.4, Rn. 62; vgl. auch *Rosenberger*, Die außervertragliche Haftung für automatisierte Fahrzeuge, S. 391; *Hey*, Die außervertragliche Haftung des Herstellers autonomer Fahrzeuge, S. 130.

777 Vgl. Erwägungsgrund (32) ProdHaftRL; *Krüger/Wagner*, ZfPC 2023, 124 (126).

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

stehen diese unter seiner Kontrolle. Der Hersteller ist daher gehalten, kontinuierlich für die Verkehrssicherheit des KI-Systems zu sorgen.[778]

cc) Entwicklungsfehler

Allerdings stellt sich bei diesen konstruktionsfehlerbehafteten Produkten die Frage, ob der Hersteller sich hinsichtlich des Autonomierisikos auf einen haftungsbefreienden Entwicklungsfehler berufen kann. Da die Weiterentwicklung und die Entscheidung des autonomen Systems in einer konkreten Gefahrensituation für den Hersteller nicht vorhersehbar sind, könnte angenommen werden, dass die entsprechende Fehlerhaftigkeit für ihn bei Inverkehrgabe auch nicht erkennbar war.[779] Allerdings kommt es wiederum auf die Erkennbarkeit des zu Grunde liegenden allgemeinen, mit der gewählten Konzeption verbundenen Fehlerrisikos an.[780] Insofern lässt sich anführen, dass für den Hersteller zwar die konkrete autonome Entscheidung des Systems und damit ein konkreter Schadensverlauf nicht vorhersehbar ist, das allgemeine Autonomierisiko – die Tatsache, dass autonome System immer mal wieder Fehlentscheidungen treffen – aber sehr wohl erkennbar ist.[781] Es lässt sich beim Autonomierisiko im Hinblick auf mögliche Haftungsfälle von einem quasi systemischen und eben nicht vermeidbaren Risiko sprechen.[782] Ähnlich wie bei der allgemeinen Fehleranfälligkeit bei der Programmierung sollte beim Hersteller aber zumindest eine bestimmte Vorstellung vom möglichen Fehler vorliegen und die abstrakte Vorstellung der Unvorhersehbarkeit selbstlernender Systeme für den

778 *Spindler*, CR 2022, 689 (693); *Krüger/Wagner*, ZfPC 2023, 124 (127); *McGuire*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 59, Rn. 34; vgl. auch Erwägungsgrund (32) ProdHaftRL.

779 So *Droste*, MPR 2018, 109 (111); *Schaub*, JZ 2017, 342 (343); wohl auch *Riehm/Meier*, in: Fischer/Hoppen/Wimmers, DGRI Jahrbuch 2018, S. 1 (Rn. 21) „gravierende Einschränkung der Herstellerhaftung" und *Spindler*, CR 2022, 689 (693); differenzierend *Leupold/Wiesner*, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 9.6.4, Rn. 64.

780 BGH, NJW 2009, 2952 (2955).

781 *Wagner,* in: MüKo, BGB, § 1 ProdHaftG, Rn. 61; *McGuire*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 58, Rn. 48; *Rosenberger*, Die außervertragliche Haftung für automatisierte Fahrzeuge, S. 394; *Hey*, Die außervertragliche Haftung des Herstellers autonomer Fahrzeuge, S. 65; *Thöne*, Autonome Systeme, S. 208 f.; *Zech*, in: Gless/Seelmann (Hg.), Intelligente Agenten und das Recht, S. 163 (192); *Wagner*, AcP 217 (2017), 707 (750).

782 So *Graf v. Westphalen*, ZIP 2019, 889 (892).

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

Ausschluss eines Entwicklungsfehlers nicht schon genügen.[783] Indes stellt sich die Vorstellung des Herstellers hinsichtlich des Autonomierisikos als deutlich konkreter dar als hinsichtlich der allgemeinen Fehleranfälligkeit bei der Softwareprogrammierung. Denn die Fehlentscheidung des autonomen Systems wird regelmäßig Folge der anfänglichen Unvollständigkeit der Trainingsdaten sein. Damit ergibt sich aber ein hinter dem Autonomierisiko stehendes konkretes Fehlerbild und nicht lediglich ein abstrakter Gefahrenverdacht. Hinzu kommt, dass die Ungewissheit gerade dem Produktkonzept immanent ist.[784] Es handelt sich um ein beabsichtigtes Verhalten, wenn sich das autonome System anhand der Trainingsdaten eigene Entscheidungsregeln gibt, um unterschiedlichste und vorher nicht feststehende Einsatzsituationen eigenständig bewältigen zu können.[785] Hinsichtlich des so verstandenen Autonomierisikos reicht die unzutreffende Annahme des Herstellers, mit tatsächlich unzureichenden Sicherungsmaßnahmen die Gefahr auf ein vertretbares Maß gebracht zu haben, nicht aus, um einen Entwicklungsfehler anzunehmen.[786] Anderes kann dies sein, wenn bisher unbekannte Aspekte des Autonomierisikos zu einer Gefährdung führen.[787]

783 *Leupold/Wiesner*, in: *Leupold/Wiebe/Glossner* (Hg.), IT-Recht, Teil 9.6.4, Rn. 64; ähnlich wohl auch *Dötsch*, Außervertragliche Haftung für KI, S. 226; *Sommer*, Haftung für autonome Systeme, S. 260 f. will dagegen darauf abstellen, ob der Schaden infolge der Risikoverwirklichung noch nicht einmal zumutbar zu versichern war, dagegen aber *Dötsch*, Außervertragliche Haftung für KI, S. 224 f.

784 So *Thöne*, Autonome Systeme, S. 207; ähnlich *Mayrhofer,* Außervertragliche Haftung für fremde Autonomie, S. 312.

785 In diese Richtung *Haagen*, Verantwortung für Künstliche Intelligenz, S. 320.

786 Vgl. *Mayrhofer,* Außervertragliche Haftung für fremde Autonomie, S. 312; allgemein BGH, NJW 2009, 2952 (2956); anders *Dötsch*, Außervertragliche Haftung für KI, S. 226, wenn sie einen Entwicklungsfehler dann für möglich hält, „wenn überhaupt keine Anhaltspunkte vorhanden waren, dass ein späteres Verhalten zu einer bestimmten, aber noch immer verallgemeinerungsfähigen Gefährdungslage" führt. Dies könne etwa dann sein, „wenn sich in allen Testverfahren überhaupt kein Ansatzpunkt gezeigt hat und es dann später im praktischen Einsatz […] zu einer – im damaligen Zeitpunkt – nicht absehbaren Fehlentscheidung kommt".

787 Ähnlich differenzierend wie hier wohl auch *Steege*, in: Buck-Heeb/Oppermann (Hg.), Automatisierte Systeme, S. 367 (390) und *Haftenberger*, Die Produkthaftung für künstlich intelligente Medizinprodukte, S. 253; vgl. auch *Mayrhofer,* Außervertragliche Haftung für fremde Autonomie, S. 312 f.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

dd) Entwicklungslücke

Allerdings ist es auch bei der Einhaltung der Sorgfaltsstandards nach dem gegenwärtigen Stand von Wissenschaft und Technik nicht möglich, eine vollständige Kontrolle über die Lernfähigkeit zu erreichen und sämtliche Entscheidungen vorherzusehen. Denn auch bei einem nach dem Stand von Wissenschaft und Technik programmierten Lernalgorithmus und entsprechend durchgeführten Tests und Verifikationen kann aufgrund der im Training eingesetzten limitierten Datenmenge nicht jede Praxissituation im Vorfeld abgebildet werden und es daher zu Fehlinterpretationen durch das System kommen, die sich dem Einfluss des Herstellers entziehen.[788] Folglich können autonome Systeme in unvorhergesehenen Situationen versagen, ohne dabei gegen den Stand der Wissenschaft und Technik zu verstoßen.[789]

(1) Keine Haftung für das Autonomierisiko nach § 823 Abs. 1 BGB

Letztlich betreffen allein diese Fälle das Autonomierisiko, da lediglich hier der Schaden nicht auf eine Sorgfaltspflichtverletzung eines Menschen zurückzuführen ist, das autonome System also nicht schon unzureichend programmiert, trainiert, überwacht oder falsch genutzt wurde.[790] Während bei einem solchen Sorgfaltspflichtenverstoß bereits ein Konstruktionsfehler vorliegt,[791] ist auch vor dem Hintergrund, dass die bloße Inverkehrgabe von autonomen Systemen noch keine Pflichtwidrigkeit des Herstellers begründet, fraglich, wie das Autonomierisiko als unvorhersehbares Restrisiko

788 *Kirn/Müller-Hengstenberg*, MMR 2014, 225 (232); mit anschaulichem Beispiel *Hey*, Die außervertragliche Haftung des Herstellers autonomer Fahrzeuge, S. 65 f.; dies verkennend *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 111 f.

789 Prägnant *Grützmacher*, CR 2016, 695 (696); ähnlich *Riehm/Meier*, in: Fischer/Hoppen/Wimmers, DGRI Jahrbuch 2018, S. 1 (Rn. 21).

790 *Burchardi*, EuZW 2022, 685 (685); *Ebert* et al., ZfPC 2023, 16 (19); *Sommer*, Haftung für autonome Systeme, S. 86 ff. spricht von einem inhärenten und besonderen Autonomierisiko; *Hinze*, Haftungsrisiken des automatisierten und autonomen Fahrens, S. 139 unterscheidet zwischen ruhendem und tatsächlichem Produktfehler.

791 *Wendt/Oberländer*, InTeR 2016, 58 (61); *Wende*, in: Sassenberg/Faber (Hg.), Industrie 4.0 und Internet of Things, § 4, Rn. 109; *Burrer*, in: Bräutigam/Kraul (Hg.), Internet of Things, § 8, Rn. 94.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

bei der Entscheidungsfindung haftungsrechtlich einzuordnen ist.[792] Beim Autonomierisiko sind trotz der Einhaltung aller erforderlichen und zumutbaren Sicherungsvorkehrungen Restgefahren zwar erkennbar, aber nach dem derzeitigen Stand technisch nicht vermeidbar, sodass eine Entwicklungslücke vorliegt.[793] Die Frage nach der Pflichtwidrigkeit des Herstellers bei der Inverkehrgabe des autonomen Systems hängt damit von einer Risiko-Nutzen-Abwägung ab (vgl. für Hochrisiko-KI-Systeme Art. 9 Abs. 5 KI-VO).[794] Werden die verbleibenden Restrisiken angesichts der mit der Nutzung des autonomen Systems verbundenen (Sicherheits-)Vorteile in Kauf genommen und instruiert[795] der Hersteller daneben ordnungsgemäß über die Restrisiken (vgl. für Hochrisiko-KI-Systeme Art. 13 Abs. 2, Abs. 3 lit. b KI-VO), ist ihm keine Pflichtwidrigkeit vorzuwerfen und muss eine Haftung nach § 823 Abs. 1 BGB entfallen.

(2) Mögliche Haftung für das Autonomierisiko nach dem ProdHaftG

Mit der Feststellung, dass den Hersteller in diesem Fall keine Pflichtwidrigkeit trifft, ist aber noch keine Entscheidung darüber gefallen, ob ihn nicht eine Haftung nach dem ProdHaftG trifft. Maßgeblich für das Vorliegen eines Fehlers sind nach § 3 Abs. 1 ProdHaftG die berechtigten Verkehrserwartungen. Diese bestimmen sich zwar grundsätzlich nach den für die objektiven Sorgfaltsanforderungen im Rahmen des § 823 Abs. 1 BGB maßgeblichen Kriterien der Erforderlichkeit und Zumutbarkeit von Sicherheitsvorkehrungen. Gleichwohl könnte bei erkennbaren, aber nach

792 *V. Bodungen*, in: Chibanguza/Kuß/Steege (Hg.), Künstliche Intelligenz, § 3, I., Rn. 27 spricht davon, dass es in diesen Fällen zum „produkthaftungsrechtlichen Schwur" kommt.

793 So auch *McGuire*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 58, Rn. 48; *Hey*, Die außervertragliche Haftung des Herstellers autonomer Fahrzeuge, S. 65; *Sosnitza*, CR 2016, 764 (769 f.); *Thöne*, Autonome Systeme, S. 209; *Rosenberger*, Die außervertragliche Haftung für automatisierte Fahrzeuge, S. 393; *Etzkorn*, MMR 2020, 360 (361); *Dötsch*, Außervertragliche Haftung für KI, S. 227 f.; wohl auch *Wagner*, AcP 217 (2017), 707 (729).

794 *Eichelberger*, in: Ebers et al., (Hg.), Künstliche Intelligenz und Robotik, S. 183; *McGuire*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 58, Rn. 48; *v. Bodungen*, in: Chibanguza/Kuß/Steege (Hg.), Künstliche Intelligenz, § 3, I., Rn. 27.

795 Nach *Lohmann*, AJP/PJA 2017, 152 (158) hat der Hersteller ein „besonderes Augenmerk auf eine sorgfältige Instruktion des Nutzers [zu] legen"; ebenso *Wendt/Oberländer*, InTeR 2016, 58 (62).

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

den technischen Möglichkeiten im Zeitpunkt des Inverkehrbringens nicht vermeidbaren Gefahren, die berechtigte Verkehrserwartung dahin gehen, keine Beeinträchtigungen durch das Produkt zu erleiden. Dann mag zwar die Inverkehrgabe insgesamt aufgrund einer Risiko-Nutzen-Abwägung hingenommen werden, nicht aber der Eintritt der konkreten Rechtsgutsverletzung. Obwohl das Produkt dem Stand von Wissenschaft und Technik entsprach und sein Inverkehrbringen zulässig war, dem Hersteller also keine Pflichtverletzung vorgeworfen werden kann, könnte das Produkt dann fehlerhaft i.S.d. ProdHaftG sein.

In diese Richtung geht die Rechtsprechung zu Naturprodukten. So weist ein Kirschgebäck keinen Produktfehler auf, nur weil sich darin noch ein Kirschkern befindet.[796] Bei Naturprodukten muss mit solchen Abweichungen gerechnet werden, jedenfalls wenn der Hersteller im Verarbeitungsprozess alle erforderlichen und zumutbaren Sicherheitsmaßnahmen zur Vermeidung von vor dem Naturprodukt ausgehenden Gesundheitsgefahren getroffen hat.[797] Diese Erwartungshaltung lässt sich damit begründen, dass die Eigenart des Naturprodukts darüber hinaus nicht vom Hersteller beeinflusst werden kann.[798] Dagegen besteht eine Erwartungshaltung, dass es in einem einwandfreien hygienischen Zustand hergestellt wurde.[799] So liegt auch dann ein Produktfehler, wenn der Hersteller eines Schmandkuchens alle erforderlichen und zumutbaren Sicherheitsvorkehrungen getroffen hat, eine infektiöse Gelbsucht des Kochs gleichwohl die Speise infiziert hat.[800] Der Schutzzweck des ProdHaftG geht gerade dahin, Verbraucher gegen Produktfehler zu schützen, die sich in der Sphäre des Produktherstellers realisieren, ohne dass es auf ein Verschulden des Herstellers ankommt.[801]

Auch bei autonomen Systemen geht ein Fehlverhalten, wie gerade dargestellt, auf die Sphäre des Herstellers zurück. Zwar entspricht es der Eigenart eines autonomen Systems, nicht vordefinierte Entscheidungen zu treffen. Diese Eigenart ist aber bei Inverkehrgabe vom Hersteller angelegt und durch Programmierung und Training beeinflusst worden. Um den Dispens zwischen grundsätzlich zulässigem Inverkehrbringen und einer im Einzelfall nicht hinnehmbaren und damit nicht von der berechtigten Sicherheitserwartung gedeckten Rechtsgutsverletzung möglichst gering zu

796 BGH, NJW 2009, 1669 (1670).
797 BGH, NJW 2009, 1669 (1670); OLG Köln, NJW 2006, 2272 (2272).
798 OLG Köln, NJW 2006, 2272 (2272).
799 OLG Köln, NJW 2006, 2272 (2272).
800 OLG Frankfurt a.M., NJW 1995, 2498 (Ls.).
801 OLG Köln, NJW 2006, 2272 (2272); OLG Frankfurt a.M., NJW 1995, 2498 (2499).

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

halten, bedarf es jedoch einschränkender Kriterien. Denn eine absolute Sicherheit ist auch nach dem ProdHaftG nicht geschuldet. Die Einhaltung objektiver Verhaltensregeln dürfte aber in jedem Fall eine berechtigte Sicherheitserwartung darstellen.[802] Dieses Ergebnis ergibt sich in Bezug auf geschädigte Dritte auch aus der Abgrenzung der Verantwortungssphären. Während der instruierte Nutzer das verbleibende Restrisiko mit seiner Erwerbsentscheidung in Kauf nimmt, ist der Rechtsverkehr nur durch die Risiko-Nutzen-Abwägung bei Inverkehrgabe geschützt. Diese bildet gerade bei autonomen Systemen aber nicht stets die berechtigte Sicherheitserwartung im Einzelfall ab. Über das ProdHaftG lässt sich damit das Autonomierisiko im Falle eines Verstoßes gegen objektive Verhaltensregeln beim Hersteller allozieren.[803] Dieses Verständnis wird künftig dadurch verstärkt, dass nach Art. 7 Abs. 2 lit. c ProdHaftRL die Lernfähigkeit explizit bei der Bewertung der Fehlerhaftigkeit eines Produkts zu berücksichtigen ist. Insoweit stellt Erwägungsgrund (32) ProdHaftRL klar, dass ein Hersteller, der ein Produkt entwickelt, das die Fähigkeit aufweist, unerwartetes Verhalten zu entwickeln, auch weiterhin für ein Verhalten haften, das einen Schaden verursacht. Auch wenn diese Formulierung eine vollständige Zuweisung des Autonomierisikos an den Hersteller nahelegt,[804] kann dies bei Einhaltung des Standes von Wissenschaft und Technik doch nur im Rahmen der berechtigten Verkehrserwartung erfolgen. Daneben sei darauf hingewiesen, dass nach Art. 10 Abs. 2 lit. c ProdHaftRL künftig ein Fehler vermutet wird, wenn nachgewiesen ist, dass der Schaden durch eine offensichtliche Funktionsstörung des Produkts bei vernünftigerweise vorhersehbarer Verwendung oder unter normalen Umständen verursacht wurde. Verhält sich das Produkt folglich anders als es von der Steuerungssoftware vorgesehen worden sein kann, weil es etwa gegen objektive Verhaltensregeln verstößt, wird der Produktfehler vermutet.[805]

802 Dahin auch der Diskussionsbeitrag von *Riehm*, DJT 2022 Diskussion, K S. 109, wonach ein Produktfehler auch dann vorliegen müsse, wenn das Überfahren einer roten Ampel nach dem Stand von Wissenschaft und Technik nicht vermeidbar war. Insoweit müsse sich ein Produkt, das auf den Markt kommt, an die objektiven Verkehrsregeln halten, die für alle gelten.

803 Ohne Einschränkung hinsichtlich eines Verstoßes gegen objektive Sorgfaltsanforderungen *McGuire*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 58, Rn. 56; für einen Gleichlauf von nationaler Produzentenhaftung und ProdHaftG dagegen *Hey*, Die außervertragliche Haftung des Herstellers autonomer Fahrzeuge, S. 124 und *Dötsch*, Außervertragliche Haftung für KI, S. 282 f.

804 In diese Richtung *Piovano/Hess*, Das neue europäische Produkthaftungsrecht, S. 88.

805 Vgl. dazu *Wagner*, JZ 2023, 1 (9).

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

e) Bedeutung für die Produktbeobachtung

Hat der Hersteller alle erforderlichen und zumutbaren Sicherungsmaßnahmen getroffen und ergibt eine Risiko-Nutzen-Abwägung ein vertretbares Restrisiko, geht das Autonomierisiko nach nationaler Produzentenhaftung zu Lasten des Nutzers. Gleiches gilt nach hier vertretener Ansicht im Rahmen des ProdHaftG außerhalb des Verstoßes gegen objektive Verhaltensregeln. Da es sich in dieser Konstellation um eine Entwicklungslücke handelt, unterliegt das Autonomierisiko nach der hier vertretenen Auffassung der Produktbeobachtungspflicht des Herstellers. Folglich wird der Hersteller über die Produktbeobachtungspflicht auch für das Autonomierisiko in Verantwortung genommen.[806] Vor diesem Hintergrund wird in der juristischen Literatur der Produktbeobachtungspflicht auch bei autonomen Systemen eine besondere Bedeutung zugeschrieben.[807] Daher verwundert es nicht, dass die Produktbeobachtung einen ausführlich geregelten Bestandteil der KI-VO darstellt.[808] Schon mit der Definition in Art. 3 Nr. 25 KI-VO, wonach unter einem System zur Beobachtung nach dem Inverkehrbringen alle Tätigkeiten zu verstehen sind, die Anbieter von KI-Systemen zur Sammlung und Überprüfung von Erfahrungen mit der Verwendung der von ihnen in Verkehr gebrachten KI-Systeme durchführen, um festzustellen, ob unverzüglich nötige Korrektur- oder Präventivmaßnahmen zu ergreifen sind, wird an das im Rahmen von § 823 Abs. 1 BGB entwickelte Verständnis angeknüpft. Nach Art. 16 lit. c, Art. 17 Abs. 1 lit. h, Art. 72 KI-VO ist ein System zur Beobachtung nach dem Inverkehrbringen einzurichten. Die mangelnde Vorhersehbarkeit des Verhaltens bzw. der Entscheidungen autonomer Systeme kann der Hersteller ein Stück weit dadurch kompensieren, dass er seiner Produktbeobachtungspflicht nachkommt und überprüft, wie die Systeme im Betrieb funktionieren.[809] Hinsichtlich des Pflichtenumfangs hat die Beobachtung daher umso engmaschiger auszufallen, je höher der Grad der Autonomie und Veränderbarkeit des Systems

806 Explizit auch *Hinze*, Haftungsrisiken des automatisierten und autonomen Fahrens, S. 139.

807 So *Zech*, in: Gless/Seelmann (Hg.), Intelligente Agenten und das Recht, S. 163 (194); *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 92; *Spindler*, in: Hornung/Schallbruch (Hg.), IT-Sicherheitsrecht, § 11, Rn. 31; *Stiemerling*, in: Kaulartz/Braegelmann (Hg.), Artificial Intelligence und Machine Learning, S. 25.

808 *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 158.

809 *Haagen*, Verantwortung für Künstliche Intelligenz, S. 274 f.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

sind.[810] Insoweit kann die Produktbeobachtungspflicht auch ein gewisses Korrektiv für das Black-Box-Problem sein, indem versucht wird, die in der Praxis getroffenen Entscheidungen nachzuvollziehen (vgl. dazu Art. 12 KI-VO).[811] Bei Systemen, die auch nach der Inverkehrgabe noch lernen und sich weiterentwickeln, dürfte der Produktbeobachtungspflicht gar eine Schlüsselrolle zukommen (vgl. Erwägungsgrund (155) KI-VO).[812] Eine besonders intensive Produktbeobachtung könnte hier gerade ein Inverkehrbringen erlauben, ohne dass der Lernfortschritt vorher zu verifizieren und per Update aufzuspielen ist.[813]

IV. Fazit zur Produktbeobachtungspflicht bei smarten Produkten

Ziel dieses Kapitels war es zu untersuchen, ob die von smarten Produkten ausgehenden Unsicherheiten an die Produktbeobachtungspflicht adressiert werden können. Dabei hat sich gezeigt, dass die Produktbeobachtungspflicht zu keiner uferlosen Einstandspflicht des Herstellers für sämtliche Unsicherheiten smarter Produkte nach Inverkehrgabe führt, sondern eine gerechte Risikozuweisung zwischen Hersteller und Nutzer vornimmt. Maßgeblich für die haftungsrechtliche Zuordnung dieser Risiken nach der Inverkehrgabe ist dabei, ob sie sich auf die Sphäre des Herstellers zurückführen lassen. Da in der Vergangenheit der Softwareentwicklung Sicherheitsstandards vernachlässigt wurden, dürfte sich eine hohe Dunkelziffer produkthaftungsrechtlich fehlerhafter smarter Produkte im Verkehr befinden, hinsichtlich derer Reaktionsmaßnahmen im Rahmen der Produktbeobachtungspflicht angezeigt sind. Hinzu kommt, dass aufgrund der Schnelllebigkeit der Softwareentwicklung mit der stetigen Schließung von Entwicklungslücken und -fehlern zu rechnen ist, die wiederum Reaktionsmaßnahmen nach sich ziehen. Keine Verantwortung trifft den Hersteller allerdings, wenn im Zuge dieser Schnelllebigkeit lediglich aufgrund der Alterung seines Produkts Sicherheitsgefahren erwachsen. Hinsichtlich der Vernetzung ist die Produktbeobachtungspflicht des Herstellers keinesfalls unüberschaubar, sondern knüpft stets an seine Verantwortungssphäre an.

---

810 *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 93.

811 Hierzu *Oechsler*, NJW 2022, 2713 (2715); *McGuire*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 58, Rn. 39.

812 Ähnlich *Chibanguza*, in: Chibanguza/Kuß/Steege (Hg.), Künstliche Intelligenz, § 5, K., Rn. 28.

813 Dazu unter D.IV.3.e).

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

Im Rahmen des Autonomierisikos kann die Produktbeobachtungspflicht ein gewisses Korrektiv für Entwicklungslücken bedeuten.

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -

https://doi.org/10.5771/9783748964490-69 - am 03.12.2025, 20:22:49. https://www.inlibra.com/de/agb - Open Access -