A. Problemstellung und Gang der Untersuchung

I. Smarte Produkte – smarte Gefahren

Im digitalen Zeitalter wird die Welt ein Stückchen smarter. Doch wird sie dadurch auch gefährlicher?

> ***Hacker steuern Jeep Cherokee fern***
> *Durch eine Schwachstelle im Infotainmentsystem konnten Sicherheitsforscher die Kontrolle über einen Jeep übernehmen – über das Internet. […] Ein erstes Update schafft Abhilfe.*[1]

> ***Rückruf: Intel ruft Basis Peak Smartwatch zurück – Dienste werden eingestellt***
> *[…] Als Grund wird eine mögliche Überhitzung bei Basis Peak Uhren (Schlaf- und Fitnesstracker) genannt. Kunden [erlitten] in einigen Fällen leichte Schmerzen, Blasenbildung oder Verbrennungen […]. In einer ersten Mitteilung vom Juni 2016 war noch davon die Rede, dass versucht werde, den Fehler durch ein Softwareupdate zu beheben. Dies ist scheinbar nicht gelungen. Endkunden können nach Unternehmensangaben noch bis zum 31. Dezember 2016 auf Ihre Daten zugreifen. Nach diesem Datum werden alle Basis-Peak-Dienste eingestellt.*[2]

> ***Galaxy Note 7 wird per Update endgültig lahmgelegt***
> *Wer sich trotz der Brandgefahr nicht von seinem Galaxy Note 7 trennen kann, darf das nächste Update nicht installieren: Samsung will in weiteren Teilen der Welt die Ladefunktion des Akkus vollständig deaktivieren.*[3]

1 https://www.heise.de/security/meldung/Hacker-steuern-Jeep-Cherokee-fern-2756331.html (Hervorhebung durch Verf.; zuletzt abgerufen am 23.09.2024).

2 https://www.produktwarnung.eu/2016/08/04/basis-informiert-zu-einer-moeglicher-ueberhitzung-bei-basis-peak-uhren/2923 (Hervorhebung durch Verf.; zuletzt abgerufen am 23.09.2024).

3 https://www.golem.de/news/samsung-galaxy-note-7-wird-per-update-endgueltig-lahmgelegt-1703-126934.html (Hervorhebung durch Verf.; zuletzt abgerufen am 23.09.2024).

Tesla beschränkt autonome Fahrfunktionen
TESLA-FAHRER TRIEBEN ZU VIEL UNSINN
[…] Aus Sicherheitsgründen hat Tesla per Update die Autopilot-Funktionen beschränkt.[4]

Den einleitenden Schlagzeilen ist gemein, dass die dort beschriebenen Produktgefahren, nicht von herkömmlichen „analogen", sondern von Produkten des digitalen Zeitalters ausgehen. Bei diesen Produkten handelt es sich um körperliche Gegenstände, deren Funktionsweise des Einsatzes von Software oder zumindest von Daten erfordert und die je nach ihrer technischen Ausgestaltung mehr oder weniger smart, vernetzt, robotisch, oder künstlich intelligent sind.[5] Als Oberbegriff sollen sie nachfolgend als „smarte Produkte" bezeichnet werden.

Ihr Versprechen geht dahin, den Alltag der Menschen zu erleichtern. Tatsächlich sind sie schon heute täglicher Begleiter in vielen Lebenslagen. So führen wir mit unseren Smartphones eine innige Beziehung und widmen ihnen regelmäßig unseren ersten und letzten Blick des Tages. Ähnliches gilt für unsere Smartwatches. Während abends die am Tag erreichte Schrittzahl und das erzielte Fitness-Level ausgewertet werden, lassen wir uns morgens die Schlafqualität der Nacht anzeigen. Wir erleben gerade, wie Science-Fiction Realität wird. Erscheinungen, welche vor nicht allzu langer Zeit der Fantasiewelt angehörten, sind längst keine Zukunftsmusik mehr, sondern durchdringen allmählich unseren Alltag. Prominentes Beispiel dafür ist das autonome Fahren. Hierfür sind die technischen Voraussetzungen bereits geschaffen, Testphasen laufen und im Alltag stellt sich ein teilautomatisiertes Fahren ein, bei dem der Fahrer zwar noch hinter dem Steuer sitzt, Assistenzsysteme aber die Spur und den Abstand zum Vordermann halten.[6] Ähnlich verhält es sich mit dem Smart-Home. Hier übernimmt idealerweise nicht nur der Saugroboter die lästige und zeitaufwendige Putzarbeit, sondern die Heizung passt sich automatisch der Außentemperatur und den Bedürfnissen der Bewohner an und spart damit Energiekosten. Während der Backofen schon mal von unterwegs per App vorgeheizt wird, bestellt der Kühlschrank die für die Zubereitung des Essens aufgewendeten Zutaten

4 https://www.motor-talk.de/news/tesla-fahrer-trieben-zu-viel-unsinn-t5553246.html (Hervorhebung durch Verf.; zuletzt abgerufen am 23.09.2024).
5 Vgl. auch *Schrader*, JA 2022, 1 (1).
6 Ein Überblick über die Stufen des selbst fahrenden Autos findet sich unter https://www.adac.de/rund-ums-fahrzeug/ausstattung-technik-zubehoer/autonomes-fahren/grundlagen/autonomes-fahren-5-stufen/ (zuletzt abgerufen am 23.09.2024).

eigenständig nach. Zugegebenermaßen verfügen aktuell noch die wenigsten Menschen über ein gänzlich vernetztes Haus, einige der vorgestellten Geräte sind allerding schon heute marktreif. Aber nicht nur der Alltag wird smarter. Vielmehr wirkt sich das digitale Zeitalter auf alle Lebensbereiche aus.[7] So wird unter dem schillernden Begriff der „Industrie 4.0" die Digitalisierung, Vernetzung und Automatisierung von Produktions- und Vertriebsprozessen entlang der gesamten Wertschöpfungskette hin zu Smart-Factories verstanden.[8]

Betrachtet man die zu Beginn aufgelisteten Meldungen, so wird deutlich, dass nicht nur die digitalen Produkte selbst, sondern auch die von ihnen ausgehenden Gefahren schon heute Realität sind. So sehr smarte Produkte das tägliche Leben einfacher und komfortabler machen und so vielfältig ihre Einsatzgebiete sind, so vielfältig sind auch die damit einhergehenden Risiken und Schadenszenarien. Denn Schadensfälle werden auch bei noch so smarten Produkten nicht ausbleiben. Es braucht daher wenig Fantasie, sich neben den eingangs genannten Produktgefahren Schlagzeilen wie *Rasenmähroboter killt preisgekrönte Rosen des Nachbarn – Hackerangriff oder Fehlfunktion?*[9] oder *Gesundheitsapp liefert Fehldiagnose – Arztbesuch kommt zu spät* vorzustellen. Dystopische Vorstellungen dagegen, wie sich Künstliche Intelligenz gegen den Menschen wendet und diesen kontrolliert, werden bewusst den Hollywood-Regisseuren überlassen. Denn Innovation und Angst sollen nicht gegeneinander ausgespielt werden.[10] Obgleich durch smarte Produkte neue Gefahren erwachsen,[11] so – und das zeigen obige Meldungen auch – entstehen andererseits neue technische Möglichkeiten, diesen schnell und effektiv zu begegnen. Im Zuge des technischen Fortschritts ist es daher ein natürlicher Prozess, dass sich nicht nur die Produkte weiterentwickeln, sondern auch die von ihnen ausgehenden Ge-

7 *Hornung/Hofmann*, in: Hornung (Hg.), Rechtsfragen der Industrie 4.0, S. 9 (9); *Beierle*, ZfPC 2022, 22 (22); eine Darstellung nach Branchen nehmen *Chibanguza/Kuß/Steege* (Hg.), Künstliche Intelligenz, 2. Teil und *Sassenberg/Faber* (Hg.), Industrie 4.0 und Internet of Things, Kap. 5 vor.

8 *Heuer-James/Chibanguza/Stücker*, BB 2018, 2818 (2819).

9 Frei nach *Rempe*, InTeR 2016, 17 (17).

10 Hierfür plädieren auch *Gondlach/Regneri*, in: Knappertsbusch/Gondlach (Hg.), Arbeitswelt und KI 2030, S. 3 (6 f.). Diese können schon keine größeren Ressentiments der Bevölkerung gegenüber KI erkennen, sondern eine Haltung „geprägt von Chancen, Bedrohungen und Widersprüchen".

11 So auch *Burrer*, in: Bräutigam/Kraul (Hg.), Internet of Things, § 8, Rn. 74.

fahren.[12] Die Produktlandschaft wird daher im digitalen Zeitalter nicht per se gefährlicher, sondern lediglich anders gefährlich.[13]

II. Unsicherheiten smarter Produkte nach der Inverkehrgabe

Technische Produktinnovationen gehen immer mit Unsicherheiten einher, da sich die Produkte nach dem Inverkehrbringen erst im Feld beweisen müssen und sich bisher unbekannte vom Produkt ausgehende Gefahren möglicherweise erst in der Praxis zeigen. Hier bilden smarte Produkte keine Ausnahme. Diese Unsicherheiten nach dem Inverkehrbringen verschärfen sich bei smarten Produkten aber. Zwar sind Komplexität und Vernetzung schon seit jeher charakterisierend für IT-Systeme und begründeten schon immer besondere haftungsrechtliche Probleme.[14] Insbesondere durch die Integration von Software in physische Produkte zeichnen sich aber Entwicklungen ab, welche diese Thematik in ein neues Licht rücken. Insoweit lässt sich vom „Aufrüsten bisher toter Produkte"[15] sprechen.

1. Integration von Software in physische Produkte

So enthalten Produkte heute fast durchgängig[16] Minicomputer oder kleine Rechner, die in dem Gesamtprodukt Regelungs-, Kontroll- und Kommunikationsaufgaben wahrnehmen (embedded systems). Dabei übernimmt eine entsprechend in das embedded system integrierte Software (embedded software) Steuerungs- und Überwachungsfunktionen und kann die unterschiedlichen Geräte über das Internet untereinander vernetzen, wodurch

12 Allgemein zum Risiko und Nutzen der Errungenschaften der modernen Zivilisation *Plagemann/Tietzsch*, „Stand der Wissenschaft" und „Stand der Technik", S. 5.

13 So wird ein autonomes Fahrzeug im Straßenverkehr zwar insgesamt weniger Unfälle verursachen als ein menschlicher Fahrer (Fahrfehler, Ablenkung, Müdigkeit etc.), aber die tatsächlich noch auftretenden Unfälle werden sich von denen unterscheiden, die ein (auch sorgfältiger) Mensch verursacht hätte, vgl. *Wagner*, AcP 217 (2017), 707 (736).

14 So *Voigt,* in: BeckOGK, BGB, § 823, Rn. 762.

15 *Klindt/Wende/Burrer*, in: Bräutigam/Klindt (Hg.), Digitalisierte Wirtschaft/Industrie 4.0, S. 100 (106).

16 So im Jahr 2013 bereits *Söbbing*, ITRB 2013, 162 (162); *Deusch/Eggendorfer*, DSRITB 2015, 833 (834).

das Internet der Dinge (Internet of Things, im Folgenden „IoT“)[17] und Smart-Homes mitgestaltet werden.[18] Können Systeme dann gleichzeitig mit der vernetzten digitalen Welt kommunizieren und mit der physischen Welt interagieren und in diese hineinwirken, spricht man von Cyber-physischen-Systemen (im Folgenden „CPS“).[19] Dadurch wird die herkömmliche Vernetzung der virtuellen Welt des Internets auf die physische Welt und ihre Gegenstände ausgedehnt.[20]

Die eben dargestellte Koppelung führt auch zu einer zunehmenden haftungsrechtlichen Relevanz.[21] Denn bisher führten Fehlfunktionen der Software oder Angriffe auf diese – etwa bei informationsverarbeitenden Systemen ohne physischen Produktbezug – regelmäßig nicht zu Schädigungen an Leib und Leben.[22] In diesem Zusammenhang waren Beeinträchtigungen des allgemeinen Persönlichkeitsrechts etwa durch die Autocomplete-Funktion von Suchmaschinen,[23] die Veränderung oder Löschung von Daten[24] oder nicht von § 823 Abs. 1 BGB geschützte Vermögensschäden denkbar.[25] Mit der beschriebenen Kopplung aber können Fehlfunktionen oder Manipulationen der Software unmittelbar mechanische Gefahren in der realen Welt auslösen und im Einflussbereich des Produkts zu physischen Schäden führen.[26] Zwar sind durch softwaregesteuerte Industrieanlagen verursachte

17 Vgl. *Dorn*, in: Hoeren/Pinelli (Hg.), Künstliche Intelligenz – Ethik und Recht, S. 17 (19 f.).

18 *Wiebe*, NJW 2019, 625 (625).

19 Vgl. *Fedler*, in: Ebers/Steinrötter (Hg.), Künstliche Intelligenz und smarte Robotik, S. 91 (94 f.).

20 *Zech*, DJT 2020 Gutachten, A S. 45 ff.

21 Anklingend bereits bei *Meier/Wehlau,* CR 1990, 95 (95).

22 *Redeker*, in: Redeker, IT-Recht, Rn. 898.

23 Vgl. BGH, NJW 2013, 2348.

24 Bei Speicherung auf einem Datenträger reflexiv über das Eigentum oder den berechtigten Besitz i.S.d. § 823 Abs. 1 BGB geschützt, vgl. *Wiesner*, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 10.6, Rn. 27; i.Ü. str. *Riehm*, VersR 2019, 714 (720 ff.) erkennt das Recht an Daten als sonstiges Recht i.S.d. § 823 Abs. 1 BGB an; zustimmend *Voigt*, in: BeckOGK, BGB, § 823, Rn. 187 ff. m.w.N. auch zur gegenteiligen Meinung.

25 *Schmid*, IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme, S. 27 spricht davon, dass die Gefahren nicht mehr auf die Informationssicherheit begrenzt sind, sondern nunmehr auch die Funktionssicherheit betreffen.

26 *Zech*, in: Gless/Seelemann (Hg.), Intelligente Agenten und das Recht, S. 163 (168) sowie *Zech*, DJT 2020 Gutachten, A S. 11, 29 ff.; *Fedler*, in: Ebers/Steinrötter (Hg.), Künstliche Intelligenz und smarte Robotik, S. 91 (103); *Ebert* et al., ZfPC 2023, 16 (16).

physische Schäden bereits bekannt.[27] Allerdings wird dies mit zunehmender Mobilität und Reichweite und der damit verbundenen Ausweitung der Einsatzgebiete und der zunehmenden Verbreitung smarter Produkte zu einem alltäglichen Phänomen.[28] Daher werden die zunehmende Teilnahme smarter Produkte am Alltag und die damit einhergehende gesteigerte Interaktion mit Menschen in quantitativer Hinsicht zu einer Steigerung der Eintrittswahrscheinlichkeit entsprechender Schädigungen führen.[29]

2. Komplexitäten bei Softwareprodukten

Moderne Software ist aber hochkomplex und deshalb fehleranfällig.[30] Zum einen kann sie nicht auf jedes potenzielle Einsatzszenario wirtschaftlich sinnvoll getestet werden.[31] Zum anderen ist Software von einer Vielzahl von Umweltvariablen abhängig, die sich im Laufe der Zeit verändern können.[32] So führt die Vernetzung mit anderen Systemen zu nicht vollumfänglich abschätzbaren Kombinationsrisiken und Fehlfunktionen ergeben sich aus dem Zusammenspiel der einzelnen Systeme.[33] Zudem werden IT-Sicherheitslücken regelmäßig erst im Laufe der Zeit bekannt und Bedrohungslagen ändern sich fortlaufend.[34] Darüber hinaus führt die Lernfähigkeit und Veränderlichkeit von Systemen dazu, dass sich auch der Sicherheitszustand ständig verändert.[35] Wie solche Systeme Entscheidungen treffen, ist ex ante nicht exakt vorhersehbar.[36]

---

27 *Voigt*, in: BeckOGK, BGB, § 823, Rn. 757.

28 *Schultz*, Verantwortlichkeit bei autonom agierenden Systemen, S. 75; *Zech,* DJT 2020 Gutachten, A S. 29; *Zech*, in: Gless/Seelemann (Hg.), Intelligente Agenten und das Recht, S. 163 (169); *Voigt*, in: BeckOGK, BGB, § 823, Rn. 757 spricht davon, dass die Risiken unvermittelter auftreten.

29 *Zech*, DJT 2020 Gutachten, A S. 29 f.; Diskussionsbeitrag von *Zech*, DJT 2020 Diskussion, K S. 81 „sicherlich kein neues Risiko […], aber es ist ein Risiko, das sich […] mehr verbreitet hat".

30 *Hoffmann*, Software-Qualität, S. 13; *Meier/Wehlau*, CR 1990, 95 (96); *Sohr/Kemmerich*, in: Kipker (Hg.), Cybersecurity, Kap. 3, Rn. 155; diese Erkenntnis hat auch Einzug in die juristische Literatur gefunden, vgl. *Raue* NJW 2017, 1841 (1841); *Oechsler*, in: Staudinger, BGB, § 3 ProdHaftG, Rn. 126 m.w.N.; *Wende*, in: Sassenberg/Faber (Hg.), Industrie 4.0 und Internet of Things, § 4, Rn. 68.

31 *Hoffmann*, Software-Qualität, 2. Aufl., 2013, S. 13, 22.

32 *Reusch*, BB 2019, 904 (907).

33 *Heckmann/Paschke*, in: Bräutigam/Kraul (Hg.), Internet of Things, § 10, Rn. 126.

34 *Raue*, NJW 2017, 1841 (1844); *Wende*, in: Sassenberg/Faber (Hg.), Industrie 4.0 und Internet of Things, § 4, Rn. 68.

Eine abschließend sichere Entwicklung „am Reißbrett" ist daher bei smarten Produkten kaum möglich.[37] Diese Ungewissheiten sind auch von Beginn an bekannt. Der Hersteller hat Kenntnis davon, dass seinen Produkten beim Inverkehrbringen eine latente Gefährlichkeit[38] anhaftet. Die Risiken können aber im Zeitpunkt des Inverkehrbringens mangels entsprechenden Wissens oder mangels technischer Möglichkeiten nicht vermieden werden. Sie sind den Produkten inhärent und gleichsam bekannt. Es ist lediglich nicht erkennbar, wann und wie bzw. ob sich diese Risiken überhaupt realisieren werden.[39] Hinzu kommt, dass die Ungewissheiten über den Lebenszyklus dieser Produkte zunehmen. Damit ist nicht der allgemeine Verschleiß bzw. die Abnutzung gemeint. Es geht um das Selbstlernen autonomer Systeme in der Nutzungsphase und die Schnelllebigkeit des technischen Fortschritts. Lernt das System aus jeder Interaktion mit der Umgebung und ändert im laufenden Betrieb selbständig ohne Update sein Verhalten, sind Entscheidungen und Ergebnisse kaum vorhersehbar. Man kann von einem Prozess der kontinuierlichen Produktveränderung sprechen. Zudem werden neue IT-Sicherheitslücken regelmäßig erst im Laufe der Zeit bekannt[40] bzw. gelingt es Hackern erst nach und nach durch innovative Angriffstechniken Zugang zum System zu erlangen, sodass sich Bedrohungslagen ändern.[41] Dem Softwaremarkt wohnt allgemein eine hohe Dynamik und Schnelllebigkeit bei, die den beim Inverkehrbringen der Produkte zu gewährleistenden Stand von Wissenschaft und Technik schnell überholt sein lässt.[42] Damit aber dynamisiert sich gleichzeitig die Gefahrenlage. Produkte, welche bei Inverkehrbringen den (historischen) Sicher-

35 *McGuire*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 59, Rn. 34 f.

36 *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 einer „Wundertüte".

37 *Schmid/Wessels*, NZV 2017, 357 (359); *Heckmann/Schmid*, Informatik Spektrum 2017, 430 (433); *Schmid*, CR 2019, 141 (141); *Schmid*, IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme, S. 89.

38 *Schmid/Wessels*, NZV 2017, 357 (359) sprechen von „latente[n] Produktfehler[n]".

39 Vgl. *Sommer*, Haftung für autonome Systeme, S. 260.

40 *Raue*, NJW 2017, 1841 (1844).

41 *Wende*, in: Sassenberg/Faber (Hg.), Industrie 4.0 und Internet of Things, § 4, Rn. 59.

42 In diese Richtung *Wende*, in: Sassenberg/Faber (Hg.), Industrie 4.0 und Internet of Things, § 4, Rn. 13; *Beierle*, Die Produkthaftung im Zeitalter des Internet of Things, S. 204.

heitserwartungen entsprachen, können in kürzester Zeit zu unsicheren Produkten werden.[43]

Daher ist es nicht verwunderlich, dass in der juristischen Literatur aufgrund dieser „mehrfachen Komplexitäten und Unsicherheiten [...] eine Schwerpunktverlagerung der herstellerseitigen Pflichten hin zur kontinuierlichen Informationsbeschaffung und Produktverbesserung nach dem Zeitpunkt der Markteinführung von Produkten" proklamiert wird.[44]

Gemeint ist damit die Produktbeobachtungspflicht. Der Hersteller ist grundsätzlich gehalten, nur sichere Produkte in den Verkehr zu geben und Produktgefahren möglichst abzuwehren.[45] Um Rechtsgutsverletzungen durch ein gefährliches Produkt und eine darauf beruhende Haftung nach § 823 Abs. 1 BGB möglichst zu vermeiden, treffen den Hersteller Verkehrssicherungspflichten.[46] Als solche besteht die Produktbeobachtungspflicht kurz gesagt in der Verpflichtung des Herstellers, seine Produkte auch noch nach dem Inverkehrbringen auf deren Produktsicherheit hin zu beobach-

43 Vgl. auch *Rockstroh/Kunkel*, MMR 2017, 77 (79).

44 So *Schmid*, CR 2019, 141 (141); vgl. auch *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 2; ähnlich *Klindt* et al., in: Bräutigam/Klindt (Hg.), Digitalisierte Wirtschaft/Industrie 4.0, S. 76 (85), welche „eine Schwerpunktverschiebung von Sorgfaltspflichten [...] hin zu umfassender Produktbeobachtung als nachgelagerter Verkehrssicherungspflicht" vorhersagen.

45 In diese Richtung schon RGZ 163, 21 (26); *Steege*, in: Buck-Heeb/Oppermann (Hg.), Automatisierte Systeme, S. 367 (382); zum Inverkehrbringen § 3 Abs. 1 Nr. 2, Abs. 2 S. 1 ProdSG.

46 Das vertragliche Gewährleistungsrecht soll dagegen nicht Gegenstand vorliegender Untersuchung sein. Da der Hersteller das Produkt in den seltensten Fällen direkt an den Endnutzer verkauft, wird es regelmäßig an einer für das Eingreifen des Gewährleistungsrechts erforderlichen Sonderverbindung fehlen, vgl. nur BGH, NJW 1969, 269 (271 ff.). In der Literatur gibt es immer wieder Versuche, einen Direktanspruch des Käufers gegen den Hersteller zu konstruieren, vgl. die Nachweise bei *Schrader/Engstler*, MMR 2018, 356 (358 f.). *Sommer*, Haftung für autonome Systeme, S. 155 ff. beschäftigt sich intensiv mit möglichen quasivertraglichen Ansprüchen gegen den Hersteller von autonomen Systemen und hält einen Anspruch aus § 311 Abs. 3 BGB und dem Vertrauensgrundsatz unter der Entwicklung einer neuen Fallgruppe „Vertrauen in komplexe Technik" für möglich. Der BGH (ebd.) erteilte solchen Ansätzen früh eine Absage, da die „durch den Vertrag gezogene Abgrenzung zwischen schuldrechtlichem und deliktischem Haftungsbereich in folgenschwerer Weise durchbrochen würde". Hier äußerte er sich auch zur grundsätzlichen Ablehnung der Einbeziehung des Käufers in den Vertrag zwischen dem Hersteller und dem Händler gem. den Grundsätzen des Vertrages mit Schutzwirkung zu Gunsten Dritter sowie zur Ablehnung der Drittschadensliquidation und der Garantiehaftung in diesen Fällen. Bei einem durch das Produkt geschädigtem vertragsexternen Dritten greifen ohnehin keine vertraglichen Rechte.

ten und gegebenenfalls Gefahrensteuerungsmaßnahmen zu ergreifen.[47] Die Produktbeobachtungspflicht begründet demnach eine Verantwortung des Herstellers für das Produkt über den Zeitpunkt des Inverkehrbringens hinaus.[48]

III. Gang der Untersuchung

Mit der vorliegenden Arbeit soll nun die Bedeutung der Produktbeobachtungspflicht für smarte Produkte mit Blick auf deren Komplexitäten und Unsicherheiten untersucht werden. Dabei kann auf den herkömmlichen Grundsätzen der Produktbeobachtungspflicht aufgebaut werden. Allerdings handelt es sich schon dabei um einen, hinsichtlich „ihre[r] konkreten Voraussetzungen und Folgen […] zu den am heftigsten umstrittenen und bisher am wenigsten geklärten Bereichen der Produkthaftung, vor allem im Hinblick auf Umfang und Reichweite".[49] Mit der vorliegenden Untersuchung soll der Stellenwert der Produktbeobachtungspflicht im Hinblick auf smarte Produkte analysiert und die Reichweite der entsprechenden Herstellerpflichten nach dem Inverkehrbringen betrachtet werden.

Um ein generelles Verständnis der Produktbeobachtung für die nachfolgende Darstellung der Produktbeobachtungspflicht im digitalen Zeitalter zu schaffen, werden zu Beginn des Hauptteils die juristischen Grundlagen der zivilrechtlichen Produktbeobachtungspflicht dargelegt. Einen ersten Schwerpunkt der Arbeit bildet dann die Untersuchung der kritischen Eigenschaften smarter Produkte und die Herausarbeitung ihrer haftungsrechtlichen Relevanz für die Produktbeobachtungspflicht. Hierzu muss zunächst der Anwendungsbereich der Produktbeobachtungspflicht geklärt werden. Kern der Arbeit ist anschließend die Untersuchung der herstellerseitigen Pflichten im Rahmen der Produktbeobachtung. Dabei scheint die Produktbeobachtungspflicht im Zusammenhang mit der Digitalisierung der Produktwelt gleich in mehrfacher Hinsicht Potential zu bergen.

Zum einen wird durch smarte Produkte eine zunehmende Datenmenge für die Hersteller über die Zustände ihrer Produkte im Feld und damit nach Inverkehrbringen verfügbar. Es handelt sich eben nicht um „tote"

47 Prägnant *Hartmann*, DAR 2015, 122 (124); *Ackermann*, in: NK-ProdR, § 823 BGB, Rn. 116; *Förster*, in: BeckOK, BGB, § 823, Rn. 735.

48 Ausführlich unter B.I.; vgl. schon jetzt *Wagner*, in: MüKo, BGB, § 823, Rn. 1109.

49 So *Klindt/Wende*, BB 2016, 1419 (1419); vgl. auch *Lenz*, in: Hamm (Hg.): Beck'sches Rechtsanwaltshandbuch, § 27, Rn. 99.

Produkte, sondern um Produkte, die fortlaufend Daten sammeln und kommunizieren können. Damit besteht für die Hersteller die Möglichkeit, diese Daten zu nutzen und anhand dieser Informationen die Produkte auf bisher unbekannte Gefahren hin zu beobachten und Produktunsicherheiten zu erkennen. Hinsichtlich dieser Datenverfügbarkeit ist zu untersuchen, inwieweit die von digitalen Produkten gelieferten Echtzeit-Daten von den Herstellern ausgewertet werden dürfen oder müssen. Dabei sind zwei Fragen voneinander zu trennen. Zum einen, inwieweit die Hersteller sensorisch erhobene und zu ihnen weitergeleitete Daten auch tatsächlich auswerten müssen. Zum anderen, ob und ggf. bei welchen Produkten diese sensorische Möglichkeit der Datenerhebung auch tatsächlich im Produkt angelegt werden muss; mit anderen Worten, ob nicht nur eine aktive Produktbeobachtung, sondern auch eine „aktivistische Produktbeobachtung" zu fordern ist. Bei diesen Fragen darf das Datenschutzrecht nicht außer Acht gelassen werden. Daneben wird zu prüfen sein, inwieweit Social-Media-Inhalte auf Meldungen hinsichtlich Produktgefahren zu untersuchen sind.

Zum anderen ermöglicht die Digitalisierung und Vernetzung dieser smarten Produkte neue Gefahrengegenmaßnahmen. Sie ermöglichen eine direkte und effektive Kommunikations- und Interaktionsebene zwischen Hersteller und Nutzer.[50] So können zur Gefahrensteuerung zielgerichtete Warnungen, fehlerbehebende Updates oder gar die Deaktivierung eines Produkts per Fernzugriff erfolgen. Hinsichtlich dieser Maßnahmen muss untersucht werden, unter welchen Voraussetzungen sie jeweils in Betracht kommen und in welchem Verhältnis sie zueinanderstehen. Sie sollen daher vor dem Hintergrund der herkömmlichen bzw. analogen Reaktionspflichten entwickelt und beleuchtet werden. Ein Fokus soll dabei auf die Frage gelegt werden, inwieweit Nutzer gegenüber Herstellern in diesem außervertraglichen Bereich Ansprüche auf die Vornahme von Updates herleiten können. In diesem Kontext darf auch eine gegenläufige Frage nicht unberücksichtigt bleiben. So wird zu untersuchen sein, wann herstellerseits mittels Fernzugriff ggf. auch gegen den Willen des Nutzers Veränderungen am Produkt durchgeführt werden können („aufgedrängte Sicherheitsbereicherung") und inwieweit Rechte der Nutzer diesem Vorgehen entgegenstehen.

Bisher fehlt es hierzu an tragfähiger und umfassender Gesetzgebung oder Rechtsprechung.[51] Entsprechend der Anerkennung der Verantwortung

50 Vgl. *Hartmann*, in: Knappertsbusch/Gondlach (Hg.), Arbeitswelt und KI 2030, S. 63 (68 f.; 71).

51 So schon *Theurer* et al., ZdiW 2021, 83 (87).

des Herstellers für die Sicherheit von Produkten während ihres gesamten Lebenszyklus und damit über den Zeitpunkt des Inverkehrbringens hinaus auch auf europäischer Ebene[52] befinden sich verschiedene produktbezogene Rechtsakte im europäischen Gesetzgebungsprozess oder haben diesen unlängst durchlaufen, bei denen deutlich wird, dass gerade bei smarten Produkten auch die Verantwortung für die Produktsicherheit nach der Inverkehrgabe in den Fokus rücken soll. Auf die entsprechende Gesetzgebung wird jeweils an geeigneter Stelle eingegangen.

52 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. 19.