Product Compliance

Carola Kaiser

# Anspruch auf IT-Sicherheitsaktualisierungen bei smarten Produkten

## Eine Analyse des Rechtsverhältnisses zwischen Verbraucher und Verkäufer

Nomos

Product Compliance

Herausgegeben von

Prof. Dr. Christian Bickenbach
Prof. Dr. Jan Eichelberger, LL.M. oec.
Prof. Dr. Anne Paschke
Prof. Dr. Björn Steinrötter
Prof. Dr. Meik Thöne
Prof. Dr. Dr. h.c. Martin Paul Waßmer
Prof. Dr. Susanne Wende, LL.M.
Prof. Dr. Janine Wendt

Band 6

Carola Kaiser

# Anspruch auf IT-Sicherheitsaktualisierungen bei smarten Produkten

## Eine Analyse des Rechtsverhältnisses zwischen Verbraucher und Verkäufer

Nomos

Onlineversion
Nomos eLibrary

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

Zugl.: Köln, Univ., Diss., 2025

ISBN 978-3-7560-4312-5 (Print)
ISBN 978-3-7489-7173-3 (ePDF)

1. Auflage 2026

# Vorwort

Die vorliegende Arbeit wurde im Wintersemester 2025/2026 von der Rechtswissenschaftlichen Fakultät der Universität zu Köln als Dissertation angenommen. Literatur und Rechtsprechung sind bis April 2025 berücksichtigt.

Der erste Dank gilt meinem Doktorvater, Prof. Dr. *Karl-Nikolaus Peifer*, zum einen für die vertrauensvolle und konstruktive Betreuung der Arbeit, zum anderen für die lehrreiche und prägende Zeit am Institut für Medienrecht und Kommunikationsrecht. Die positive Arbeitsatmosphäre und der Austausch mit der Institutsgemeinschaft haben nicht nur maßgeblich zum Gelingen der Arbeit beigetragen, sondern mich darüber hinaus juristisch und menschlich sehr bereichert. Prof. Dr. *Klaus Peter Berger*, LL.M. danke ich für die zügige Erstellung des Zweitgutachtens.

Den Herausgeberinnen und Herausgebern der Schriftenreihe „Product Compliance" danke ich für die Aufnahme der Arbeit und dem Team des Nomos-Verlags für die professionelle Betreuung, die eine schnelle Drucklegung ermöglicht hat.

Besonderer Dank gebührt auch Prof. Dr. *Haimo Schack*, LL.M. und der Studienstiftung *ius vivum* für einen großzügigen Druckkostenzuschuss.

Darüber hinaus habe ich während der Promotionszeit Unterstützung von einer Vielzahl von Kolleginnen und Kollegen sowie Freundinnen und Freunden erhalten, für die ich von Herzen dankbar bin. Folgende Personen möchte ich namentlich erwähnen.

Prof. Dr. *Karina Grisse*, LL.M. war jederzeit zu intensiven Diskussionen über digitale Produkte bereit, die für mich immer überaus gewinnbringend waren. Dr. *Patrik Kassel* hat mir nicht nur bei der einen oder anderen Computerkrise geholfen; auch bei allen weiteren Themen im Promotionsalltag stand seine Tür stets offen. Besonders danke ich Dr. *Florian Priemel* für die gemeinsame Mitarbeiterzeit sowie nicht zuletzt dafür, dass der Humor auch in herausfordernden Situationen nie zu kurz kam.

Außerdem bin ich *Dominic Dresen*, LL.M. oec. für die produktiven Stunden im Doktorandenraum, *Silke Kletzien* für die täglichen Gespräche und *Hendrik Risthaus* für die Unterstützung vor der Disputation dankbar.

Dr. *Karsten Müller* gebührt Dank für die vielfältige Unterstützung während der Promotionszeit, vor allem für den Zuspruch in schwierigen Phasen sowie für die Korrektur wesentlicher Teile des Manuskripts. Für die

Korrektur weiterer Manuskriptteile danke ich zudem Dr. *Anna-Frederike Schaube* und *Karina* sehr.

Der größte Dank gilt schließlich meiner Familie, insbesondere meinen Eltern *Monika* und Dr. *Michael Kaiser*. Ihre uneingeschränkte Unterstützung und ihr beständiger Rückhalt sind unersetzlich. Sie als Gesprächspartner und Ratgeber an meiner Seite zu haben, ist für mich das größte Glück.

Düsseldorf, im Februar 2026 *Carola Kaiser*

# Inhaltsverzeichnis

# Abkürzungen

Abkürzungen werden im Text eingeführt; im Übrigen entsprechen sie *Kirchner*, Abkürzungsverzeichnis der Rechtssprache, 11., neu bearbeitete und erweiterte Auflage, 2024.

# A. Einleitung

IT-Sicherheit zu gewährleisten, ist ein fortlaufender Prozess.[1] Softwareelemente, die ein angemessenes IT-Sicherheitsniveau aufweisen sollen, bedürfen stetiger Anpassungen im Laufe ihrer Nutzungszeit. Typischerweise werden diese Anpassungen mittels Aktualisierungen der Software vorgenommen. Dieses Phänomen stellt das Vertragsrecht vor Herausforderungen. So ist einer der zentralen Vertragstypen – der Kaufvertrag gem. § 433 BGB – im Ursprung durch einen punktuellen Leistungsaustausch charakterisiert.[2] Die prägenden Leistungshandlungen erschöpften sich bis zur Neufassung der Regelungen zum Verbrauchsgüterkauf zum 1.1.2022 in einer einmaligen Übergabe und Übereignung der (mangelfreien) Kaufsache gegen eine einmalige Zahlung des Kaufpreises. In der Konsequenz traten die Gewährleistung von IT-Sicherheit und die Charakteristik des Kaufvertrags in ein Spannungsverhältnis zueinander, wenn eine Ware, die Softwareelemente enthält – aufgrund des dadurch generierten Leistungsgewinns unter bestimmten Voraussetzungen auch als „smartes Produkt" bezeichnet –,[3] verkauft wurde. Unter anderem dies bot Anlass für den Unionsgesetzgeber, die Regelungen zum Verbrauchsgüterkauf zu überarbeiten. Daran anknüpfend soll die Arbeit die Frage beantworten, inwieweit der Käufer eines smarten Produkts als Verbraucher nach der aktuellen Rechtslage einen Anspruch auf IT-Sicherheitsaktualisierungen gegen den Verkäufer hat. Dabei lassen sich sowohl praxisbezogene als auch dogmatische Erkenntnisse über die aktuelle Rechtslage im Verbrauchsgüterkauf gewinnen.

1 *Eckert*, IT-Sicherheit, S. 7, 169 f.; *Fedler*, in: Ebers/Steinrötter, Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 91 (120 f.); s. auch *Bundesamt für Sicherheit in der Informationstechnik*, Online-Kurs IT-Grundschutz, 7.8.2018, S. 14, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Webkurs/onlinekurs2018.pdf?__blob=publicationFile&v=1 (zuletzt abgerufen am 28.4.2025).

2 Vgl. *Schmidt-Kessel*, liber amicorum Storme, 683 (684, 688).

3 S. hierzu B.I.1.

## I. Anlass der Untersuchung

Smarte Produkte erfreuen sich in verschiedenen Lebensbereichen wachsender Beliebtheit.[4] Ein Bereich, in dem smarte Produkte regelmäßig auch von privaten Endverbrauchern eingesetzt werden, ist der Haushalt bzw. die Wohnung, die dadurch zum sogenannten „Smart Home" wird.[5] Sobald es um Softwareelemente geht, stellt sich die Frage nach ihrer IT-Sicherheit. IT-Sicherheit beschreibt den Schutz eines Systems „*vor unautorisierten Ein- oder Zugriffen*"[6] und richtet sich damit im Kern gegen Angriffe auf das System von außen bzw. durch Dritte.[7] Weisen die Softwareelemente eines smarten Produkts IT-Sicherheitslücken auf, so können sich Angreifer solche Lücken für Cyberangriffe auf das Produkt zunutze machen. Cyberangriffe können durchaus schwerwiegende Auswirkungen nach sich ziehen: So kann ein Angreifer beispielsweise aus der Ferne ein smartes Türschloss gegen den Willen des Nutzers auf- und zuschließen.[8] Ebenso ist z.B. denkbar, dass ein Angreifer einen smarten Kühlschrank mit Mikrofon angreift und jegliche Gespräche in der Küche abhört.[9] Darüber hinaus können Angreifer smarte Produkte in ein sogenanntes „Botnetz" integrieren, welches sodann für weitergehende, größer angelegte Angriffe auf andere (kritische) Einheiten genutzt wird.[10]

Um ein angemessenes Niveau an IT-Sicherheit zu gewährleisten und aufrechtzuerhalten, sind allerdings – selbst wenn eine Software mit Blick auf

4 Vgl. zur prognostizierten Verbreitung smarter Produkte *Hagemann*, BdW 2017, 166 (166 f.).

5 *Ametsbichler*, in: Taeger, Die Macht der Daten und der Algorithmen, 497 (497); *Bundesamt für Sicherheit in der Informationstechnik*, Informationen und Empfehlungen zum Smart Home, abrufbar unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Internet-der-Dinge-Smart-leben/Smart-Home/smart-home_node.html (zuletzt abgerufen am 28.4.2025).

6 *Fedler*, in: Ebers/Steinrötter, Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 91 (99); ähnlich Kipker/*Kipker*, Hdb Cybersecurity, Kapitel 1. Rn. 6; *Eckert*, IT-Sicherheit, S. 6.

7 Kipker/*Kipker*, Hdb Cybersecurity, Kapitel 1. Rn. 6; *Fedler*, in: Ebers/Steinrötter, Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 91 (99).

8 Kipker/*Lapp*, Hdb Cybersecurity, Kapitel 10. Einführung; *Pohlmann*, DuD 2021, 95 (99); zu einem durchgeführten Testangriff auf ein smartes Türschloss s. *Wollerton*, 25.8.2016, abrufbar unter: https://www.cnet.com/home/smart-home/august-smart-lock-hacked/ (zuletzt abgerufen am 28.4.2025).

9 Vgl. *Guillet,* Reducing Cybersecurity Risks, S. 36 f. zu einem Testangriff auf einen smarten Kühlschrank.

10 *Wiesemann/Mattheis/Wende*, MMR 2020, 139 (139 f.); *Wilczek*, DuD 2021, 79 (81).

ihre IT-Sicherheit einwandfrei hergestellt wird – IT-Sicherheitsaktualisierungen im Laufe der Nutzungszeit der Software notwendig. Das liegt daran, dass sich das Umfeld einer Software typischerweise stetig ändert, was dazu führen kann, dass neue IT-Sicherheitslücken aufkommen. Folglich sind IT-Sicherheitsaktualisierungen, welche aufkommende IT-Sicherheitslücken verhindern oder zumindest schließen, unerlässlich für ein konstant gewahrtes angemessenes IT-Sicherheitsniveau einer Software und somit auch eines smarten Produkts. Im Idealfall werden IT-Sicherheitsaktualisierungen über die Nutzungszeit eines smarten Produkts hinweg durch den Hersteller freiwillig bereitgestellt.[11] In der Realität bleiben IT-Sicherheitsaktualisierungen jedoch regelmäßig aus.[12] So zeigen Berichte des *Bundesamtes für Sicherheit in der Informationstechnik (BSI),* dass smarte Produkte – gerade auch im privaten Bereich wie dem Smart Home – häufig gravierende IT-Sicherheitslücken aufweisen, weil keine Aktualisierungen bereitgestellt werden.[13] Und auch wenn Aktualisierungen freiwillig bereitgestellt werden, kann die konkrete Umsetzung für den Verbraucher nachteilig sein. So handelt es sich beispielsweise bei den freiwillig bereitgestellten Aktualisierungen oftmals nicht ausschließlich um IT-Sicherheitsaktualisierungen, sondern um Kombinationen mit ggf. weitreichenden anderen Änderungen der Software. Auch ist denkbar, dass ein Verbraucher mangels adäquater Benachrichtigung nicht bemerkt, dass eine (IT-Sicherheits-)Aktualisierung bereitsteht.

Entscheidend ist in diesen Fällen, welche *rechtlichen* Möglichkeiten ein Verbraucher hat, IT-Sicherheitsaktualisierungen auf die gewünschte Art und Weise durchzusetzen. Da viele der smarten Produkte, insbesondere zum privaten Gebrauch, *gekauft* werden, stellt sich die Frage, ob die kaufrechtlichen Regelungen die Notwendigkeit von IT-Sicherheitsaktualisierungen hinreichend abbilden.

Der Kaufvertrag gem. § 433 BGB zeichnet sich, wie bereits erwähnt, im Ursprung durch einen punktuellen Leistungsaustausch in Form einmaliger Übergabe und Übereignung gegen einmalige Kaufpreiszahlung aus. Über

11 Vgl. *Jung/Rolsing*, Die Bereitstellung digitaler Produkte, S. 17 zu Aktualisierungen allgemein.

12 *Guillet,* Reducing Cybersecurity Risks, S. 37; vgl. *Jung/Rolsing*, Die Bereitstellung digitaler Produkte, S. 17 zu Aktualisierungen allgemein.

13 *Bundesamt für Sicherheit in der Informationstechnik*, Bericht zum Digitalen Verbraucherschutz 2020, S. 15; s. zum Problem nicht behobener IT-Sicherheitslücken im Smart Home auch *Bundesamt für Sicherheit in der Informationstechnik*, Bericht zum Digitalen Verbraucherschutz 2022, S. 23 f.; *Bundesamt für Sicherheit in der Informationstechnik*, Digitaler Verbraucherschutz: BSI-Jahresrückblick 2024, S. 8.

lange Zeit beschränkten sich die zentralen Leistungshandlungen darauf. Ferner knüpften an den punktuellen Leistungsaustausch, konkret an den Moment des Gefahrübergangs hinsichtlich der Kaufsache, auch die meisten weiteren Rechte aus dem Kaufvertrag an, vornehmlich die Mangelgewährleistungsrechte gem. § 437 BGB.[14] Diese greifen bei Vorliegen eines Mangels, der sich gem. § 434 BGB a.F. ausschließlich auf den Zeitpunkt des Gefahrübergangs bezog. Hier zeigte sich eine Diskrepanz zwischen der neuen Wirklichkeit bei Softwareprodukten und den bisherigen Prinzipien des Kaufvertragsrechts.[15] Dies galt auch konkret für die dargestellten IT-Sicherheitsaktualisierungen. Denn Aktualisierungen, welche erst im Laufe der Nutzungszeit des smarten Produkts und somit nach dem Gefahrübergang notwendig werden, ließen sich über die skizzierten kaufrechtlichen Regelungen nicht erfassen.[16]

Unter anderem dieses Problem wurde im Rahmen der „Digitalisierung des Vertragsrechts" auf unionsrechtlicher Ebene aufgegriffen. Im Jahr 2019 erließ der Unionsgesetzgeber zum einen die Warenkauf-Richtlinie (im Folgenden „WK-RL")[17] und zum anderen die Digitale-Inhalte-Richtlinie (im Folgenden „DI-RL").[18] Beide Richtlinien können als das Ergebnis eines langjährigen Reformprozesses im (Verbraucher-)Vertragsrecht auf unionsrechtlicher Ebene, zuletzt geprägt durch digitale Entwicklungen, angesehen werden.[19] Umgesetzt in das nationale Vertragsrecht wurden sie vornehmlich durch die §§ 475b ff. BGB und die §§ 327 ff. BGB, die für ab dem 1.1.2022 geschlossene Verbraucherverträge gelten.[20] Die Richtlinien sehen mit Art. 7 Abs. 3 WK-RL sowie Art. 8 Abs. 2 DI-RL objektive Aktualisierungspflichten im Rahmen der Vertragsregelungen betreffend Verbraucherverträge vor –

14 Vgl. *Schmidt-Kessel*, liber amicorum Storme, 683 (688).

15 *Schmidt-Kessel*, in: Beyer/Erler/Hartmann/Kramme/Müller/Pertot/Tuna/Wilke, Privatrecht 2050 – Blick in die digitale Zukunft, 9 (15 f.).

16 S. hierzu auch C.I.1.

17 Richtlinie (EU) 2019/771 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte des Warenkaufs, zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie 2009/22/EG sowie zur Aufhebung der Richtlinie 1999/44/EG.

18 Richtlinie (EU) 2019/770 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen.

19 S. zu einer Darstellung der Entwicklung des unionsrechtlichen Verbrauchervertragsrechts, die zu den beiden Richtlinien geführt hat, *Gsell*, ZUM 2018, 75 (77 ff.); *Staudenmayer*, ZEuP 2019, 663 (664 ff.); ausführlich *Busch*, in: Artz/Gsell, Verbrauchervertragsrecht und digitaler Binnenmarkt, 1 (1 ff.).

20 S. zur zeitlichen Anwendbarkeit Art. 229 § 57 EGBGB.

auch im Kaufvertragsrecht. Diese unionsrechtlich vorgegebenen objektiven Aktualisierungspflichten finden im nationalen Recht in § 475b Abs. 4 Nr. 2 BGB sowie in § 327f BGB ihre Entsprechung, wobei sich im weiteren Verlauf der Arbeit zeigen wird, dass für den Kauf eines smarten Produkts vornehmlich § 475b Abs. 4 Nr. 2 BGB eine Rolle spielt.[21]

Jene Aktualisierungsregelungen wurden bereits früh als „*Durchbruch für den Verbraucherschutz*" bezeichnet.[22] Die Einführung der Aktualisierungspflicht gem. § 475b Abs. 4 Nr. 2 BGB hat gleichwohl Fragen hervorgerufen. So werden die Aktualisierungspflichten – sowohl auf der unionsrechtlichen als auch auf der nationalen Ebene – als komplexe Regelungen bewertet, die erhebliche Interpretationsschwierigkeiten hervorbringen.[23] Das gelte auch für das Verhältnis der Aktualisierungspflichten zu den daneben bestehenden Vertragsregelungen.[24] Die resultierenden und in dieser Arbeit interessierenden Fragen lassen sich grob zwei Kategorien zuordnen: Die erste Kategorie betrifft die Funktions- und Wirkungsweise der Aktualisierungspflicht nach § 475b Abs. 4 Nr. 2 BGB aus praktischer Sicht; die zweite Kategorie bezieht sich auf die Dogmatik der Aktualisierungspflicht nach § 475b Abs. 4 Nr. 2 BGB im Gesamtsystem des Kaufvertragsrechts.

Innerhalb der ersten Kategorie stellt sich zuvörderst die Frage nach dem genauen Umfang der geschuldeten Aktualisierungen. In der bereits existierenden Literatur zur Aktualisierungspflicht gem. § 475b Abs. 4 Nr. 2 BGB bzw. § 327f BGB wird regelmäßig erwähnt, dass Unklarheiten hinsichtlich des Umfangs der geschuldeten Aktualisierungen bestehen.[25] Es bedarf somit einer näheren Analyse, ob und ggf. welche IT-Sicherheitsaktualisierungen von der Aktualisierungspflicht gem. § 475b Abs. 4 Nr. 2 BGB erfasst sind. Zudem ist für einen Verbraucher entscheidend, wann genau und auf

21 S. hierzu C.III.

22 *Wendehorst*, NJW 2021, 2913 (2917) (zu § 327f BGB); ähnlich *Metzger*, JZ 2019, 577 (581) (zu Art. 8 Abs. 2 DI-RL).

23 *Jung/Rolsing*, Die Bereitstellung digitaler Produkte, S. 18 (zu § 327f BGB); *Erdelt*, K&R 2022, 803 (808) (zu § 327f BGB): „*[…] viele Fragen offen oder ungeregelt*"; *Rieländer*, GPR 2021, 257 (267): „*Ihre defizitär-lückenhafte Ausgestaltung wirft eine Vielzahl komplexer Auslegungs- und Rechtsfragen auf, […]*".

24 Schmidt-Kessel/Kramme/*Schmidt-Kessel*, Hdb Verbraucherrecht, Kapitel 14 Rn. 123 (zu § 327f BGB): „*Dabei ist das Regelungskonzept nicht mehr ohne weiteres schlüssig […]*"; *Jung/Rolsing*, Die Bereitstellung digitaler Produkte, S. 18 (zu § 327f BGB).

25 *Jung/Rolsing*, Die Bereitstellung digitaler Produkte, S. 22 (zu § 327f BGB); *Redeker*, IT-Recht, Rn. 756 (zu § 327f BGB); *Voß*, in: Raue, Digitale Resilienz: Effektives Recht auf sichere Software, 97 (101); *Ehle/Kreß*, CR 2019, 723 (728) (zur unionsrechtlichen Ebene); ähnlich *Schneider*, CR 2022, 1 (9) (zu § 327f BGB).

welche Art und Weise er die Aktualisierungen erhält, ebenso ob und wie er erfährt, um welche Aktualisierung es sich genau handelt. Weiterhin ist der Frage nach dem Aktualisierungszeitraum nachzugehen. Betreffend den Zeitraum wird die offene Fassung des Gesetzes („*während des Zeitraums, den [der Verbraucher] aufgrund der Art und des Zwecks der Ware und ihrer digitalen Elemente sowie unter Berücksichtigung der Umstände und der Art des Vertrags erwarten kann, […]*“) in der Literatur neben den Unklarheiten zum Umfang der geschuldeten Aktualisierungen regelmäßig als Belastung für den Rechtsanwender herausgestellt.[26] Darüber hinaus ist es von praktischem Interesse, welche Möglichkeiten der Verkäufer hat, um die Aktualisierungspflicht zu seinen Gunsten auszugestalten oder sogar abzubedingen.

Die dogmatische Herausforderung fußt darauf, dass die neu eingeführte Aktualisierungspflicht gem. § 475b Abs. 4 Nr. 2 BGB gerade einen Bruch mit dem davor existierenden, dargestellten Kaufrechtscharakter bedeutet.[27] Davon ausgehend werden die Aktualisierungspflichten auch als Paradigmenwechsel dargestellt, welcher „*[klassische] Zielschuldverhältnisse in latente Dauerschuldverhältnisse*“ umwandele.[28] Zum klassischen Kaufvertrag würde das nicht passen.[29] Das ist Anlass zu untersuchen, wie sich die Aktualisierungspflicht dogmatisch in die bestehenden Regelungen zum Kaufvertrag einfügt, sowie ob und ggf. an welchen Stellen sich das dogmatische Verständnis des Kaufvertrags ändert.

Eine detaillierte Auseinandersetzung mit der Aktualisierungspflicht gem. § 475b Abs. 4 Nr. 2 BGB auf die dargestellte Art und Weise ist zum einen geboten, um gestützt auf ein möglichst umfassendes Verständnis der Pflicht ihr Potenzial in der Praxis vollumfänglich nutzen zu können. Zum anderen ist sie geboten, da der Kaufvertrag innerhalb der bestehenden Vertragstypen eine zentrale Stellung einnimmt,[30] sodass eine genaue Beurtei-

26 Brönneke/Föhlisch/Tonner/*Tamm/Tonner*, Neues Schuldrecht, § 2 Rn. 125 (zu § 327f BGB); *Redeker*, IT-Recht, Rn. 756 (zu § 327f BGB); *Ehle/Kreß*, CR 2019, 723 (728) (zur unionsrechtlichen Ebene); *Spindler*, MMR 2021, 451 (455) (zu § 327f BGB).

27 S. *Hunzinger*, CR 2022, 349 (351) (zu § 327f BGB); *Sattler*, CR 2020, 145 (149): „*echte[r] Systembruch*“ (zu Art. 8 Abs. 2 DI-RL).

28 *Wendehorst*, in: Stabentheiner/Wendehorst/Zöchling-Jud, Das neue europäische Gewährleistungsrecht, 111 (111); ähnlich Brönneke/Föhlisch/Tonner/*Brönneke/Schmitt/Willburger*, Neues Schuldrecht, § 4 Rn. 53; *Schmidt-Kessel*, in: Beyer/Erler/Hartmann/Kramme/Müller/Pertot/Tuna/Wilke, Privatrecht 2050 – Blick in die digitale Zukunft, 9 (16): partielles Dauerschuldverhältnis; s. auch *Riehm/Abold*, CR 2021, 530 (538): asymmetrisches Dauerschuldverhältnis.

29 *Metzger*, JZ 2019, 577 (585) (zu Art. 8 Abs. 2 DI-RL).

30 S. dazu *Schmidt-Kessel*, liber amicorum Storme, 683 (684 ff.).

lung, welche dogmatischen Veränderungen die Aktualisierungspflicht gem. § 475b Abs. 4 Nr. 2 BGB herbeigeführt hat, erstrebenswert ist.

## II. Untersuchungsgegenstand und Arbeitshypothesen

Ausgehend davon untersucht die Arbeit, inwieweit der Käufer eines smarten Produkts als Verbraucher nach aktueller Rechtslage einen Anspruch auf IT-Sicherheitsaktualisierungen gegen den Verkäufer hat.

Dabei legt die Arbeit zum einen die These zugrunde, dass die Aktualisierungspflicht nach § 475b Abs. 4 Nr. 2 BGB das Interesse des Käufers an IT-Sicherheitsaktualisierungen aus *praktischer* Sicht hinreichend abdeckt. Zum anderen stellt sie die These auf, dass die Einführung der Aktualisierungspflicht nach § 475b Abs. 4 Nr. 2 BGB das *dogmatische* Konzept des Kaufvertrags nur punktuell statt übergreifend verändert und sich der Kaufvertrag auch unter Geltung der Aktualisierungspflicht noch von reinen Dauerschuldverhältnissen unterscheidet.

Im Einklang mit dem dargestellten Anlass der Untersuchung konzentriert sich der Untersuchungsgegenstand dabei auf solche IT-Sicherheitsaktualisierungen, welche aufgrund von Umfeldveränderungen erst im Laufe der Nutzungszeit des smarten Produkts notwendig werden, während IT-Sicherheitsaktualisierungen, mittels derer schon bei Übergabe des Produkts bestehende, vermeidbare Mängel behoben werden sollen, unberücksichtigt bleiben.

Zudem beschränkt sich der Untersuchungsgegenstand auf das Vertragsverhältnis zwischen Verbraucher und Verkäufer, in welchem die Aktualisierungspflicht gem. § 475b Abs. 4 Nr. 2 BGB ausdrücklich greift. Nicht thematisiert wird demnach die Frage, inwieweit ein *Unternehmer* einen Anspruch auf IT-Sicherheitsaktualisierungen gegen den Verkäufer hätte. Auch klammert die Arbeit damit das Rechtsverhältnis des Verkäufers zum Hersteller des smarten Produkts bzw. zu den Herstellern einzelner Softwareelemente weitestgehend aus. Zwar kommt diesen Rechtsverhältnissen Relevanz zu mit Blick auf die Regressmöglichkeiten eines Verkäufers, der gem. § 475b Abs. 4 Nr. 2 BGB Aktualisierungen schuldet.[31] Gleichwohl würde eine umfassende Analyse jener Rechtsverhältnisse den Rahmen der Arbeit übersteigen.

Ferner konzentriert sich die Untersuchung auf die *objektive* Aktualisierungspflicht gem. § 475b Abs. 4 Nr. 2 BGB. Soweit zwischen Käufer und

31 S. hierzu E.III.2.b)aa)(1).

Verkäufer *subjektive* Aktualisierungspflichten festgesetzt werden, fallen diese unter § 475b Abs. 3 Nr. 2 BGB. Letzteres ist bei smarten Verbraucherprodukten im Massenvertrieb jedoch überwiegend praxisfern. Die subjektiven Aktualisierungspflichten gem. § 475b Abs. 3 Nr. 2 BGB werden deshalb nur angesprochen, wenn dies für das Gesamtverständnis der kaufvertraglichen Regelungen zuträglich ist.

Überdies sind mögliche (Direkt-)Ansprüche des Käufers gegen den Hersteller des smarten Produkts bzw. gegen den Hersteller betroffener Softwareelemente nicht von der Untersuchung erfasst. Dies gilt zum einen für die vertragsrechtliche Ebene, auf welcher insbesondere sogenannte „Endnutzervereinbarungen" (ENV) und „End-User-Licence-Agreements" (EULA) zwischen Erwerber und Hersteller bestehen können. Es geht vorliegend auch nicht um die Frage, welcher Akteur als vertraglicher Anspruchsgegner sinnvoller wäre oder ob eine Relativität der Vertragsbeziehungen angepasst werden sollte in Anbetracht der Tatsache, dass beim Verkauf smarter Produkte statt einer starren Vertriebskette eine Form der Multipolarität besteht.[32] Zum anderen gilt dies für potenzielle deliktsrechtliche Ansprüche im Kontext von IT-Sicherheitsaktualisierungen. Zwar beziehen sich deliktsrechtliche Pflichten zunehmend auch ausdrücklich auf Softwareaktualisierungen.[33] Ein Anspruch setzt indes überwiegend – lediglich bei § 823 Abs. 2 BGB ist dies anders zu beurteilen – auch eine eingetretene Rechtsgutverletzung beim Anspruchsteller voraus, sodass präventiv, also unabhängig von einer konkreten Rechtsgutverletzung,[34] bereitgestellte IT-Sicherheitsaktualisierungen darüber bereits aus dem Grund nicht erfasst werden.

Die Thematik der IT-Sicherheitsprobleme und entsprechender Aktualisierungen ist auch zu trennen von Problemen, welche durch bewusstes Fehlverhalten des Herstellers bzw. vom Hersteller (zum Betrieb des

32 S. dazu exemplarisch *Firsching,* Vertragsstrukturen IoT-Produkte, S. 170 ff.; *Grünberger*, AcP 2018, 213 (280 ff.).

33 S. insbesondere Art. 11 Abs. 2 lit. b und c der neuen Produkthaftungs-Richtlinie, Richtlinie (EU) 2024/285 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über die Haftung für fehlerhafte Produkte und zur Aufhebung der Richtlinie 85/374/EWG des Rates. Ausführlich zum Entwurf der neuen Produkthaftungs-Richtlinie *Meier*, Produkthaftung für Computerprogramme, S. 439 ff.

34 Ausbleibende, präventive IT-Sicherheitsaktualisierungen dürften auch nicht zu einer Eigentumsverletzung führen, da sie zusätzliche Leistungen darstellen würden, vgl. dazu im Kontext von Serverabschaltungen *Magnus*, Fernkontrolle im Internet der Dinge, S. 222 ff.; a.A. im Kontext von Serverabschaltungen *Solmecke/Vondrlik*, MMR 2013, 755 (758 ff.).

Backend-Servers) beauftragter Dritter[35] entstehen. Dazu gehört vornehmlich eine datenschutzrechtswidrige Nutzung der durch das smarte Produkt generierten Daten auf Seiten des Herstellers bzw. beauftragter Dritter.[36] Ein solches Fehlverhalten ist grundsätzlich ohne die Ausnutzung von klassischen IT-Sicherheitslücken möglich. Es gehört nicht zur Thematik der IT-Sicherheit, die sich auf den Schutz gegen Angriffe auf das System von außen bzw. durch Dritte richtet.[37]

Schließlich sei darauf hingewiesen, dass ein Verbraucher rein praktisch betrachtet auf aufkommende IT-Sicherheitslücken, die sein smartes Produkt betreffen, wohl kaum eigenständig aufmerksam wird.[38] Denn IT-Sicherheitslücken selbst haben im Grundsatz noch keine wahrnehmbaren Auswirkungen auf das smarte Produkt. Gleichwohl gibt es je nach Konstellation Möglichkeiten des Verbrauchers, von solchen sein Produkt betreffenden IT-Sicherheitslücken zu erfahren. So hat beispielsweise das *BSI* verschiedene Kompetenzen, Verbraucher unter bestimmten Voraussetzungen über IT-Sicherheitslücken in Produkten zu informieren.[39] In der Arbeit wird vorausgesetzt, dass ein Verbraucher auf eine aufgekommene IT-Sicherheitslücke, die sein smartes Produkt betrifft, aufmerksam geworden ist und eine entsprechende IT-Sicherheitsaktualisierung erhalten möchte.

## III. Stand der Rechtsprechung und der Forschung

Die Frage nach IT-Sicherheitsaktualisierungen, die nach aktueller Rechtslage im Rahmen eines Kaufvertrags über ein smartes Produkt geschuldet werden, fristet bis jetzt in der Rechtsprechung ein Schattendasein.

35 S. hierzu B.III.

36 Dazu exemplarisch *Morgenstern/Pursche/Clausing*, DuD 2021, 102 (105 f.); besondere Gefahren stellen in dem Zusammenhang smarte Produkte mit Spracherkennungsdiensten dar, bei welchen das konstante Mithören (gewollter) Teil des Systems ist, beispielsweise Amazons Lautsprecher „Echo" oder die „Hello Barbie" von Mattel. Zu einer datenschutzrechtswidrigen Produktgestaltung ausführlich *Eichfeld,* Datenschutzkonformität, S. 218 ff.

37 S. hierzu B.II.1.a).

38 S. auch *Voß*, in: Raue, Digitale Resilienz: Effektives Recht auf sichere Software, 97 (100).

39 Aus § 7 BSIG ergeben sich allgemeine Befugnisse zur Warnung vor IT-Sicherheitslücken, s. dazu Kipker/Reusch/Ritter/*Leisterer*, Informationssicherheit, § 7 BSIG Rn. 1 ff. Aus § 9c Abs. 8 S. 2 BSIG ergibt sich eine Befugnis zur Warnung vor IT-Sicherheitslücken im Zusammenhang mit einem (freiwilligen) IT-Sicherheitskennzeichen für ein Produkt, s. dazu Kipker/Reusch/Ritter/*Glade*, Informationssicherheit, § 9c BSIG Rn. 52 ff.

Zwar gibt es nunmehr erste Entscheidungen, in denen auch die Aktualisierungspflicht nach § 327f BGB eine Rolle spielt.[40] Diese Entscheidungen basieren allesamt auf der Konstellation, dass Batteriespeicher im Laufe der Nutzungszeit durch den Hersteller in ihrer Speicherkapazität gedrosselt wurden, um eine Brandgefahr zu reduzieren. Hiergegen wandten sich die Erwerber der Batteriespeicher auch über das Vertragsrecht und nahmen den jeweiligen Vertriebspartner in Anspruch. In dem Zusammenhang ordneten die Gerichte den Batteriespeicher als Ware mit digitalen Elementen nach §§ 475b Abs. 1 S. 1, 327a Abs. 3 S. 1 BGB ein und stützten einen Sachmangel der Ware mit digitalen Elementen unter anderem auf eine Verletzung der Aktualisierungspflicht durch die Drosselung – wobei sie insofern inkonsequent § 327f BGB heranzogen.[41] Die Entscheidungen beziehen sich also nicht auf IT-Sicherheitsaktualisierungen; auch weisen sie hinsichtlich allgemeiner Anhaltspunkte zur Funktions- und Wirkungsweise der Aktualisierungspflicht systematische Unstimmigkeiten auf. Ferner bleiben zahlreiche Fragen zur Dogmatik der Aktualisierungspflicht offen. Die darüber hinaus bereits bestehenden Urteile zur aktuellen Rechtslage im Vertragsrecht bzw. Kaufrecht beziehen sich schwerpunktmäßig auf die Vorschriften jenseits digitaler Aspekte.[42]

In der Rechtsliteratur ist die Thematik hingegen bereits auf reges Interesse gestoßen. Doch liegt bis dato keine monografische Aufarbeitung vor, welche die Aktualisierungspflicht nach § 475b Abs. 4 Nr. 2 BGB konkret mit Blick auf IT-Sicherheitsaktualisierungen bei smarten Produkten beleuchtet oder zu den gleichen Erkenntnissen hinsichtlich ihrer dogmatischen Einordnung kommt wie die vorliegende Arbeit.

Die „Digitalisierung des Vertragsrechts" durch die Umsetzung der WK-RL und der DI-RL wurde in der Rechtsliteratur umfassend begleitet. Dabei wurde auch den Aktualisierungspflichten – sowohl auf unionsrechtlicher Ebene gem. Art. 7 Abs. 3 WK-RL bzw. Art. 8 Abs. 2 DI-RL als auch auf nationaler Ebene gem. § 475b Abs. 4 Nr. 2 BGB bzw. § 327f BGB – viel

40 *LG Münster*, Urt. v. 16.12.2024, Az. 12 O 81/24, BeckRS 2024, 47425; *LG Frankfurt a.M.*, Urt. v. 19.9.2024, Az. 2-31 O 77/24, VuR 2025, 106; *LG Münster*, Urt. v. 31.7.2024, Az. 216 O 109/23, BeckRS 2024, 48197.

41 *LG Münster*, Urt. v. 16.12.2024, Az. 12 O 81/24, BeckRS 2024, 47425 unter I. 2. c.; *LG Frankfurt a.M.*, Urt. v. 19.9.2024, Az. 2-31 O 77/24, VuR 2025, 106 (109); *LG Münster*, Urt. v. 31.7.2024, Az. 216 O 109/23, BeckRS 2024, 48197.

42 So auch *Steinrötter*, NJW 2025, 249 (249 ff.); ein Gegenbeispiel ist die Entscheidung des *OLG München*, unter anderem zum Verhältnis von § 327r BGB und den AGB-Vorschriften, *OLG München*, Urt. v. 11.10.2024, Az. 39 U 2482/23 e, MMR, 288 (290).

Beachtung geschenkt. Grundlegende Ausführungen finden sich in der einschlägigen Kommentarliteratur[43] sowie in Beiträgen, die vor allem einen Überblick über die neuen Aktualisierungspflichten verschaffen.[44] Daneben finden sich auch einige Abhandlungen, welche die Aktualisierungspflichten im systematischen Gesamtzusammenhang analysieren[45] oder im Hinblick auf einen konkreten Aspekt, beispielsweise die Beweislastumkehr gem. § 477 BGB, beleuchten.[46] Auch wird von einigen Beiträgen das Thema der IT-Sicherheitsaktualisierungen bei Softwareprodukten im Rahmen eines Kaufvertrags behandelt.[47] Unter anderem werden dabei Vorschläge zum vertragsrechtlich (objektiv) geschuldeten IT-Sicherheitsniveau unterbreitet,[48] Überlegungen zur Art der geschuldeten IT-Sicherheitsaktualisierungen angestellt[49] sowie IT-Sicherheitsaktualisierungen im Rahmen von Miet- und Kaufmodellen gegenübergestellt.[50] Zudem existieren bereits

43 Zur unionsrechtlichen Ebene: Schulze/Staudenmayer/*Staudenmayer/Bertelmann*, EU Digital Law, Art. 7 SGD Rn. 83 ff.; Schulze/Staudenmayer/*Staudenmayer*, EU Digital Law, Art. 8 DCD Rn. 110 ff.; zur nationalen Ebene exemplarisch: BeckOK BGB/*Faust*, 2025, § 475b BGB Rn. 1 ff.; BeckOGK BGB/*Fries*, § 327f BGB Rn. 1 ff.; MüKoBGB/*Lorenz*, 2024, § 475b BGB Rn. 1 ff.; MüKoBGB/*Metzger*, § 327f BGB Rn. 1 ff.

44 Exemplarisch *Wendehorst*, in: Stabentheiner/Wendehorst/Zöchling-Jud, Das neue europäische Gewährleistungsrecht, 111; *Bach*, NJW 2019, 1705 (1707); *Spindler/Sein*, MMR 2019, 488 (489); *Spindler*, MMR 2021, 451 (455 f.).

45 Insbesondere Schmidt-Kessel/Kramme/*Schmidt-Kessel*, Hdb Verbraucherrecht, Kapitel 14 Rn. 123 ff.; Schreiber/*Schreiber/Esser*, Digitale Angebote, § 5 III. Rn. 51 ff.; *Brießmann,* Bereitstellung digitaler Produkte, S. 106 ff., S. 188 ff.; *Jung/Rolsing*, Die Bereitstellung digitaler Produkte, S. 17 ff.; S. 51 ff., S. 75 ff., S. 98 ff.; *Martens,* Schuldrechtsdigitalisierung, Rn. 258 ff.; *Staudinger/Artz*, Neues Kaufrecht und Verträge über digitale Inhalte, Rn. 147 ff., Rn. 168 ff.; *Bergmann*, FS Martinek, 21 (36 ff.); *Jung/Rolsing*, ZfDR 2023, 399; *Leithäuser*, RDi 2023, 274.

46 Zur Beweislastumkehr nach § 477 BGB im Kontext der Aktualisierungspflicht gem. § 475b Abs. 4 Nr. 2 BGB *Lang/Rösch*, CR 2024, 477.

47 Insbesondere Kipker/*Gaden*, Hdb Cybersecurity, Kapitel 20.3 Rn. 1 ff.; *Riehm/Leithäuser/Brenner*, in: Raue, Digitale Resilienz: Effektives Recht auf sichere Software, 5 (12 ff.); *Braun*, CR 2022, 727; *Kipker/Walkusz*, RDi 2021, 30; *Klett/Gehrmann*, MMR 2022, 435; *Schmidt-Kessel*, ZfPC 2022, 117.

48 *Riehm/Leithäuser/Brenner*, in: Raue, Digitale Resilienz: Effektives Recht auf sichere Software, 5 (15 ff.); *Klett/Gehrmann*, MMR 2022, 435 (437).

49 S. *Riehm/Leithäuser/Brenner*, in: Raue, Digitale Resilienz: Effektives Recht auf sichere Software, 5 (22) zu geschuldeten IT-Sicherheitsaktualisierungen in Abgrenzung zur Behebung von IT-Sicherheitslücken im Rahmen der Nacherfüllung gem. §§ 327l Abs. 1, 439 Abs. 1 BGB; s. *Braun*, CR 2022, 727 (730) zu möglichen Erheblichkeitsschwellen.

50 *Riehm/Leithäuser/Brenner*, in: Raue, Digitale Resilienz: Effektives Recht auf sichere Software, 5 (21 ff.).

Monographien von *Fida* und *Manhardt*, welche sich primär mit den Aktualisierungspflichten beschäftigen.[51] *Fida* nimmt dabei vornehmlich eine umfassende Darstellung der Richtlinienvorgaben sowie ihrer Umsetzung in das österreichische Gewährleistungsrecht vor. *Manhardt* nähert sich der Aktualisierungspflicht gem. § 475b Abs. 4 Nr. 2 BGB unter einem systematisch-dogmatischen Blickwinkel und untersucht insbesondere, wie sie sich systematisch in die kaufvertragsrechtlichen Regelungen einfügt.[52] Er kommt dabei allerdings zu einem anderen Ergebnis mit Blick auf die systematische Einordnung der Aktualisierungspflicht als diese Arbeit und lässt weitere dogmatische Aspekte, die im Zusammenhang mit der Aktualisierungspflicht relevant sind, unbeantwortet.

Insgesamt verbleiben Forschungslücken mit Blick auf den Untersuchungsgegenstand der Arbeit. So versucht die vorliegende Arbeit erstmalig, die IT-Sicherheitsprobleme, welche die infragestehenden IT-Sicherheitsaktualisierungen erst erforderlich machen, darzustellen und insbesondere zu kategorisieren. Ferner wird erstmalig eingehend analysiert, welches IT-Sicherheitsniveau bei smarten Produkten Teil der objektiven Vertragsmäßigkeit gem. § 434 Abs. 3 BGB ist und davon ausgehend, in welchem Umfang IT-Sicherheitsaktualisierungen bei smarten Produkten nach § 475b Abs. 4 Nr. 2 BGB geschuldet werden. Überdies kommt die vorliegende Arbeit zu bisher noch nicht vertretenen dogmatischen Einordnungen im Kontext der Aktualisierungspflicht gem. § 475b Abs. 4 Nr. 2 BGB – insbesondere bei der Frage, wie sich eine notwendige dynamische Weiterentwicklung von Vertragsmäßigkeitsanforderungen systematisch in das System des kaufrechtlichen Mangelgewährleistungsrechts einfügt. Diese Einordnungen ermöglichen, die weiteren Facetten der Aktualisierungspflicht sowie ihre Durchsetzbarkeit dogmatisch konsequent und abgestimmt auf das Gesamtsystem der kaufvertraglichen Regelungen zu erfassen und umfassend zu erörtern.

## IV. Gang der Darstellung

Die Arbeit beginnt mit einer Darstellung technischer Grundlagen zu IT-Sicherheitsaktualisierungen bei smarten Produkten in Kapitel B., um das erforderliche Grundverständnis für die rechtliche Analyse der Aktualisie-

51 *Fida*, Updates, Patches & Co; *Manhardt,* Aktualisierungspflicht.
52 *Manhardt,* Aktualisierungspflicht, S. 105 ff.; *Manhardt*, JZ 2024, 394.

rungspflicht nach § 475b Abs. 4 Nr. 2 BGB im Hinblick auf IT-Sicherheitsaktualisierungen zu setzen.

Anschließend geht die Arbeit in Kapitel C. über zur rechtlichen Untersuchung, indem der dauerhafte Erwerb eines smarten Produkts unter Berücksichtigung der notwendigen IT-Sicherheitsaktualisierungen vertragsrechtlich eingeordnet wird. Dies legt den Grundstein für die weitere rechtliche Analyse. Während nur ein kurzer Blick auf die unsichere Ausgangssituation vor Umsetzung der WK-RL und der DI-RL geworfen wird, steht hier die Frage im Fokus, ob auf den Kauf eines smarten Produkts die §§ 475b ff. BGB oder die §§ 327 ff. BGB anzuwenden sind.

Den Schwerpunkt der Arbeit stellt sodann Kapitel D. dar, in welchem die Aktualisierungspflicht gem. § 475b Abs. 4 Nr. 2 BGB umfassend analysiert wird. Den Einstieg in diese Analyse bildet eine systematische Einordnung der Aktualisierungspflicht innerhalb des Kaufvertragsrechts. Daran anknüpfend werden die Kernelemente der Aktualisierungspflicht beleuchtet, die sich aus dem Umfang der geschuldeten Aktualisierungen, der geschuldeten Bereitstellung und Informierung sowie dem Aktualisierungszeitraum zusammensetzen. Ein besonderes Augenmerk wird dabei auf die dogmatische Einordnung des „Erhalts der Vertragsmäßigkeit" im Zusammenhang mit dem Umfang der geschuldeten Aktualisierungen geworfen. Auf den Kernelementen aufbauend werden schließlich potenzielle Gestaltungsmöglichkeiten des Verkäufers evaluiert sowie die möglichen Beweislastregelungen betrachtet.

In Kapitel E. wird im Anschluss erarbeitet, inwiefern die Aktualisierungspflicht gem. § 475b Abs. 4 Nr. 2 BGB zu einem Anspruch des Käufers auf IT-Sicherheitsaktualisierungen im Rahmen der Nacherfüllung führen kann.

Hinsichtlich beider aufgestellter Thesen – zur Funktions- und Wirkungsweise der Aktualisierungspflicht aus praktischer Sicht auf der einen Seite und zur Dogmatik der Aktualisierungspflicht im Gesamtsystem des Kaufvertragsrechts auf der anderen Seite – werden die Erkenntnisse nicht an einer bestimmten, sondern an vielen Stellen im Verlauf der Untersuchung gewonnen. Demnach ist ihnen nicht jeweils ein eigenes bzw. ausdrückliches Kapitel gewidmet; vielmehr werden sie am Ende der Arbeit ausgehend von den Untersuchungsergebnissen zusammengeführt.

Die Arbeit schließt folglich mit einer Zusammenfassung der Untersuchungsergebnisse und einem Fazit in Kapitel F. Die Untersuchungsergebnisse ermöglichen es dabei, die aufgestellten Thesen abschließend zu bewerten.

# B. Technische Grundlagen zu IT-Sicherheitsaktualisierungen bei smarten Produkten

Zunächst wird erläutert, was ein smartes Produkt ausmacht. Im Anschluss wird gezeigt, weshalb IT-Sicherheitsaktualisierungen bei smarten Produkten notwendig sind. Der Teil schließt mit einer Darstellung der bei Herstellung, Vertrieb und Aktualisierung smarter Produkte typischerweise beteiligten Akteure.

## I. Smarte Produkte

Sowohl in der Rechtsliteratur als auch in der Literatur aus der Informatik existiert kein einheitliches Verständnis des Begriffs „smartes Produkt". Abweichungen ergeben sich vornehmlich bei der Frage, was ein Produkt genau „smart" werden lässt. Im Folgenden wird zunächst das in dieser Arbeit zugrunde gelegte Begriffsverständnis erläutert. Sodann wird es zum Begriff „künstliche Intelligenz" abgegrenzt, da diese Abgrenzung im Kontext des Begriffsverständnisses die bedeutendste ist. Schließlich werden klassische Anwendungen smarter Produkte im Smart Home dargestellt.

### 1. Charakteristische Merkmale im Überblick

Die Basis eines smarten Produkts bildet stets die körperliche Ware. „Smart" wird diese Ware nach dem dieser Arbeit zugrunde gelegten Begriffsverständnis sodann durch verschiedene, mit ihr verbundene Softwareelemente. Zu diesen zählt zunächst die in die Ware integrierte Software. Ferner gehören ausgelagerte, über das Internet verbundene Softwareelemente dazu, namentlich ein Backend-Server und eine Steuerungs-App.

Dieses Begriffsverständnis entspricht einem vor allem in der Rechtsliteratur dargelegten Verständnis von Produkten, die Teil des „Internets der Dinge" (auch „Internet of Things" oder kurz „IoT") sind.[53] Regelmäßig

53 S. dazu *Firsching,* Vertragsstrukturen IoT-Produkte, S. 21 f.; *Wendehorst,* Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet

werden die Bezeichnungen als smartes Produkt oder als „IoT-Produkt" auch synonym verwendet.[54] Zudem werden smarte Produkte aufgrund der Zusammensetzung aus mehreren verschiedenen Elementen auch als „hybride Produkte" beschrieben.[55]

### a) Körperliche Ware

Die körperliche Ware eines smarten Produkts ähnelt vom äußeren Erscheinungsbild in vielen Fällen rein analogen Waren.[56] Bekannt als smarte Produkte sind beispielsweise Kraftfahrzeuge,[57] Kühlschränke,[58] Staubsauger,[59] Überwachungskameras[60] oder Uhren,[61] welche es allesamt auch in einer ähnlichen analogen Form gibt oder gab. Teilweise weicht das äußere Erscheinungsbild eines smarten Produkts aber auch vom analogen Pendant ab. Das ist z.B. der Fall bei einem smarten Türschloss, dessen körperlicher Warenbestandteil dem eigentlichen analogen Türschloss übergesetzt wird.[62]

Zudem hat es auch auf die körperlichen Warenbestandteile Einfluss, dass in eine solche Ware Softwareelemente integriert sind bzw. sie mit solchen verbunden ist. So wird zum einen Software nicht isoliert in die Ware

---

der Dinge, S. 2; *Grünberger*, AcP 2018, 213 (285 f.); *Heydn*, MMR 2020, 503 (503). Zum Ursprung des Begriffs s. Bräutigam/Kraul/*Bräutigam*, Hdb IoT, 1. Teil § 1 Rn. 5; Bräutigam/Rücker/*Dienst/Falke*, Hdb E-Commerce, 14. Teil A. Rn. 2.

54 Exemplarisch *Firsching,* Vertragsstrukturen IoT-Produkte, S. 21; *Wendehorst*, in: Wendehorst/Zöchling-Jud, Ein neues Vertragsrecht für den digitalen Binnenmarkt?, 45 (48); *Firsching*, ZUM 2021, 210 (211); *Grünberger*, AcP 2018, 213 (285); ähnlich *Pardo/Ivens/Pagani*, Industrial Market Management 2020, 205 (205 f.); ausführlich *Felk,* Kaufrechtliche Mängelgewährleistung smarter Produkte, S. 49 ff.

55 *Grünberger*, AcP 2018, 213 (285).

56 *Firsching,* Vertragsstrukturen IoT-Produkte, S. 22.

57 Klassisches Beispiel sind die Fahrzeuge von Tesla, etwa das Tesla Model 3, https://www.tesla.com/de_de/model3 (zuletzt abgerufen am 28.4.2025).

58 S. beispielsweise https://www.samsung.com/de/refrigerators/my-refrigerators/?productl=rs6ga852lb1/eg&product2=rs6ga853ls9/eg&product3=rs6ja8810s9/eg#food-cam (zuletzt abgerufen am 28.4.2025).

59 S. beispielsweise https://www.ecovacs.com/de/deebot-robotic-vacuum-cleaner/deebot-t50-max-pro-omni-white?utm_source=google&utm_campaign=pmax&gad_source=1&gclid=EAIaIQobChMIkcio-si3jAMV5JODBx0zJxAzEAAYASAAEgJtPfD_BwE (zuletzt abgerufen am 28.4.2025).

60 S. beispielsweise https://www.philips-hue.com/de-de/p/hue-secure-kamera-schwarz-kabellos/8719514492776 (zuletzt abgerufen am 28.4.2025).

61 S. beispielsweise https://www.apple.com/de/watch/ (zuletzt abgerufen am 28.4.2025).

62 S. beispielsweise https://nuki.io/de-de?srsltid=AfmBOoobDCOpO2r0v8pfolLDnz9gjPYzBVWo2TDZWOUMBOeurgCnSz40 (zuletzt abgerufen am 28.4.2025).