

Product Compliance

Raphael Brenner

Die Produktbeobachtungspflicht im digitalen Zeitalter

Chancen und Herausforderungen für Hersteller



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 4

Raphael Brenner

Die Produktbeobachtungspflicht im digitalen Zeitalter

Chancen und Herausforderungen für Hersteller



Nomos

Die Dissertation entstand im Zuge des vom Bayerischen Staatsministerium für Wissenschaft und Kunst geförderten Forschungsverbundes „Sicherheit in der Alltagsdigitalisierung (ForDaySec)“

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

Zugl.: Passau, Univ., Diss., 2025

1. Auflage 2025

© Der Autor

Publiziert von
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Gesamtherstellung:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN (Print): 978-3-7560-3426-0
ISBN (ePDF): 978-3-7489-6449-0

DOI: <https://doi.org/10.5771/9783748964490>



Onlineversion
Nomos eLibrary



Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung 4.0 International Lizenz.

Vorwort

Die nachfolgende Arbeit wurde im Oktober 2024 als Dissertation bei der juristischen Fakultät der Universität Passau eingereicht. Literatur und Rechtsprechung wurden bis zu diesem Zeitpunkt berücksichtigt.

Mein Dank gilt zunächst meinem Doktorvater *Herrn Professor Dr. Thomas Riehm* für die Betreuung der Arbeit. Während des gesamten Promotionsvorhabens hat er mich stets gefördert und unterstützt und damit maßgeblich zum Gelingen der Arbeit beigetragen. *Herrn Professor Dr. Michael Beurskens* danke ich für die zügige Erstellung des Zweitgutachtens.

Die Arbeit entstand im Zuge des vom Bayerischen Staatsministerium für Wissenschaft und Kunst geförderten Forschungsverbundes „Sicherheit in der Altagsdigitalisierung (ForDaySec)“.

In diesem Zusammenhang möchte ich auch meinen Kollegen des Forschungsverbunds danken. Dies gilt zum einen für die Kollegen aus der Wissenschaft, die mit ihrem Blick aus der Informatik oder Soziologie dazu beigetragen haben, dass die entwickelten Thesen dem Praxistest standhalten. Dadurch wurde die Arbeit an zahlreichen Stellen bereichert. Dies gilt zum anderen aber auch für die Kollegen aus der Geschäftsstelle, die bei organisatorischen Themen mit Rat und Tat zur Seite standen.

Weiter möchte ich meinem Kollegen aus dem Forschungsverbund und Lehrstuhlkollegen *Malte Leithäuser* für den fachlichen und persönlichen Austausch während des gesamten Promotionsvorhabens danken. *Felix Richter* danke ich für die Korrekturlektüre der Dissertation.

Ganz besonders möchte ich meiner Familie, meinem Bruder *Manuel Brenner*, meiner Mama *Ingrid Brenner* und meinem Papa *Markus Brenner* danken. Mein Bruder stand mir als Informatiker stets geduldig bei der Beantwortung technischer Fragen zur Seite. Meine Eltern haben mich bereits während der Zeit des Studiums und nun auch während der Dissertation bedingungslos unterstützt. Ohne sie wäre ich nicht da, wo ich heute bin. Mein Papa konnte die Fertigstellung der Dissertation leider nicht mehr erleben, wäre nun aber mit Sicherheit unheimlich stolz. Ihm sei diese Arbeit gewidmet.

Inhaltsverzeichnis

A. Problemstellung und Gang der Untersuchung	19
I. Smarte Produkte – smarte Gefahren	19
II. Unsicherheiten smarter Produkte nach der Inverkehrgabe	22
1. Integration von Software in physische Produkte	22
2. Komplexitäten bei Softwareprodukten	24
III. Gang der Untersuchung	27
B. Die Produktbeobachtungspflicht in der Produkthaftung	31
I. Die Produktbeobachtungspflicht als Verkehrspflicht des Herstellers	31
1. Die Sorgfaltspflichtverletzung als Anknüpfungspunkt der Haftung	32
2. Bedeutung der Verkehrspflichten	33
a) Begründung von Verkehrspflichten	33
b) Umfang der Verkehrspflichten	35
aa) Erforderlichkeit von Sicherungsmaßnahmen	37
bb) Zumutbarkeit von Sicherungsmaßnahmen	38
3. Pflichtenbereiche des Herstellers	39
a) Inverkehrbringen als Zäsur	40
b) Haftungserweiterung für Zeitraum ab dem Inverkehrbringen	42
4. Der Produktbeobachtungsfehler	45
II. Exkurs: Die weiteren Herstellerpflichten im Überblick	47
1. Das Verhältnis von Produzentenhaftung und ProdHaftG	48
2. Der Konstruktionsfehler	50
a) Erforderlichkeit	50
b) Zumutbarkeit	53
3. Der Fabrikationsfehler	54
4. Der Instruktionsfehler	56
5. Der Entwicklungsfehler	59
6. Die Entwicklungslücke	62
7. Keine Produktbeobachtungspflicht nach dem ProdHaftG	64

III. Fazit zum Produktrecht	66
C. Smarte Produkte im Anwendungsbereich der Produktbeobachtungspflicht	69
I. Technikneutrale Ausgestaltung der deliktischen Produzentenhaftung	69
II. Die Bedeutung technischen Fortschritts für die Produktbeobachtungspflicht	71
1. Fehlerhaftigkeit bei Inverkehrgabe	71
2. Verschleiß	72
3. Entwicklungslücken und „Produktalterung“	73
a) Abgrenzung	74
b) Keine Fehlerhaftigkeit durch spätere Produktverbesserung	74
c) Abgrenzung der Verantwortungsbereiche	76
aa) Vergleichsüberlegung: Kombinationsgefahren	76
bb) Vergleichsüberlegung: Fehlgebrauch	79
cc) Verantwortungsbereich und eigene Verkehrssicherungspflichten des Nutzers	80
d) OLG München zur Produktverbesserung	82
e) Anwendung auf die Entwicklungslücke	83
f) Anwendung auf die „Produktalterung“	86
g) Fazit	89
III. Haftungsrechtliche Relevanz der kritischen Eigenschaften smarter Produkte für die Produktbeobachtungspflicht	90
1. (Un)vermeidbarkeit von Softwarefehlern	90
a) Tatsächliche Herausforderung	90
b) Softwarefehler als rechtliche Kategorie	92
aa) Softwarefehler als produkthaftungsrechtlich relevanter Fehler	93
bb) Ableitungen aus dem vertraglichen Mangelbegriff	94
cc) Maßgeblichkeit der berechtigten Verkehrserwartung	95
dd) Entwicklungsfehler	97
c) Bedeutung für die Produktbeobachtung	99
2. Digitale Resilienz	100
a) Tatsächliche Herausforderung	100

b) IT-Sicherheit als Element des produkthaftungsrechtlichen Fehlerbegriffs	101
c) Status Quo der gesetzlichen Lage in Deutschland	102
d) IT- Sicherheit im Rahmen der Produzentenhaftung	104
aa) Schutzzumfang des Haftungsrechts bei Cyberangriffen	105
bb) Reichweite der Herstellerverantwortung bei Cyberangriffen	108
(1) Sicherungsmaßnahmen bei Produktfehlgebrauch und Produktmissbrauch	109
(2) Sicherungsmaßnahmen bei Fehlverhalten Dritter	111
α) Allgemeines Deliktsrecht	111
β) Übertragung auf die Produkthaftung am Beispiel der Produktsabotage	113
(3) Übertragung auf Cyberangriffe	116
α) Ausnutzen einer Sicherheitslücke	117
i) Besondere Gefahrenlage und nicht lediglich äußerer Zusammenhang	117
ii) Umfang der zu gewährleistenden IT- Sicherheit	120
iii) Haftungsrelevante Konstellationen	122
β) Social Engineering-Angriff	124
i) Besondere Gefahrenlage	124
ii) Umfang der zu gewährleistenden IT- Sicherheit	124
γ) DDoS-Angriff	126
e) Künftige normative Berücksichtigung der Cybersicherheit	126
f) Bedeutung für die Produktbeobachtung	130
3. Vernetzung	132
a) Tatsächliche Herausforderung	132
b) Haftungsrechtliche Einordnung eines zunehmenden „Unbundlings“	133
c) Kombinationsgefahren	135
aa) Betrachtung des Zubehörbegriffs	136
bb) Einheitliche Herstellung	137
cc) Zulieferkomponenten	138

dd) Bereitstellung durch Drittanbieter	139
(1) Eigener App-Store	140
α) Einflussnahmemöglichkeit und entgegengebrachtes Vertrauen	140
β) Keine Privilegierung nach TMG	141
(2) Schnittstellenzugang	143
α) Fehlende Einflussnahmemöglichkeit	143
β) Übertragung der Honda-Rechtsprechung	144
ee) Zwischenfazit Kombinationsgefahren	147
d) Fehlervermittelte Gefahren	148
aa) Konstellationen der fehlervermittelten Gefahren	149
bb) Geschlossene Systeme	150
cc) Offene Systeme	152
(1) Keine Übertragung der Honda-Rechtsprechung	153
(2) Konstruktive Sicherheitsmaßnahmen bei Systemstörungen	155
e) Bedeutung für die Produktbeobachtung	156
4. KI und Autonomie	159
a) Begriff und Bedeutungsgehalt	159
b) Eingeschränkte Vorhersehbarkeit	164
c) Fehlende Nachvollziehbarkeit	166
d) Haftungsrechtliche Einordnung	166
aa) Keine Pflichtwidrigkeit durch Inverkehrgabe	167
bb) Fehlerhaftigkeit bei Inverkehrgabe	169
cc) Entwicklungsfehler	171
dd) Entwicklungslücke	173
(1) Keine Haftung für das Autonomierisiko nach § 823 Abs. 1 BGB	173
(2) Mögliche Haftung für das Autonomierisiko nach dem ProdHaftG	174
e) Bedeutung für die Produktbeobachtung	177
IV. Fazit zur Produktbeobachtungspflicht bei smarten Produkten	178

D. Verantwortung des Herstellers bei zunehmender Datenverfügbarkeit	181
I. Passive Produktbeobachtungspflicht	182
1. Bedeutung der öffentlich-rechtlichen Produktbeobachtungspflicht	182
a) Errichtung eines Risikomanagementsystems, § 6 Abs. 2 ProdSG	182
b) Öffentlich-rechtliche Produktbeobachtungspflicht, § 6 Abs. 3 ProdSG	183
c) Auswirkungen auf die zivilrechtliche Produktbeobachtungspflicht	184
aa) Bedeutung des New-Approach	184
bb) Gegenläufige Entscheidung des OLG Düsseldorf bzgl. der Produktbeobachtung	186
2. Produzentenhaftungsrechtlicher Pflichtenkreis	187
II. Aktive Produktbeobachtungspflicht	189
III. Social-Media-Monitoring	190
1. Neue Kommunikationswege	190
2. Entwicklung falscher Sicherheitserwartungen	191
a) Selbst generierter Content	191
b) Nutzergenerierter Content	192
3. Meldungen von Produktgefahren	194
a) Eigene Social-Media-Präsenz des Herstellers	194
b) Sonstige öffentlich zugängliche Social-Media-Kanäle	196
aa) Geeignetheit zur Gewinnung sicherheitsrelevanter Erkenntnisse	196
bb) Erwägungen der Erforderlichkeit	198
cc) Erwägungen der Zumutbarkeit	200
dd) Sorgfältige Prüfung des Verschuldens	201
IV. Auswertung von Sensor-Daten	202
1. Potential der Auswertung von Sensor-Daten	202
2. Pflicht zur Auswertung bereits erhobener Sensor-Daten	204
a) Datenkategorien und Datenübermittlung	205
b) „Erhobene“ Daten im Rahmen der passiven Produktbeobachtung	206

3. Pflicht zur Erhebung und Übermittlung von angefallenen Sensor-Daten	208
a) Weiterentwicklung der aktiven Produktbeobachtung	209
aa) Herkömmliche Reichweite der aktiven Produktbeobachtungspflicht	209
(1) Durchführung von Stichproben	209
(2) Generierung neuer wissenschaftlicher Erkenntnisse	211
bb) Bedeutung für die Erhebung von Sensor-Daten	214
b) Allgemeine Erwägungen der Zumutbarkeit	215
aa) Übergang zum Äquivalenzinteresse	216
bb) Endlose Flut theoretisch verfügbarer Daten	216
cc) Stichprobenerhebung sicherheitsrelevanter Daten	218
dd) Integrierte Produktbeobachtung	218
ee) Zwischenfazit	219
c) Individuelle Erwägungen der Zumutbarkeit	220
d) Beispiel Automotiv-Sektor und selbstlernende KI-Systeme	221
4. Beweislastverteilung unter Berücksichtigung des Data Acts	223
V. Aspekte des Datenschutzes	225
1. Anwendbarkeit des Datenschutzrechts – Personenbezug	226
a) Abgrenzung zum reinen Sachdatum	226
b) Bestimmbarkeit einer natürlichen Person	227
aa) Identifikatoren	228
bb) Berücksichtigung von Zusatzwissen	229
cc) Auswirkungen von Big Data	231
c) Fazit	232
2. Rechtmäßigkeit der Datenverarbeitung	233
a) Einwilligung	233
b) Erfüllung eines Vertrags	234
c) Rechtliche Verpflichtung	235
d) Wahrung lebenswichtiger Interessen	236
e) Berechtigtes Interesse – Interessenabwägung	237
f) Fazit	239
3. Bedeutung der E-Privacy-RL und des TTDSG	240
a) Anwendungsbereich und Verhältnis zur DS-GVO	240
b) Auslegung der Rechtfertigungsgründe des § 25 Abs. 2 TTDSG	241

4. Bedeutung des Data Acts	244
VI. Fazit zur Herstellerverantwortung bei zunehmender Datenverfügbarkeit	244
E. Smarte Reaktionspflichten des Herstellers	247
I. Bedeutung der Reaktionspflichten	247
II. Herkömmliche Reaktionspflichten	248
1. Ausgangspunkt: Pflegebetten-Entscheidung des BGH	249
2. Effektivität der Gefahrenabwehr als Maxime	250
3. Verhältnis von Warnung und Rückruf	252
a) Ausgangslage	252
b) Fallgruppen einer Rückrufflicht	253
aa) Warnung nicht ausreichend zur Gefahreinschätzung und Verhaltensanpassung	253
bb) Hinwegsetzen über eine Warnung	256
(1) Drittgefährdung als zentrale Voraussetzung	256
(2) Übereinstimmung mit Systematik des Produkthaftungsrechts	259
α) Vergleich mit Instruktionspflicht	259
β) Objektiv zu bestimmende Sorgfaltsanforderungen	262
(3) „Grund zu der Annahme“	263
α) Verkennung der Produktgefahr	264
β) Unzumutbare Gefahrensteuerung	265
4. Ausgestaltung der Rückrufflicht	267
a) Abgrenzung des Äquivalenz- vom Integritätsinteresse	268
b) Relevante Kriterien des Einzelfalls	270
aa) Eigene Pflichten des Nutzers zum Schutz Dritter	271
(1) Indizwirkung bei kodifizierten Pflichten	272
(2) Bedeutung der Adressatenkreise	273
bb) Identifizierbarkeit der Produktnutzer	274
(1) Bedeutung des marktüberwachungsrechtlichen Tätigwerdens	275
(2) Geringe Bedeutungskraft des Kriteriums	276
cc) Fehlertypen	277
dd) Gefährlichkeit	279
5. Kostentragung	281
a) Effektivität der Gefahrenabwehr als Maxime	281

b)	Bedeutung für die Fallgruppen der Rückrufflicht	283
c)	Weitere Differenzierungsansätze	284
6.	Bedeutung der Boston Scientific-Entscheidung	285
a)	Berücksichtigung der Pflegebetten-Entscheidung	286
b)	Argumentationslinien des EuGH	287
c)	Bewertung der Boston Scientific-Entscheidung	288
III.	Smarte Reaktionspflichten	289
1.	Updatepflichten	290
a)	Gefahrenabwehr durch Updates	290
b)	Verhältnis von Warnung und Updates	292
aa)	Geeignetheit der Warnung	293
bb)	Warnung nicht ausreichend zur Gefahrenereinschätzung und Verhaltensanpassung	295
cc)	Hinwegsetzen über eine Warnung	296
(1)	Verkennung der Produktgefahr bei Sicherheitslücken	297
(2)	Unzumutbarkeit der Gefahrensteuerung jenseits von Sicherheitslücken und bei CPS	299
α)	Angewiesenheit auf den Hersteller	299
β)	Angewiesenheit auf das Produkt	300
γ)	Erhöhte Einflussmöglichkeit des Herstellers	302
dd)	Identifizierbarkeit der Produktnutzer	304
c)	Fazit	305
2.	Ausgestaltung der Updatepflicht	305
a)	Bedeutung der vertraglichen Aktualisierungspflicht aus § 327f BGB	305
b)	Abgrenzung zwischen Äquivalenz- und Integritätsinteresse	306
c)	Effektivität der Gefahrenabwehr als Maxime	308
aa)	Aufgedrängte Sicherheitsbereicherung als Rechtseingriff	309
(1)	Schutz des softwarebasierten Gebrauchs	310
(2)	Schutz des netzbasierten Gebrauchs	311
α)	Parallele zur Versorgungssperre	311
β)	Bedeutung des Entzugs des gebrauchsnotwendigen Netzzugangs	312
(3)	Zwischenfazit	315

bb) Interessenlage im Rahmen der aufgedrängten Sicherheitsbereicherung	315
cc) Schuldvertragliche Gestattung der aufgedrängten Sicherheitsbereicherung	316
(1) Vertragsverhältnis zwischen Hersteller und Eigentümer	317
(2) AGB-Kontrolle	318
α) Fernstilllegung als überraschende Klausel	318
β) Unangemessene Benachteiligung bei funktionsändernden Updates	319
γ) Abweichung vom gesetzlichen Leitbild bei fehlerbehebenden Updates	321
dd) Rechtmäßigkeit aufgrund Einwilligung	322
(1) Voreingestellter Opt-out-Mechanismus	322
α) Konkludente Einwilligung in Datenveränderung	322
β) Keine konkludente Einwilligung in Nutzungsbeeinträchtigung	323
γ) Konkludente Einwilligung in Funktionsänderungen	324
(2) Aufrechterhaltung der Schnittstellenkonnektivität	326
(3) Ausdrückliche Einwilligung	326
ee) Zwischenfazit	327
ff) Weitere gesetzliche Rechtfertigungsgründe	327
(1) Nothilfe, gem. § 227 BGB	327
(2) Defensivnotstand, gem. § 228 S. 1 BGB	329
α) Notstandslage	329
β) Erforderlichkeit der Maßnahme	331
γ) Verhältnismäßigkeit der Maßnahme	333
δ) Drohender Schadensersatzanspruch nach § 228 S. 2 BGB	334
d) Bedeutung für die Effektivität der Gefahrenabwehr und Ausgestaltung der Updatepflicht	335
e) Zumutbarkeitsgesichtspunkte	336
f) Fazit	340
3. Kostentragungspflicht bei Sicherheitsupdates	340
4. Weitere gesetzliche Updatepflichten und deren Bedeutung	342
a) Bedeutung des ProdSG	342

b)	Künftige Bedeutung der GPSR	344
aa)	Das neue Recht auf Abhilfe nach Art. 37 GPSR	345
bb)	Bedeutung für die zivilrechtliche Produktbeobachtungspflicht	346
c)	Bedeutung des Marktüberwachungsrechts	349
aa)	Grundlagen der Marktüberwachung	349
bb)	Anordnungsbefugnis bzgl. Updates	351
d)	Künftige Bedeutung der KI-VO	355
e)	Künftige Bedeutung des CRA	355
aa)	Schwachstellenmanagement und Sicherheitsaktualisierungen	356
bb)	Bedeutung für die zivilrechtliche Produktbeobachtungspflicht	357
f)	Künftige Bedeutung der neuen Produkthaftungsrichtlinie	358
aa)	Zeitliche Dynamisierung des Fehlerbegriffs	358
bb)	Verengte Entlastungsgründe und produkthaftungsrechtliche Updatepflicht	359
g)	Fazit	361
5.	Updateansprüche	362
a)	Praxisrelevanz	363
b)	Rückrufanspruch aufgrund des deliktsrechtlichen Beseitigungsanspruchs nach §§ 823 Abs. 1, 249 S. 1 BGB	365
c)	Rückrufanspruch nach 1004 Abs. 1 BGB (analog)	367
aa)	Anwendbarkeit des Unterlassungsanspruchs	368
bb)	Tatbestandsmäßigkeit des Unterlassungsanspruchs	371
(1)	Konkrete Gefahr	371
α)	Inhaltliche Konkretisierung	371
β)	Personelle Konkretisierung	372
(2)	Hersteller als Störer	373
α)	Allgemeine Erwägungen	373
β)	Bedeutung für die individuellen Gefahrenabwehransprüche	374
d)	Fazit	376
e)	Bedeutung des Rechts auf Reparatur	377
IV.	Fazit zu den smarten Reaktionspflichten des Herstellers	378

F. Dauer der Produktbeobachtungspflicht	381
I. Fehlen eines zeitlich starren Rahmens	381
1. Abschwächung der Produktbeobachtungspflicht	382
2. Besonderheiten bei smarten Produkten	382
II. Differenzierung zwischen Beobachtung und Reaktion	383
1. Abschwächung der Rückrufpflicht zur Warnpflicht	383
2. Maßgeblicher Zeitpunkt der Abschwächung der Rückrufpflicht	384
a) Einstellung der Weiterentwicklung und des Vertriebs des Produkts	384
b) Erwartete maximale Lebensdauer eines Produkts	385
c) Fristen nach anderen Vorschriften	387
III. Fazit	388
G. Zusammenfassung	391
H. Literaturverzeichnis	403

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 allerdings 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 Schadensszenarien. 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/Stege (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 Burrel, 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 durchgängig¹⁶ 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 Daten²⁴ 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/Seeleemann (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/Seeleemann (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 Gefährlichkeit³⁸ 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 Schnellebigkeit 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 bekannt⁴⁰ 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 Schnellebigkeit 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 geschädigten 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 herstellereits 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 Ebene⁵² 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.

B. Die Produktbeobachtungspflicht in der Produkthaftung

In folgendem Kapitel sollen die juristischen Grundlagen für die nachfolgende Darstellung der Produktbeobachtungspflicht im digitalen Zeitalter dargestellt werden. Die Produktbeobachtungspflicht lässt sich dem Produktrecht zuordnen. Das Produktrecht selbst fußt auf drei Säulen. Hierzu gehören das dem öffentlichen Recht zuzuordnende behördliche Produktsicherheitsrecht, die zivilrechtliche Produzenten- und Produkthaftung sowie die strafrechtliche Produktverantwortung. Das Produktrecht stellt demnach eine Querschnittsmaterie dar, welche naturgemäß Interdependenzen zwischen den einzelnen Teildisziplinen aufweist. In all diesen Teilbereichen kommt auch der Produktbeobachtung – freilich mit unterschiedlicher Akzentuierung – Bedeutung zu. Ausgehend von der zivilrechtlichen Produktbeobachtungspflicht im Rahmen des Produkthaftungsrechts wird im Laufe der Arbeit daher auch auf mögliche Implikationen insbesondere aus dem öffentlich-rechtlichen Produktrecht einzugehen sein.

Unter Produkthaftung wird die zivilrechtliche Einstandspflicht für Schäden aufgrund der Benutzung fehlerhafter Produkte verstanden. Dem deutschen Recht liegt dabei eine zweispurige Betrachtungsweise zu Grunde. Zu unterscheiden ist die vertragliche und die außervertragliche bzw. deliktische Haftung.⁵³ Letztere unterteilt sich sodann in die Produzentenhaftung nach § 823 Abs. 1 BGB und die Haftung nach dem ProdHaftG⁵⁴. Die Produkthaftung – wie die deliktische Haftung im Allgemeinen – verfolgt das Ziel der Schadenskompensation und des Schadensausgleichs einerseits sowie der Prävention und der Schadensverhütung anderseits.⁵⁵

I. Die Produktbeobachtungspflicht als Verkehrspflicht des Herstellers

Anknüpfungspunkt für die deliktsrechtliche Produktbeobachtungspflicht ist § 823 Abs. 1 BGB. Bei der Norm handelt es sich um die zentrale An-

53 Vgl. Lenz, in: Lenz, Produkthaftung, § 3, Rn. 1 f.; beide Haftungssysteme bestehen nebeneinander und schließen sich nicht aus, vgl. BGH, NJW 1977, 379 (380); BGH, NJW 1992, 1039 (1041); Wagner, in: MüKo, BGB, § 823, Rn. 1035 f.

54 Das ProdHaftG geht auf die Produkthaftungsrichtlinie 85/374/EWG zurück.

55 Ausführlich statt aller m.w.N. Thöne, Autonome Systeme, S. 57 ff.

spruchsgrundlage des nationalen Deliktsrechts und die Grundlage für die Haftung des Warenherstellers.⁵⁶ Terminologisch spricht man von der Produzentenhaftung.⁵⁷

1. Die Sorgfaltspflichtverletzung als Anknüpfungspunkt der Haftung

Der Hersteller ist grundsätzlich gehalten, nur sichere Produkte in den Verkehr zu geben und Produktgefahren möglichst abzuwehren.⁵⁸ Eine Rechtsgutsverletzung, die durch ein gefährliches Produkt hervorgerufen wird, begründet für sich genommen aber noch keine Einstandspflicht des Herstellers nach § 823 Abs. 1 BGB. Denn die Rechtsgutsverletzung kommt nicht durch eine direkte Verletzungshandlung des Herstellers zustande. Vielmehr beruht sie entweder auf einem mittelbaren Tun oder einem Unterlassen des Herstellers, wobei die Verletzung erst durch die Benutzung der Sache eintritt. Den genauen Anknüpfungspunkt der schadensstiftenden Handlung im Rahmen der Produzentenhaftung zu erfassen, erweist sich als schwierig. Einerseits kann auf die gesamte Produktion bzw. den einzelnen Produktionsschritt ohne Berücksichtigung der erforderlichen Sicherheitsmaßnahmen oder die Inverkehrgabe des fehlerhaften Produkts als aktive Handlung abgestellt werden.⁵⁹ Andererseits kann auch darauf abgestellt werden, dass es bei einem Produktionsschritt unterlassen wurde, sicherzustellen, dass von dem Produkt keine Gefahren ausgehen.⁶⁰ Da im Rahmen des Produktionsprozesses die genauen Verhaltensformen verschwimmen, ist eine trennscharfe Abgrenzung nicht möglich.⁶¹ Sie ist aber auch gar nicht

56 Vgl. Piovano/Schucht/Wiebe, Produktbeobachtung in der Digitalisierung, S. 16 f.

57 Zur (nicht zwingenden) Terminologie Müller, Software als „Gegenstand“ der Produkthaftung, S. 38 f.

58 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.

59 So Sprau, in: Grüneberg, BGB, § 823, Rn. 171; Larenz/Canaris, Lehrbuch des Schuldrechts II/2, S. 402; tendenziell ablehnend Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 22, Rn. 2 f. wohl unter Verweis darauf, dass das aktive Tun angesichts des gesamten Herstellungsverfahrens regelmäßig nicht den Schwerpunkt der Vorwerfbarkeit bildet.

60 Vgl. Lenz, in: Lenz, Produkthaftung, § 3, Rn. 186 unter Nennung von Beispielen: Unterlassen der ordnungsgemäßen Beobachtung des Kontrollvorgangs, Unterlassene Erprobung, Unterlassene Warenausgangskontrolle.

61 Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 22, Rn. 2 ff.

nötig, da sowohl bei einer mittelbaren Verletzungshandlung als auch bei einem Unterlassen die Pflichtwidrigkeit des Verhaltens positiv festzustellen ist. Denn in diesen Fällen ist die Rechtswidrigkeit des Verhaltens nicht durch die Rechtsgutsverletzung indiziert, sondern ergibt sich erst durch den Verstoß gegen eine Verkehrspflicht bzw. bei Bestehen einer Pflicht zum Handeln.⁶² Durch die Haftung für entsprechende Sorgfaltspflichtverletzungen soll sichergestellt werden, dass der Hersteller seine Möglichkeiten der Gefahrensteuerung ausschöpft und so dem Interesse der Produktsicherheit gerecht wird.⁶³ Als solche Verkehrspflicht stellt sich auch die Produktbeobachtungspflicht dar.

2. Bedeutung der Verkehrspflichten

a) Begründung von Verkehrspflichten

Verkehrspflichten wurden zunächst außerhalb der Produzentenhaftung entwickelt und waren allgemein mit der Pflicht verbunden, auf die Rechte und Rechtsgüter anderer Rücksicht zu nehmen.⁶⁴ Für das Bestehen einer Verkehrspflicht ist die Möglichkeit der Gefahrensteuerung unabdingbare Voraussetzung.⁶⁵ Fehlt es jemandem schon an dieser, macht es im Interesse der Verkehrssicherheit keinen Sinn, ihm eine entsprechende Verpflichtung aufzuerlegen, da er die Gefahr gar nicht beherrschen kann.⁶⁶ Eine faktische Möglichkeit der Gefahrenbeherrschung begründet aber allein auch noch keine Verkehrspflicht.⁶⁷ Vielmehr bedarf es einer Verantwortlichkeit für die Gefahrenquelle.⁶⁸

62 Looschelders, Schuldrecht BT, § 59, Rn. 3 ff.; Sprau, in: Grüneberg, BGB, § 823, Rn. 25 f.; Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 22, Rn. 4; § 23, Rn. 5 f.; zu diesen zwei Funktion der Verkehrspflichten Hager, in: Staudinger, BGB, § 823, Rn. E 3.

63 So Wagner, in: MüKo, BGB, § 823, Rn. 512.

64 So schon RGZ 52, 373 (373 ff.); zu dieser „Leerformel“ Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 23, Rn. 10.

65 Vgl. BGH, NJW 1954, 1403 (1403).

66 Wagner, in: MüKo, BGB, § 823, Rn. 5.

67 Wagner, in: MüKo, BGB, § 823, Rn. 503; Larenz/Canaris, Lehrbuch des Schuldrechts II/2, S. 412 f.; Voigt, in: BeckOGK, BGB, § 823, Rn. 407; Hager, in: Staudinger, BGB, § 823, Rn. E 25; Förster, in: BeckOK, BGB, § 823, Rn. 302.

68 Wagner, in: MüKo, BGB, § 823, Rn. 503; Förster, in: BeckOK, BGB, § 823, Rn. 303.

Eine entsprechende Verantwortlichkeit ergibt sich für denjenigen, der eine Gefahr im eigenen Einflussbereich schafft oder andauern lässt (sog. Bereichshaftung). Denn er hat für den Zustand seines Bereichs einzustehen,⁶⁹ ohne dass es zur Begründung der Verkehrspflicht auf eine erhöhte Gefahrenlage ankommt.⁷⁰ Dahinter steckt der Gedanke der Zusammengehörigkeit von Verantwortung und Bestimmungsgewalt. Der Inhaber der Bestimmungsgewalt vermag den Vorteil aus der Gefahrenquelle zu ziehen und ist jedenfalls zur Beherrschung der Gefahrenquelle in der Lage.⁷¹ Darüber hinaus vertrauen Personen, die sich im Gefahrenbereich aufhalten, darauf, dass Gefahrenquellen ausreichend gesichert sind.

Daneben begründet auch die Übernahme einer Aufgabe einen Zurechnungsgrund und entsprechende Verantwortlichkeit (sog. Übernahmehaftung). Hier ermöglicht die Übernahme der Aufgabe zunächst, die Gefahr zu beherrschen. Gleichzeitig führt die Übernahme der Aufgabe aber auch dazu, dass sich eigener Selbstschutz verringert und entsprechende Maßnahmen heruntergefahren werden. Hierin liegt die maßgebliche Gefahrenschaffung. Zudem ist damit regelmäßig ein Vertrauen dergestalt verbunden, dass der Übernehmende seine Aufgabe ordentlich erledigen wird.⁷²

Ferner können sich auch aus einem vorangegangenen Tun, ohne dass eine Aufgabe übernommen oder für den Zustand des eigenen Bereiches einzustehen ist, Verkehrspflichten ergeben (teilweise Ingerenz). Da die den übrigen Zurechnungsgründen zugrundeliegenden Erwägungen hier aber keine Rolle spielen, droht eine Konturlosigkeit des Zurechnungsgrunds. Vor diesem Hintergrund muss die geschaffene Gefahr über das allgemeine Lebensrisiko hinausgehen.⁷³ Eine Sorgfaltsanforderung kann nicht auf die Vermeidung einer Gefahr gerichtet sein, die nicht über das hinausgeht, was im täglichen Zusammenleben ohnehin hingenommen werden muss.⁷⁴ Da

69 Vgl. *Hager*, in: Staudinger, BGB, § 823, Rn. E 16.

70 *Wagner*, in: MüKo, BGB, § 823, Rn. 503; *Förster*, in: BeckOK, BGB, § 823, Rn. 303.

71 *Larenz/Canaris*, Lehrbuch des Schuldrechts II/2, S. 407 f.; *Hager*, in: Staudinger, BGB, § 823, Rn. E 16; *Voigt*, in: BeckOGK, BGB, § 823, Rn. 409.

72 *Larenz/Canaris*, Lehrbuch des Schuldrechts II/2, S. 408 ff.; *Hager*, in: Staudinger, BGB, § 823, Rn. E 21; mit Zurückhaltung auch *Voigt*, in: BeckOGK, BGB, § 823, Rn. 411.

73 Vgl. *Larenz/Canaris*, Lehrbuch des Schuldrechts II/2, S. 410 f.; *Voigt*, in: BeckOGK, BGB, § 823, Rn. 408; *Wagner*, in: MüKo, BGB, § 823, Rn. 514: „vorangegangenes gefährliches Tun“; speziell in Bezug auf die Produzentenhaftung *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 177; nach *Hager*, in: Staudinger, BGB, § 823, Rn. E 13 bedarf es dagegen keiner besonderen Gefahr.

74 Vgl. *Oetker*, in: MüKo, BGB, § 249, Rn. 194.

auch im Rahmen des vorangegangenen Tuns der Gefahrenschaftung und -beherrschung maßgebliche Bedeutung zukommt, kommt es auch nicht darauf an, ob das betreffende Verhalten für sich genommen rechtswidrig war oder nicht.⁷⁵

Zusammenfassend lässt sich eine Verkehrspflicht demnach im Wesentlichen darauf zurückführen, dass eine Gefahrenquelle geschaffen oder unterhalten wird.⁷⁶ Damit ist „derjenige, der eine Gefahrenlage – gleich welcher Art – schafft, grundsätzlich verpflichtet, die notwendigen und zumutbaren Vorkehrungen zu treffen, um eine Schädigung anderer möglichst zu verhindern.“⁷⁷ Ausgehend von dieser stehenden Formulierung der Rechtsprechung handelt es sich bei den Verkehrspflichten um „Gefahrenvermeidungs- und -abwendungspflichten.“⁷⁸ Die Zuordnung zu einem der vorgestellten Zurechnungsgründe⁷⁹ stellt dabei einen Anknüpfungspunkt für das Bestehen einer Verkehrspflicht dar, wobei stets eine inhaltliche Abwägung der genannten Kriterien erforderlich ist und diese regelmäßig erst in ihrem kombinatorischen Zusammenwirken zu einer Verkehrspflicht führen.⁸⁰

b) Umfang der Verkehrspflichten

Die Verkehrssicherungspflichten sind in ihrem Umfang und ihrer Intensität nach aber nicht grenzenlos. Vielmehr umfasst die „rechtlich gebotene Verkehrssicherung [...] diejenigen Maßnahmen, die ein umsichtiger und verständiger, in vernünftigen Grenzen vorsichtiger Mensch für notwendig und ausreichend hält, um andere vor Schäden zu bewahren. Dabei ist zu berücksichtigen, dass nicht jeder abstrakten Gefahr vorbeugend begegnet werden kann. Ein allgemeines Verbot, andere nicht zu gefährden, wäre

75 Larenz/Canaris, Lehrbuch des Schuldrechts II/2, S. 410.

76 Larenz/Canaris, Lehrbuch des Schuldrechts II/2, S. 407; Voigt, in: BeckOGK, BGB, § 823, Rn. 408.

77 Ständige Rspr., so wörtlich BGH, NJW 2007, 762 (763); in diese Richtung schon RGZ 163, 21 (26); BGH, NJW 1952, 1050 (1051) und BGH, NJW 1964, 814.

78 Larenz/Canaris, Lehrbuch des Schuldrechts II/2, S. 402.

79 Hager, in: Staudinger, BGB, § 823, Rn. E 12 weist darauf hin, dass die Fallgruppen nur als Aufgreifkriterien dienen und oft ineinander übergehen.

80 So Larenz/Canaris, Lehrbuch des Schuldrechts II/2, S. 413; Voigt, in: BeckOGK, BGB, § 823, Rn. 413.

unrealistisch. Eine Verkehrssicherung, die jede Schädigung ausschließt, ist im praktischen Leben nicht erreichbar“.⁸¹

Maßgeblich für die Bestimmung der Verkehrspflichten sind demnach die berechtigten Sicherheitserwartungen des Verkehrs.⁸² Bei der berechtigten Sicherheitserwartung handelt es sich um keine rein empirisch festzustellende Tatsache, sondern um eine Verkehrsanschauung, die sich nur im Wege wertender Betrachtung bestimmen lässt.⁸³ Dabei wird auch die Möglichkeit des Geschädigten berücksichtigt, sich selbst vor der Gefahr zu schützen. Ist ein solcher Selbstschutz möglich, kann eine Verkehrspflicht schon tatbestandlich entfallen oder reduziert sein.⁸⁴ Ist eine Gefahr gerade mit den Händen zu greifen oder kann ihr ohne Weiteres ausgewichen werden, kann der Verkehrssicherungspflichtige darauf vertrauen, dass der Betroffene dies erkennt und sich selbst schützt.⁸⁵ Der Sorgfaltsstandard weist folglich eine gewisse Wechselseitigkeit auf und ist durch den Vertrauensgrundsatz gekennzeichnet.⁸⁶ Damit lässt sich bereits festhalten, dass der Betroffene nicht vor allen möglichen Gefahren zu schützen ist, sondern nur vor solchen, die über das übliche Risiko⁸⁷ hinausgehen und die von ihm nicht erkannt und beherrscht werden können.⁸⁸ Welche Sicherheitsvorkehrungen dann konkret zu ergreifen sind, bestimmt sich einzelfallabhängig nach Art eines beweglichen Systems,⁸⁹ wobei die zwei Kenngrößen der Erforderlichkeit und Zumutbarkeit das Mindest- und Höchstmaß der geforderten objektiven Sorgfalt festlegen.⁹⁰

81 Vgl. erneut die ständige Rspr. und stehende Formulierung, so wörtlich BGH, NJW 2007, 762 (763); in diese Richtung schon RGZ 163, 21 (26); BGH, NJW 1952, 1050 (1051) und BGH, NJW 1964, 814.

82 Vgl. auch Voigt, in: BeckOGK, BGB, § 823, Rn. 414; Hager, in: Staudinger, BGB, § 823, Rn. E 27.

83 v. Bar, in: Lieb (Hg.), Produktverantwortung und Risikoakzeptanz, S. 29 (32); Voigt, in: BeckOGK, BGB, § 823, Rn. 414.

84 Vgl. Larenz/Canaris, Lehrbuch des Schuldrechts II/2, S. 414.

85 Je m.w.N. zur Rspr.: Wagner, in: MüKo, BGB, § 823, Rn. 533; Voigt, in: BeckOGK, BGB, § 823, Rn. 422; Hager, in: Staudinger, BGB, § 823, Rn. E 32a.

86 Wagner, in: MüKo, BGB, § 823, Rn. 534.

87 Zur Üblichkeit von Sicherungsvorkehrungen auch Larenz/Canaris, Lehrbuch des Schuldrechts II/2, S. 416.

88 Vgl. Wagner, in: MüKo, BGB, § 823, Rn. 534.

89 So Larenz/Canaris, Lehrbuch des Schuldrechts II/2, S. 413 f.

90 Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 1.

aa) Erforderlichkeit von Sicherungsmaßnahmen

Für die Frage der Erforderlichkeit von Sicherungsmaßnahmen ist der Erwartungshorizont des gefährdeten und des durchschnittlichen Verkehrsteilnehmers maßgeblich.⁹¹

Dabei können die Verkehrssicherungspflichten nicht dazu herangezogen werden, jegliche Schädigung zu vermeiden. Denn die Verkehrssicherungspflichten sind verhaltens- und nicht erfolgsbezogen, sodass allein aus der Existenz einer Gefahrenquelle noch keine Pflichtverletzung abgeleitet werden kann.⁹² Von dem Verkehrssicherungspflichtigen kann nichts Unmögliches verlangt werden. Alles andere würde den Charakter der Verkehrssicherungspflichten als „ernstzunehmende Verhaltensnormen, deren Einhaltung realistischer- und gerechterweise verlangt werden kann“, überstrapazieren und letztendlich allein der nachträglichen Konstruktion einer Haftung dienen.⁹³ Da eine absolute Sicherheit nicht gefordert wird und daneben auch von den Verkehrsteilnehmern nicht erwartet werden kann, wird eine Gefahr erst dann haftungsbegründend, wenn sie nach dem Stand von Wissenschaft und Technik für den Pflichtigen auch objektiv erkennbar und vermeidbar gewesen ist.⁹⁴ Sicherungspflichten können demnach immer nur im Rahmen der dem Sicherungspflichtigen in der konkreten Handlungssituation ex ante zur Verfügung stehenden tatsächlichen und rechtlichen Handlungsmöglichkeiten bestehen.⁹⁵ Aus dem Umstand, dass nach der berechtigten Verkehrserwartung nicht in jeder Situation eine absolute Sicherheit verlangt werden kann, folgt auch, dass allein die theoretische Möglichkeit der Verletzung von Rechtsgütern anderer nicht zwangsläufig zu entsprechenden Sicherungspflichten führt. Es muss nicht jeder abstrakten Gefahr durch vorbeugende Maßnahmen begegnet werden.⁹⁶

91 Vgl. BGH, NJW 1990, 906 (907).

92 BGH, NJW 1981, 1606 (1608).

93 Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 23, Rn. 12.

94 Hierzu Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 23, Rn. 14; Hager, in: Staudinger, BGB, § 823, Rn. E 30 mit dem Hinweis, dass es aufgrund des objektiven Maßstabs nicht darauf ankommt, ob der Pflichtige die Gefahr auch tatsächlich erkannt hat; BGH, NJW 1981, 1606 (1608).

95 Wagner, in: MüKo, BGB, § 823, Rn. 527.

96 BGH, BeckRS 1975, 30391745; BGH, NJW 2013, 1302 (1303); Voigt, in: BeckOGK, BGB, § 823, Rn. 414; Hager, in: Staudinger, BGB, § 823, Rn. E 35.

Allerdings ist bei der Beurteilung der Erforderlichkeit auch die Gefährlichkeit des Verhaltens zu berücksichtigen.⁹⁷ Die Gefährlichkeit hängt im Wesentlichen von der Höhe des Schadens und dem Grad der Eintrittswahrscheinlichkeit ab.⁹⁸ Die Schadenshöhe wird dabei vom Rang des betroffenen Rechtsguts und der Intensität seiner Verletzung bestimmt.⁹⁹ Daraus ergibt sich, dass je höherwertiger die Rechtsgüter sind und je schwerer der drohende Schaden ist, desto höher auch die Anforderungen sind, die an die Verkehrssicherungspflichten auch gegen relativ unwahrscheinliche Gefahren gestellt werden.¹⁰⁰

bb) Zumutbarkeit von Sicherungsmaßnahmen

Die Sorgfaltspflichten enden aber nicht erst an der Grenze des technisch und rechtlich Möglichen, sondern bereits an der Grenze des Zumutbaren.¹⁰¹ Nicht alle Sicherungsmaßnahmen, die objektiv möglich sind, werden vom Verkehrssicherungspflichtigen auch gefordert.¹⁰² Unter der Zumutbarkeit ist dabei der vom Verkehrssicherungspflichtigen zu ergreifende Sicherheitsaufwand zu verstehen. In diesem Rahmen wird der Umfang der Verkehrspflicht auf das beschränkt, was „billige Rücksicht nach der Verkehrsauffassung“ gebietet.¹⁰³

Auch beim zu ergreifenden Sicherheitsaufwand spielt die Größe der Gefahr eine entscheidende Rolle. So sind Sicherungsmaßnahmen umso eher zumutbar, je größer die Gefahr und die Wahrscheinlichkeit ihrer Verwirklichung ist.¹⁰⁴ Der wirtschaftliche Aufwand der Sicherheitsmaßnahmen ist vor diesem Hintergrund in Relation zu ihrem Nutzen und damit dem

97 Vgl. BGH, NJW 1965, 197 (199): „Mit der Größe der Gefahr wächst auch das Maß der vom Verkehrssicherungspflichtigen zu erwartenden Sorgfalt“; Voigt, in: BeckOGK, BGB, § 823, Rn. 414.

98 BGH, NJW 2007, 732 (763); Wagner, in: MüKo, BGB, § 823, Rn. 530; Förster, in: BeckOK, BGB, § 823, Rn. 702.

99 Wagner, in: Eifert (Hg.), Produktbeobachtung durch Private, S. 115 (122); Voigt, in: BeckOGK, BGB, § 823, Rn. 414.

100 Voigt, in: BeckOGK, BGB, § 823, Rn. 414.

101 Wagner, in: MüKo, BGB, § 823, Rn. 528.

102 Vgl. BGH, NJW 1964, 814 (816 f.), Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 23, Rn. 15.

103 BGH, NJW 1985, 270 (270); BGH, NJW 1972, 724 (726).

104 Vgl. nur BGH, NJW 2007, 762 (763); Wagner, in: MüKo, BGB, § 823, Rn. 530; Hager, in: Staudinger, BGB, § 823, Rn. E 35.

Wert der insgesamt zu vermeidenden Schäden zu setzen.¹⁰⁵ Daher gilt: Je höher der zu erwartende Schaden, je wahrscheinlicher dessen Eintritt und je geringer der Aufwand der Sicherungsmaßnahmen, desto eher können diese dem Verkehrssicherungspflichtigen zugemutet werden.¹⁰⁶ Soweit sich aber die vom Geschädigten erlittene Rechtsgutsverletzung nicht durch zumutbare Sorgfaltsmaßnahmen hätte verhindern lassen, verwirklicht sich kein „Unrecht“ des Schädigers, sondern erleidet der Geschädigte ein „Unglück“.¹⁰⁷

3. Pflichtenbereiche des Herstellers

Diese allgemeinen Grundsätze der Verkehrssicherungspflichten können auch auf die Produzentenhaftung übertragen werden.¹⁰⁸ Im Rahmen der Produzentenhaftung haben sich hinsichtlich der Sorgfaltsanforderungen die Kategorien des Konstruktions-, Fabrikations-, Instruktions- sowie Produktbeobachtungsfehlers herausgebildet. Dass die Kategorien terminologisch an einen Produktfehler anknüpfen und gegenständlich formuliert sind, darf nicht darüber hinwegtäuschen, dass sich dahinter die Pflicht zu sorgfältigem Handeln in diesen Bereichen verbirgt und es sich auch bei der Produzentenhaftung um eine Haftung für objektive Sorgfaltspflichtverletzungen handelt.¹⁰⁹ In einem Produktfehler vereint sich damit das Vorliegen eines objektiven Produktmangels in Form eines Sicherheitsdefizits bzw.

105 Wagner, in: MüKo, BGB, § 823, Rn. 531.

106 Vgl. auch Larenz/Canaris, Lehrbuch des Schuldrechts II/2, S. 414.

107 BGH, BeckRS 1975, 30391745; BGH, NJW 2006, 2326 (2362); Wagner, in: MüKo, BGB, § 823, Rn. 528.

108 Hierzu Kullmann, VersR 1988, 655 m.w.N. zur Rechtsprechung in Fn. 9; zur Geltung der allgemeinen Grundsätze auch Voigt, in: BeckOGK, BGB, § 823, Rn. 640 und Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 1; grundlegend BGH, NJW 1969, 269.

109 Vgl. Wagner, in: MüKo, BGB, § 823, Rn. 1068 mit dem Hinweis, dass die Kategorisierung auf der komplexen Beweislastverteilung beruht; hierzu auch Riehm/Meier, EuCML 2019, 161 (163) mit dem Hinweis, dass beim Vorhandensein eines solchen Fehlers auch regelmäßig auf die Verletzung der Sorgfaltspflicht zu schließen ist; Lüftenecker, Die Rückruffpflicht des Herstellers, S. 64 sieht in dem Fehler die Manifestation der Sorgfaltspflichtverletzung; Wagner, Deliktsrecht, Kap. 9, Rn. 12 spricht davon, dass Sorgfaltspflichtverletzungen zu bestimmten Fehlerkategorien verschlüsselt werden; Thöne, Autonome Systeme, S. 126 verweist darauf, dass es eine terminologische Frage darstellt, ob von einem entsprechenden Produktfehler oder einem fahrlässig produzierten Produkt gesprochen wird; Ackermann, in: NK-ProdR, § 823 BGB, Rn. 87 ff. spricht von Konstruktionspflichtverletzung, etc.

einer Verkehrswidrigkeit und die Verkehrspflichtverletzung des Herstellers. Eine Aufspaltung des Begriffs des Produktfehlers erfolgt dann lediglich im Rahmen des Beweisrechts.¹¹⁰ Während der Geschädigte grundsätzlich nur den Produktmangel als Sicherheitsdefizit nachzuweisen hat, muss sich der Hersteller hinsichtlich der dann vermuteten Verkehrspflichtverletzung entlasten.

a) Inverkehrbringen als Zäsur

Maßgeblich für die Bestimmung der Sorgfaltsanforderungen ist nach den allgemeinen Grundsätzen der Zeitpunkt, zu dem eine Schadensabwendung in Betracht kam.¹¹¹ Damit ist grundsätzlich ex ante auf den Zeitpunkt der für die Rechtsgutsverletzung ursächlichen Handlung abzustellen.¹¹² Im Rahmen der Produzentenhaftung ist dies der Zeitpunkt des Inverkehrbringens¹¹³ des Produkts.¹¹⁴ Denn erst mit der Inverkehrgabe des Produkts wird eine Gefahrenlage für Dritte geschaffen und gewinnt das Verhalten des Herstellers an haftungsrechtlicher Relevanz.¹¹⁵

Die Verantwortlichkeit des Herstellers ergibt sich dabei unter dem Gesichtspunkt der Bereichshaftung.¹¹⁶ Die Verkehrspflichten des Herstellers, verschlüsselt zu den Fehlerkategorien, gründen darauf, dass der Hersteller

110 Vgl. Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 30, Rn. 27.

111 Lorenz, in: BeckOK, BGB, § 276, Rn. 27; BGH, NJW 1981, 1603 (1604).

112 Wagner, in: MüKo, BGB, § 823, Rn. 549.

113 Eine Definition des Inverkehrbringens findet sich im Produkthaftungsrecht – auch im Rahmen des ProdHaftG – nicht. Es wird darauf abzustellen sein, dass ein Dritter bestimmungsgemäß mit dem Produkt in Kontakt kommen kann, vgl. Hager, in: Staudinger, BGB, § 823, Rn. F 2. Im ProdHaftG wird es für erforderlich gehalten, dass der Hersteller sein Produkt aufgrund eines freien Willensentschlusses „in die Umwelt entlassen“ hat. Ob das Produkt darüber hinaus auch an eine Person außerhalb der Herrschaftssphäre des Herstellers übergeben werden muss („Werkstorprinzip“), ist streitig, vor dem europarechtlichen Hintergrund aber wohl abzulehnen, vgl. Förster, in: BeckOK, BGB, § 823, Rn. 678 m.w.N.

114 Allgemeine Meinung, vgl. nur Wagner, in: MüKo, BGB, § 823, Rn. 1081.

115 Wagner, AcP 217 (2017), 707 (749) weist zu Recht darauf hin, dass es aus deliktsrechtlicher Sicht jedermann freisteht, hochgefährliche Produkte herzustellen und dies erst dann relevant wird, wenn Dritte damit in Berührung kommen können.

116 Die Produzentenhaftung wird regelmäßig der Bereichshaftung zugerechnet, vgl. Lorenz/Canaris, Lehrbuch des Schuldrechts II/2, S. 408; Hager, in: Staudinger, BGB, § 823, Rn. E 20.

bis zum Zeitpunkt der Inverkehrgabe das Produkt in seiner Gewalt¹¹⁷ hat und es seiner Risikosphäre unterliegt, die er durch Steuerung und Einflussnahme beherrschen kann. Durch den entsprechenden Gewinn zieht der Hersteller auch den maßgeblichen Vorteil aus der Schaffung der Gefahrenquelle. Der Vorteil aus der Schaffung der Gefahrenquelle und die Nähe zu ihr sind folglich die ausschlaggebenden Abwägungskriterien für die Begründung der Verkehrspflichten des Herstellers bis zur Inverkehrgabe.¹¹⁸ Hinzu kommt, dass der mit einer eigenen Beurteilung der Produktsicherheit überforderte Produktnutzer auch im Ausgangspunkt auf die Sicherheit des Produkts vertraut.¹¹⁹ Da der Hersteller hinsichtlich des Produktionsprozesses Inhaber der Bestimmungsgewalt ist und demnach für den Zustand seines Bereichs einzustehen hat,¹²⁰ kommt es auch nicht auf eine durch das Produkt bzw. den entsprechenden Fehler geschaffene erhöhte Gefahrenlage an.¹²¹

Die Maßgeblichkeit des Zeitpunkts des Inverkehrbringens ergibt sich auch aus einer Abgrenzung der Verantwortungsbereiche. So beruhen bereits die allgemeinen Verkehrspflichten auf dem Gedanken der Abgrenzung der jeweiligen Verantwortungsbereiche und der Risikoverteilung, indem ein Ausgleich zwischen den Integritätsinteressen und der Handlungsfreiheit vorgenommen wird.¹²² Im Rahmen der Produzentenhaftung wird diese Abgrenzung der Verantwortungsbereiche¹²³ anhand der Fehlerkategorisierung deutlich. Demnach lassen sich zwei maßgebliche Verantwortungssphären ausmachen: Diejenige des Herstellers, wozu auch der Zulieferer, Programmierer, etc. zu rechnen sind und diejenige des Nutzers (einschließlich des Bedieners).¹²⁴ Die Konstruktions-, Fabrikations- sowie Instruktionspflichten beziehen sich auf den Herstellungsprozess und auf den Zeitraum

117 Förster, in: BeckOK, BGB, § 823, Rn. 703.

118 Voigt, in: BeckOGK, BGB, § 823, Rn. 410.

119 Vgl. Bodewig, Der Rückruf fehlerhafter Produkte, S. 172.

120 Nach Larenz/Canaris, Lehrbuch des Schuldrechts II/2, S. 408 ist sowohl die bewegliche Sache als auch das Unternehmen die Gefahrenquelle.

121 Hager, in: Staudinger, BGB, § 823, Rn. E 20.

122 So schon Steffen, VersR 1980, 409; Thöne, Autonome Systeme, S. 108.

123 Insoweit zur Produkthaftung Reusch, in: Kaulartz/Braegelmann (Hg.), Artificial Intelligence und Machine Learning, S. 87; speziell zur Verantwortung bei Innovationen Röthel, in: Eifert/Hoffmann-Riem (Hg.), Innovationsverantwortung, S. 335 (338).

124 Vgl. Borges, NJW 2018, 977 (980); Zech, in: Gless/Seelmann (Hg.), Intelligente Agenten und das Recht, S. 163 (177) spricht von Produzenten- und Anwenderseite; Thöne, Autonome Systeme, S. 196.

vor dem Inverkehrbringen. Sie sind präventiv darauf gerichtet Fehler zu vermeiden, um möglichst nur fehlerfreie Produkte auf den Markt zu bringen.¹²⁵ Anknüpfend an diese jeweiligen Fehler werden Bereiche definiert, in denen die produktrechtliche Gefahrensteuerung dem Hersteller und nicht dem Produktnutzer obliegt. Während es am Hersteller ist, für eine fehlerfreie Beschaffenheit der von ihm in Verkehr gebrachten Ware zu sorgen, unterliegt der Produktnutzer den Sorgfaltsanforderungen beim jeweiligen Einsatz des Gegenstands.¹²⁶ Nach dem Zeitpunkt der Inverkehrgabe verliert der Hersteller herkömmlich die Kontrolle über das Produkt. Eine herstellerseitige Gefahrensteuerung ist danach nur noch begrenzt möglich. Aus diesem Grund konkretisieren sich die deliktsrechtlichen Sorgfaltspflichten des Herstellers und die Sicherheitserwartungen an das Produkt zu dem Zeitpunkt des Inverkehrbringens.¹²⁷ Als Zäsur für die haftungsrechtliche Zuweisung der Risikosphären kann demnach der Zeitpunkt des Inverkehrbringens ausgemacht werden.

b) Haftungsweiterung für Zeitraum ab dem Inverkehrbringen

Allerdings können auch nach der eigentlichen schadensursächlichen Handlung neue Pflichten entstehen.¹²⁸ Für die Produzentenhaftung bedeutet das, dass die Verantwortung des Herstellers nicht mit dem Zeitpunkt des Inverkehrbringens des Produkts endet.¹²⁹ Für die Zeit nach der Inverkehrgabe trifft den Hersteller die Produktbeobachtungspflicht.

Hinsichtlich der Produzentenhaftung ist zunächst zu konstatieren, dass das Produkt mit dem Inverkehrbringen die Sphäre des Herstellers verlässt und eine unmittelbare Einflussnahme auf die Verwendung des Produkts herkömmlicherweise nicht mehr möglich ist. Allerdings verfügt der Hersteller auch noch nach der Inverkehrgabe über die Möglichkeit der Gefahrensteuerung als unabdingbare Voraussetzung für die Begründung einer Verkehrspflicht. Denn mit den Möglichkeiten einer Warnung oder eines

125 *Lüftenegger*, Die Rückrufpflicht des Herstellers, S. 77.

126 *Wagner*, in: MüKo, BGB, § 823, Rn. 512.

127 Vgl. zum Ganzen *Schrader*, in: Buck-Heeb/Oppermann (Hg.), Automatisierte Systeme, S. 333 (336); *Wagner*, in: MüKo, BGB, § 823, Rn. 1109; *Helte*, Anforderungen an die Produktsicherheit, S. 15; *Thöne*, Autonome Systeme, S. 198.

128 *Lorenz*, in BeckOK, BGB, § 276, Rn. 27.

129 So bereits RGZ 163, 21 (26); mittlerweile stehende Formulierung vgl. BGH, NJW 2009, 1080 (1081).

Rückrufs verbleiben ihm auch nach diesem Zeitpunkt Mittel der Gefahrensteuerung bei erkannten Produktgefahren.¹³⁰ Außerdem kann der Hersteller die aus dem Herstellungsprozess bekannten Produkteigenschaften mit den ihn erreichenden neuesten Erkenntnissen aus der Nutzungsphase in Relation setzen und verfügt aufgrund dieses überlegenen Wissens über die besten Voraussetzungen für eine effektive und individuelle Gefahrenabwehr.¹³¹ Daneben stellt sich der mit der Produktbeobachtung verbundene Aufwand für den Hersteller regelmäßig als gering dar.¹³² Denn mit Blick auf das Inverkehrbringen künftiger Produkte ist der Hersteller ohnehin dazu angehalten, schon vermarktete Produkte auf bisher unbekannte Gefahren zu beobachten, um dann erforderlichenfalls seine Produktion anpassen zu können und so hinsichtlich dieser noch in den Verkehr zu bringender Produkte dem Vorwurf einer Sorgfaltspflichtverletzung zu entgehen.¹³³

Neben der Möglichkeit der Beherrschung der Gefahrenquelle ist zur Begründung einer Verkehrspflicht aber auch die Verantwortlichkeit für die Gefahrenquelle erforderlich.¹³⁴ Zwar geht die Gefahrenquelle mit der Inverkehrgabe des Produkts auf den Hersteller zurück, allerdings muss der Zustandsverantwortliche nicht mit demjenigen identisch sein, der eine Gefahrenquelle geschaffen hat,¹³⁵ so dass auch eine Verkehrspflicht des Nutzers als nunmehrigem Inhaber der Bestimmungsmacht in Betracht kommt. Verkehrspflichten zum Schutz fremder Rechtsgüter vor Gefahren aus der eigenen Sphäre des Rechtsgutsträgers können nur ausnahmsweise

130 Wagner, in: MüKo, BGB, § 823, Rn. 1109; Bodewig, Der Rückruf fehlerhafter Produkte, S. 169.

131 Förster, in: BeckOK, BGB, § 823, Rn. 735; Wagner, AcP 217 (2017), 707 (751); Lenz, in: Lenz, Produkthaftung, § 3, Rn. 223; Bodewig, Der Rückruf fehlerhafter Produkte, S. 174 f.; Klinger, Die Produktbeobachtungspflicht bezüglich Fremdzubehörteilen, S. 35 f. sieht aufgrund dieser Faktoren ein allgemein gesteigertes und schutzwürdiges Vertrauen der Nutzer; eine Begründung für die Verantwortung des Herstellers im Hinblick auf die Produktbeobachtung findet sich in der zivilrechtlichen Judikatur dagegen kaum. In strafrechtlicher Hinsicht äußerte sich der BGH in seiner berühmten Lederspray-Entscheidung aber genau in der dargestellten Weise, vgl. BGH, NJW 1990, 2560 (2564).

132 Vgl. hierzu Wagner, AcP 217 (2017), 707 (751). Dieser spricht davon, dass der Hersteller folglich „cheapest cost avoider“ ist.

133 Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 372.

134 Explizit im hiesigen Kontext Ulmer, ZHR 152 (1988), 564 (571); v. Bar, in: Lieb (Hg.), Produktverantwortung und Risikoakzeptanz, S. 29 (36) fordert einen „Zurechnungsgrund“.

135 Voigt, in: BeckOGK, BGB, § 823, Rn. 409.

bestehen.¹³⁶ Insoweit ist zu konstatieren, dass eine Gefahrenquelle abstrakter Natur stets mit dem Inverkehrbringen eines Produkts geschaffen wird, da sich eine völlige Gefährlosigkeit über den gesamten Lebenszyklus hinweg nie sicher vorhersagen lässt.¹³⁷

Geht die Gefahr auf den Produktionsvorgang zurück, hat der Hersteller hierfür die Bestimmungsgewalt und schafft er folglich mit der Inverkehrgabe eine andauernde Gefahrenquelle, die ursprünglich aus seiner Sphäre stammt und nun in die Nutzungsphase hineinragt.¹³⁸ Geht eine Gefahr aber derart von der eigenen Sphäre aus, ist jeder ohne Weiteres verpflichtet, sein Verhalten und seine Sachen so einzurichten, dass eine Verletzung von Rechtsgütern Dritter möglichst vermieden wird.¹³⁹ Ferner besteht gerade auch ein schutzwürdiges Vertrauen der Nutzer darauf, dass der Hersteller in diesem Fall Gefahrenabwehrmaßnahmen ergreift.¹⁴⁰ Immerhin verfügt der Hersteller nicht nur aufgrund des Entwicklungs- und Herstellungsprozesses über sämtliche Informationen über das Produkt, sondern ihn erreichen auch Gefahren- oder Schadensmeldungen – ggf. unter Zwischenschaltung der Händler – zuvörderst. Damit begründet sich in diesen Fällen die Verkehrspflicht des Herstellers auch für den Zeitraum nach der Inverkehrgabe nach den Grundsätzen der Bereichshaftung.¹⁴¹

Geht die Produktgefahr dagegen nicht auf die Sphäre des Herstellers zurück, kommt eine Verantwortung des Herstellers nur unter dem Gesichtspunkt des vorangegangenen gefährlichen Tuns in Betracht.¹⁴² Allerdings kommt eine allgemeine deliktsrechtliche Pflicht zur Fürsorge für fremde Rechtsgüter gerade nicht in Betracht.¹⁴³ Vor diesem Hintergrund muss im Einzelfall berücksichtigt werden, ob die dem Hersteller abverlangte Gefahrensteuerung noch in einem angemessenen Verhältnis zu dem von ihm gesetzten Risiko steht.¹⁴⁴ Welche Qualität diese Gefahrschaffung bei der Inverkehrgabe zur Begründung einer entsprechenden Verkehrspflicht haben

136 Wagner, in: MüKo, BGB, § 823, Rn. 504.

137 Vgl. Bodewig, Der Rückruf fehlerhafter Produkte, S. 167.

138 Vgl. dazu Voigt, in: BeckOGK, BGB, § 823, Rn. 674; Hager, VersR 1984, 799; Sommer, Haftung für autonome Systeme, S. 275; Ulmer, ZHR 152 (1988), 564 (571).

139 Wagner, in: MüKo, BGB, § 823, Rn. 504.

140 Vgl. Bodewig, Der Rückruf fehlerhafter Produkte, S. 172.

141 Dazu Bodewig, Der Rückruf fehlerhafter Produkte, S. 177 f.

142 So allgemein ohne Differenzierung Ulmer, ZHR 152 (1988), 564 (571).

143 Wagner, in: MüKo, BGB, § 823, Rn. 504.

144 Diesen Zusammenhang mahnt auch Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 25, Rn. 222 an.

muss, ist dabei noch wenig geklärt.¹⁴⁵ Dieser Frage soll kontextbezogen bei der Klärung des Anwendungsbereichs der Produktbeobachtungspflicht nachgegangen werden.¹⁴⁶

4. Der Produktbeobachtungsfehler

Die Pflichten des Herstellers enden damit nicht mit der Inverkehrgabe des Produkts. Vielmehr hat ein Hersteller, der erst nach dem Inverkehrbringen erfährt, dass von seinem Produkt Gefahren ausgehen, „alles [zu] tun, was ihm den Umständen nach zugemutet werden kann, um sie abzuwenden.“¹⁴⁷ Mit der Statuierung dieser Gefahrenabwehrpflicht hat das Reichsgericht die Produktbeobachtungspflicht schon implizit angesprochen. Später stellte der BGH dann fest, dass es allein mit der Gefahrenabwehrpflicht nicht sein Bewenden haben kann. Denn der Hersteller darf sich nicht darauf verlassen, mehr oder weniger zufällig von solchen Gefahren Kenntnis zu erlangen. Vielmehr ist er verpflichtet, seine Produkte sowohl auf noch nicht bekannte schädliche Eigenschaften hin zu beobachten als auch sich über deren sonstige, eine Gefahrenlage schaffende Verwendungsfolgen zu informieren.¹⁴⁸

Die Produktbeobachtungspflicht nimmt aber nicht nur in zeitlicher Hinsicht eine Sonderrolle im Pflichtengefüge des Herstellers ein. Denn ihre Verletzung führt nicht zu einem Produktfehler im Sinne einer sicherheitskritischen Eigenschaft.¹⁴⁹ Die sicherheitskritische Produkteigenschaft liegt vielmehr bereits unabhängig von der Verletzung der Beobachtungspflicht vor. Ausgehend von dieser bestehenden Produktgefahr dient die Produktbeobachtungspflicht dazu, Gefahren rechtzeitig zu erkennen und zu steuern

145 Voigt, in: BeckOGK, BGB, § 823, Rn. 674 spricht von „Schaffung einer andauernden Gefahrenquelle, deren Ursache aus der Sphäre des Herstellers stammt, unabhängig davon, welcher Fehlerkategorie sie angehört“; Lenz, in: Lenz, Produkthaftung, § 4, Rn. 39 erachtet eine „rudimentäre Ursache“ für ausreichend; Thöne, Autonome Systeme, S. 211 scheint auf eine durch die Herstellung und Vermarktung geschaffene „Dauergefahr“ abzustellen; allgemein Larenz/Canaris, Lehrbuch des Schuldrechts II/2, S. 410, 412.

146 Dazu unter C.II.

147 RGZ 163, 21 (26).

148 So grundlegend BGH, NJW 1981, 1606 (1607 f.) und BGH, NJW 1981, 1603 (1604).

149 In diese Richtung Wagner, in: MüKo, BGB, § 823, Rn. 1108.

und damit den Eintritt eines Schadens zu verhindern.¹⁵⁰ Der Produktfehler und der daraus resultierende Schaden entsteht aber nicht durch die reine Nichtbeobachtung, sondern ist bereits im Produkt angelegt¹⁵¹ und kann sich dadurch realisieren, dass der Hersteller auf im Wege der Beobachtung gewonnene Gefahrenkenntnisse nicht reagiert oder sich dieser Reaktionsmöglichkeit aufgrund unterlassener Informationserhebung von vornherein begeben hat.¹⁵² Der Produktbeobachtungspflicht wohnen damit zwei Komponenten inne. Zum einen die Gefahrerkennung (Beobachtungspflicht i.e.S.), zum anderen die Gefahrensteuerung (Reaktionspflicht).¹⁵³

Der Produktbeobachtungspflicht kommt eine gewisse Auffangfunktion zu.¹⁵⁴ Durch die Pflicht, Produktgefahren nach Inverkehrgabe zu erkennen und abzuwehren, sollen gefahrtechnisch verbleibende Lücken geschlossen werden. Dem Hersteller wird aufgegeben, das zur Abwendung der Gefahr Erforderliche zu tun, um auszugleichen, was zuvor in Abweichung von dem Grundsatz, dass nur sichere Produkte in den Verkehr gebracht werden dürfen, versäumt wurde.¹⁵⁵ Dabei spielen jedenfalls im Ausgangspunkt die Gründe, warum ein gefahrträchtiges Produkt in den Verkehr gelangt ist, keine Rolle. Daher findet die Produktbeobachtungspflicht unabhängig davon Anwendung, ob ein Produktfehler vorliegt oder es sich um einen nachträglichen sicherheitsrelevanten Erkenntnisgewinn handelt.¹⁵⁶ Es kommt damit nicht darauf an, welcher Fehlerkategorie die Produktgefahr zuzuordnen ist oder ob der Hersteller überhaupt pflichtwidrig gehandelt hat.¹⁵⁷ Hinsichtlich der haftungsbegründenden Relevanz kommt der

150 Vgl. *Taschner*, ZEuP 2012, 560 (563): „Produkthaftung und Produktbeobachtung sind zwei völlig verschiedene Dinge: Produktbeobachtung ist präventiv. Sie hat zum Inhalt die Vorsorge, künftige Schadensfälle zu verhindern. Produkthaftung blickt zurück.“

151 *Förster*, in: BeckOK, BGB, § 823, Rn. 735 spricht von der Realisierung von Gefahren, die „im Verborgenen geschlummert haben“.

152 *Wagner*, in: MüKo, BGB, § 823, Rn. 1112; *Rudkowski*, VersR 2018, 65 (70 f.) spricht daher speziell in Bezug auf den Rückruf von einer unbefriedigenden dogmatischen Einordnung im Rahmen der Verkehrssicherungspflichten.

153 Prägnant *Lüftenegger*, Die Rückruffpflicht des Herstellers, S. 81.

154 *Lüftenegger*, Die Rückruffpflicht des Herstellers, S. 82 spricht von „Auffangbecken“ unter den Sorgfaltspflichten“.

155 Vgl. *Förster*, in: BeckOK, BGB, § 823, Rn. 742; in diese Richtung schon RGZ 163, 21 (26).

156 *Sprau*, in: Grüneberg, BGB, § 823, Rn. 179.

157 Vgl. *Hager*, in: Staudinger, BGB, § 823, Rn. F 20; *Foerste*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 374 f; *Voigt*, in: BeckOGK, BGB, § 823, Rn. 674.

Produktbeobachtungspflicht dagegen bei Vorliegen eines ursprünglichen Produktfehlers nur subsidiäre Bedeutung zu. Denn kommt es aufgrund eines schuldhaften Verstoßes gegen eine Konstruktions-, Fabrikations-, oder Instruktionspflicht zu einem Schaden, haftet der Hersteller schon deswegen aus § 823 Abs. 1 BGB, ohne dass es aufgrund derselben Gefahr bzw. desselben Fehlers auf eine Nichtreaktion und damit die Verletzung der Produktbeobachtungspflicht ankäme.¹⁵⁸ In diesem Fall kommt der Produktbeobachtungspflicht nur noch haftungsvermeidende Wirkung zu, sollte die Reaktion des Herstellers den Eintritt eines Schadens noch vermeiden.¹⁵⁹ Anders ist dies, sollte dem Hersteller bei Inverkehrgabe kein Pflichtenverstoß angelastet werden können. In diesem Fall wird die Produktverantwortung des Herstellers über die Produktbeobachtungspflicht über den Zeitpunkt des Inverkehrbringens hinaus perpetuiert.¹⁶⁰

Es lässt sich festhalten, dass sich der Hersteller auch bei sorgfältiger Konstruktion, Fabrikation und Instruktion nicht auf die Fehlerfreiheit und Ungefährlichkeit seiner in den Verkehr gegebenen Produkte verlassen darf. Er hat zu prüfen, wie sich seine Produkte in der Praxis bewähren und muss erforderlichenfalls Gefahrenabwehrmaßnahmen einleiten. Der Umfang der zu ergreifenden Maßnahmen sowohl hinsichtlich der Beobachtungspflicht i.e.S. als auch hinsichtlich der Reaktionspflicht ergibt sich wiederum anhand der Kenngrößen der Erforderlichkeit und der Zumutbarkeit.¹⁶¹

II. Exkurs: Die weiteren Herstellerpflichten im Überblick

Da im Laufe der Untersuchung immer wieder auf die einzelnen Produzentenpflichten Bezug genommen wird, soll hier ein kurzer Überblick über die weiteren Pflichten des Herstellers gegeben werden.

158 Vgl. Hager, VersR 1984, 799; Hager, in: Staudinger, BGB, § 823, Rn. F 20; Förster, in: BeckOK, BGB, § 823, Rn. 741; Schwenger, JZ 1987, 1059 (1063); Bodewig, Der Rückruf fehlerhafter Produkte, S. 181 „weitere Verkehrspflichtverletzung als ein zusätzlicher Haftungsgrund“.

159 Ulmer, ZHR 152 (1988), 564 (570 f.); Bodewig, Der Rückruf fehlerhafter Produkte, S. 181 f.

160 Nach Wagner, in: MüKo, BGB, § 823, Rn. 1109 stellt die Produktbeobachtungspflicht in gewissem Sinne ein Gegenstück zu den sonstigen zeitpunktbezogenen Sorgfaltspflichten des Herstellers dar, welche auf einer historischen Risikoeinschätzung und Gefahrsteuerungsmöglichkeiten beruhen.

161 Explizit klarstellend Wagner, in: MüKo, BGB, § 823, Rn. 1110; s. auch BGH, NJW-RR 1995, 342 (343).

1. Das Verhältnis von Produzentenhaftung und ProdHaftG

Betrachtet man im Rahmen der Produzentenhaftung nach § 823 Abs. 1 BGB die Fehlerbegriffe bzw. die korrespondierenden Sorgfaltsanforderungen an den Hersteller, so ist letztendlich die interne Unternehmensorganisation angesprochen. Durch diese soll sichergestellt werden, dass es möglichst zu keinen Schädigungen durch fehlerhafte Produkte kommt. Im Kern handelt es sich damit bei der Produzentenhaftung um eine Verantwortlichkeit für Organisationsmängel.¹⁶²

Anders als im Rahmen der Produzentenhaftung nach § 823 Abs. 1 BGB knüpft die Einstandspflicht des Herstellers nach dem ProdHaftG¹⁶³ nicht an die Verletzung einer Verkehrssicherungspflicht und damit nicht an ein Verhalten, sondern gegenstandsbezogen an die Fehlerhaftigkeit eines Produktes (vgl. § 1 Abs. 1 S. 1, § 3 Abs. 1 ProdHaftG) an.¹⁶⁴ Für den die Haftung begründenden Produktfehler kommt es nach § 3 Abs. 1 ProdHaftG auf die berechnete Sicherheitserwartung der Verkehrsteilnehmer im Zeitpunkt des Inverkehrbringens (§ 3 Abs. 1 lit. c, Abs. 2 ProdHaftG) an. Im Ausgangspunkt ist damit zwar allein die Integritätserwartung der Verkehrsteilnehmer und die für diese ausgehenden Gefahren entscheidend, während die Ursachen der Gefahren keine Rolle spielen.¹⁶⁵ Allerdings ist allgemein anerkannt, dass sich die maßgeblichen Sicherheitserwartungen nach § 3 Abs. 1 ProdHaftG grundsätzlich nach denselben objektiven Maßstäben wie die Verkehrspflichten des Herstellers im Rahmen der deliktischen Haftung gem. § 823 Abs. 1 BGB beurteilen.¹⁶⁶ Die dort im Rahmen der objek-

162 So Hager, in: Staudinger, BGB, § 823, Rn. F 2; Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 391.

163 Mit dem ProdHaftG wird die europäische Produkthaftungsrichtlinie 85/374/EWG in nationales Recht umgesetzt. Die Haftung nach dem ProdHaftG stellt die zweite Schiene der deliktischen Haftung in Deutschland dar. Nach § 15 Abs. 2 ProdHaftG bleibt die deliktische nationale Haftung nach §§ 823 ff. BGB in ihrer Anwendung unberührt, h.M. vgl. Wagner, in: MüKo, BGB, § 15 ProdHaftG, Rn. 4 f.; Spickhoff, in: BeckOGK, BGB, § 15 ProdHaftG, Rn. 11 ff.; Oechsler, in: Staudinger, BGB, § 15 ProdHaftG, Rn. 12 ff.; a.A. Riehm, in: Langenbuecher (Hg.), Europäisches Privatrecht und Wirtschaftsrecht § 3, Rn. 50 ff.

164 Vgl. Viehweg, in: Schulte/Schröder (Hg.), Handbuch des Technikrechts, S. 337 (347); Müller, Software als „Gegenstand“ der Produkthaftung, S. 63.

165 Oechsler, in: Staudinger, BGB, § 3 ProdHaftG, Rn. 5.

166 Allgemeine Meinung, vgl. Graf v. Westphalen, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 48, Rn. 14; Oechsler, in: Staudinger, BGB, § 3 ProdHaftG, Rn. 13; Wagner, in: MüKo, BGB, § 3 ProdHaftG, Rn. 3; Förster, in: BeckOK, BGB, § 3 ProdHaftG, Rn. 6 abstellend auf die gleichermaßen verfolgte Zielsetzung,

tiven Sorgfaltsanforderungen maßgeblichen Kriterien der Erforderlichkeit und Zumutbarkeit von Sicherungsmaßnahmen determinieren also die Verkehrserwartung im Rahmen des Fehlerbegriffs nach § 3 Abs. 1 ProdHaftG. Eine absolute Sicherheit kann der Produktnutzer nicht erwarten – auch nicht auf Grundlage des ProdHaftG.¹⁶⁷ Damit kann aber im Grundsatz von einer Einheitlichkeit der Fehlerbegriffe der deliktischen Produzentenhaftung nach § 823 Abs. 1 BGB und des ProdHaftG ausgegangen werden.¹⁶⁸ Die prima facie strikt erscheinende Haftung nach dem ProdHaftG wird folglich durch die berechtigten Sicherheitserwartungen des Verkehrs relativiert.¹⁶⁹ Vor diesem Hintergrund ist auch die dogmatische Klassifizierung der Haftung nach dem ProdHaftG nicht eindeutig. Regelmäßig wird sie als Kombination aus Gefährdungshaftung und verschuldensunabhängiger Haftung eingeordnet.¹⁷⁰ Anders als bei der Gefährdungshaftung im Allgemeinen wird nicht an die eigennützige Beherrschung einer erhöhten Gefahrenquelle angeknüpft, die auch bei Beachtung aller möglichen und zumutbaren Sicherheitsvorkehrungen unvermeidbar ist. Denn eine solche besondere Schadensneigung¹⁷¹ ist der Herstellung von Produkten nicht immanent. Vielmehr geht es dem ProdHaftG um eine gerechte Risikoverteilung entlang der bereits beschriebenen Verantwortungsbereiche.¹⁷²

Die verschiedenen Bezugspunkte der deliktischen Produzentenhaftung nach § 823 Abs. 1 BGB und der Haftung nach § 1 Abs. 1 S. 1, § 3 Abs. 1 ProdHaftG, nämlich die Verletzung von Verkehrssicherungspflichten bzw.

Nutzer und Dritte vor Gefahren aufgrund sicherheitsrelevanter Defizite von Produkten zu schützen; BGH, NJW 2009, 2952 (2953).

167 Wagner, Deliktsrecht, Kap. 9, Rn. 23; im Ausgangspunkt auch *Taschner*, NJW 1986, 611 (614).

168 Vgl. schon BT-Drs. 11/2447, S. 17; BGH, NJW 2009, 2952 (2953); Wagner, in: MüKo, BGB, § 3 ProdHaftG, Rn. 43 spricht davon, dass der Fehlerbegriff des ProdHaftG „entschlüsselt“ die deliktsrechtlichen Verhaltenspflichten ergibt; krit. *Helte*, Anforderungen an die Produktsicherheit, S. 50 ff.

169 Zudem wird ein fehlendes Verschulden über den Ausschluss des Entwicklungsfehlers in § 1 Abs. 2 Nr. 5 ProdHaftG berücksichtigt, vgl. B.II.5.

170 Vgl. *Graf v. Westphalen*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 45, Rn. 9; Wagner, in: MüKo, BGB, Einl. ProdHaftG, Rn. 25; *Oechsler*, in: Staudinger, BGB, Einl. ProdHaftG, Rn. 27.

171 Für die Beurteilung einer besonderen Schadensneigung spielt die Eintrittswahrscheinlichkeit, der Umfang des Schadens und die Ungewissheit über das Risiko eine Rolle, vgl. *Zech*, JZ 2013, 21 (25).

172 Vgl. Erwägungsgrund (1) Rechtsvereinheitlichung und Erwägungsgrund (4) Verbraucherschutz der RL 85/374/EWG. *Zech*, JZ 2013, 21 (23) stellt nicht zu Unrecht auf eine dahinterstehende Informationsasymmetrie zwischen Hersteller und Nutzer ab; krit. Wagner, in: MüKo, BGB, Einl. ProdHaftG, Rn. 17.

die Fehlerhaftigkeit eines Produkts, werden daher kaum einmal zu unterschiedlichen Ergebnissen führen, auch wenn die dogmatischen Begründungen divergieren. Im Folgenden wird daher grundsätzlich eine gemeinsame Darstellung der Herstellerpflichten gewählt und nur insoweit eine Trennung der beiden Haftungsregime vorgenommen, als spezifische Unterschiede bestehen.

2. Der Konstruktionsfehler

Ein Konstruktionsfehler liegt vor, wenn das Produkt schon seiner Konzeption nach unter dem gebotenen Sicherheitsstandard bleibt.¹⁷³ Konstruktionsfehler betreffen folglich die Planungs- und Entwicklungsphase eines Produkts und sind in dessen Bauplan angelegt. Aus diesem Grund haften Konstruktionsfehler allen Produkten einer Serie an.¹⁷⁴ Da diese Fehlerkategorie dem eigentlichen Produktionsprozess vorgelagert ist und die Konzeption am Zeichenbrett betrifft, stellt sich hier die Frage, welches Maß an Sicherheit der Hersteller dem Produkt in der Entwicklung überhaupt auf den Weg geben muss.¹⁷⁵ Geboten ist den allgemeinen Grundsätzen folgend die Sicherheit, die erforderlich und zumutbar ist.

a) Erforderlichkeit

Den Ausgangspunkt im Rahmen der Erforderlichkeit bildet der Erwartungshorizont der Verkehrsteilnehmer. Dieser wird nicht lediglich von den Produktnutzern oder dem Adressatenkreis des vermarkteten Produkts bestimmt, sondern auch von unbeteiligten Dritten (innocent bystander), die mit dem Produkt in Berührung kommen können.¹⁷⁶ Mit der Forderung nach einer maximalen Sicherheit wäre jedenfalls den Produktnutzern freilich wenig gedient. Denn weitergehende Sicherheitsmaßnahmen würden sich im Preis des Produkts niederschlagen oder gar zu einem gänzlichen

173 BGH, NJW 2009, 2952 (2953); *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), *Produkthaftungshandbuch*, § 24, Rn. 71.

174 *Wagner*, in: *MüKo*, BGB, § 823, Rn. 1071; *Sprau*, in: *Grüneberg*, BGB, § 3 Prod-HaftG, Rn. 8; *Förster*, in: *BeckOK*, BGB, § 823, Rn. 705.

175 Ähnlich stellt diese Frage auch *Wagner*, *Deliktsrecht*, Kap. 9, Rn. 14.

176 BGH, NJW 2009, 1669 (1670); *Staudinger*, in: *NK-BGB*, § 823, Rn. 169; *Schrader*, *DAR* 2018, 314 (317).

Verschwinden des Produktes auf dem Markt führen.¹⁷⁷ Während beispielsweise die Angleichung der sicherheitsrelevanten Fahrerassistenzsysteme bei Klein- und Luxusklassewagen zu einem Preisanstieg bei erstgenannter Fahrzeugklasse führen würde, würden Suchtmittel wie Alkohol oder Zigaretten aufgrund der ihr zwangsläufig anhaftenden und konstruktiv nicht zu ändernden Gesundheitsrisiken gar nicht mehr abgegeben werden.¹⁷⁸ Da die mit diesen Produkten verbundenen Gefahren allerdings offen zu Tage treten und für den Nutzer ohne weiteres ersichtlich sind und bei der Entscheidung zum Erwerb des Produkts einkalkuliert werden, bezieht sich hierauf – anders als bei Gefahren, vor denen sich der Verwender nicht schützen kann – die Konstruktionsverantwortung des Herstellers nicht.¹⁷⁹ Obwohl der Hersteller über überlegene Gefahrensteuerungsmöglichkeiten im Rahmen der Konstruktion verfügt, überlagert hier die eigenverantwortliche Nutzerentscheidung die Verantwortung des Herstellers.¹⁸⁰ Dies muss jedenfalls dann gelten, wenn der Nutzer die erhöhte Gefährlichkeit erkennen und sein Nutzungsverhalten darauf einstellen kann und zumindest eine Basissicherheit gewährleistet ist.¹⁸¹ Denn insoweit besteht eine Wechselbeziehung zwischen den Sorgfaltsanstrengungen des Herstellers und den Eigenschutzmaßnahmen des Nutzers. Beide Parteien dürfen darauf vertrauen, dass die jeweiligen Sorgfaltsstandards eingehalten werden.¹⁸²

Ausgehend von der Verkehrserwartung können nur solche Sicherungsmaßnahmen erforderlich sein, die sich innerhalb der Grenzen des technisch Möglichen halten. Abzustellen ist dabei auf den im Zeitpunkt des Inverkehrbringens des Produkts vorhandenen neuesten Stand der Wissenschaft und Technik. Dabei ist die Möglichkeit der Gefahrvermeidung gegeben, wenn nach gesichertem Fachwissen praktisch einsatzfähige Lösungen zur Verfügung stehen. Der Hersteller ist dagegen nicht dazu verpflichtet, solche Sicherheitskonzepte umzusetzen, die bisher nur „auf dem Reißbrett erarbeitet“ wurden oder noch in der Erprobung sind. Vielmehr muss eine

177 Instrukтив *Geistfeld*, Cal. L. Rev. 105 (2017), 1611 (1666).

178 Beispiele nach *Wagner*, Deliktsrecht, Kap. 9, Rn. 15.

179 *Wagner*, Deliktsrecht, Kap. 9, Rn. 15.

180 Allgemein *Edenfeld*, VersR 2002, 272 (272 ff.); vgl. auch *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), Produkthaftungshandbuch, § 24, Rn. 7 ff.

181 *Wagner*, in: *MüKo*, BGB, § 823, Rn. 1075; *Staudinger*, in: *NK-BGB*, § 823, Rn. 198; vgl. auch BGH, NJW 1990, 908 (909); prägnant OLG Naumburg, BeckRS 2014, 5588; zum ProdHaftG bereits BT-Drs. 11/2447, S. 18.

182 *Wagner*, in: *MüKo*, BGB, § 823, Rn. 533; dazu auch *v. Bar*, in: *Lieb* (Hg.), Produktverantwortung und Risikoakzeptanz, S. 29 (31).

„sicherheitstechnisch überlegene Alternativkonstruktion zum Serieneinsatz reif“ sein.¹⁸³

Maßgeblichen Einfluss auf die Verkehrserwartung hat der jeweilige Verwendungszweck des Produkts. Denn im Rahmen des bestimmungsgemäßen Gebrauchs vertraut der Nutzer in hohem Maße auf den Schutz vor schädlichen Verwendungsfolgen.¹⁸⁴ Wie weit dagegen die Verantwortung des Herstellers bei einem bestimmungswidrigen Gebrauch reicht, hängt maßgeblich davon ab, inwieweit er sich noch in den Grenzen des ursprünglichen Verwendungszwecks hält und wie nahe- oder fernliegend der Fehlgebrauch ist.¹⁸⁵ Zwar fällt die unmittelbare Nutzung des Produkts in die Verantwortungssphäre des Nutzers,¹⁸⁶ allerdings verfügt der Hersteller mit Blick auf die Erkennung und Vermeidung von Gefahren über derart überlegene Erkenntnismöglichkeiten, dass er gewisse Anwendungsfehler zu berücksichtigen hat.¹⁸⁷ Im Rahmen der normativ zu bestimmenden Verkehrserwartung begründet diese asymmetrische Verteilung der Gefahrensteuerungsmöglichkeiten damit eine Verantwortlichkeit des Herstellers und führt zu einer gewissen Ausdehnung des Vertrauensgrundsatzes.¹⁸⁸ Allein auf die bloße Gefahrenbeherrschung abzustellen greift zur Begründung von Verkehrspflichten indes zu kurz.¹⁸⁹ Daher muss der Hersteller auch einen zurechenbaren Anlass für die bestimmungswidrige Verwendung gesetzt haben.¹⁹⁰ Dies ist dann der Fall, wenn der Fehlgebrauch in den Herstellerhinweisen (vgl. § 2 Nr. 5 lit. a ProdSG) oder der Produktgestaltung (vgl. § 2 Nr. 5 lit. b ProdSG) angelegt ist und sich daher innerhalb des Verwendungszwecks des Produkts hält.¹⁹¹ Auch wenn die schadensverursachende Produktnutzung innerhalb des Verwendungszwecks liegt, haftet der Hersteller nur, wenn es sich um einen vorhersehbaren Fehlgebrauch handelt. Gemeint sind dabei solche Nutzungen, bei denen das Schadensrisiko nicht

183 So BGH, NJW 2009, 2952 (2953); vgl. auch *Klindt/Handorn*, NJW 2010, 1105 (1106).

184 *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), *Produkthaftungshandbuch*, § 24, Rn. 72 f.; v. *Bar*, in: *Lieb* (Hg.), *Produktverantwortung und Risikoakzeptanz*, S. 29 (32).

185 Ausführlich *Arndt/Wende*, ZfPC 2023, 110 (111 ff.).

186 Vgl. schon BGH, NJW 1975, 1827 (1829).

187 *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), *Produkthaftungshandbuch*, § 24, Rn. 127.

188 *Wagner*, in: *MüKo, BGB*, § 823, Rn. 537.

189 Vgl. bereits unter B.I.2.a).

190 Prägnant *Hornung/Fuchs*, *PharmR* 2012, 501 (507); *Oechsler*, in: *Staudinger, BGB*, § 3 ProdHaftG, Rn. 64.

191 *Arndt/Wende*, ZfPC 2023, 110 (111).

schon offensichtlich zu Tage tritt, die aber naheliegend und vorhersehbar sind und mit denen folglich gerechnet werden muss.¹⁹² Diesem so verstandenen Fehlgebrauch hat der Hersteller jedenfalls im Ausgangspunkt schon mit konstruktiven Sicherungsmaßnahmen entgegenzuwirken.¹⁹³

b) Zumutbarkeit

Die sich in diesem Sinne als erforderlich herausgebildeten Sicherheitsmaßnahmen sind in einem zweiten Schritt durch die wirtschaftliche Zumutbarkeit begrenzt. Es geht darum, unrealistische Anforderungen an die berechtigterweise zu erwartenden Sicherheitsstandards zu vermeiden.¹⁹⁴ Der Umfang der Verkehrspflicht wird auf das beschränkt, was „billige Rücksicht nach der Verkehrsauffassung“ gebietet.¹⁹⁵ Nicht alle Sicherungsmaßnahmen, die objektiv möglich sind, werden vom Verkehrssicherungspflichtigen auch gefordert.¹⁹⁶ Dabei sind sämtliche Umstände des Einzelfalls zu berücksichtigen. Insbesondere stehen sich die Größe der vom Produkt ausgehenden Gefahr und die wirtschaftlichen Auswirkungen der Sicherungsmaßnahme gegenüber.¹⁹⁷ Je größer die Gefahr ist, desto mehr kann dem Pflichtigen zugemutet werden. Die Gefährlichkeit richtet sich dabei nach der Höhe des Schadens und dem Grad der Eintrittswahrscheinlichkeit, wobei die Schadenshöhe vom Rang des betroffenen Rechtsguts und der Intensität seiner Verletzung bestimmt wird.¹⁹⁸

Der wirtschaftliche Aufwand der Sicherheitsmaßnahmen ist vor diesem Hintergrund in Relation zu ihrem Nutzen und damit dem Wert der ins-

192 *Wagner*, in: MüKo, BGB, § 3 ProdHaftG, Rn. 26 f.

193 Zum Spannungsfeld, das sich daraus ergibt, dass der Hersteller den Verwendungszweck durch Hinweise im Sinne einer Instruktion mitbeeinflussen kann, gleichzeitig aber einen vorhersehbaren Fehlgebrauch konstruktiv zu verhindern hat, *Schrader*, DAR 2018, 314 (319), in Bezug auf das autonome Fahren; vgl. auch LG Düsseldorf, NJW-RR 2006, 1033 (1034); *Reusch*, in: Kaulartz/Braegelmann (Hg.), Artificial Intelligence und Machine Learning, S. 119 f. positioniert sich überzeugend gegen eine vornehmliche Beeinflussung des Verwendungszwecks durch herstellerseitige Instruktionen.

194 So *Klindt/Handorn*, NJW 2010, 1105 (1106).

195 BGH, NJW 1985, 270 (270); BGH, NJW 1972, 724 (726).

196 Vgl. BGH, NJW 1964, 814 (816 f.), *Foerste*, in: *Foerste / Graf v. Westphalen* (Hg.) Produkthaftungshandbuch, § 23, Rn. 15.

197 Vgl. BGH, NJW 2009, 2952 (2953 f.).

198 Vgl. schon allgemein unter B.I.2.b)aa).

gesamt vermiedenen Schäden zu setzen.¹⁹⁹ Maßgeblich ist damit eine Kosten-Nutzen-Abwägung. Daher gilt: Je höher der zu erwartende Schaden, je wahrscheinlicher dessen Eintritt und je geringer der Aufwand der Sicherungsmaßnahmen, desto eher können diese dem Verkehrssicherungspflichtigen zugemutet werden. Sind die Mehrkosten einer Alternativkonstruktion gegenüber der tatsächlich gewählten Konstruktion höher als die Summe der dadurch vermiedenen Schäden, ist die Zumutbarkeit grundsätzlich zu verneinen und ein Konstruktionsfehler liegt nicht vor.²⁰⁰ Bei erheblichen Gefahren für Leben und Gesundheit von Menschen sind dem Hersteller dagegen weitergehende Maßnahmen zumutbar.²⁰¹ Richtig verstanden führt die Kosten-Nutzen-Rechnung auch nicht dazu, dass der Hersteller aufgrund seiner wirtschaftlichen Belastung den Sicherheitsstandard absenken und die Fehlerhaftigkeit des Produktes selbst bestimmen kann.²⁰² Denn der Nutzen zielt nicht lediglich auf die gebrauchstypischen Vorteile eines Produkts ab, sondern meint ausgehend von der Kenngröße der Gefährlichkeit insbesondere den Sicherheitsgewinn.²⁰³

3. Der Fabrikationsfehler

Von einem Fabrikationsfehler ist die Rede, wenn aufgrund eines Mangels im tatsächlichen Herstellungsprozess von den konstruktiven Vorgaben abgewichen wird oder diese nicht ordnungsgemäß umgesetzt werden, diese Tatsache nicht entdeckt wird, und dadurch ein mit einem Sicherheitsrisiko belastetes Produkt in den Verkehr gelangt. Das in den Entwurfszeichnungen und Konstruktionsplänen pflichtgemäß angelegte Sicherheitsniveau wird folglich in der Realität des Fertigungsprozesses nicht erreicht.²⁰⁴ Die dahintersteckende Sorgfaltspflicht des Herstellers geht dahin, seinen Herstellungsprozess so auszugestalten, dass Fabrikationsfehler vermieden bzw. Qualitätskontrollen durchgeführt werden, um mangelhafte Produktex-

199 Wagner, in: MüKo, BGB, § 823, Rn. 531.

200 Wagner, in: MüKo, BGB, § 823, Rn. 1091.

201 BGH, NJW 2009, 2952 (2954).

202 In diese Richtung krit. aber Taschner, ZeuP 2012, 560 (564).

203 Dies fordert zu Recht Schrader, in: Buck-Heeb/Oppermann (Hg.), Automatisierte Systeme, S. 333 (354 f.); so aber ohnehin Wagner, AcP 217 (2017), 707 (732 f.).

204 Vgl. Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 177; Lüftenegger, Die Rückrufpflicht des Herstellers, S. 78 f.; Wagner, Deliktsrecht, Kap. 9, Rn. 21 f. Abweichung der „Istbeschaffenheit des Produkts von der vom Hersteller selbst angestrebten Sollbeschaffenheit“.

emplare vor dem Warenausgang auszusortieren.²⁰⁵ An einer Pflichtverletzung kann es aber bei einem sog. „Ausreißer“ fehlen. Dabei handelt es sich um menschliches Fehlverhalten oder technische Defekte, die trotz Einhaltung aller Sorgfaltspflichten nicht auszuschließen und daher unvermeidbar sind.²⁰⁶ Denn eine Null-Fehlerquote schuldet der Hersteller im Rahmen der Fabrikation ebenfalls nicht. Auch insoweit ist zunächst auf die allgemeinen Grundsätze zurückzugreifen, wonach Sicherungsmaßnahmen insbesondere auf das zumutbare Maß begrenzt sind.²⁰⁷ Kommt der Hersteller seinen an diesen Maßstäben zu messenden Sorgfaltspflichten im Fabrikationsbereich nach, haftet er schon nicht für ein fehlerhaft hergestelltes Produkt, auch wenn dessen Inverkehrgabe durch eine engmaschigere (aber nicht zumutbare) Produktkontrolle hätte vermieden werden können.²⁰⁸ Sind bei äußerster Sorgfalt und unter Einhaltung der zumutbaren Sicherheitsvorkehrungen fehlerhafte Exemplare gleichwohl unvermeidbar, bleibt kein Anknüpfungspunkt mehr für die Verletzung einer Sorgfaltspflicht, da dem Hersteller insoweit nichts Unmögliches abverlangt werden kann.

Dass sich die Haftung nach dem ProdHaftG für Fabrikationsfehler auch bei Ausreißern „bis auf Haaresbreite“ an die deliktische Produzentenhaftung angenähert hat,²⁰⁹ verwundert nicht. Denn wenn im Rahmen der deliktsrechtlichen Verkehrspflichten ein technisch möglicher Sicherheitsaufwand insbesondere bei der Warenausgangskontrolle für den Hersteller aufgrund hoher Kosten und demgegenüber geringem Gefährdungspotential unzumutbar sein kann, können die Verkehrsteilnehmer solche Maßnahmen im Rahmen des § 3 Abs. 1 ProdHaftG auch berechtigterweise nicht erwarten. Die dann von dem Produkt ausgehenden Gefahren sind hinzunehmen

205 Eine Auflistung der diesbezüglichen Organisationspflichten im Einzelnen findet sich bei *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), *Produkthaftungshandbuch*, § 24, Rn. 181 ff.

206 Vgl. nur *Voigt*, in: *BeckOGK*, BGB, § 823, Rn. 657.

207 Vgl. explizit zum Fabrikationsfehler BGH, NJW 2009, 1669 (1670); *Wagner*, *Deliktsrecht*, Kap. 9, Rn. 22.

208 Hält man die Möglichkeit eines Ausreißers aufgrund der heutigen technischen Möglichkeiten der Endkontrolle für faktisch ausgeschlossen bzw. bestimmt man die auf die Verhinderung von Fabrikationsfehlern gerichteten Organisationspflichten nahezu lückenlos, verkennt man das einschränkende Kriterium der Zumutbarkeit. So aber *Wilhelmi*, in: *Erman*, BGB, § 823, Rn. 117; dagegen *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), *Produkthaftungshandbuch*, § 24, Rn. 178 f. und *Voigt*, in: *BeckOGK*, BGB, § 823, Rn. 657.

209 So *Wagner*, *Deliktsrecht*, Kap. 9, Rn. 23; *Wagner*, *AcP* 217 (2017), 707 (712).

und ein Produktfehler ist abzulehnen.²¹⁰ Damit dürfte die Haftung nach dem ProdHaftG für Ausreißer nur noch dann über die deliktische Haftung hinausgehen,²¹¹ wenn trotz Anwendung äußerster Sorgfalt und unter Einhaltung der zumutbaren Sicherungsmaßnahmen ein Fabrikationsfehler unvermeidbar ist. In diesem Kontext hat der Hersteller nach dem ProdHaftG jedenfalls auch für Ausreißer im Rahmen der Fabrikation einzustehen. Denn auf die Verletzung einer Verkehrspflicht kommt es eben bei der Fehlerbestimmung nach § 3 ProdHaftG nicht an. Darüber hinaus handelt es sich bei Ausreißern regelmäßig um erkennbare, aber nicht vermeidbare Gefahren, sodass der Anwendungsbereich des Haftungsausschlusses des § 1 Abs. 2 Nr. 2 ProdHaftG unabhängig von der Frage der generellen Anwendbarkeit auf Fabrikationsfehler nicht eröffnet ist.²¹²

4. Der Instruktionsfehler

Dem Instruktionsbereich kommt mit Blick auf die Verhinderung von Produktgefahren zweierlei Bedeutung zu. Zum einen sollen dem Nutzer alle Informationen zur Verfügung gestellt werden, mit deren Hilfe er das Produkt richtig und sicher verwenden kann („Verwendungshinweise“). Zum anderen soll er auf die Gefahren hingewiesen werden, die trotz sorgfältiger Konstruktion und Fabrikation von einem Produkt ausgehen können („Gefahren- oder Sicherheitshinweise“).²¹³ Demnach liegt ein Instruktions-

210 Zu dieser Argumentation BGH, NJW 2009, 1669 (1670 f.); krit. *Taschner*, ZEuP 2012, 560 (564), der von der fehlenden Zumutbarkeit – wohl aufgrund der Ablehnung der reinen Berücksichtigung der Kosten – nicht auf eine fehlende Verkehrserwartung schließt, sondern anhand des Kriteriums der Sozialadäquanz wohl aber zu gleichen Ergebnissen kommt; krit. auch *Helte*, Anforderungen an die Produktsicherheit, S. 52 f. der von einer zweifelhaften Fiktion der Sicherheitserwartung spricht. Diese Sichtweisen verkennen aber, dass die Unzumutbarkeit nicht allein an den herstellerseitig anfallenden Kosten zu messen ist, sondern stets die Gefährlichkeit miteinbezieht (s. schon o.). Daher verwundert es nicht, dass der BGH – anders als bei einem in einem Kirschtaler (Gebäck) verbliebenen Kirschkern (BGH, NJW 2009, 1669) – bei zerberstenden Glasflaschen eine Aussonderung (BGH, NJW 1995, 2162) dieser mit Rissen versehenen Flaschen fordert, eine dahingehende Verkehrserwartung und damit einen Fehler annimmt, auch wenn eine Risikoflasche beim Hersteller nicht mit absoluter Sicherheit erkannt und aussortiert werden kann (vgl. auch OLG München, BeckRS 2011, 10312).

211 Ohne Einschränkung *Lenz*, in: *Lenz*, Produkthaftung, § 3, Rn. 325.

212 Vgl. *Oechsler*, in: *Staudinger*, BGB, § 3 ProdHaftG, Rn. 107.

213 Diese Zweiteilung erkennen u.a. *Lüftenegger*, Die Rückrufpflicht des Herstellers, S. 80; *Wagner*, Deliktsrecht, Kap. 9, Rn. 27 und *Steege*, NZV 2021, 6 (10); in diese

fehler vor, wenn diese Hinweise unterlassen oder unklar, unvollständig oder mit fehlendem Nachdruck formuliert wurden. Mit der Information trägt der Hersteller seinem überlegenen Kenntnisstand über die Produkteigenschaften Rechnung. Die Verwendungshinweise sollen den Nutzer in die Lage versetzen, das Produkt eigenverantwortlich zu verwenden. Die Gefahrenhinweise knüpfen dort an, wo die Konstruktions- und Fabrikationsverpflichtungen ihr Ende finden.²¹⁴ Denn gehen von einem Produkt bei der Verwendung Gefahren aus, weil Sicherungsmaßnahmen nicht erforderlich, insbesondere technisch nicht möglich oder dem Hersteller nicht zumutbar waren, trifft ihn die Pflicht, die Produktnutzer vor denjenigen Gefahren zu warnen, die bei bestimmungsgemäßem Gebrauch oder naheliegendem Fehlgebrauch drohen und die nicht zum allgemeinen Gefahrenwissen des Benutzerkreises gehören.²¹⁵

Anders als im Rahmen des Produktsicherheitsrechts, wo es grundsätzlich dem Hersteller überlassen bleibt, auf welche Weise er das vorgegebene Schutzziel der Produktsicherheit erreichen will,²¹⁶ macht schon diese dem BGH entnommene Formulierung ein Stufenverhältnis deutlich. Erst wenn Produktgefahren nicht durch erforderliche und zumutbare Sicherungsmaßnahmen abgewehrt werden können, darf sich der Hersteller subsidiär auf eine Instruktion hinsichtlich der verbleibenden Restrisiken²¹⁷ zurückziehen. Es gilt der Vorrang der Konstruktion vor der Instruktion.²¹⁸ Eine noch

Richtung auch *Wagner*, in: MüKo, BGB, § 823, Rn. 1098: „Die Schadensneigung eines Produkts hängt nicht nur von seinen Sicherheitseigenschaften ab, sondern auch von der Art und Weise, wie der Nutzer Gebrauch von ihm macht.“

214 So treffend *Wagner*, Deliktsrecht, Kap. 9, Rn. 27.

215 Vgl. BGH, NJW 2009, 2952 (2954).

216 *Schucht/Klindt*, in: Klindt, ProdSG, § 2, Rn. 224 mit Verweis auf OLG Hamm, NJW-RR 2009, 1537 (1538), wonach bzgl. der Verwechslung von Zapfsäulen deutliche Warnhinweise (mehrfache Beschriftungen sowie durch Aufkleber sogar auf der Zapfpistole (als „letzte Instanz“)) als hinreichende Schutzmaßnahme vor Fehlanwendungsgefahren ausreichend seien, vgl. hierzu *Molitoris/Klindt*, NJW 2010, 1569 (1572); *Schucht*, BB 2020, 1990 (1992); anders aber *Heuser*, in: NK-ProdR, § 2 ProdSG, Rn. 180; differenzierend *Reusch*, BB 2017, 2248 (2249 f.), welcher im B2B-Bereich eine vorrangige Warnung für ausreichend hält, nicht aber im B2C-Bereich.

217 Diese Formulierung verwendet *Lenz*, in: Lenz, Produkthaftung, § 3, Rn. 205.

218 Vgl. *Ackermann*, in: NK-ProdR, § 823 BGB, Rn. 110; *Wagner*, Deliktsrecht, Kap. 9, Rn. 27; *Foerste*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 127; *Klindt/Handorn*, NJW 2010, 1105 (1105); implizit BGH, NJW 2009, 2952 (2954); LG Düsseldorf, NJW-RR 2006, 1033 (1034) allerdings in Bezug auf eine Maschine, die der Maschinenrichtlinie 2006/42/EG unterfällt, welche in Anhang I Nr. 1.1.2 lit. B ohnehin den Vorrang inhärent sicherer Konstruktion vor reinen Sicherheitshinweisen normiert; OLG Naumburg, BeckRS 2014, 5588.

so umfassende Instruktion kann den Hersteller – und dies gilt auch hinsichtlich des vorhersehbaren Fehlgebrauchs²¹⁹ – nicht von der Pflicht zur sicheren Konstruktion und Fabrikation befreien. Folglich können Pflichtverletzungen des Herstellers in diesen Bereichen nicht durch eine Instruktion geheilt werden.²²⁰ Anknüpfend an die Tatsache, dass nicht sämtliche Gefahren präventiv zu vermeiden sind, soll es dem Nutzer durch die Gefahrenhinweise ermöglicht werden, selbst abzuwägen, ob er das Produkt aufgrund seiner Vorteile trotz der mit seiner Verwendung verbundenen Restrisiken nutzen möchte. Darüber hinaus soll er in die Lage versetzt werden, sich auch selbst vor diesen Gefahren zu schützen.²²¹ Der Grund für dieses Vorrangverhältnis kann wiederum in der Abgrenzung der Verantwortungsbereiche gesehen werden. Da der Herstellungsprozess eigentümlich der Sphäre des Herstellers zuzuordnen ist, hat er diesen so zu organisieren, dass Gefahren für Dritte erst gar nicht entstehen. Er ist damit im Rahmen des Erforderlichen und Zumutbaren verpflichtet, nur sichere Produkte in den Verkehr zu geben und darf diese Gefahrsteuerungslast nicht im Wege der Instruktion auf den Produktnutzer abwälzen.²²² Soweit sich die Gefahren bereits im Herstellungsprozess erkennen und zumutbar vermeiden lassen, wäre eine solche Verantwortungsverschiebung auf den Nutzer auch in Anbetracht der Vorteile, die der Hersteller in Form des Gewinns aus der Vermarktung des Produkts zieht, nicht gerechtfertigt. Hinzu kommt, dass Warnungen aufgrund der schieren Masse der Produkte auf dem Markt von den Nutzern gar nicht vollumfänglich befolgt werden könnten. Dies würde mit einem Sicherheitsverlust auf dem gesamten Produktmarkt einhergehen und den Vertrauensgrundsatz aushöhlen.²²³

219 Wie im Rahmen der Konstruktionspflichten endet die Verantwortung des Herstellers grundsätzlich dort, wo der Bereich des naheliegenden Fehlgebrauchs überschritten wird; vgl. statt aller mit Beispielen aus der Rspr. Förster, in: BeckOK, BGB, § 823, Rn. 724 ff.

220 Ackermann, in: NK-ProdR, § 823 BGB, Rn. 110; Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 220.

221 Vgl. BGH, NJW 2009, 2952 (2954).

222 So Wagner, in: MüKo, BGB, § 823, Rn. 1092; vgl. auch LG Düsseldorf, NJW-RR 2006, 1033 (1034), wonach es dem Hersteller ansonsten leicht möglich wäre, durch umfangreiche Angaben und Hinweise sämtliche Sicherheitsanforderungen zu umgehen und lediglich auf die Risiken zu verweisen oder jegliche gefahrbringende Verwendung auszuschließen.

223 In diese Richtung Wagner, in: MüKo, BGB, § 823, Rn. 1092. Zum Vertrauen, das Produktnutzer der Sicherheit von Produkten berechtigterweise entgegenbringen dürfen Wilhelmi, in: Erman, BGB, § 823, Rn. 112 und Klinger, Die Produktbeobachtungspflicht bezüglich Fremdzubehörteilen, S. 35.

Das Stufenverhältnis²²⁴ reicht über die Instruktion hinaus. Denn sind die mit der Produktnutzung verbundenen Restrisiken nach dem maßgeblichen Stand von Wissenschaft und Technik nicht oder nicht zumutbar zu vermeiden, ist unter Abwägung von Art und Umfang der Risiken, der Wahrscheinlichkeit ihrer Verwirklichung und des mit dem Produkt verbundenen Nutzens zu prüfen, ob das gefahrträchtige Produkt überhaupt in den Verkehr gebracht werden darf.²²⁵ Diese Abwägung ist selbst bei Gefahren für Leib und Leben möglich.²²⁶ Bei solch schützenswerten Rechtsgütern müssen die Risiken allerdings minimal sein.²²⁷ Angesprochen ist in jedem Fall wieder eine zu gewährleistende Basissicherheit.²²⁸ Fällt diese Abwägung negativ aus, ist auch eine Warnung aufgrund der verbundenen Schwere der Gefahr nicht ausreichend.²²⁹ Ergibt sich dagegen eine positive Risiko-Nutzen-Abwägung, darf das Produkt in den Verkehr gegeben werden und wird die Risikotragung sowohl den Benutzern als auch den innocent bystandern aufgebürdet.²³⁰

5. Der Entwicklungsfehler

Keine Fehlerkategorie im eigentlichen Sinne bildet der Entwicklungsfehler. Vielmehr geht es dabei um Produktgefahren, welche auch nach dem neusten Stand der Technik nicht vermieden werden können²³¹ und daher die herstellereitige Pflichtverletzung in Frage stellen.²³²

Ein Entwicklungsfehler im klassischen Sinne liegt vor, wenn der den Schaden verursachende Fehler des Produkts im Zeitpunkt seiner Inver-

224 Vgl. *Sommer*, Haftung für autonome Systeme, S. 234.

225 BGH, NJW 2009, 2952 (2953); bereits BGH, NJW 1972, 2217 (2220).

226 *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), Produkthaftungshandbuch, § 24, Rn. 61.

227 *Ebers*, in: *Oppermann/Stender-Vorwachs* (Hg.), Autonomes Fahren, 1. Aufl., S. 93 (110); vgl. allgemein zu akzeptierten Restrisiken *Schulz*, NZV 2017, 548 (550 f.).

228 In diesem Kontext *Goehl*, in: BeckOGK, BGB, § 3 ProdHaftG, Rn. 32.

229 *Wagner*, in: MüKo, BGB, § 823, Rn. 1090; unter dem Gesichtspunkt des Handelns auf eigene Gefahr tendenziell weniger restriktiv *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), Produkthaftungshandbuch, § 24, Rn. 110.

230 *Klindt et al.*, in: *Bräutigam/Klindt* (Hg.), Digitalisierte Wirtschaft/Industrie 4.0, S. 76 (89).

231 Grundlegend zur Unvermeidbarkeit von Risiken *Haagen*, in: Beck/Kusche/Valerius (Hg.): Digitalisierung, Automatisierung, KI und Recht, S. 215 (224 f.).

232 Vgl. *Lüftenegger*, Die Rückrufpflicht des Herstellers, S. 80 f; *Krause*, in: *Viehweg* (Hg.), Risiko – Recht – Verantwortung, S. 451 (453).

kehrgabe nach dem damaligen Stand von Wissenschaft und Technik nicht erkennbar²³³ war.²³⁴ Von einem Entwicklungsfehler ist regelmäßig die Konstruktion betroffen, wenngleich er auch im Rahmen der Instruktion oder Fabrikation denkbar ist.²³⁵ Da sich die Sorgfaltspflichten des Herstellers ex ante auf den Zeitpunkt des Inverkehrbringens beziehen, kommt es allein auf das historische Erkenntniswissen zu diesem Zeitpunkt an.²³⁶ Wo ein umsichtiger Hersteller im Zeitpunkt des Inverkehrbringens nicht erkennen konnte, dass von seinem Produkt Gefahren ausgehen, fehlt es an einer Verkehrspflichtverletzung.²³⁷ Da das entsprechende Risikowissen nicht verfügbar ist, lässt sich nämlich schon kein entsprechendes Verhaltensgebot

233 Zur Frage, wann eine Gefahr in diesem Sinne erkennbar ist bzw. welche Anstrengungen zur Aufklärung des Risikopotentials erwartet werden können *Röthel*, in: Eifert/Hoffmann-Riem (Hg.), Innovationsverantwortung, S. 335 (340 f.).

234 Vgl. BGH, NJW 2009, 2952 (2955).

235 Für den Fabrikationsbereich vgl. *Foerste*, in: Foerste/Graf v. Westphalen, Produkthaftungshandbuch, § 24, Rn. 104; für den Instruktionsbereich siehe BGH, NJW 2009, 2952 (2955). Im Rahmen des Produkthaftungsgesetzes ist streitig, ob sich der Hersteller auch bei Fabrikationsfehlern auf das Vorliegen eines Entwicklungsrisikos berufen kann, vgl. *Wagner*, in: MüKo, BGB, § 3 ProdHaftG, Rn. 55; ablehnend BGH, NJW 1995, 2162 (2163).

236 *Wagner*, in: MüKo, BGB, § 823, Rn. 1082; *Wagner*, Deliktsrecht, Kap. 9, Rn. 20; BGH, NJW 1981, 1603 (1604).

237 Hier zeigt sich der im Rahmen der Produzentenhaftung nach § 823 Abs. 1 BGB liegende Unterschied zwischen einem Produktmangel in Form eines Sicherheitsdefizits und der daneben erforderlichen Sorgfaltspflichtverletzung. Da ein Entwicklungsfehler zwar nicht erkannt werden konnte, aber bei Erkennen technisch vermeidbar gewesen wäre, geht regelmäßig der Erwartungshorizont der Verkehrsteilnehmer dahin, dass sie vor den schädlichen Verwendungsfolgen geschützt werden. Damit liegt aber ein objektiver Mangel vor, ohne dass den Hersteller eine objektive Pflichtwidrigkeit trifft, vgl. in diese Richtung *Hager*, in: Staudinger, BGB, § 823, Rn. E 25 und *Hager*, VersR 1984, 799: Auch bei einem Entwicklungsfehler liegt eine aus der Sphäre des Herstellers stammende Ursache für den Schaden des Nutzers vor; zum Fehlen der objektiven Pflichtwidrigkeit BGH, NJW 2009, 2952 (2955); aus diesem Grund bedarf es im Rahmen des ProdHaftG eines explizit geregelten Ausschlussstatbestands, vgl. § 1 Abs. 2 Nr. 5 ProdHaftG. Nimmt man im Rahmen des § 823 Abs. 1 BGB die zwei Komponenten des Fehlerbegriffs ernst, dürfte man m.E. folglich terminologisch schon gar nicht von einem Fehler sprechen (so wohl auch *Etzkorn*, MMR 2020, 360 (362)). Ansonsten würde man eine unmöglich zu erfüllende Sorgfaltspflicht zu einem Fehler verschlüsseln. Dies legt eine in Nuancen abweichende Bestimmung der Fehlerbegriffe im Rahmen des § 823 Abs. 1 BGB und § 3 Abs. 1 ProdHaftG nahe (s.u.).

an den Hersteller zur Gefahrenvermeidung adressieren.²³⁸ Bezugspunkt der Erkennbarkeit ist dabei nicht der konkrete Fehler des schadensstiftenden Produkts, sondern das zu Grunde liegende allgemeine, mit der gewählten Konzeption verbundene, Fehlerrisiko, also die potenzielle Gefährlichkeit des Produkts.²³⁹ Von den Verantwortungssphären her gedacht, verfügt der Hersteller bei einem Entwicklungsfehler über keine besseren Erkenntnisse als der Produktnutzer. Dieses Fehlen der Informationsasymmetrie rechtfertigt es, dass der Produktnutzer seinen Schaden selbst zu tragen hat.²⁴⁰

Im Rahmen des ProdHaftG ist der Entwicklungsfehler als Haftungsausschluss eigens in § 1 Abs. 2 Nr. 5 ProdHaftG geregelt. Die Tatsache, dass es für den Entwicklungsfehler einen eigenen Ausschlussstatbestand²⁴¹ braucht, zeigt, dass die Haftung gegenständlich allein an die Fehlerhaftigkeit des Produkts anknüpft und es auf eine Verkehrspflichtverletzung des Herstellers nicht ankommt, gleichzeitig Verschuldenselemente aber doch berücksichtigt werden. Insoweit kann die berechtigte Verkehrserwartung nach § 3 Abs. 1 ProdHaftG die objektiven Sorgfaltspflichten des Herstellers im Rahmen von § 823 Abs. 1 BGB nur teilweise abbilden.²⁴² Denn die Nichterkennbarkeit von Produktgefahren als begrenzte menschliche Erkenntnis betrifft nicht die Erforderlichkeit und Zumutbarkeit, sondern einen weiteren Aspekt der objektiven Pflichtwidrigkeit, der sich nicht in der berechtigten Verkehrserwartung niederschlägt und damit keine Auswirkung auf das Vorliegen eines Fehlers hat. Dort nämlich, wo die Integritätserwartung des Produktnutzers nicht durch Erwägungen der Erforderlichkeit oder Zumutbarkeit eingeschränkt wird, ist ein Produkt – bei vorausgesetzter Kausalität – allein aufgrund des Eintrittes einer Beeinträchtigung fehlerhaft, ohne dass es darauf ankommt, ob der Hersteller die Gefahr erkennen konnte. Es kommt auf die Enttäuschung der – unter Berücksichtigung der Erforderlichkeit und Zumutbarkeit – berechtigten Sicherheitserwartung an, nicht auf die Gründe der unterlassenen Sicherungsmaßnahmen.²⁴³ Einem

238 Röthel, in: Eifert/Hoffmann-Riem (Hg.), Innovationsverantwortung, S. 335 (338 f.); Krause, in: Viehweg (Hg.), Risiko – Recht – Verantwortung, S. 451 (453).

239 BGH, NJW 2009, 2952 (2955).

240 Vgl. Zech, JZ 2013, 21 (23).

241 Technische Gefährdungshaftungen wie das AMG oder das GenTG enthalten einen Ausschlussstatbestand für Entwicklungsrisiken gerade nicht. Auch dies zeigt die Sonderrolle des ProdHaftG.

242 In diese Richtung auch Helte, Anforderungen an die Produktsicherheit, S. 50 f. und Krause, in: Viehweg (Hg.), Risiko – Recht – Verantwortung, S. 451 (467 f.).

243 Hierzu Oechsler, in: Staudinger, BGB, § 1 ProdHaftG, Rn. 120a f.; Taschner, NJW 1986, 611 (615).

solchen Fehler kann der Hersteller dann erst auf zweiter Verteidigungslinie mit dem Haftungsausschluss des § 1 Abs. 2 Nr. 5 ProdHaftG begegnen.²⁴⁴ Dagegen liegt schon kein Fehler und damit zwangsläufig auch kein Fall für den Haftungsausschluss vor, wenn das Produkt die historischen Sicherheitserwartungen zum Zeitpunkt des Inverkehrbringens erfüllt hat (vgl. § 3 Abs. 1 lit. c ProdHaftG). Technischer Fortschritt, welcher im Nachhinein zu höheren Sicherheitserwartungen und damit zu verschärften Anforderungen führt, kann ein ursprünglich den Sicherheitserwartungen jener Zeit entsprechendes und damit fehlerfreies Produkt nicht nachträglich zu einem fehlerhaften Produkt machen (insoweit klarstellend § 3 Abs. 2 ProdHaftG).²⁴⁵

6. Die Entwicklungslücke

Von einem Entwicklungsfehler im klassischen Sinne ist die sog. Entwicklungslücke zu unterscheiden. Bei dieser war die Produktgefahr ex ante zwar bekannt oder erkennbar, allerdings bestand zum maßgeblichen Zeitpunkt des Inverkehrbringens nach dortigem Stand von Wissenschaft und Technik keine hinreichende Möglichkeit, die Gefahr zu vermeiden.²⁴⁶ Zwar mangelte es hier ex ante gesehen nicht am erforderlichen Erkenntniswissen, wohl aber an den zum Zeitpunkt der Inverkehrgabe zur Verfügung stehenden Sicherheitstechnologien. Damit kann dem Hersteller im Ausgangspunkt auch hinsichtlich der Entwicklungslücke kein Sorgfaltsverstoß angelastet werden.²⁴⁷ Gleichwohl greift es zu kurz davon zu sprechen, dass eine Entwicklungslücke stets zu Lasten des Geschädigten geht.²⁴⁸ Denn zu beachten ist wiederum das bereits dargestellte Stufenverhältnis. Danach kann die Pflichtverletzung des Herstellers darin gesehen werden, dass er ein Produkt trotz vorhandener Restrisiken in den Verkehr gibt, das nicht die berechtig-

244 Vgl. Förster, in: BeckOK, BGB, § 1 ProdHaftG, Rn. 53; Kort, VersR 1989, 1113 (1113 ff.).

245 Allgemeine Meinung, vgl. Taschner, NJW 1986, 611 (614 f.); Kort, VersR 1989, 1113 (1113 ff.); Förster, in: BeckOK, BGB, § 1 ProdHaftG, Rn. 53.

246 Vgl. Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 107; Wagner, in: MüKo, BGB, § 823, Rn. 1082; Foerste, JZ 1995, 1063 (1063); Viehweg, in: Schulte/Schröder (Hg.): Handbuch des Technikrechts, S. 337 (378).

247 Daher ohne terminologische Differenzierung Wagner, Deliktsrecht, Kap. 9, Rn. 20; mit Differenzierung Wagner, in: MüKo, BGB, § 823, Rn. 1082 und Röthel, in: Eifert/Hoffmann-Riem (Hg.), Innovationsverantwortung, S. 335 (339).

248 So aber Röthel, in: Eifert/Hoffmann-Riem (Hg.), Innovationsverantwortung, S. 335 (339); dagegen Hager, in: Staudinger, BGB, § 823, Rn. E 25.

terweise zu erwartende Mindestsicherheit bietet²⁴⁹ und trotz der mit seiner Verwendung verbundenen Vorteile zu gefährlich ist.²⁵⁰ Mit der Inverkehrgabe ist eine Risikoeinschätzung²⁵¹ des Herstellers verbunden, gegenüber deren Folgen er sich nicht damit entlasten kann, dass er den Eintritt des Risikos nicht vermeiden konnte.²⁵² Lediglich im Übrigen, dort also wo der hinreichend instruierte Produktnutzer das mit der Verwendung des Produkts bekannte Risiko weitgehend hinnimmt, geht der Risikoeintritt zu Lasten des Nutzers.

Im ProdHaftG ist die Entwicklungslücke nicht vom Haftungsausschluss des § 1 Abs. 2 Nr. 5 ProdHaftG umfasst.²⁵³ Denn § 1 Abs. 2 Nr. 5 ProdHaftG stellt schon vom Wortlaut allein auf die fehlende Erkennbarkeit, nicht dagegen auf die fehlende Vermeidbarkeit der Gefahr ab.²⁵⁴ Geht folglich bei einer erkennbaren, aber nach den technischen Möglichkeiten im Zeitpunkt des Inverkehrbringens nicht vermeidbaren Gefahr, die berechtigte Verkehrserwartung dahin, keine Beeinträchtigungen durch das Produkt zu erleiden, liegt ein Produktfehler vor, für den kein Ausschlusstatbestand

249 Da anders als im Falle eines Entwicklungsfehlers die Gefahrenbeseitigung technisch unmöglich ist und eine Sicherungsmaßnahme mangels verfügbarer Alternativkonstruktion gar nicht erforderlich sein kann, stellt sich hier die Frage, ob überhaupt von einem Produktmangel gesprochen werden kann, in verschärfter Form. Ausgehend von der berechtigten Verkehrserwartung vor den schädlichen Verwendungsfolgen geschützt zu werden, lässt sich jedenfalls ein Sicherheitsdefizit annehmen. Gleichwohl fehlt es an der objektiven Pflichtwidrigkeit. Im Rahmen von § 823 Abs. 1 BGB dürfte damit m.E. schon das Vorliegen eines Fehlers abzulehnen sein (s.o. Fn. 238). Anzuknüpfen ist daher m.E. an einer von den Fehlerkategorien losgelösten Verkehrspflicht, die unabhängig von einem Produktfehler an der Inverkehrgabe eines erkannt gefährlichen Produkts anknüpft. Dies entspricht der Dogmatik der Verkehrssicherungspflicht im Rahmen der Haftung nach § 823 Abs. 1 BGB besser als an die konstruktiv nicht erreichte Mindestsicherheit anzuknüpfen.

250 Vgl. allgemein BGH, NJW 2009, 2952 (2953); *Wagner*, in: MüKo, BGB, § 823, Rn. 1090; *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), *Produkthaftungshandbuch*, § 24, Rn. 110.

251 Hier liegt gerade der Unterschied zu nicht erkennbaren Risiken. Mit der Entscheidung der Inverkehrgabe trotz des Wissens um die Gefahreneigenschaft und in gegenüber dem Nutzer überlegener Kenntnis der Produkteigenschaften verfügt der Hersteller über eine Gefahrensteuerungsmöglichkeit. Die Erkennbarkeit der Gefahr macht es ihm möglich, Risikominimierung zu betreiben und durch technische Weiterentwicklung der Gefahr zu begegnen. Bis dahin besteht die Möglichkeit der Versicherung, vgl. – wenn auch zur Begründung einer Gefährdungshaftung bei innovativen Techniken im Allgemeinen – *Zech*, JZ 2013, 21 (24 f.).

252 Vgl. *Oechsler*, in: *Staudinger*, BGB, § 1 ProdHaftG, Rn. 120.

253 Vgl. BGH, NJW 1995, 2162 (2163).

254 *Foerste*, JZ 1995, 1063 (1063); *Oechsler*, in: *Staudinger*, BGB, § 1 ProdHaftG, Rn. 120.

greift.²⁵⁵ Ein Fehler i.S.d. § 3 Abs. 1 ProdHaftG liegt lediglich dann nicht vor, wenn die Produktnutzer die schadenstiftende Eigenschaft als unvermeidbares Risiko aufgrund einer Risiko-Nutzen-Abwägung hingenommen haben.²⁵⁶ Dann fehlt es gerade an einer auf die Ungefährlichkeit gerichteten Integritätserswartung.

7. Keine Produktbeobachtungspflicht nach dem ProdHaftG

Ein wesentlicher Unterschied der beiden Haftungssysteme liegt darin, dass sich dem ProdHaftG keine Pflicht zur Produktbeobachtung entnehmen lässt.²⁵⁷ Denn für die Haftung nach dem ProdHaftG kommt es allein auf die Fehlerfreiheit des Produkts im Zeitpunkt des Inverkehrbringens an, § 3 Abs. 1 lit. c ProdHaftG.²⁵⁸ Nach § 1 Abs. 2 Nr. 2 i.V.m. Abs. 4 S. 2 ProdHaftG kann sich der Hersteller von der Haftung befreien, wenn das Produkt den Fehler zum Zeitpunkt des Inverkehrbringens noch nicht aufwies. Aufgrund dieses Stichtagsprinzips spielen Verhaltenspflichten des Herstellers nach dem Inverkehrbringen keine Rolle.²⁵⁹ Mittelbar allerdings kann der Produktbeobachtungspflicht auch im Rahmen des ProdHaftG Bedeutung zukommen. Denn für das Vorliegen eines Produktfehlers kommt es stets auf das Inverkehrbringen des konkreten Produkts an. Da die berechtigten Sicherheitserwartungen aufgrund der technischen Weiterentwicklung einem ständigen Wandel unterliegen, hat sich der Hersteller, um einer drohenden Haftung zu entgehen, vor der Inverkehrgabe weiterer Produkte zu vergewissern, ob er die Produktion nicht aufgrund bisher unbekannter Gefahren oder neuer Sicherheitsmaßnahmen anpassen muss.²⁶⁰ Insoweit können ihm die bereits auf dem Markt befindlichen Produkte Anhaltspunkte geben,

255 Haagen, in: Beck/Kusche/Valerius (Hg.), Digitalisierung, Automatisierung, KI und Recht, S. 215 (228) spricht daher von einer nur teilweisen Haftungsbefreiung für technisch nicht vermeidbare Risiken, nämlich nur im Falle der Nichterkennbarkeit.

256 Wagner, in: MüKo, BGB, § 3 ProdHaftG, Rn. 47.

257 Vgl. auch BT-Drs. 11/2447, S. 18.

258 Mayrhofer, Außervertragliche Haftung für fremde Autonomie, S. 293 f. geht dagegen progressiv davon aus, dass schon die berechtigte Verkehrserwartung bei Inverkehrgabe unterlaufen wird, sollte Software nicht auf eine spätere Veränderung des Sicherheitsstandards angepasst werden.

259 Vgl. nur Michalski, BB 1998, 961 (962); Chibanguza/Schubmann, GmbHR 2019, 313 (314); Taeger, in: NK-ProdR, § 3 ProdHaftG, Rn. 74; Wagner, in: MüKo, BGB, § 1 ProdHaftG, Rn. 63; Wagner, VersR 2014, 905 (907); Graf v. Westphalen, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 48, Rn. 8.

260 Hierzu Wagner, in: MüKo, BGB, § 1 ProdHaftG, Rn. 63.

die gegenwärtigen Sicherheitserwartungen bzgl. der noch nicht in den Verkehr gebrachten Produkte zu erfüllen.²⁶¹ Kommt der Hersteller dieser Produktbeobachtung nicht nach, lassen sich zwar für die bereits in Verkehr gebrachten Produkte keine Pflichten und Haftungsrisiken nach dem ProdHaftG ableiten, läuft er aber Gefahr, fehlerhafte Produkte in den Verkehr zu bringen, für die er dann in Anspruch genommen werden kann.²⁶²

Dies ändert sich mit der Umsetzung der neuen Produkthaftungsrichtlinie (im Folgenden „ProdHaftRL“)²⁶³. Zwar kann sich der Hersteller nach Art. 11 Abs. 1 lit. c ProdHaftRL auch entlasten, wenn die Fehlerhaftigkeit bei Inverkehrbringen noch nicht bestanden hat. Allerdings sieht Art. 11 Abs. 2 lit. c ProdHaftRL eine Ausnahme von dieser Haftungsbefreiung vor, wenn die Fehlerhaftigkeit durch ein Softwareupdate später hätte behoben werden können. In Anerkennung ihrer Verantwortung für die Sicherheit von Produkten über den gesamten Lebenszyklus sollen Hersteller auch für das Ausbleiben von für die Softwaresicherheit erforderlichen Updates haftbar gemacht werden können (vgl. Erwägungsgrund (51) ProdHaftRL). Entsprechend kommt es für die Bestimmung der berechtigten Sicherheitserwartungen und damit für die Fehlerhaftigkeit eines Produkts nach Art. 7 Abs. 2 lit. e ProdHaftRL nicht mehr allein auf den Zeitpunkt des Inverkehrbringens des Produkts an, sondern ist der gesamte Zeitraum entscheidend, in dem das Produkt unter der Kontrolle des Herstellers steht. Der Hersteller wird damit zur Aufrechterhaltung der Sicherheit seines Produkts auch über den Zeitpunkt des Inverkehrbringens hinaus verpflichtet. Dies jedenfalls dort, wo er durch ein entsprechendes Softwareupdate reagieren kann. Insofern obliegen dem Hersteller künftig auch über die ProdHaftRL Reaktionspflichten im Hinblick auf die Produktsicherheit.²⁶⁴

261 Vgl. Taeger, in: NK-ProdR, § 3 ProdHaftG, Rn. 75.

262 Sprau, in: Grüneberg, BGB, § 3 ProdHaftG, Rn. 4; Beierle, Die Produkthaftung im Zeitalter des Internet of Things, S. 201; vgl. auch BT-Drs. 11/2447, S. 18.

263 Die Arbeit basiert auf dem Standpunkt des Europäischen Parlaments, festgelegt in erster Lesung am 12.3.2024 im Hinblick auf den Erlass der Richtlinie (EU) 2024/... des Europäischen Parlaments und des Rates über die Haftung für fehlerhafte Produkte und zur Aufhebung der Richtlinie 85/374/EWG des Rates. Nachdem der Rat seine noch erforderliche Zustimmung bereits signalisiert hat, ist mit einem Inkrafttreten der neuen Vorschriften noch im Jahr 2024 zu rechnen. Geltung beanspruchen diese Vorschriften dann gem. Art. 1 Nr. 1 ProdHaftRL für Produkte, die 24 Monate nach dem Inkrafttreten in den Verkehr gebracht oder in Betrieb genommen werden. Bis zu diesem Zeitpunkt haben die Mitgliedsstaaten gem. Art. 22 Abs. 1 ProdHaftRL zur entsprechenden Umsetzung Zeit. Voraussichtlich werden die neuen Vorschriften ab Herbst 2026 gelten.

III. Fazit zum Produktrecht

Das Produktrecht im Allgemeinen und die entsprechend statuierte Verantwortung des Herstellers weisen eine hohe Affinität zu dem Zeitpunkt des Inverkehrbringens auf. Die zeitpunktbezogene Prüfung kann aber nicht mit einer ebenso zeitlich begrenzten Sicherheitsaussage korrelieren. Vielmehr muss das Produkt über seine ganze Lebensdauer sicher sein.²⁶⁵ Vor diesem Hintergrund wird im öffentlich-rechtlichen Produktsicherheitsrecht in § 3 Abs. 2 S. 2 Nr. 1 ProdSG ausdrücklich die Gebrauchsdauer als berücksichtigungsfähiger Aspekt bei der Bestimmung der Produktsicherheit normiert. Das öffentlich-rechtliche Produktsicherheitsrecht soll sicherstellen, dass sich nur sichere Produkte auf dem Markt befinden und dass von den Produkten keine Gefahren für die nach dem Schutzzweck der jeweiligen Vorschriften geschützten Rechtsgüter ausgehen. Es stellt dazu präventiv Mindestanforderungen an Produkte hinsichtlich ihrer Bereitstellung auf dem Markt, deren Erfüllung zwingende Voraussetzung und maßgeblich für die Verkehrsfähigkeit ist. In diesem Sinne regelt § 3 ProdSG als zentrale Vorschrift hinsichtlich der Sicherheitsanforderung an Produkte,²⁶⁶ dass ein Produkt nur auf dem Markt bereitgestellt werden darf, wenn es bei bestimmungsgemäßer oder vorhersehbarer Verwendung die Sicherheit und Gesundheit von Personen nicht gefährdet (§ 3 Abs. 1 Nr. 2, Abs. 2 S. 1 ProdSG). Folglich ist ein Produkt dann nicht verkehrsfähig ist, wenn sich schon bei seiner Abgabe abzeichnet, dass es nicht über die gesamte voraussichtliche

264 Dötsch, Außervertragliche Haftung für KI, S. 406 und Mayr/Rauner/Schweiger, ZfPC 2023, 2 (5) sprechen dagegen schon weitergehend von Produktbeobachtungspflicht auch im Rahmen der neuen Produkthaftungsrichtlinie. Indes lässt die implizit eingeführte Updateverpflichtung noch keinen Schluss auf eine Beobachtungspflicht i.e.S. zu.

265 Schucht, BB 2020, 1990 (1991).

266 Das ProdSG geht zurück auf das Gerätesicherheitsgesetz von 1968, setzt daneben horizontal die für alle Produkte geltende Allgemeine Produktsicherheitsrichtlinie 2001/95/EG sowie weitere vertikale, also bestimmte Produktgattungen betreffende EU-Richtlinien, um. Das ProdSG kommt für alle Produkte zur Anwendung, für die es keine spezialgesetzlichen Vorschriften gibt (Auffangfunktion). Dies führt dazu, dass ein produktsicherheitsrechtlicher Mindeststandard etabliert wird. Daneben kommt dem ProdSG auch eine Dachfunktion zu. Denn soweit es zwar Spezialgesetze gibt, dort aber bestimmte Anforderungen an die Bereitstellung auf dem Markt nicht konkreter geregelt sind als im ProdSG, kommt es insoweit zur Anwendung, vgl. § 1 Abs. 3 ProdSG sowie Schucht, in: Klindt, ProdSG, § 1, Rn. 81 und Falk, in: NK-ProdR, § 1 ProdSG, Rn. 47 ff.

Gebrauchsdauer sicher verwendet werden kann.²⁶⁷ Produkthaftungsrechtlich gesprochen erfüllt es dann nicht die berechtigten Verkehrserwartungen und ist bereits bei Inverkehrgabe fehlerhaft. Ist ein Produkt daher zum Zeitpunkt des Inverkehrbringens sicher, hat also der Hersteller alles Erforderliche und Zumutbare getan, geht damit herkömmlicherweise ein gewisses Vertrauen einher, dass das Produkt auch über seinen Lebenszyklus hinweg sicher bleibt. Aufgrund des sich stets fortentwickelnden Stands von Wissenschaft und Technik und der zunehmenden Erfahrung im Umgang mit dem Produkt genießt ein Produkt mit dem Inverkehrbringen aber keinen Bestandsschutz.²⁶⁸ Hier knüpft die Produktbeobachtungspflicht quasi als zweites Sicherheitsnetz an, sodass eine Dynamisierung der Herstellerverantwortung über den Zeitpunkt des Inverkehrbringens hinaus entsteht.²⁶⁹ Die Ausdifferenzierung der Produktbeobachtungspflicht trägt dabei dem Verständnis der jeweiligen Verantwortungssphären Rechnung. Bis zum Zeitpunkt der Inverkehrgabe hat der Hersteller als „Herr des Herstellungsprozesses“ die volle Kontrolle über das Produkt; danach verfügt er zwar weiterhin über überlegenes Produktwissen, allerdings beschränken sich seine Eingriffsmöglichkeiten.

267 Zum Ganzen überzeugend *Schucht*, BB 2020, 1990 (1991).

268 *Wagner/Ruttloff/Miederhoff*, CCZ 2020, 1 (5).

269 *Handorn/Juknat*, MPR 2022, 77 (87).

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).

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 ProdHaft-RL 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, 1313 (1317)), 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, RD 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.).

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.

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 Rechtsanwaltslexikon, § 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.

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 Instrukativ mit Beispielen nochmals Taschner, NJW 1986, 611 (615).

a) Abgrenzung

Schon eine klare Abgrenzung²⁹⁰ 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 Tammé, 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.

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.

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 Zubehöriteil 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.

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 Gefahrschaffung 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.

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 Zubehörs 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 Gefahrschaffung 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 Gefahrschaffung 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).

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.), Produkthaftungsbandbuch, § 24, Rn. 309.

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.

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 Instrukтив 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).

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.

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 beigespflichtet 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-

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

pfligt 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 Einflussosphäre 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:

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).

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.

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.

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

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.), *Produkthaftungsbandbuch*, § 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.), *Produkthaftungsbandbuch*, § 24, Rn. 309 fehlt.

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

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.).

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).

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 behaftet 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).

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 Authentifizierung³⁷⁹ – 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).

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“.

Schadensrisiken an, die sich verwirklichen können. Mit der Umsetzung der Warenkaufrichtlinie³⁸⁹ und der Richtlinie über digitale Inhalte und digitale Dienstleistungen³⁹⁰ 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.

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/Gehrman*, 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 Nutzungsbe-
reich der Software und den Gegenstand der Software als mögliche Kriterien zur Bestimmung der Mangelhaftigkeit im Vertragsrecht.

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 Programmierung

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),

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.

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.), *Produkthaftungsbandbuch*, § 57, Rn. 21; Chibanguza, in: Chibanguza/Kuß/Stege (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).

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.

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.

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 2.0⁴²⁵ 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 no lens 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

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 Informationsicherheitsmanagements 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-

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.

aa) Schutzzumfang des Haftungsrechts bei Cyberangriffen

Hinsichtlich der Frage des Schutzzumfangs 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.).

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 Schutzzumfang 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 Schutzzumfangs 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 cyber-physischer Systeme, S.183; Koch, NJW 2004, 801 (802) spricht von mittelbaren Beeinträchtigungen.

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

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 *Rosnagel/Schnabel*, NJW 2008, 3534 (3537) und *Heydn* in: Schuster/Grützmaker (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.).

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 Schadensseintritts 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).

(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 Fehlverhalten 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).

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 Andererseits 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.

(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.

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 Geschehens⁴⁸³ 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

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 so- dann die Üblichkeit von Sicherungsvorkehrungen eine entscheidende Rol- le. 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 Siche- rungspflichten 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).

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.

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 spurloses 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).

Produktmanipulation nach dem Inverkehrbringen⁵⁰⁴ 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).

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 zerstochnen 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.

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 sind⁵¹⁵ 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.

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 Sicherheitsvorkehrungen 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“.

dem Verantwortungsbereich des Herstellers stammt und daher die Wahrscheinlichkeit der Rechtsgutsverletzung erhöht wurde. Da bei der aktuellen Bedrohungslage⁵²¹ 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 berechnete 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 berechnete 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 wären⁵²⁶ 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 *Rofßnagel/Schnabel*, NJW 2008, 3534 (3536): „Was in diesem [„Informationsverkehr“] Sicherheit bedeutet, wird künftig auch durch das neue Grundrecht bestimmt“.

525 *Rofßnagel/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.

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).

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/Braegelman (Hg.), Artificial Intelligence und Machine Learning, S. 134.

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

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

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.

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.).

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 Gefahrenpotenzialen 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. I; 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.

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 Webserver, 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 beimesen 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.

erlassene delegierte Verordnung zur RED⁵⁵¹ 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 Produkthanforderungen 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-

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-Systeme⁵⁵⁹ 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. I, 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.

sämtliche Neufahrzeuge⁵⁶² 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, RDt 2024, 345 (350 f.).

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: Knapertsbusch/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.

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.

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 Speicker gen. Döhmman, 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.

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.

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“.

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.

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 wird⁵⁹⁸ – 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.

diesem Hintergrund stellt auch Software ohne Weiteres ein Zubehör im produkthaftungsrechtlichen Sinne dar (sog. digitales Zubehör).⁶⁰⁰ Schwieriger ist diese Einordnung 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.

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 Steuerungssapp 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.

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. 1 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.

lediglich eine Bereitstellung durch Drittanbieter ermöglicht. Gerade im Automobilsektor 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-angekündigt-35296445.html> (zuletzt abgerufen am 23.09.2024).

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 Gefahrenabwehrpflichten 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 Gefahrenabwehrpflichten des Quasi-Herstellers in dieser Vertrauenskonstellation BGH, VersR 1977, 839.

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

(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 Einordnung 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 Diensteanbieter die Inhalte vorab auf Vollständigkeit und Richtigkeit überprüft hat.⁶²⁹ Eine andere Ansicht stellt allein auf die Herrschaftsmacht des Diensteanbieters 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 Diensteanbieters 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*, RD 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.

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 Einflussphäre 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.

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 funktionsfähig 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 *Sosnitzka*, CR 2016, 764 (769) und *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 82; offen gelassen von *Reusch*, in: Kaulartz/Braegelman (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.

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 gebräuchlichem⁶⁴⁶ 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 Zubehöriteile] 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“.

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 ökonomischen 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.

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. 1 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.

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.

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 selbstständig 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. III f.

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

Konstellationen besteht ein grundlegender Unterschied. Bei Kombinationsgefahren geht es um die Neuordnung 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. *Xyländer*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 51.

667 In diese Richtung *Wagner*, in: MüKo, BGB, § 823, Rn. 1042 f.

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).

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 herstellereitigen 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 Schnellebigkeit, 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.

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 Zubehöriteil 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 Zubehöriteils. 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 Zubehöriteil 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 Fremdzubehöriteilen, 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.

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 meteorologischen Sicherung des Luftverkehrs; ferner zur Verkehrsregelung mit entsprechenden Infrastrukturanlagen, S. 181 ff.

(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.

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.

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).

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 Kommissionsentwurf⁷⁰¹ 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 Dienstbringer 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. Erwägungsgrund (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).

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 Kommissionsvorschlag⁷¹² 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); Stiernerling, 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.

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 *Stiernerling*, 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 *Stege*, 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).

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 Trainings⁷¹⁹ 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.

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/Seeleemann (Hg.), *Intelligente Agenten und das Recht*, S. 163 (171).

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

729 Vgl. Zech, in: Gless/Seeleemann (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/Seeleemann (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*,

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]“.

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 statistischen 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/Braegelman (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.

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/Braegelman (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/Braegelman (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.

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/Braegelman (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.).

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; *Haa-gen*, *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.

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).

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/Braegelman (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).

parametern 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 Inverkehrgabe 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).

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).

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 *Steegen*, 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.

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. III 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.

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 instruiert⁷⁹⁵ 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 Sicherungsvorkehrungen. 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).

den technischen Möglichkeiten im Zeitpunkt des Inverkehrbringens nicht vermeidbaren Gefahren, die berechnete 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).

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 berechnete 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 berechnete 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. Insofern 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. Insofern 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: Foerster/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).

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.

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).

Im Rahmen des Autonomierisikos kann die Produktbeobachtungspflicht ein gewisses Korrektiv für Entwicklungslücken bedeuten.

D. Verantwortung des Herstellers bei zunehmender Datenverfügbarkeit

In dem vorangegangenen Kapitel wurde gezeigt, dass aufgrund der zunehmenden Digitalisierung der Produktlandschaft die Produktbeobachtungspflicht des Herstellers einen zentralen Stellenwert im Rahmen der deliktischen Produzentenhaftung einnehmen wird und dabei besonders intensiv ausfallen kann. Im Folgenden soll nun betrachtet werden, wie der Hersteller seiner Produktbeobachtungspflicht im digitalen Zeitalter nachkommen kann und welche Verantwortlichkeiten ihn hierbei treffen. Dabei ist die Produktbeobachtungspflicht als Verkehrspflicht stets am aktuellen Stand von Wissenschaft und Technik auszurichten, sodass die technische Weiterentwicklung auch den Umfang der Produktbeobachtungspflicht prägt.⁸¹⁴

Im Rahmen der Produktbeobachtung i.e.S. kann der Hersteller durch die Generierung einer Vielzahl an Daten sowie durch die Nutzung neuer Technologien, um diese Daten zu erfassen, zu bündeln und zu analysieren, ein viel umfassenderes Bild von der Bewährung seines Produkts im Feld erhalten, als dies bisher durch einzelne Aussagen und Stichproben möglich war.⁸¹⁵ Eine der größten Herausforderungen in diesem Bereich dürfte es daher sein, die „sich bietenden Möglichkeiten von Big Data organisatorisch und strukturell in der Unternehmenspraxis so zu nutzen, dass sie den Anforderungen des Produkthaftungsrechts genügen.“⁸¹⁶ So könnte die zunehmende Datenverfügbarkeit und Datenkenntnis auch zu einer Ausdehnung der Verantwortung bei der Produktbeobachtung i.e.S. führen. Vor diesem Hintergrund soll nachfolgend untersucht werden, welche Daten vom Hersteller erhoben und ausgewertet werden müssen. Herkömmlich wird dabei zwischen der passiven und der aktiven Beobachtung unterschieden.⁸¹⁷

814 So auch *Wende*, in: Sassenberg/Faber (Hg.), *Industrie 4.0 und Internet of Things*, § 4, Rn. 22 und *Piovano/Schucht/Wiebe*, *Produktbeobachtung in der Digitalisierung*, S. 70.

815 Vgl. *Reusch*, in: Kaulartz/Braegelmann (Hg.), *Artificial Intelligence und Machine Learning*, S. 109.

816 So *Hartmann*, DAR 2015, 122 (124).

817 Diese Unterscheidung verwendet nicht nur die Literatur (vgl. statt aller *Wagner*, in: MüKo, BGB, § 823, Rn. 1110 f.), sondern auch der BGH (vgl. BGH, NJW 1994, 517 (519)).

I. Passive Produktbeobachtungspflicht

Bei der passiven Produktbeobachtung geht es darum, jene Informationen entgegenzunehmen und auszuwerten bzw. zu analysieren, die von außen an das Unternehmen herangetragen werden.⁸¹⁸

1. Bedeutung der öffentlich-rechtlichen Produktbeobachtungspflicht

Normative Verankerung findet diese passive Pflicht in der öffentlich-rechtlichen Produktbeobachtungspflicht nach § 6 Abs. 3 S. 1 Nr. 2 ProdSG.⁸¹⁹

Auch wenn der primäre Fokus des öffentlich-rechtliche Produktsicherheitsrechts – das zeigt bereits der Anwendungsbereich des ProdSG, welcher sich gem. § 1 Abs. 1 ProdSG⁸²⁰ auf das Bereitstellen auf dem Markt, das Ausstellen und das erstmalige Verwenden bezieht – nicht auf Produkten, welche bereits auf dem Markt bereitgestellt wurden, liegt, hält das ProdSG gleichwohl Vorschriften bereit, welche den Umgang mit unsicheren Produkten auf dem Markt regeln.⁸²¹

a) Errichtung eines Risikomanagementsystems, § 6 Abs. 2 ProdSG

In diesem Sinne hat insbesondere der Hersteller⁸²² bei Verbraucherprodukten gem. § 6 Abs. 2 ProdSG Vorkehrungen für geeignete Maßnahmen zur Vermeidung von Risiken zu treffen, die mit dem auf dem Markt bereitgestellten Verbraucherprodukt verbunden sein können. Adressiert wird damit die Pflicht zur Errichtung eines Risikomanagementsystems.⁸²³ Dabei sind unternehmensintern organisatorische Vorkehrungen zu treffen, um bei auftretenden Gefahren effektive Risikovermeidungsmaßnahmen treffen zu können. Welche Vorkehrungen im Einzelnen zu treffen sind, wird von § 6

818 Vgl. nur *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 23.

819 Es ist darauf hinzuweisen, dass in der historischen Entwicklung die deliktsrechtliche Produktbeobachtungspflicht den spezialgesetzlichen Beobachtungspflichten des Produktsicherheitsrechts vorausging, vgl. *Wagner*, VersR 2014, 905 (906).

820 Eine ähnliche Regelung enthält bspw. auch Art. 1 Abs. 1 MDR.

821 Vgl. zum Ganzen *Lach/Polly*, Produkt-Compliance, S. 4 und *Krey/Kapoor*, Praxisleitfaden Produktsicherheitsrecht, S. 4.

822 Die nachfolgend dargestellten Pflichten werden an den Hersteller, Bevollmächtigten und Einführer adressiert. Da vorliegend der Fokus auf dem Hersteller liegen soll, wird nur dieser genannt.

823 Zu den unterschiedlichen Begrifflichkeiten *Kapoor*, in: *Klindt*, ProdSG, § 6, Rn. 49.

Abs. 2 ProdSG allerdings nicht näher konkretisiert. Insoweit sieht Art. 9 Abs. 11 GPSR künftig konkreter vor, dass der Hersteller Kommunikationskanäle einrichten muss, die es den Verbrauchern ermöglichen, Beschwerden einzureichen.

Aus der Organisationspflicht lässt sich aber keine Pflicht zur Produktbeobachtung ableiten. Zwar ließe sich eine solche Produktbeobachtungspflicht als Vorkehrung begreifen, welche eine frühzeitige Gefahrenerkennung und anschließende Folgemaßnahmen ermöglichen soll. Insofern ließe sich die Produktbeobachtung als notwendige Effektivierung für spätere zielgerichtete und schnelle Reaktionsmaßnahmen bzgl. Produktgefahren begreifen. Allerdings lässt sich die Produktbeobachtung entsprechend der im Gesetzeswortlaut angelegten Trennung zwischen „Vorkehrungen“ und „Maßnahmen“ in unternehmensinterne organisatorische Vorbereitungen und die Durchführungen unterteilen. Damit wird aber deutlich, dass die Produktbeobachtung selbst die „Maßnahme“ darstellt. Zwingend wird dieses Ergebnis mit dem systematischen Blick auf § 6 Abs. 3 ProdSG, welcher klassische Tätigkeiten aus dem Spektrum der Produktbeobachtung normiert und deutlich macht, dass die Produktbeobachtungspflicht hier zu verorten ist.⁸²⁴ Darüber hinaus passt die Produktbeobachtungspflicht als eine der Bereitstellung auf dem Markt nachgelagerte Pflicht auch nicht zu den vorbereitenden Vorkehrungen, die bereits zu dem Zeitpunkt der Bereitstellung des Produkts auf dem Markt getroffen sein müssen.⁸²⁵ § 6 Abs. 2 ProdSG lässt sich damit den Vor-Marktpflichten zuordnen,⁸²⁶ auch wenn sich das Risikomanagementsystem freilich erst im Fall der Produktkrise und damit zeitlich nachgelagert beweisen muss.

b) Öffentlich-rechtliche Produktbeobachtungspflicht, § 6 Abs. 3 ProdSG

Als echte Nach-Marktpflicht stellt sich dagegen § 6 Abs. 3 S. 1 ProdSG dar.⁸²⁷ Hiernach hat der Hersteller bei den bereits auf dem Markt bereitge-

824 Zum Ganzen ausführlich *Hofmann*, Öffentlich-rechtlich statuierte Produktbeobachtungspflichten, S. 169 ff.

825 *Kapoor*, in: *Klindt*, ProdSG, § 6, Rn. 47.

826 So auch *Schucht*, BB 2020, 1990 (1996).

827 Diese Nach-Marktpflichten sind zwar nicht bußgeldbewehrt, mittlerweile können die Marktüberwachungsbehörden aber den Hersteller nach § 25 Abs. 7 ProdSG bei Nichterfüllung seiner Produktbeobachtungspflicht aus § 6 Abs. 3 ProdSG auffordern, dieser Pflicht nachzukommen, und diesen Verwaltungsakt anschließend auch mit Mitteln des Verwaltungszwangs durchsetzen, vgl. *Schucht*, PHi 2023, 126 (132).

stellten Verbraucherprodukten Beschwerden zu prüfen und erforderlichenfalls ein Beschwerdebuch zu führen (Nr. 2). Schon dem Wortlaut nach bezieht sich die Norm damit auf bereits bereitgestellte Produkte und statuiert eine öffentlich-rechtliche Pflicht zur Produktbeobachtung. Sowohl die Pflicht zur Produktbeobachtung als auch das Ziel der Erkennung von Produktgefahren werden zwar selbst nicht erwähnt, ergeben sich aber, indem die notwendigen Verhaltensweisen als Pflichtenkanon vorgegeben werden.⁸²⁸ Die Verpflichtung zur Führung eines Beschwerdebuchs verdeutlicht, dass alle die Sicherheit von Produkten betreffenden Informationen nicht nur entgegengenommen und berücksichtigt, sondern auch systematisch ausgewertet werden müssen.⁸²⁹ Art. 9 Abs. 12 GPSR erstreckt die Untersuchungspflicht des Herstellers künftig neben Beschwerden auch auf Informationen über Unfälle, schränkt sie dann aber ein, indem sie sich nur auf Produkte bezieht, die vom Beschwerdeführer als gefährlich bezeichnet werden.⁸³⁰

c) Auswirkungen auf die zivilrechtliche Produktbeobachtungspflicht

aa) Bedeutung des New-Approach

Da unterschiedliche nationale Regelungen zur Produktsicherheit zu unterschiedlichen Schutzniveaus führen würden und damit geeignet wären, den innergemeinschaftlichen Handel zu beeinträchtigen, ist das Produktsicherheitsrecht heute im Wesentlichen europäisch harmonisiert.⁸³¹ Die Harmonisierungsvorschriften legen dabei nach dem sog. New-Approach lediglich grundlegende Anforderungen mit Blick auf den verfolgten Schutzzweck und in Bezug auf die wesentlichen Sicherheitsanforderungen des Produkts fest. Sie nehmen gerade keine Detailharmonisierung vor. Die konkrete Ausgestaltung dieser wesentlichen Anforderungen hat der EU-Gesetzgeber auf private Institutionen verlagert, die diesem Auftrag durch die Erstellung har-

828 Ähnlich *Kapoor*, in: Klindt, ProdSG, § 6, Rn. 57 und *Hofmann*, Öffentlich-rechtlich statuierte Produktbeobachtungspflichten, S. 174; *Eifert*, in: Eifert (Hg.), Produktbeobachtung durch Private, S. 9 (15). Dieser weist darauf hin, dass die Produktbeobachtung gesetzgeberisch kaum ausdrücklich als solche bezeichnet und ausgestaltet wurde.

829 *Schütte*, in: NK-ProdR, § 6 ProdSG, Rn. 47.

830 Vgl. auch *Schucht*, PHi 2023, 148 (155).

831 Vgl. *Falk*, in: NK-ProdR, § 1 ProdSG, Rn. 2.

monisierter technischer Normen nachkommen. Diese unterliegen in ihrer Entstehung nicht dem starren und ggf. trägen Gesetzgebungsverfahren und bieten daher größere Flexibilität, um mit dem aktuellen technischen Stand Schritt halten zu können. Sie verfügen aber aufgrund ihrer mangelnden demokratischen Legitimation über keine Rechtsverbindlichkeit. Vielmehr sollen sie dem Hersteller eine Hilfestellung und ein Orientierungsrahmen bei der Erfüllung der Anforderungen sein. Damit bleibt ihre Befolgung durch den Hersteller freiwillig und es ist ihm selbst überlassen, wie er die verbindlichen Sicherheitsanforderungen aus der Harmonisierungsvorschrift erfüllt. Sollte er sich für die Einhaltung der harmonisierten technischen Normen entscheiden, wird zu seinen Gunsten widerleglich vermutet, dass sein normkonform hergestelltes Produkt auch den Sicherheitsanforderungen der Harmonisierungsvorschrift entspricht. Gleichwohl bleibt es dem Hersteller unbenommen, eigene – möglicherweise sogar bessere – Lösungen anzuwenden, sodass eine Innovations- und Technologieoffenheit gewährleistet ist.⁸³²

Entsprechend dem Regelungskonzept des New-Approach beschränkt sich das ProdSG auf die Festlegung der grundlegenden Anforderungen auch an die Produktbeobachtung im Hinblick auf den Gesundheitsschutz der Verbraucher nach dem Inverkehrbringen.⁸³³ Die konkrete Ausgestaltung ist produktspezifisch dem Hersteller überlassen.⁸³⁴ Haftungsrechtlich bedeutet die allgemeine Regelungsstruktur des New-Approach, dass die Nichtbeachtung der grundlegenden Anforderungen des öffentlich-rechtlichen Produktsicherheitsrechts regelmäßig einer Verletzung von Verkehrssicherungspflichten gleichsteht.⁸³⁵ Art. 10 Abs. 2 lit. b ProdHaftRL sieht insofern künftig eine Vermutung für die Fehlerhaftigkeit eines Produkts vor, als es verbindliche gesetzliche Produktsicherheitsanforderungen nicht.⁸³⁶

832 Vgl. zum New-Approach *Krey/Kapoor*, Praxisleitfaden Produktsicherheitsrecht, S. 180 ff., sowie *Reusch*, BB 2017, 2248 (2249).

833 *Eifert*, in: *Eifert* (Hg.), Produktbeobachtung durch Private, S. 9 (17) spricht davon, dass kaum mehr als eine Erwartung formuliert wird.

834 *Eifert*, in: *Eifert* (Hg.), Produktbeobachtung durch Private, S. 9 (18) weist darauf hin, dass besonders risikobehaftete Produkte regelmäßig einer Zulassungspflicht unterliegen und die Produktbeobachtung dann als Nebenbestimmung zur Zulassung individuell und produktbezogen konkretisiert werden kann und muss.

835 Vgl. *Schucht*, BB 2016, 456 (457); anders bei einem Verstoß gegen anwendbare technische Normen, welche lediglich die Verletzung der privatrechtlichen Verkehrspflicht indiziert, vgl. auch *Wagner*, VersR 2014, 905 (911).

836 Vgl. auch Erwägungsgrund (46) ProdHaftRL.

Dagegen bewirkt das öffentlich-rechtliche Produktsicherheitsrecht keine abschließende Konkretisierung der zivilrechtlichen Verkehrspflichten.⁸³⁷

bb) Gegenläufige Entscheidung des OLG Düsseldorf bzgl. der Produktbeobachtung

Allerdings hat das OLG Düsseldorf diese allgemeinen Grundsätze im Hinblick auf die Produktbeobachtungspflicht in Zweifel gezogen. Konkret ging es um die Frage der eigenen Verantwortlichkeit einer Vertriebsgesellschaft für die Produktbeobachtung. Das OLG Düsseldorf sah die in der damals geltenden Medizinprodukte-Sicherheitsplanverordnung (im Folgenden „MPSV“) normierten Pflichten im Hinblick auf das dort hinsichtlich der Verantwortlichkeit der einzelnen Akteure detailliert ausgearbeitete und wohlabgewogene Konzept zur Erfassung, Bewertung und Abwehr von Risiken als abschließende Festlegung der deliktsrechtlichen Produktbeobachtungspflicht bei Medizinprodukten an, so dass sich aus den allgemeinen Verkehrssicherungspflichten keine weitergehenden Pflichten ergeben können.⁸³⁸ Da die Vertriebsgesellschaft nach § 3 Abs. 3 S. 2 MPSV lediglich die Pflicht traf, ihr mitgeteilte Informationen über Vorkommnisse insbesondere an den Hersteller weiterzuleiten, nicht aber eigene Analysen der Informationen durchzuführen oder gar eigenständig Warnungen herauszugeben oder Rückrufe durchzuführen, nahm das Gericht auch zivilrechtlich keine weitergehenden Produktbeobachtungspflichten an.

Dass der zu entscheidende Fall mit angemessenem Ergebnis aufgegangen ist, darf aber nicht darüber hinwegtäuschen, dass dies nur auf die Besonderheit des Sachverhalts zurückzuführen war. Bei der vom Produkt ausgehenden Gefahr handelte es sich nicht um ein unbekanntes Risiko, das plötzlich aufgetreten ist, sondern um ein bekanntes Risiko, das bereits bei Inverkehrgabe berücksichtigt werden musste. Hinzu kommt, dass es sich um ein hochkomplexes medizintechnisches Produkt handelte, bei dem die Vertriebsgesellschaft bereits die ihr übermittelten Informationen nicht hinreichend überprüfen kann und daher auf die Informationen und Anweisungen des Herstellers angewiesen ist. In dieser Konstellation kann die Vertriebsgesellschaft auch keine allgemeine Verkehrssicherungspflicht treffen,

837 Allgemeine Meinung, vgl. nur *Wagner*, in: MüKo, BGB, § 823, Rn. 1116; konkret in Bezug auf die Produktbeobachtung *Schucht*, PHi 2023, 148 (155).

838 OLG Düsseldorf, NJOZ 2012, 1404 (1412).

die über die Informationsweitergabe an den Hersteller hinausgeht.⁸³⁹ Dies zeigt aber, dass Wertungen öffentlich-rechtlicher Normen im Rahmen der Bestimmung der Reichweite deliktsrechtlicher Regelungen herangezogen werden können, diese aber die Reichweite der deliktsrechtlichen Pflichten nicht abschließend festlegen können.⁸⁴⁰ Vielmehr müssen die Verkehrspflichten einzelfallabhängig anhand der Kriterien der Erforderlichkeit und Zumutbarkeit beurteilt werden. Folglich besteht auch bei der Produktbeobachtungspflicht ein Ergänzungsverhältnis von öffentlichem Sicherheits- und privatem Haftungsrecht.⁸⁴¹

2. Produzentenhaftungsrechtlicher Pflichtenkreis

Damit sind die produktsicherheitsrechtlichen Vorgaben zur Entgegennahme und Prüfung von Beschwerden in ihrer Abstraktheit nicht geeignet, den produzentenhaftungsrechtlichen Pflichtenkreis zu überformen.⁸⁴² Neben der produktsicherheitsrechtlich ausdrücklich vorgesehenen Überprüfung von Beschwerden (und künftig Unfällen) müssen im Rahmen der Produzentenhaftung auch Informationen über sicherheitsrelevante Fortschritte in Wissenschaft und Technik, über die tatsächliche Verwendung des Produkts sowie über alle neuen Umstände entgegengenommen werden, unter denen das Produkt gefährlich werden könnte.⁸⁴³

Maßgebliche Relevanz kommt dabei der Entgegennahme von Kundenbeschwerden sowie deren Überprüfung und systematischer Auswertung zu. Denn diesen Rückmeldungen der Nutzer kommt ein hoher Nutzen zu, da es sich um Erfahrungen aus dem Feld und damit aus dem praktischen Einsatz handelt. Diese sicherheitsrelevanten Informationen werden dem

839 Hierauf stützt das OLG Düsseldorf, NJOZ 2012, 1404 (1412 f.) seine Entscheidung im Übrigen; zustimmend *Lach/Schönberger*, MPR 2012, 73 (78 f.).

840 Krit. zur Entscheidung des OLG Düsseldorf daher auch *Wagner*, in: MüKo, BGB, § 823, Rn. 1116 und *Chibanguza* in: Chibanguza/Kuß/Steeger (Hg.), Künstliche Intelligenz, § 4, E., Rn. 13; im Sinne der Rechtssicherheit zustimmend dagegen *Lach/Schönberger*, MPR 2012, 73 (78 f.).

841 So *Wagner*, VersR 2014, 905 (912); vgl. auch *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 13.

842 *Schucht*, PHi 2023, 148 (156).

843 *Foerste*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 312; ebenso *Röthel*, in: Eifert/Hoffmann-Riem (Hg.), Innovationsverantwortung, S. 335 (341). Diese spricht von der „Überwindung unspezifischen Nichtwissens“.

Hersteller zwar aus dem Markt zugetragen, sodass keine Kosten für eigene Test- und Untersuchungsverfahren anfallen.⁸⁴⁴ Mit erheblichem Aufwand dagegen ist die systematische Auswertung dieser Informationen verbunden. Eine solche kann regelmäßig nur durch ein im Unternehmen organisatorisch integriertes Beschwerdemanagement gewährleistet werden.⁸⁴⁵ Zu Beginn steht dabei die Einrichtung eines Kanals für Kundenbeschwerden, auf welchen die Produktnutzer auch hinzuweisen sind.⁸⁴⁶ Erforderlich und unerlässlich ist dann die Filterung der eingehenden Rückmeldungen hinsichtlich sicherheitsrelevanter Aspekte, die Zerlegung der Inhalte in einzelne Aussagen, die richtige Zuordnung und Bündelung dieser einzelnen Aussagen, die Zusammenführung mit Erkenntnissen aus der aktiven Produktbeobachtung sowie die Weiterleitung an eine zentrale Stelle im Unternehmen. Nur dadurch kann sichergestellt werden, dass mehrere sicherheitskritische Informationen zu einem bestimmten Produkt nicht als unabhängige Einzelfälle abgetan werden und sich ein ganzheitliches Bild über die Bewährung dieses Produkts im Feld ergibt.⁸⁴⁷ In das Beschwerdemanagement sind auch die Händler einzubeziehen.⁸⁴⁸ Denn aufgrund ihrer Brückenstellung zwischen dem Hersteller und dem Verbraucher erreichen Reklamationen häufig zuerst die Händler, weshalb die Weiterleitung an die Hersteller sichergestellt sein muss.⁸⁴⁹

844 Zu dem positiven Verhältnis von Kosten und Nutzen *Wagner*, in: MüKo, BGB, § 823, Rn. 1110 und *Lenz*, in: *Lenz*, Produkthaftung, § 3, Rn. 227.

845 Hierzu im Zusammenhang mit der Produktbeobachtungspflicht aus § 823 Abs. 1 BGB *Klindt/Wende*, BB 2016, 1419 (1419); in diese Richtung auch *Droste*, CCZ 2015, 105 (106); allgemeine Hinweise zu einer möglichen Umsetzung eines solchen Beschwerdemanagementsystems bei *Hauschka/Klindt*, NJW 2007, 2726 (2728) und *Klindt/Wende*, Rückrufmanagement S. 64 ff.

846 *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), Produkthaftungshandbuch, § 24, Rn. 380; *Schmid*, CR 2019, 141 (142).

847 *Klindt/Wende*, BB 2016, 1419 (1421); *Ackermann*, in: NK-ProdR, § 823 BGB, Rn. 123; *Lenz*, in: *Lenz*, Produkthaftung, § 3, Rn. 228 zählt diese Organisation allerdings schon zur aktiven Produktbeobachtung; ein anschauliches Negativbeispiel unter Verdeutlichung auch der strafrechtlichen Konsequenzen geben *Hauschka/Klindt*, NJW 2007, 2726 (2726).

848 So auch zum ProdSG *Kapoor*, in: *Klindt*, ProdSG, § 6, Rn. 63.

849 Dazu *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), Produkthaftungshandbuch, § 24, Rn. 381, § 26, Rn. 42.

II. Aktive Produktbeobachtungspflicht

Der Hersteller darf sich aber nicht nur auf die Entgegennahme von Beschwerden beschränken und auf die passive Produktbeobachtung verlassen. Auch hier zeigt § 6 Abs. 3 S. 1 Nr. 1 ProdSG, dass durch Stichproben (Nr. 1) selbst an der Informationsgewinnung mitzuwirken ist. Eine Pflicht zur Erhebung von Stichproben ist dagegen nach der neuen GPSR nicht mehr vorgesehen.⁸⁵⁰ Weitere aktive Maßnahmen zur Informationsbeschaffung, welche über die Durchführung von Stichproben hinausgehen, werden allerdings vom ProdSG nicht gefordert. Daher sind zufällige und außerhalb des Beschwerdemanagements zur Kenntnis genommene produktsicherheitsrelevante Informationen jedenfalls nach dem ProdSG lediglich zu bewerten; aktiv ist aber nicht nach solchen Hinweisen zu suchen.⁸⁵¹ Diese nach dem ProdSG als einzig aktive Handlung geforderte Stichprobenentnahme⁸⁵² kann für die aktive deliktsrechtliche Produktbeobachtungspflicht aber wiederum lediglich als Mindestanforderung angesehen werden. Vielmehr muss der Hersteller aus eigener Initiative Informationen über mögliche Produktgefahren aktiv beschaffen und den Fortgang der Entwicklung von Wissenschaft und Technik verfolgen.⁸⁵³ Dabei hat er sämtliche Quellen auszuwerten, aus denen sich sicherheitsrelevante Informationen über die Produkte erwarten lassen.⁸⁵⁴ Zu diesen Erkenntnisquellen können bspw. Zeitungs- und Testberichte, Fachzeitschriften und Fachkongresse⁸⁵⁵ sowie Erkenntnisse der Unfallforschung gehören.⁸⁵⁶ Wiederum ist auf die Wich-

850 Ausführlicher unter D.IV.3.a)aa)(1).

851 So *Kapoor*, in: *Klindt*, ProdSG, § 6, Rn. 64; *Schütte*, in: *NK-ProdR*, § 6 ProdSG, Rn. 52; *Wagner*, VersR 2014, 905 (915); *Schucht*, Phi 2023, 126 (129 f.); offen gelassen von *Klindt/Wende*, BB 2016, 1419 (1419); a.A. *Piltz/Reusch*, BB 2017, 841 (844).

852 Diese wird auch ohne Anlehnung an das ProdSG zum Pflichtenprogramm der deliktischen Produktbeobachtungspflicht gerechnet, vgl. *Ackermann*, in: *NK-ProdR*, § 823 BGB, Rn. 124; *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 153; *Wilhelmi*, in: *Erman*, BGB, § 823, Rn. 119 „eigene laufende Überwachung durch Produkttests“.

853 Diese aktive Produktbeobachtungspflicht adressierte der BGH schon in seiner grundlegenden Entscheidung BGH, NJW 1981, 1606 (1607).

854 *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), Produkthaftungshandbuch, § 24, Rn. 378.

855 BGH, NJW 1981, 1606 (1608).

856 *Michalski*, BB 1998, 961 (963); *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), Produkthaftungshandbuch, § 24, Rn. 378; vgl. auch die Aufzählung bei *Klindt/Wende*, Rückrufmanagement, S. 57.

tigkeit hinzuweisen, sämtliche Informationen zusammenzuführen.⁸⁵⁷ Da die aktive Produktbeobachtungspflicht gerade selbst darauf angelegt ist, eine Gefahrenkenntnis hervorzubringen, beginnt sie mit Inverkehrgabe des Produkts und bedarf keines Anlasses.⁸⁵⁸

III. Social-Media-Monitoring

1. Neue Kommunikationswege

Nicht unmittelbar mit der Digitalisierung der Produktlandschaft, aber untrennbar mit dem durch die Digitalisierung veränderten technologischen Umfeld der Social-Media-Kommunikation, verbunden ist die Frage der Ausdehnung der Pflicht des Herstellers zur Informationsauswertung und -beschaffung auch auf das Internet („Web-Screening“). Durch die Vielzahl an Informationen, die jedermann frei zugänglich sind, bieten sich dem Hersteller entsprechend viele Quellen, um produktsicherheitsrelevante Erkenntnisse über sein Produkt im Feld in Erfahrung zu bringen.

Der bloße Wechsel der Publikationsform hin zu Online-Veröffentlichungen kann dabei keinen Einfluss auf den Umfang der Produktbeobachtungspflicht haben. Die Verdrängung klassischer Print-Medien hin zu Onlinepräsenzen betrifft nicht nur wissenschaftliche Beiträge und Forschungsberichte, die nunmehr über Datenbanken veröffentlicht werden, sondern auch Informationen von Unternehmen, Verbänden und Behörden, die nun auf den entsprechenden Internetseiten verfügbar sind.⁸⁵⁹ Was früher gedruckt veröffentlicht wurde und von der Produktbeobachtungspflicht umfasst war, muss freilich auch bei einer Online-Veröffentlichung vom Hersteller verfolgt werden.

Im Mittelpunkt des Interesses stehen vielmehr neue Kommunikationswege, die das Internet eröffnet hat und die einen interaktiven Austausch ermöglichen. Dabei geht es nicht um klassische Inhalte, sondern um nutzergenerierten Content in Internetforen, Bewertungsportalen, Blogs oder

857 Vgl. auch *Klindt/Wende*, BB 2016, 1419 (1420).

858 BGH, NJW 1987, 1009 (1010); *Schmid*, CR 2019, 141 (143 f.); *Röthel*, in: Eifert/Hoffmann-Riem (Hg.), Innovationsverantwortung, S. 335 (341) spricht von „Ungerichtetheit der nachträglichen Risikoerforschungspflichten“; i.E. auch *Foerste*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 376.

859 Zum Ganzen zu Recht *Helte*, Anforderungen an die Produktsicherheit, S. 81.

anderen Social-Media-Kanälen wie Facebook, X und Co.⁸⁶⁰ Inhalte auf solchen Plattformen stellen keinen Ersatz klassischer Publikationen dar, sondern sind Meinungsäußerungen, die bisher dem öffentlichen Raum entzogen waren.⁸⁶¹ Um die Frage nach dem Umfang eines solchen „Social-Media-Monitorings“ beantworten zu können, muss zwischen verschiedenen Konstellationen differenziert werden.

2. Entwicklung falscher Sicherheitserwartungen

Zunächst werden Konstellationen betrachtet, in denen auf Social-Media-Kanälen Produktinformationen verbreitet werden, die eine fehlerhafte oder gefährliche Verwendung des Produkts präsentieren und so fälschliche Sicherheitserwartungen im Zusammenhang mit dem Produkt wecken können.

a) Selbst generierter Content

Handelt es sich um Inhalte, die vom Hersteller im Zusammenhang mit seinem Produkt selbst generiert und auf den eigenen Kanälen veröffentlicht werden, betrifft das im Ausgangspunkt die Darbietung des Produkts. Nach § 3 Abs.1 lit.b ProdHaftG beeinflusst diese Darbietung – hierzu gehören insbesondere auch Werbeaussagen⁸⁶² – maßgeblich die berechnete Sicherheitserwartung. Durch eine irreführende oder fälschliche Darstellung – man denke an ein die Gefahren verharmlosendes Produktvideo – im Rahmen der eigenen Social-Media-Präsenz kann ein Produkt nachträglich fehlerhaft werden.⁸⁶³ Da diese Fehlerhaftigkeit aber noch nicht im maßgeblichen Zeitpunkt des Inverkehrbringens vorlag,⁸⁶⁴ ist die Produkt-

860 Vgl. auch *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 114.

861 *Helte*, Anforderungen an die Produktsicherheit, S. 82 vergleicht sie daher am ehesten mit Leserbriefen oder Diskussionsbeiträgen (Fn. 83).

862 BT-Drucks 11/2447, S. 18; allgemeine Meinung vgl. nur *Taeger*, in: NK-ProdR, § 3 ProdHaftG, Rn. 28; *Lenz*, in: *Lenz*, Produkthaftung, § 3, Rn. 316; *Sprau*, in: *Grüneberg*, BGB, § 3 ProdHaftG, Rn. 5; *Ruttloff/Wagner/Schuster*, BB 2022, 67 (67).

863 *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 117 f.

864 Vgl. *Oechsler*, in: *Staudinger*, BGB, § 3 ProdHaftG, Rn. 43a; *Goehl*, in: *BeckOGK*, BGB, § 3 ProdHaftG, Rn. 57; *Förster*, in: *BeckOK*, BGB, § 3 ProdHaftG, Rn. 14; *Wilhelmi*, in: *Erman*, BGB, § 3 ProdHaftG, Rn. 4.

beobachtungspflicht des Herstellers angesprochen.⁸⁶⁵ Dieser kann auch nicht darauf verweisen, dass ursprünglich eine fehlerfreie Instruktion z.B. durch eine beigelegte Bedienungsanleitung erfolgte. Denn eine solche wird durch den zeitlich nachfolgenden und für die Nutzer vermeintlich neuen Social-Media-Inhalt überlagert.⁸⁶⁶ Es ist daher am Hersteller, im Rahmen seiner Produktbeobachtungspflicht diese Inhalte auf ihre inhaltliche Richtigkeit und Angemessenheit zu überprüfen.⁸⁶⁷ Ebenso muss sich der Hersteller Werbeaussagen eines von ihm beauftragten Influencers zurechnen lassen.⁸⁶⁸ Zwar können im Rahmen der Produktbeobachtungspflicht als Teil der verschuldensabhängigen Produzentenhaftung nach § 823 Abs. 1 BGB nicht sämtliche Äußerungen als persönliche Vorwerfbarkeit zugerechnet werden.⁸⁶⁹ Indes kann es keinen Unterschied machen, ob der Hersteller selbst eine produktbezogene Aussage tätigt oder er einen weiteren Akteur zwischenschaltet, über den er die Aussage steuert.⁸⁷⁰

Damit lässt sich festhalten, dass nicht nur das Produkt selbst, sondern auch produktbezogene Werbe- und Marketingmaßnahmen von der Produktbeobachtungspflicht umfasst sind.⁸⁷¹

b) Nutzergenerierter Content

Schwieriger stellt sich die Lage bei sonstigem nutzergeneriertem Content über die Produkte des Herstellers dar. Denn hier stellt sich gerade die Frage, inwieweit dieser noch dem Hersteller zuzurechnen ist und eine

865 Vgl. in anderer Konstellation Lenz, in: Lenz, Produkthaftung, § 3, Rn. 315.

866 Piovano/Schucht/Wiebe, Produktbeobachtung in der Digitalisierung, S. 117; dies verschärft sich, handelt es sich nicht lediglich um ein Webevideo des Herstellers, sondern um ein instruktives Produktvideo, welches bspw. über einen QR-Code in der Bedienungsanleitung abrufbar ist, vgl. Ruttloff/Wagner/Schuster, BB 2022, 67 (67).

867 Piovano/Schucht/Wiebe, Produktbeobachtung in der Digitalisierung, S. 117 f.

868 Taeger, in: NK-ProdR, § 3 ProdHaftG, Rn. 28, 39; Piovano/Schucht/Wiebe, Produktbeobachtung in der Digitalisierung, S. 117 f.; Ruttloff/Wagner/Schuster, BB 2022, 67 (68).

869 Zur Situation im Rahmen der Haftung nach dem ProdHaftG Oechsler, in: Staudinger, BGB, § 3 ProdHaftG, Rn. 43a und Goehl, in: BeckOGK, BGB, § 3 ProdHaftG, Rn. 57.

870 Allgemein Wagner, in: MüKo, BGB, § 3 ProdHaftG, Rn. 23, wonach Werbeaussagen zu berücksichtigen sind, die vom Hersteller veranlasst wurden; speziell Piovano/Schucht/Wiebe, Produktbeobachtung in der Digitalisierung, S. 118.

871 Piovano/Schucht/Wiebe, Produktbeobachtung in der Digitalisierung, S. 118.

berechtigte Sicherheitserwartung begründen kann. Im analogen Bereich wird dafür plädiert, dass sich der Hersteller „eigenmächtige“ Werbung Dritter nicht zurechnen lassen muss.⁸⁷² Anderes soll nur dann gelten, wenn der Hersteller diese Aussagen billigt.⁸⁷³ Jedenfalls für den Fall, dass es sich um Kommentare auf den eigenen Social-Media-Kanälen des Herstellers handelt, müssen die Aussagen dem Hersteller zugerechnet werden, sollte dieser die irreführenden Inhalte nicht löschen. Andernfalls ist von einer stillschweigenden Billigung auszugehen.⁸⁷⁴ Insoweit drängt sich ein Vergleich zur Rechtsscheinhaftung auf. Im Rahmen der Duldungsvollmacht hat der Vertretene eine Erklärung gegen sich gelten zu lassen, wenn er es wissentlich zulässt, dass ein anderer für ihn wie ein Vertreter auftritt und der Geschäftsgegner dieses Dulden nach Treu und Glauben dahin verstehen darf, dass der als Vertreter Handelnde tatsächlich bevollmächtigt ist.⁸⁷⁵ Nun handelt es sich bei produktbezogenen Aussagen zwar nicht um Willenserklärungen, gleichwohl kann die der Zurechnung zugrundeliegende Wertung übertragen werden. Für den Hersteller stellt sich die Lage so dar, dass der gesamte Inhalt seiner Social-Media-Kanäle als Kenntnisstand gelten muss. Vor dem Hintergrund, dass Hersteller ihre Social-Media-Präsenz schon aus Imagegründen ständig aktualisieren und pflegen, wird ein Produktnutzer einen dort platzierten Inhalt als vom Hersteller wahrgenommen und autorisiert ansehen.

Anders könnte die Konstellation zu beurteilen sein, in der ein Post oder Kommentar nicht auf den Social-Media-Kanälen des Herstellers erfolgt, sondern auf anderen öffentlich zugänglichen Internetquellen. Hier eine entsprechende Kenntnis des Herstellers anzunehmen, liefe auf eine Fiktion hinaus. Vielmehr stellt sich parallel zur Anscheinsvollmacht die Frage, ob der Hersteller diesen Post bei pflichtgemäßer Sorgfalt hätte erkennen können und der Produktnutzer von einer Duldung und Billigung des Herstellers ausgehen durfte.⁸⁷⁶ Vor diesem Hintergrund wird nach der Größe und dem Bekanntheitsgrad des betreffenden Social-Media-Kanals in der jeweiligen

872 *Wagner*, in: MüKo, BGB, § 3 ProdHaftG, Rn. 23; *Lenz*, in: *Lenz, Produkthaftung*, § 3, Rn. 315; *Taeger*, in: NK-ProdR, § 3 ProdHaftG, Rn. 39; *Graf v. Westphalen*, in: Foerste/Graf v. Westphalen (Hg.), *Produkthaftungshandbuch*, § 48, Rn. 51.

873 *Wagner*, in: MüKo, BGB, § 3 ProdHaftG, Rn. 23; *Graf v. Westphalen*, in: Foerste/Graf v. Westphalen (Hg.), *Produkthaftungshandbuch*, § 48, Rn. 51.

874 So auch *Piovano/Schucht/Wiebe*, *Produktbeobachtung in der Digitalisierung*, S. 121 f.

875 Vgl. nur *Ellenberger*, in: Grüneberg, BGB, § 172, Rn. 8.

876 Zur Anscheinsvollmacht *Ellenberger*, in: Grüneberg, BGB, § 172, Rn. 11.

Branche differenziert.⁸⁷⁷ Diese Fokussierung allein auf die Perspektive des Herstellers verkennt aber, dass bereits Werbeaussagen eine haftungsbegründende Funktion nur dann erfüllen können, wenn sie beim Adressaten eine ernsthafte und konkrete Sicherheitsvorstellungen wecken.⁸⁷⁸ Produktbezogene Aussagen anderer Nutzer auf Social-Media-Kanälen, die keine Rückschlüsse auf die Autorität des Herstellers zulassen, sind aber gerade nicht geeignet solche ernsthaften Sicherheitsvorstellungen zu erzeugen.⁸⁷⁹ Freilich tut ein Hersteller trotzdem gut daran, sollte er solche irreführenden Inhalte über das eigene Produkt entdecken, einen Kommentar über diese inakzeptable Nutzung zu veröffentlichen.⁸⁸⁰

3. Meldungen von Produktgefahren

Neben der Beeinflussung der Sicherheitserwartungen können Social-Media-Inhalte im Zusammenhang mit einem Produkt aber auch Aufschluss über sicherheitskritische Eigenschaften des Produkts im Feld liefern.

a) Eigene Social-Media-Präsenz des Herstellers

Zunächst soll der Fall betrachtet werden, dass Nutzer produktbezogene Informationen auf einer unternehmenseigenen Internetseite des Herstellers oder auf externen Seiten auf einem vom Hersteller eingerichteten Unternehmensprofil posten.

Interessant ist in diesem Zusammenhang ein Blick auf die öffentlich-rechtlichen Regelungen des Arzneimittelrechts. Nach § 63b Abs. 1 AMG ist der Zulassungsinhaber verpflichtet, ein Pharmakovigilanzsystem einzurichten und zu betreiben und anhand dessen sämtliche relevante Informationen wissenschaftlich auszuwerten (§ 63b Abs. 2 Nr. 1 AMG). Über Modul IV, Ziff. VI.B. 1.1.4 der GVP-Guideline⁸⁸¹ wird der Zulassungsinhaber ange-

877 So Piovano/Schucht/Wiebe, Produktbeobachtung in der Digitalisierung, S. 123 f.; noch weitergehend wohl Gauger/Hartmannsberger, NJW 2014, 1137 (1140).

878 Vgl. Oechsler, in: Staudinger, BGB, § 3 ProdHaftG, Rn. 45.

879 Wohl auch Ruttloff/Wagner/Schuster, BB 2022, 67 (68) „Dem Hersteller ist dieses Verhalten des Dritten nicht zurechenbar, solange keine Verbindung zu ihm besteht“.

880 Hierauf weist Piovano/Schucht/Wiebe, Produktbeobachtung in der Digitalisierung, S. 124 hin; ähnlich Taeger, in: NK-ProdR, § 3 ProdHaftG, Rn. 39; Ruttloff/Wagner/Schuster, BB 2022, 67 (68).

881 EMA, Guideline on good pharmacovigilance practices, EMA/873138/2011 Rev 2.

wiesen, im Rahmen des Pharmakovigilanzsystems auch Internetangebote und digitale oder soziale Medien, die unter seiner Verwaltung oder seiner Verantwortung stehen, auf mögliche Verdachtsfälle von Nebenwirkungen zu prüfen. Konkretisierend wird ausgeführt, dass dabei alle Internetangebote umfasst sein sollen, die dem Zulassungsinhaber gehören, von ihm finanziert oder von ihm kontrolliert werden. Neben den eigenen Internetangeboten sowie den eigens eingerichteten Social-Media-Kanälen sollen damit auch Internetangebote Dritter geprüft werden, die vom Unternehmer finanziell unterstützt werden.⁸⁸²

Dieser Gedanke lässt sich über das Pharmarecht hinaus verallgemeinern. Ein Hersteller, der einen Kommunikationsweg zum Nutzer öffnet oder kontrolliert, muss Informationen, die auf diesem Wege adressiert werden, auch wahrnehmen.⁸⁸³ Hinzu kommt, dass die direkte und unmittelbare Kommunikation einen hohen Nutzen für den Hersteller erzeugt. So kann dieser auch jenseits expliziter Beschwerden aus Erfahrungsberichten der Nutzer produktsicherheitsrelevante Rückschlüsse ziehen.⁸⁸⁴ Daneben fallen Verzögerungen oder eine lückenhafte Weitergabe der Informationen, die sich aus der Zwischenschaltung möglicherweise mehrerer Vertriebsstufen ergeben, weg. Da diese rein passive Produktbeobachtungspflicht mit wenig Aufwand einhergeht und die Hersteller ihre eigenen Kanäle bereits zu Werbezwecken ständig pflegen, ist sie auch unter Gesichtspunkten der Zumutbarkeit vom Pflichtenprogramm des Herstellers umfasst.⁸⁸⁵ Ebenfalls als an den Hersteller adressierte Kommunikation können Beiträge gelten, in denen der Hersteller getaggt ist und durch diese Markierung eine Vernetzung zu einem Unternehmensprofil des Herstellers stattfindet. Denn durch das Unternehmensprofil auf der jeweiligen Plattform ermöglicht der Hersteller eine den entsprechenden Gepflogenheiten folgende Interaktion und einen Kommunikationskanal. Anders verhält es sich, wenn der Name des Herstellers in der entsprechenden Markierung falsch geschrieben wurde oder die Verlinkung aus sonstigen Gründen nicht funktioniert. In diesem Fall ist nämlich nicht nur die bloße Entgegennahme der Information i.S. einer passiven Produktbeobachtung erforderlich. Vielmehr wäre nach dem Beitrag aktiv zu suchen.

882 Zum Ganzen *Altschwager*, PharmR 2021, 461 (466 f.).

883 Zu diesem allgemeinen Argument *Helte*, Anforderungen an die Produktsicherheit, S. 83.

884 *Klindt/Wende*, Rückrufmanagement, S. 63.

885 *Dötsch*, Außervertragliche Haftung für KI, S. 255; *Klindt*, in: Eifert (Hg.): Produktbeobachtung durch Private, S. 55 (59); *Klindt/Wende*, Rückrufmanagement, S. 63; *Helte*, Anforderungen an die Produktsicherheit, S. 83.

b) Sonstige öffentlich zugängliche Social-Media-Kanäle

Weniger eindeutig stellt sich die Lage allerdings bei der Frage nach einer aktiven Produktbeobachtungspflicht hinsichtlich der Durchsuchung sämtlicher anderen öffentlich zugänglichen Internetquellen dar.⁸⁸⁶ Ein solches Web-Screening von herstellerunabhängigen Social-Media-Kanälen begegnet vor dem Hintergrund mangelnder Qualität der erlangten Daten und begrenzter technischer Möglichkeiten der Überprüfung Bedenken.⁸⁸⁷ Die Beantwortung der Frage hat sich wieder danach zu richten, was an Verkehrspflichten erforderlich und dem Hersteller zumutbar ist.

aa) Geeignetheit zur Gewinnung sicherheitsrelevanter Erkenntnisse

Vor diesem Hintergrund werden zunächst Zweifel geäußert, ob eine solches Social-Media-Monitoring überhaupt geeignet ist, sicherheitsrelevante Erkenntnisse in Erfahrung zu bringen. Insoweit wird angeführt, dass aus den im Internet häufig abgegebenen „saloppe[n] Meinungsäußerung[en]“ keine seriösen und belastbaren Produktgefahren ableiten ließen.⁸⁸⁸ Es fehle bei diesen neuen Medien im Vergleich zu Online-Publikationen an einer vorherigen journalistischen Überprüfung des Inhalts- und Wahrheitsgehalts, wobei sich die Problematik durch häufig fehlende Klarnamen des Urhebers

886 Eine solche wird von der wohl h.M. pauschal und ohne Begründung bejaht, vgl. *Droste*, CCZ 2015, 105 (106); *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), *Produkthaftungshandbuch*, § 24, Rn. 378; *Chibanguza*, in: *Buck-Heeb/Oppermann* (Hg.), *Automatisierte Systeme*, S. 407 (410); mittelfristig auch *Reusch*, in: *Kaulartz/Braegelmann* (Hg.), *Artificial Intelligence und Machine Learning*, S. 110; *Veltins*, in: *Moosmayer/Lösler* (Hg.), *Corporate Compliance*, § 34, Rn. 4; wohl auch *Gauger/Hartmannsberger*, NJW 2014, 1137 (1140), die darauf hinweisen, dass im Rahmen des ProdSG anders gelte, da § 6 Abs. 3 S. 1 Nr. 2 ProdSG ausdrücklich von „Beschwerden“ spricht, die typischerweise unmittelbar an Hersteller gerichtet sind, weshalb Aussagen außerhalb der Sphäre der Normadressaten, etwa in Internet-Foren oder Ähnlichem, nicht erfasst seien; argumentativ aber *Hauschka/Klindt*, NJW 2007, 2726 (2729) und *Klindt/Wende*, BB 2016, 1419 (1420); offen gelassen von *Wendt/Oberländer InTeR* 2016, 58 (63).

887 Eine diesbezügliche Pflicht daher ablehnend *Helte*, Anforderungen an die Produktsicherheit, S. 82 und *Klindt*, in: *Eifert* (Hg.), *Produktbeobachtung durch Private*, S. 55 (59); zurückhaltend auch *Chibanguza*, in: *Chibanguza/Kuß/Steege* (Hg.), *Künstliche Intelligenz*, § 5, K, Rn. 22.

888 *Klindt*, in: *Eifert* (Hg.), *Produktbeobachtung durch Private*, S. 55 (59); auch *Helte*, Anforderungen an die Produktsicherheit, S. 82 „nicht geeignet einen Anfangsverdacht zu begründen, der weitere Reaktionen des Herstellers erfordert“.

eines Beitrags und damit einer fehlenden Identifizierbarkeit nochmals steigern. Hinzu komme, dass eine in die Anonymität des Internets abgegebene Erfahrung mit dem Produkt im Gegensatz zu einer direkten Meldung an den Hersteller Zweifel aufkommen lasse, dass der Vorfall tatsächlich stattgefunden hat.⁸⁸⁹

Auch wenn diese Einwände nicht von der Hand zu weisen sind, darf nicht übersehen werden, dass ein solcher Social-Media-Post als ungefilterte Meinung aus dem Feld auch großes Informationspotential für den Hersteller birgt. Denn Social-Media-Posts sind nicht auf Beschwerde- oder Schadensmeldungen begrenzt, sondern lassen umfassende Rückschlüsse auf das Verhalten und den Einsatz des Produkts im Feld zu. Ein prominentes Beispiel stellen Produktvideos dar, die von Nutzern auf Social-Media-Plattformen hochgeladen werden und aus denen sich Anhaltspunkte ergeben können, wie das Produkt zumindest auch verwendet wird. Hinzu kommt, dass instruktive Tutorial-Videos gerade darauf angelegt sind, die Verwendungspraxis anderer Nutzer zu beeinflussen. Für den Hersteller bietet sich daher eine Erkenntnisquelle hinsichtlich sich manifestierender Fehlgebräuche.⁸⁹⁰ Auch aus einschlägigen Foren oder entsprechenden Kommentierungen unter Beiträgen zum Produkt lässt sich ein Bild der tatsächlichen Verwendungsweise im Feld ziehen.⁸⁹¹ Auch wenn solche Posts auf externen Kanälen nicht geeignet sind, die berechtigte Sicherheitserwartung anderer Nutzer zu beeinflussen (s.o.), lassen sich doch Rückschlüsse ziehen, dass die ursprüngliche Instruktion bei Inverkehrgabe nicht ausreichend gewesen sein kann bzw. sich das tatsächliche Nutzerverhalten schlicht anders darstellt als damit gerechnet wurde. Aber nicht nur ein etwaiger Fehlgebrauch lässt sich anhand von Social-Media-Beiträgen erkennen, sondern auch erste Anzeichen sicherheitstechnischer Fehlfunktionen des Produkts. Denn hinsichtlich benötigter Instruktionen wurde zunehmend die Intelligenz bzw. die Erfahrung der Masse im Internet erster Ansprechpartner des Nutzers. Ebenso wie Tutorial-Videos in der Praxis das Lesen von Gebrauchsanweisungen ersetzen, wird sich mit Problemen, die bei der Verwendung des Produkts auftauchen, zunächst über entsprechende Foren an die Masse des

889 Insgesamt *Helte*, Anforderungen an die Produktsicherheit, S. 82 f.

890 Insgesamt zu instruktiven Produktvideos *Ruttloff/Wagner/Schuster*, BB 2022, 67 (68).

891 So auch das Bundesministerium für Wirtschaft und Klimaschutz (Mittelstand Digital), Produktsicherheit dank sozialer Medien, <https://www.mittelstand-digital.de/MD/Redaktion/DE/Unternehmerfragen/Standardartikel/5-wie-funktioniert-es-sicher-praxisbeispiel-produktsicherheit-dank-sozialer-medien.html> (zuletzt abgerufen am 23.09.2024).

Netzes gewandt und abgefragt, ob sich auch andere Nutzer mit ähnlichen Komplikationen konfrontiert sehen.

Die Beispiele verdeutlichen, dass den Hersteller über ein Social-Media-Monitoring Informationen auch unterhalb einer Schwelle erreichen, als dies ansonsten der Fall wäre. Denn die „Kommunikation“ findet nicht erst bei einer handgreiflichen Beschwerde statt, sondern ermöglicht es dem Hersteller, frühzeitig auf sich abzeichnende Entwicklungen einzugehen. Damit erhält der Hersteller zusätzliche Informationen über das Produkt, die qualitativ schwerlich mit einzelnen konkreten und direkt an ihn gerichteten Beschwerden vergleichbar sind. Gerade Aussagen, die der Nutzer als für den Hersteller nicht relevant und damit als nicht beschwerdetauglich einschätzt, können für den Hersteller aufgrund seines technischen Konstruktionsverständnisses sicherheitsrelevante Rückschlüsse zulassen oder ein weiteres Informationspuzzlestück für ein einheitliches Sicherheitsbild seines Produkts darstellen. Die Tatsache, dass nicht alle produktbezogenen Beiträge einen Mehrwert für den Hersteller generieren, ist keine Besonderheit von Social-Media-Posts, sondern tritt bei herkömmlichen Beschwerden ebenso auf. Gleichwohl wird die Filterung von relevanten und irrelevanten Informationen gerade vor dem Hintergrund, dass Nutzer Beiträge im Internet aufgrund des Gefühls der Anonymität unreflektierter und womöglich aus einer Laune heraus in das Netz stellen, an Bedeutung gewinnen. Dieser Faktor mag die Zumutbarkeit beeinflussen, kann die Geeignetheit eines Social-Media-Monitorings hinsichtlich der Gewinnung sicherheitsrelevanter Erkenntnisse aber nicht schlechthin in Frage stellen.

bb) Erwägungen der Erforderlichkeit

Auf der anderen Seite konnte noch vor wenigen Jahren keine berechtigte Verkehrserwartung dahingehend angenommen werden, dass ein Hersteller „jede an noch so beliebiger Stelle im Internet wiedergegebene Kritik an einem seiner Produkte auffinden müsste“.⁸⁹² Dem standen auch fehlende technische Mittel der Auswertung des Internets entgegen.⁸⁹³ Freilich gab es die Möglichkeit, über Suchmaschinen und die Eingabe von Begriffen wie „Fehler“, „Gefahr“ oder „Beanstandung“ in Verbindung mit dem Namen des

⁸⁹² *Klindt*, in: Eifert (Hg.), *Produktbeobachtung durch Private*, S. 55 (59).

⁸⁹³ *Klindt*, in: Eifert (Hg.), *Produktbeobachtung durch Private*, S. 55 (59); *Helte*, *Anforderungen an die Produktsicherheit*, S. 82.

eigenen Produkts oder der Produktkategorie Informationen in Erfahrung zu bringen.⁸⁹⁴ Dieses auf Zufallsfunden beruhende Internet-Screening kann aber – wenn überhaupt – nur an der Oberfläche kratzen. Sicherheitsrelevante Informationen, die sich in den Tiefen sozialer Netzwerke verbergen, können damit aber kaum aufgefunden werden. Auch die Einrichtung eines „Google-Alert“ zu den entsprechenden Suchbegriffen erscheint wenig erfolgsversprechend.⁸⁹⁵ Denn dieser automatisiert lediglich den Suchvorgang, ist aber ebenso wie die manuelle Suche darauf angewiesen, dass Google neue Seiten in seine Ergebnislisten aufnimmt und eignet sich daher nicht zum Auffinden spezifischer Beiträge in sämtlichen sozialen Netzwerken. Den herkömmlichen Methoden eines Internet-Screenings konnte daher in der Tat mangelnde Effektivität und eine lückenhafte Informationsbeschaffung nachgesagt werden.⁸⁹⁶ Mittlerweile ermöglichen aber spezielle Dienstleister ein qualitativ hochwertiges Web-Monitoring.⁸⁹⁷ Durch KI gestützte Software werden gesamte Beiträge ausgelesen und der komplette Inhalt, die Textstruktur sowie alle Metainformationen (Quelle, Autor, Links, Zeit etc.) ausgewertet.⁸⁹⁸

In einer Zeit, in der Daten für Unternehmen das neue Gold sind und ein Social-Media-Monitoring zu Zwecken des Reputationsmanagements, der Kundenzufriedenheit, der Wettbewerbsbeobachtung und der Marktanalyse ohnehin, ggf. auch ausgelagert durch externe Dienstleister, betrieben wird, ist auch eine entsprechende Beobachtung zur Gefahrenabwehr erforderlich.

894 Hierauf abhebend *Stempfle*, in: Pfeifer/Schmitt (Hg.), *Masing Handbuch Qualitätsmanagement*, S. 974.

895 So aber *Hauschka/Klindt*, NJW 2007, 2726 (2729); einschränkend schon *Klindt/Wende*, BB 2016, 1419 (1420).

896 *Helte*, Anforderungen an die Produktsicherheit, S. 82; *Klindt/Wende*, BB 2016, 1419 (1420).

897 Solche Lösungen bereits antizipiert haben *Klindt/Wende*, BB 2016, 1419 (1420); vgl. auch *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 72, 129 f., allerdings zurückhaltend mit Blick darauf, dass eine solche Einbindung von Datenintermediären noch in den „Kinderschuh“ stecke.

898 Vgl. folgenden Pressebericht zum Anbieter Conslin AG (<https://conslin.com/safety-recall-monitoring/>), <https://www.presseportal.de/pm/28739/3683209> (beide zuletzt abgerufen am 23.09.2024).

cc) Erwägungen der Zumutbarkeit

Die Zumutbarkeit wird dabei umso eher zu bejahen sein, wenn der Hersteller ohnehin bereits aus anderen Gründen ein Social Media Monitoring betreibt. Das Monitoring kommt auch nicht erst dann in Betracht, wenn der Hersteller auf andere Weise konkrete Hinweise auf eine Produktgefahr erlangt hat.⁸⁹⁹ Denn die Informationen aus dem Social-Media-Monitoring eignen sich weniger zu Verifizierung eines bereits bestehenden Verdachts, sondern begründen ihrer Art nach einen solchen erst. Eine Überprüfung kann dann möglicherweise durch einen Abgleich der Daten erfolgen, die aus den eigenen Produkten gewonnen werden.⁹⁰⁰ In diesem Sinne führt die den Hersteller erreichende Datenflut zwar zu einem erheblichen Aufwand bei der Filterung und Auswertung, gleichzeitig ermöglichen aber Querabgleiche eine jeweilige Verifizierung der Daten. Auch hierbei können Dienstanbieter unter Zugrundelegung KI-gestützter Big Data-Plattformen eingeschaltet werden.⁹⁰¹ Einen weiteren Vorteil der KI-gestützten Erfassung und Auswertung von Informationen bildet der Wegfall von Sprachbarrieren beim Social-Media-Monitoring, sodass produktbezogene Beiträge weltweit verfolgt werden können.⁹⁰² Von einer Unzumutbarkeit des Aufwands kann daher nicht pauschal gesprochen werden.⁹⁰³

899 So aber *Helte*, Anforderungen an die Produktsicherheit, S. 83.

900 So auch *Chibanguza*, in: Buck-Heeb/Oppermann (Hg.), *Automatisierte Systeme*, S. 407 (410).

901 Vgl. folgenden Pressebericht zur Conslin AG <https://www.presseportal.de/pm/28739/4541677> (zuletzt abgerufen am 23.09.2024).

902 In diese Richtung schon *Klindt/Wende*, BB 2016, 1419 (1420). Für die Auswertung herkömmlicher Informationsquellen ist streitig, ob diese auch in fremden Sprachen berücksichtigt werden müssen. Für Fachzeitschriften wird dies mit dem Argument abgelehnt, dass sich Informationen von einigem Gewicht regelmäßig in kürzester Zeit auch in englischsprachigen Publikationen niederschlagen, vgl. dazu *Wagner*, VersR 2014, 905 (906).

903 Anders aber *Dötsch*, Außervertragliche Haftung für KI, S. 256, die eine zielgerechte Adressierung an den Hersteller fordert; zurückhaltend auch *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 126, 129, die auf die Größe des Herstellers und den Bekanntheitsgrad und die Reichweite der jeweiligen Plattform abheben und die Einbindung von Dienstleistern lediglich als optionale Möglichkeit ansehen.

dd) Sorgfältige Prüfung des Verschuldens

Indes darf nicht übersehen werden, dass die Ausdehnung der aktiven Produktbeobachtungspflicht auf Social-Media-Monitoring auch erhebliche Rechtsunsicherheiten für die Hersteller birgt. Denn in Produkthaftungsprozessen wird sich in diesen Fällen immer die Frage stellen, ob der konkrete Social-Media-Beitrag tatsächlich vom Hersteller hätte gefunden werden müssen.⁹⁰⁴ Hinzu kommt, dass sich Hersteller beim Social-Media-Monitoring laufend neuen Herausforderungen aufgrund neuer Funktionalitäten der Plattformen ausgesetzt sehen. So stellen beispielsweise die vielfach genutzten Story-Postings aufgrund ihrer zeitlich auf einen Tag begrenzten Verfügbarkeit ein Problem dar. Die Gerichte werden daher gut daran tun, die Anforderungen nicht zu überspannen. Denn die verbleibende Verantwortung auch nach dem Inverkehrbringen eines Produktes darf nicht dazu führen, dass unerfüllbare und unrealistische Anforderungen an den Hersteller gestellt werden. In der bisherigen Rechtsprechung zur Produktbeobachtungspflicht konnte eine begrüßenswerte Trennung zwischen dem Bestehen der Produktbeobachtungspflicht und deren schuldhafter Verletzung festgestellt werden.⁹⁰⁵ Diese sollte auch konsequent beim Social-Media-Monitoring durchgehalten werden. Nur durch eine solche Handhabung ist gewährleistet, dass das Social-Media-Monitoring als das gesehen wird, was es ist: Nämlich eine Chance, die Produktbeobachtungspflicht noch feingranularer erfüllen zu können und schneller auf kritische Entwicklungen reagieren zu können,⁹⁰⁶ nicht aber ein Mittel, um einem geschädigten Nutzer zu einem Schadensersatz zu verhelfen. Vor diesem Hintergrund bietet es sich an, eine Parallele zur Ausreißer-Problematik beim Fabrikationsfehler zu ziehen. Ebenso wie beim grundsätzlich fehleranfälligen Produktionsprozess kann auch beim Social-Media-Monitoring trotz des Treffens aller zumutbaren Sicherheitsvorkehrungen keine vollständige Sicherheit erwartet werden. Einzelne Produktinformationen können vom Monitoring ebenso unerfasst bleiben wie einzelne fehlerhafte Produkte von der Qualitätskontrolle im Rahmen der Produktion. Kommt der Hersteller daher seinen Organisationspflichten bzgl. des Social-Media-Monitorings nach, muss es ihm offenbleiben, sich hinsichtlich eines „Ausreißers“ zu entlasten.

904 Herkömmlich schon *Helte*, Anforderungen an die Produktsicherheit, S. 15; *Thöne*, Autonome Systeme, S. 86.

905 So v. *Bar*, in: *Lieb* (Hg.), Produktverantwortung und Risikoakzeptanz, S. 29 (36 f.) in Bezug auf BGH, NJW 1994, 3349.

906 Ähnlich auch *Reusch*, in: *Kaulartz/Braegelman* (Hg.), Artificial Intelligence und Machine Learning, S. 143.

IV. Auswertung von Sensor-Daten

Neben der Möglichkeit, das Internet auf sicherheitsrelevante Informationen zum eigenen Produkt zu durchsuchen, ergibt sich durch die Digitalisierung der Produktlandschaft eine weitere und besonders relevante Erkenntnisquelle. Durch die Vernetzung von IoT-Produkten und deren Anbindung über das Internet können die Produkte selbst als Datenlieferanten für sicherheitsrelevante Erkenntnisse begriffen werden. Technische Sensor-Daten können rund um die Uhr ausgewertet, analysiert und der Zustand eines Produkts damit fortwährend überwacht werden. Dadurch bietet sich die Chance, Fehler in Echtzeit zu erkennen und auf diese zu reagieren.⁹⁰⁷

Hinsichtlich dieser neuen Datenverfügbarkeit müssen aber zwei grundlegende Fragen voneinander getrennt werden.⁹⁰⁸ Zum einen, inwieweit die Hersteller sensorisch bereits erhobene Daten tatsächlich auswerten müssen. Zum anderen und weitergehend, ob die Hersteller aufgrund der technisch zur Verfügung stehenden Zugriffsmöglichkeiten auch zur Datenerhebung verpflichtet sind bzw. eine solche in dem Produkt konstruktiv anlegen müssen.

1. Potential der Auswertung von Sensor-Daten

Bevor diese Fragen geklärt werden, soll zunächst untersucht werden, wie sich eine derartige unmittelbare Beobachtung der Produkte zu den bisherigen Produktbeobachtungspflichten des Herstellers verhält. Dazu ist auf das Potential der Auswertung von Sensor-Daten einzugehen.

907 Dieses Potential wird in der juristischen Literatur allgemein erkannt, vgl. nur *Droste*, CCZ 2015, 105 (110); *Gomille*, JZ 2016, 76 (80); v. *Bodungen/Hoffmann*, NZV 2016, 503 (506); *Hartmann*, DAR 2015, 122 (124); *Chibanguza/Schubmann*, GmbHR 2019, 313 (315); *Ackermann*, in: NK-ProdR, § 823 BGB, Rn. 125; *Hey*, Die außervertragliche Haftung des Herstellers autonomer Fahrzeuge, S. 91 f.; *Steege*, in: *Buck-Heeb/Oppermann* (Hg.), *Automatisierte Systeme*, S. 367 (396); *Dötsch*, Außervertragliche Haftung für KI, S. 255; *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 108; gleichwohl ist noch kaum geklärt, welche Maßnahmen hierfür zu ergreifen sind und ob und in welchem Umfang diese Daten auszuwerten sind, vgl. *Wiesemann/Mattheis/Wende*, MMR 2020, 139 (140) und *Sedlmaier*, in: *Kühne/Nack* (Hg.), *Connected Cars*, S. 40.

908 In dieser Deutlichkeit nur *Klindt*, DAR 2023, 7 (8) und *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 110.

Die bisherigen Erkenntnisquellen sowohl der aktiven als auch der passiven Produktbeobachtungspflicht sind durch eine Abhängigkeit dergestalt gekennzeichnet, dass Produktgefahren erst einmal an den Hersteller herangetragen werden müssen und der Hersteller von einer Fehlermeldung tatsächlich Kenntnis erlangen muss. Damit ist aber eine hohe Dunkelziffer an Produktgefahren verbunden, die den Hersteller nie erreichen.⁹⁰⁹ Hinzu kommt, dass Meldungen über Produktgefahren den Hersteller regelmäßig erst dann erreichen, wenn sich die Gefahr bei zumindest einem Produktexemplar ausgewirkt hat und es bei einem Nutzer zu einem Schadenseintritt gekommen ist.⁹¹⁰ Aufgrund der Haftungsfreistellung im Falle eines Entwicklungsfehlers kann damit eine Haftungslücke entstehen. Denn erst mit dem ersten Schadensereignis wird der Entwicklungsfehler identifiziert und kann der Hersteller für die restlichen bereits im Verkehr befindlichen Produkte über die Produktbeobachtungspflicht in Verantwortung genommen werden.⁹¹¹ Auch wenn die Produktbeobachtungspflicht zukunftsbezogen darauf gerichtet ist, Schädigungen zu vermeiden, setzt sie in der Regel mit dem erstmaligen Schadenseintritt ein reaktives Momentum voraus. Dieses in zeitlicher Hinsicht bestehende Defizit verstärkt sich dadurch, dass zwischen dem Schadenseintritt, seiner Veröffentlichung und der Kenntnisnahme durch den Hersteller eine lange Latenzzeit liegen kann.⁹¹² Je mehr Zeit aber verstrichen ist, desto schwieriger stellt sich die Ursachenforschung für den Hersteller dar und desto größer kann das Schadensausmaß sein, da mittlerweile bereits weitere Exemplare der Produktserie betroffen sein können.⁹¹³ Daneben tragen in Laiensprache formulierte Kundenbeschwerden nicht immer zur raschen und lösungsorientierten Fehleranalyse bei, sondern können Unsicherheiten erst hervorrufen.⁹¹⁴

Die Auswertung der vom IoT-Gerät erhobenen Daten hat das Potential, diese Defizite bei der herkömmlichen Produktbeobachtung auszuglei-

909 Hierzu *Schmid*, IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme, S. 206; *Schmid*, CR 2019, 141 (142).

910 *Schmid*, IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme, S. 206; *Schmid*, CR 2019, 141 (142).

911 Dazu *Hofmann*, CR 2020, 282 (286).

912 *Schmid*, IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme, S. 206; *Schmid*, CR 2019, 141 (142).

913 *Schmid*, IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme, S. 206.

914 *Schmid*, CR 2019, 141 (142).

chen.⁹¹⁵ Durch die Möglichkeit, Daten direkt und in Echtzeit von dem Gerät abzurufen, gelangt der Hersteller deutlich schneller und ohne Latenzzeit an sicherheitsrelevante Informationen.⁹¹⁶ Er ist nicht mehr darauf angewiesen, dass die Nutzer sich an ihn wenden, sondern er kann sich die Informationen ohne Zutun eines Dritten selbst beschaffen.⁹¹⁷ Daneben ermöglicht der Zugriff auf die Rohdaten eine schnelle Ursachenforschung, ohne dass Kundenbeschwerden langwierig möglichen Fehlerursachen zugeordnet werden müssen.⁹¹⁸ Schließlich können auch für den Nutzer versteckte, weil noch nicht zu Tage getretene Produktgefahren identifiziert werden.⁹¹⁹ Dadurch können Produktgefahren im Idealfall noch vor der ersten Schadensverursachung erkannt werden.⁹²⁰ Neben der besseren und breiteren Datenbasis,⁹²¹ die Querabgleiche ermöglicht und Informationen aus anderen Quellen der Produktbeobachtung verifizieren kann, liegt darin die größte Chance für ein effektiveres Management von Produktkrisen in der Möglichkeit, Gefahren deutlich schneller als bisher auf den Grund gehen zu können.⁹²²

2. Pflicht zur Auswertung bereits erhobener Sensor-Daten

Die Frage, ob und welche vom Produkt sensorisch erhobenen Daten vom Hersteller auszuwerten sind, hängt maßgeblich davon ab, wann von „erhobenen“ Daten gesprochen werden kann.

915 Hartmann, PHi 2017, 42 (42) spricht überspitzt davon, dass „Hersteller in der ‚Welt der alten Produkte‘ oft relativ „taub“ und „blind“ hinsichtlich des Verhaltens ihrer Produkte nach der Inverkehrgabe“ waren, wohingegen „in der Welt von morgen eine komplette Transparenz zwischen Hersteller und Produktzustand/-bewährung „im Feld“ bestehen“ könne.

916 Gomille, JZ 2016, 76 (80); Schmid, CR 2019, 141 (142); Chibanguza/Schubmann, GmbHR 2019, 313 (316); Chibanguza, in: Chibanguza/Kuß/Steege (Hg.), Künstliche Intelligenz, § 5, K., Rn. 24.

917 Wagner, AcP 217 (2017), 707 (751); Schreck, Fahrzeugdaten, S. 228; Grünvogel/Dörrenbächer, ZVertriebsR 2019, 87 (89).

918 Gomille, JZ 2016, 76 (80).

919 Schmid, IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme, S. 207.

920 Eichelberger, in: Ebers et al., (Hg.), Künstliche Intelligenz und Robotik, S. 186; Schmid, IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme, S. 207; Sedlmaier, in: Kühne/Nack (Hg.), Connected Cars, S. 40; Wiesemann/Mattheis/Wende, MMR 2020, 139 (141).

921 Vgl. auch Weisser/Färber, MMR 2015, 506 (508).

922 In diese Richtung auch Hartmann, DAR 2015, 122 (124).

a) Datenkategorien und Datenübermittlung

Insoweit ist festzuhalten, dass in smarten Produkten eine Vielzahl verschiedener Daten erzeugt, verarbeitet, gespeichert, teilweise wieder gelöscht, aber auch weitergeleitet werden.⁹²³ Zum einen interessieren für die Produktbeobachtungspflicht im Wesentlichen nur vom Gerät erzeugte technische Daten, nicht aber Komfortdaten oder vom Nutzer selbst eingebrachte Daten. Zum anderen führt die bloße Tatsache, dass eine Vielzahl an Daten erhoben wird,⁹²⁴ noch nicht dazu, dass diese Daten auch für den Hersteller verfügbar sind. Denn häufig werden Daten nur für die Dauer des jeweiligen Vorgangs, für den sie benötigt werden, flüchtig gespeichert. Andere Daten werden zwar kurzfristig gespeichert, aber bei fehlenden Auffälligkeiten ständig mit aktuellen Daten überschrieben. Insbesondere Daten, die im Zusammenhang mit einem Fehler gespeichert werden, bleiben aber regelmäßig länger erhalten, entweder bis der Fehler nicht mehr auftritt oder bis zur nächsten Wartung.⁹²⁵ Neben der Speicherung solcher Fehler- und Wartungsdaten ist es gerade in der Automobilbranche üblich, weitere Daten verschlüsselt und nur für den Hersteller zugänglich zu speichern.⁹²⁶

Weiter ist zwischen Offline- und Online-Geräten zu unterscheiden. Während Letztere bestimmte Daten vom Gerät an den Hersteller übertragen und dort in der Regel auf Backendservern gespeichert werden, findet bei Offline-Geräten eine Speicherung nur in den Speichereinheiten des Geräts selbst statt, ohne dass der Hersteller unmittelbaren Zugriff auf diese Daten hätte.⁹²⁷ Vielmehr ist für eine Übermittlung dieser generierten Daten ein konventionelles Auslesen mithilfe von Diagnosegeräten oder Computern an entsprechenden Schnittstellen notwendig.⁹²⁸ Zu einem solchen Auslesen der Daten durch den Hersteller kommt es bei Offline-Geräten in der Regel nur im Rahmen von Wartungs- oder Reparaturarbeiten zum Zwecke der

923 In Bezug auf Fahrzeuge Krauß/Waidner, DuD 2015, 383 (384).

924 Zum Vorgang der Datenerhebung mittels Steuergeräten Raith, Das vernetzte Automobil, S. 10 f.

925 Vgl. zu den unterschiedlichen Speicherdauern Mielchen, SVR 2014, 81 (82 f.); Hinrichs/Becker, ITRB 2015, 164 (165); Krauß/Waidner, DuD 2015, 383 (385).

926 Vgl. Mielchen, SVR 2014, 81 (82) spricht von „geheimen Daten“ und sieht den Grund der Verschlüsselung in der Sorge der Hersteller, dass der Gebrauchsmusterschutz bezüglich der Algorithmen zur Regelung der Fahrerassistenzsysteme gefährdet werden könnte.

927 Hierzu im Kontext von Fahrzeugdaten Nugel, ZD 2019, 341 (342).

928 Hinrichs/Becker, ITRB 2015, 164 (165).

Fehleranalyse.⁹²⁹ Online-Geräte verfügen dagegen über eine permanente Möglichkeit der Datenübertragung auch außerhalb von physisch am Gerät stattfindenden Inspektionstätigkeiten. Über Mobilfunk und mobiles Internet können die generierten Daten auf verschiedene Arten in Echtzeit übertragen werden.⁹³⁰

Durch die zunehmende Anzahl an vernetzten Produkten liegt hierin das große Potential im Bereich der Datenauswertung. Denn vernetzte Produkte verfügen über Kommunikationsmöglichkeiten nach außen.⁹³¹ War eine Offline-Datenauswertung bisher insbesondere im Automotive-Sektor gängig, ist eine Online-Datenauswertung künftig bei jedem IoT-Gerät denkbar. Dabei braucht es wenig Fantasie sich vorzustellen, dass die Hersteller diese Möglichkeit der Datenübermittlung nutzen werden, um sich ein möglichst genaues Bild vom Nutzungsverhalten ihres Produktes zu machen. Neben den Fehler- und Wartungsdaten wird es auch zu einer Auslesung der verschlüsselten Daten kommen.⁹³² Diese können dann zu weiterem Erkenntnisgewinn genutzt werden, um aus dem Nutzungsverhalten Schlüsse für zukünftige Produktverbesserung und -weiterentwicklung zu ziehen, um zielgerichtete Marketingkampagnen zu starten oder aber auch um ungerechtfertigte Produkthaftungsansprüche abzuwehren.⁹³³

b) „Erhobene“ Daten im Rahmen der passiven Produktbeobachtung

Die gemachten Differenzierungen zeigen aber, dass längst nicht alle sensorisch erhobenen Daten den Hersteller auch erreichen. Vielmehr sind unter „erhobenen“ Daten solche Daten zu verstehen, die nicht nur vom Gerät erzeugt wurden, sondern auch gespeichert und ausgelesen bzw. tatsächlich an den Hersteller übermittelt werden.

929 Vgl. *Hinrichs/Becker*, ITRB 2015, 164 (165).

930 Vgl. *Hinrichs/Becker*, ITRB 2015, 164 (165).

931 Auch zum technischen Hintergrund der Funktionsweise der Vernetzung *Schreck*, Fahrzeugdaten, S. 40.

932 Vgl. eine Untersuchung des ADAC zu der Sammlung und Übermittlung von Fahrzeugdaten, <https://www.adac.de/rund-ums-fahrzeug/ausstattung-technik-zubehoer/assistentensysteme/daten-modernes-auto/> (zuletzt abgerufen am 23.09.2024). Danach übermittelt bspw. der BMW i3 per sog. Last State Call automatisch nach jedem Ausschalten der Zündung und Absperren des Fahrzeugs einen umfangreichen Datensatz. Dieser enthält neben sicherheitsrelevanten Daten wie dem Inhalt der Fehlerspeicher und Daten der Antriebsbatterie (Ladezustand, Zelltemperaturen usw.) auch den gewählten Fahrmodus und Informationen zum Ladevorgang.

933 Vgl. *Raith*, Das vernetzte Automobil, S. 147.

Stehen dem Hersteller die Daten in diesem definierten Umfang zur Verfügung, lässt sich hinsichtlich seiner Produktbeobachtungspflicht an die herkömmliche Dogmatik anknüpfen. Die passive Produktbeobachtungspflicht umfasst im herkömmlichen Sinn die Entgegennahme und Auswertung erhaltener Kundenbeschwerden. Mit der Erweiterung der technischen Möglichkeiten hat sich aber auch die passive Produktbeobachtungspflicht zu erweitern. Der Hersteller darf sich nicht auf die Entgegennahme von Kundenbeschwerden beschränken, sondern muss auch Informationen sammeln und auswerten, die ihn auf anderem Wege erreichen.⁹³⁴ Insoweit kommt es lediglich darauf an, dass eine Information die Sphäre des Herstellers erreicht. Keinen Unterschied kann es machen, wie die Information in den Herrschaftsbereich des Herstellers gelangt. Es ist daher irrelevant, ob der Hersteller über einen Nutzer oder über Daten, die das Produkt selbst liefert, Kenntnis von einer möglichen Produktgefahr erhält. Denn der „Kenntnisstand des Herstellers gilt als produktbeobachtungsrechtliche Quelle“ auszuwertender Informationen, sodass ein Hersteller nicht einwenden kann, dass er „Daten aktiv besaß, aber passiv ungenutzt ließ“.⁹³⁵ Daher muss der Hersteller im Rahmen seiner Produktbeobachtungspflicht auch die Daten berücksichtigen, die von seinen bereits auf dem Markt befindlichen Produkten ohnehin generiert und übermittelt werden.⁹³⁶

Lässt sich ein Hersteller Daten übermitteln, haben diese regelmäßig einen wirtschaftlichen Wert für ihn und fallen daher für die Produktbeobachtung quasi als Nebenprodukt an.⁹³⁷ Vor diesem Hintergrund ist auch die Zumutbarkeit der Datenauswertung für die Produktbeobachtung zu sehen. Wo Daten bspw. zu Vertriebs- und Marketingzwecken erfasst und ausgewertet werden, müssen sie auch als Grundlage für die Produktbeobachtungspflicht herangezogen werden.⁹³⁸ Insoweit ist zu konstatieren, dass

934 Wagner, AcP 217 (2017), 707 (751); wohl auch Hartmann, PHi 2017, 42 (43).

935 Prägnant Klindt, DAR 2023, 7 (8).

936 Vgl. Hartmann, DAR 2015, 122 (124); Redeker, in: Redeker, IT-Recht, Rn. 901; Chibanguza, in: Chibanguza/Kuß/Steege (Hg.), Künstliche Intelligenz, § 5, K., Rn. 22; Hartl, in: Kühne/Nack (Hg.), Connected Cars, S. 108; Klindt, DAR 2023, 7 (8); Hartmann, PHi 2017, 42 (43); Schreck, Fahrzeugdaten, S. 227 f.; Wagner, AcP 217 (2017), 707 (751); Haagen, Verantwortung für Künstliche Intelligenz, S. 250 f.; Piovano/Schucht/Wiebe, Produktbeobachtung in der Digitalisierung, S. 110.

937 In diese Richtung Chibanguza/Schubmann, GmbHR 2019, 313 (316, 321).

938 Wende, in: Sassenberg/Faber (Hg.), Industrie 4.0 und Internet of Things, § 4, Rn. 23; Piovano/Schucht/Wiebe, Produktbeobachtung in der Digitalisierung, S. 110.

eine erhöhte Datenkenntnis auch mit einer erweiterten Verantwortung des Herstellers im Rahmen der Produktbeobachtung einhergeht.⁹³⁹

3. Pflicht zur Erhebung und Übermittlung von angefallenen Sensor-Daten

Da es aber der Hersteller selbst in der Hand hat, welche Daten anfallen, wie lange sie gespeichert werden und welche Daten tatsächlich übermittelt werden,⁹⁴⁰ stellt sich die spannendere Frage, ob der Hersteller, wenn er solche Daten schon erheben könnte, weil die technischen Voraussetzungen geschaffen sind, die Sensorik schon eingebaut ist und die Vernetzung steht, diese auch erheben und übermitteln lassen muss.⁹⁴¹

Die Vernetzung der Geräte ermöglicht es, nicht nur bestimmte – vom Hersteller als wirtschaftlich wertvoll erachtete – Daten zu übertragen, sondern sämtliche erhobenen Daten an den Hersteller zu übermitteln. Dadurch besteht die Möglichkeit, den Zustand eines in den Verkehr gebrachten Produkts fortwährend zu beobachten und das Auftreten etwaiger Fehlfunktionen in Echtzeit zu überwachen.⁹⁴² Fraglich erscheint, ob sich aus der bereits dargestellten Effektivität der Sammlung und Beobachtung dieser Sensor-Daten auch eine Pflicht des Herstellers ergibt, angefallene Daten zu erheben. Es geht damit um die Frage, ob die technologische Zugriffsmöglichkeit auf diese Daten den Hersteller auch rechtlich zum Zugriff verpflichtet – mit der Konsequenz, dass ein Datenbestand generiert wird, der nach dem oben Gesagten nicht unausgewertet bleiben darf.⁹⁴³ Ferner muss sich die Frage anschließen, ob der Hersteller auch verpflichtet sein kann, Sensorik und Schnittstellen zur Erfüllung der Produktbeobachtung speziell in sein Produkt zu integrieren.⁹⁴⁴

939 Piovano/Schucht/Wiebe, Produktbeobachtung in der Digitalisierung, S. 108.

940 Hierzu Krauß/Waidner, DuD 2015, 383 (384 f.); Mielchen, SVR 2014, 81 (82).

941 So auch Klindt, DAR 2023, 7 (8).

942 Vgl. Grünvogel/Dörrenbächer, ZVertriebsR 2019, 87 (88); Kahl/Behrendt, RAW 2020, 82 (84).

943 Diese Frage aufwerfend, i.E. aber zweifelnd Klindt, DAR 2023, 7 (8).

944 So auch Piovano/Schucht/Wiebe, Produktbeobachtung in der Digitalisierung, S. 109.

a) Weiterentwicklung der aktiven Produktbeobachtung

Auch hier stellt sich die Frage, wie eine entsprechende Verpflichtung in die bisherige Dogmatik der Produktbeobachtungspflicht einzuordnen ist. Da sich eine solche Pflicht nicht in der Entgegennahme von Informationen erschöpft, sondern die aktive Beschaffung von Daten betrifft, scheint die aktive Produktbeobachtungspflicht betroffen zu sein. Allerdings betrifft die aktive Produktbeobachtung regelmäßig das Beschaffen von bereits vorhandenen Informationen, etwa aus Fachzeitschriften. Eine Pflicht zur Erhebung von Sensor-Daten würde dagegen ein aktives Erschließen neuer, bisher nicht vorhandener Erkenntnisquellen bedeuten und über die Informationsbeschaffung aus öffentlich zugänglichen Quellen hinausgehen.⁹⁴⁵

aa) Herkömmliche Reichweite der aktiven Produktbeobachtungspflicht

Das selbständige Generieren von Informationen über das Produkt nach dem Inverkehrbringen durch den Hersteller ist jedoch nicht völlig neu und durchaus bereits Bestandteil der aktiven Produktbeobachtung.

(1) Durchführung von Stichproben

So normiert § 6 Abs. 3 S. 1 Nr. 1 ProdSG die Pflicht zur Durchführung von Stichproben. Dadurch sollen Rückschlüsse auf das Verhalten der Produkteigenschaften in verschiedenen Lebensphasen ermöglicht werden und Erkenntnisse geliefert werden, wie sich das Produkt aufgrund unterschiedlicher Einflüsse außerhalb der Sphäre des Herstellers verändert.⁹⁴⁶ Die konkrete Ausgestaltung der Durchführung (Art, Umfang, Häufigkeit, etc.) ist gem. § 6 Abs. 3 S. 2 ProdSG von dem Produktrisiko und der Möglichkeit zur Risikovermeidung abhängig.

Vor diesem Hintergrund wird in der Literatur vertreten, dass Stichproben der Produktbeobachtung nachgelagert seien.⁹⁴⁷ Zwar wird die Stichprobenentnahme selbst auch als Teil der Produktbeobachtung gesehen,

945 Klindt, DAR 2023, 7 (8); vgl. auch Schmid, IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme, S. 206.

946 Vgl. Wagner/Ruttloff/Miederhoff, CCZ 2020, 1 (4 f.); Kapoor, in: Klindt, ProdSG, § 6, Rn. 59.

947 So Wilrich, ProdSG, Rn. 444.

allerdings könne diese ohne eine vorherige Beobachtung der Produkte im Feld nicht sinnvoll durchgeführt werden. Begründet wird dies damit, dass die Gebotenheit der Durchführung von Stichproben erst durch die Beobachtung der Produkte im Feld beurteilt werden könne.⁹⁴⁸ So verstanden stellte sich die Stichprobenentnahme allerdings lediglich als Reaktion auf einen anderweitig durch die Produktbeobachtung gewonnenen Gefahrenverdacht dar und diene der weiteren Abklärung dieses Verdachts. Es erschließt sich allerdings nicht, warum die Bewertung der Gebotenheit der Stichprobenentnahme nicht abstrakt an der Produktgattung bzw. an dem vor Herstellungsbeginn prognostiziertem Risiko⁹⁴⁹ festgemacht werden kann.⁹⁵⁰ Würde man die Pflicht zur Durchführung von Stichproben erst nach vorherigen sicherheitsrelevanten Erkenntnissen aus der Produktbeobachtung bejahen, ließe man die Chance verstreichen, durch Stichproben selbst (erste) Erkenntnisse zu gewinnen. Freilich kann eine Stichprobe auch einen vorherigen aufgrund einer Beschwerde ausgelösten Verdacht erhärten. Als solche Maßnahme begriffen, stellte sich die Stichprobenentnahme allerdings schon als Reaktion im Sinne weiterer Aufklärung auf eine erkannte Gefahr dar. Reaktionspflichten sind aber vom ProdSG nicht vorgesehen.⁹⁵¹ Damit ist die Pflicht zur Durchführung von Stichproben als Maßnahme zu sehen, die unabhängig von einem Gefahrenverdacht und damit anlasslos auch selbst Auskünfte über die Bewährung der Produkte im Feld liefern soll.⁹⁵²

Diese öffentlich-rechtliche Pflicht zur Durchführung von Stichproben ist als Mindeststandard auch Teil des zivilrechtlichen Pflichtenprogramms des Herstellers im Rahmen der aktiven Produktbeobachtung.⁹⁵³ Vor dem Hintergrund, dass das öffentliche Recht lediglich Mindeststandards festlegt⁹⁵⁴ und die Pflicht zur Durchführung von Stichproben auch im zivilrechtlichen Pflichtenprogramm des Herstellers verankert ist, ändert sich hieran auch dadurch nichts, dass die neue GPSR keine Stichprobenpflicht mehr

948 Vgl. *Hofmann*, Öffentlich-rechtlich statuierte Produktbeobachtungspflichten, S. 175 f.

949 So *Kapoor*, in: Klindt, ProdSG, § 6, Rn. 58.

950 Hiervon geht auch *Schucht*, PHi 2023, 126 (130) aus.

951 Ausführlich unter E.III.4.a).

952 *Schucht*, PHi 2023, 126 (130).

953 *Ackermann*, in: NK-ProdR, § 823 BGB, Rn. 124; *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 153; *Schucht*, PHi 2023, 148 (155 f.); *Wilhelmi*, in: Erman, BGB, § 823, Rn. 119 „eigene laufende Überwachung durch Produkttests“.

954 Vgl. allgemein *Wagner*, in: MüKo, BGB, § 823, Rn. 1077; konkret in Bezug auf die Produktbeobachtung *Schucht*, PHi 2023, 148 (155).

vorsieht.⁹⁵⁵ Nach Art. 10 Abs. 6 i.V.m. Anhang I Abschnitt 2 Abs. 3 CRA wird dem Hersteller dagegen aufgegeben, sicherzustellen, dass die Sicherheit des Produkts im Hinblick auf Schwachstellen regelmäßig und wirksam getestet und überprüft wird.

(2) Generierung neuer wissenschaftlicher Erkenntnisse

Jedoch sind bereits vor dem Inverkehrbringen eines Produkts die eigenen Forschungspflichten eines Herstellers zur Generierung neuen Gefahrenwissens eingeschränkt. Dieser kann sich grundsätzlich auf den bestehenden Stand der Wissenschaft und Technik verlassen. Anders ist dies nur dann, wenn dem Hersteller aufgrund der Komplexität oder dem abstrakten Gefahrenpotential eine vertiefte Risikoforschung zugemutet werden kann.⁹⁵⁶ Eine Sonderrolle in diesem Zusammenhang nehmen Neuentwicklungen ein.⁹⁵⁷ Aufgrund des zwangsläufig begrenzten allgemein verfügbaren Erkenntniswissens kann hier nicht von einem gesicherten Stand von Wissenschaft und Technik gesprochen werden, auf den der Hersteller zurückgreifen kann. Die von Neuentwicklungen ausgehenden Risiken stehen noch kaum fest und Standards haben sich noch nicht abgezeichnet. Diese Tatsachen spitzen sich zu, wenn der Hersteller mit seiner Innovation (zunächst) in einer Wettbewerbsnische agiert und den Stand von Wissenschaft und Technik allein und selbst bestimmt. Im Interesse eines möglichst umfassenden Schutzes vor Produktgefahren ist hier aktive Forschung durch den

955 Ausführlich insoweit zum Gesetzgebungsprozess *Schucht*, PHi 2023, 148 (155).

956 Vgl. *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), *Produkthaftungshandbuch*, § 24, Rn. 21; auch *Ackermann*, in: *NK-ProdR*, § 823 BGB, Rn. 69 welcher angibt, dass der Hersteller sein Produkt als ungefährlich bezeichnen kann, wenn die zuständigen Fachleute es für unbedenklich halten; *Wagner*, in: *MüKo*, BGB, § 823, Rn. 1081 spricht allgemein davon, dass sich die Anstrengungen für die Erforschung und Entwicklung von Sicherheitstechnologien danach bestimmen, was ein vernünftiger Beobachter in der Lage des Herstellers getan und aufgewandt hätte. Dabei soll der Innovationsgrad, die drohende Schadenshöhe und die Eintrittswahrscheinlichkeit maßgebend sein; dezidiert a.A. *Graf v. Westphalen*, ZIP 1992, 18 (22 f.): „Er kann und darf dann sich nicht darauf verlassen, daß ihm die einschlägige Wissenschaft schon die erforderlichen Daten liefert. Vielmehr obliegt ihm eine eigene Prüfpflicht als typische Vorpflicht, die dem Inverkehrbringen des Produkts vorausgeht.“ Nachfolgend wird dies auf Produkte, die geeignet sind, Gefahren für Leib, Leben und Gesundheit zu verursachen, (marginal) eingeschränkt.

957 *Röthel*, in: *Eifert/Hoffmann-Riem* (Hg.), *Innovationsverantwortung*, S. 335 (340) „umso höhere Anforderungen, je neuartiger“.

Hersteller zu betreiben.⁹⁵⁸ Die gerade gezeichnete Pflicht, eine wirksame Gefahrensteuerung durch die Entwicklung von Wissenschaft und Technik voranzutreiben, endet aber grundsätzlich mit dem Inverkehrbringen des Produkts.⁹⁵⁹ Denn zu diesem Zäsurzeitpunkt hat das Produkt dem maßgeblichen Stand von Wissenschaft und Technik zu entsprechen.

Allerdings hat die Rechtsprechung über die Durchführung von Stichproben hinaus gerade bei Neuentwicklungen eine Verpflichtung des Herstellers angenommen, auch nach der Inverkehrgabe mögliche Gefahren und neue wissenschaftliche Erkenntnisse über das Produkt zu erforschen.⁹⁶⁰ Mit Erforschung ist in diesem Kontext die eigenständige Weiterentwicklung des Standes von Wissenschaft und Technik gemeint. Es geht folglich um die Frage der anlasslosen Durchführung eigener Laborprüfungen bzw. Testverfahren mit der als Teil der aktiven Produktbeobachtung neue wissenschaftliche Erkenntnisse über das Produkt nach dem Inverkehrbringen im Wege der Forschung generiert werden sollen. Diese Pflicht bzgl. der eigenen Forschungsanstrengungen geht damit weit über die Durchführung von Stichproben hinaus, welche lediglich den aktuellen Status quo des Produktes im Feld erfassen sollen. Nicht zu verwechseln ist diese Forschungspflicht mit Fällen, in denen der Hersteller aufgrund seiner durchgeführten Produktbeobachtung bereits Hinweise auf eine möglicherweise sicherheitskritische Eigenschaft seiner Produkte im Feld hat und er diesem Verdacht nun mittels eigener Prüfverfahren nachgeht.⁹⁶¹ Diese Frage betrifft bereits die Reaktion auf eine (wenn auch im Verdachtsstadium) erkannte Gefahr.

Nach dem Inverkehrbringen müssen sicherheitstechnische Entwicklungen zwar weiter beachtet werden, grundsätzlich aber nicht selbst zu Tage gefördert werden. Die Verantwortung des Herstellers wird aber überstrapaziert, wenn aufwendige Untersuchungs- und Testverfahren ohne Anhaltspunkte für das Vorliegen einer vom Produkt ausgehenden Gefahr gefordert werden; dies gilt insbesondere dann, wenn man dies nur an der generellen Geeignetheit des Produkts, Leib, Leben und Gesundheit zu

958 Vgl. hierzu *Plagemann/Tietzsch*, „Stand der Wissenschaft“ und „Stand der Technik“, S. 23; i.E. auch *Wagner*, in: MüKo, BGB, § 823, Rn. 1081.

959 *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), *Produkthaftungshandbuch*, § 24, Rn. 311.

960 BGH, NJW 1992, 560 (562).

961 Dies wird leider allzu oft vermengt, vgl. *Helte*, *Anforderungen an die Produktsicherheit*, S. 90; ebenso *Meyer*, *VersR* 2010, 869 (872). Nur eine Differenzierung erlaubt es aber, zu sachgerechten Ergebnissen zu kommen, da die Anknüpfungstatsachen (anlasslos vs. Gefahrenverdacht) andere sind.

gefährden, festmacht, da diese bei Lichte betrachtet nahezu jedem Produkt zumindest potenziell anhaftet.⁹⁶² Es ist daher nicht verwunderlich, dass der BGH einem Hersteller von zuckerhaltigen Teeprodukten für Säuglinge eine eigenständige Prüfpflicht dahingehend aufgibt, zahnmedizinisch noch nicht bekannte Risiken des sog. Dauernuckelns zu erkennen, gleichzeitig aber zu Erwägungen der Erforderlichkeit und Zumutbarkeit einer solchen Forschungspflicht schweigt.⁹⁶³ Auch unter Berücksichtigung der besonders schutzwürdigen Personengruppe und der Tatsache, dass der Hersteller das Produkt als wohltuenden Gute-Nacht-Trunk bewarb und damit eine Sicherheit suggerierte, kann eine Forschungspflicht des Herstellers nicht erforderlich und zumutbar sein.⁹⁶⁴ Einem Lebensmittelhersteller bei einem Produkt wie einem Kindertee die labormäßige Überprüfung von noch nicht einmal in der Zahnmedizin diskutierten Risiken aufzugeben, bringt die Gefährlichkeit des Produkts und den Sicherheitsaufwand in kein angemessenes Verhältnis.⁹⁶⁵

Dass eine solche Abwägung gleichwohl anders ausfallen kann, zeigen Neuentwicklungen. Aufgrund des nicht gesicherten Stands von Wissenschaft und Technik ist hier schon vor Inverkehrgabe aktive Forschung durch den Hersteller zu betreiben (s.o.). Diese Pflicht setzt sich grundsätzlich auch nach dem Inverkehrbringen fort.⁹⁶⁶ Grund hierfür ist, dass sich

962 i.E. auch Voigt, in: BeckOGK, BGB, § 823, Rn. 675; Röthel, in: Eifert/Hoffmann-Riem (Hg.), Innovationsverantwortung, S. 335 (341) stellt bzgl. der anlasslosen Erforschung daher nur auf die Rezeption des den gesamten Forschungs- und Erfahrungsbestands ab, nicht aber auf eigene Untersuchungspflichten.

963 BGH, NJW 1992, 560 (562).

964 A.A. wohl Helte, Anforderungen an die Produktsicherheit, S. 102, der davon spricht, dass das durch die besondere Eigenschaftszusicherung begründete Vertrauen der Nutzer nicht durch unzulängliche technische Möglichkeiten relativiert werden könne. Allerdings stellt er auch darauf ab, dass ein Hersteller, der weiß, dass er sein Sicherheitsversprechen nicht halten kann, davon Abstand nehmen müsse. Ob zur Überwindung von Nichtwissen ohne Anhaltspunkte eigene Forschung zu betreiben ist, bleibt damit aber offen.

965 Ebenso kritisch Klindt, NJW 2017, 3087 (3088); anders Graf v. Westphalen, ZIP 1992, 18 (23); unklar Meyer, VersR 2010, 869 (872). Dieser spricht als Konsequenz der Kindertee I Entscheidung von einer eigenständigen Prüfpflicht bzgl. Produktgefahren, die das Produkt für die Anwendergruppe auslösen könnte, verweist dann aber auf einen Verdachtsgrad bzw. ein nicht zu vernachlässigendes Anfangsindiz für mögliche Schädigungen, ab dem die Erforschungspflichten erst bestehen.

966 Eichelberger, in: Ebers et al., (Hg.), Künstliche Intelligenz und Robotik, S. 186; Wagner, in: MüKo, BGB, § 823, Rn. 1110 spricht allgemein von besonders intensiver Produktbeobachtung; OLG Karlsruhe, VersR 1978, 550; mit Fokus auf eigene Prüfpflichten LG Münster, NJW-RR 1986, 947 (952 f.): Insbesondere bei neuartigen Pro-

bei Neuentwicklungen häufiger Entwicklungsfehler zeigen als bei bloßen Produktweiterentwicklungen.⁹⁶⁷ Wenn man so will, haftet Innovationen stets ein diffuser Gefahrenverdacht an,⁹⁶⁸ welcher im Rahmen der Zumutbarkeit aufgrund der abstrakt höheren Eintrittswahrscheinlichkeit von Schäden den Ausschlag für eine eigene Prüfpflicht geben kann. Gleiches hat bei einem Produkt von hoher Komplexität oder abstraktem Gefahrenpotential zu gelten.

bb) Bedeutung für die Erhebung von Sensor-Daten

An diese Erkenntnisse lässt sich auch hinsichtlich der in Rede stehenden Erhebung von Sensor-Daten anknüpfen. Auch wenn sich eine solche Datenerhebung als ein ständiges Erheben von Stichproben begreifen lässt,⁹⁶⁹ ist freilich zu konstatieren, dass die kontinuierliche Erhebung von Sensor-Daten eine ganz andere Qualität als eine periodische Stichprobenkontrolle hat. Indes zeigt gerade die von der Rechtsprechung vorgenommene Weiterentwicklung der aktiven Produktbeobachtungspflicht insbesondere bei Neuentwicklungen, dass an die Gefährdungslage angepasste Anforderungen an die Produktbeobachtung gestellt werden und diese nicht starr zu verstehen ist. Betrachtet man die bei smarten Produkten ausgemachten Unsicherheiten nach Inverkehrgabe, lässt sich durchaus eine Parallele zum diffusen Gefahrenverdacht bei Neuentwicklungen ziehen, bei denen eigene Prüfpflichten nach dem Inverkehrbringen anerkannt wurden. Ähnlich wie Neukonstruktionen kann auch smarten Produkten eine generell erhöhte Gefährlichkeit zugeschrieben werden, welche eine erweiterte Produktbeobachtung rechtfertigt. Eine an die nunmehr vorhandenen Möglichkeiten der Sensor-Datenerhebung vorgenommene Weiterentwicklung der Produktbeobachtungspflicht ließe sich somit in die bestehende Dogmatik der Produktbeobachtungspflicht einordnen.

Gleichwohl muss konstatiert werden, dass eine derart lückenlose Überwachung im Wege der Erhebung von Sensor-Daten zu einer Revolution

duktionsverfahren handelt ein Hersteller geradezu leichtfertig, wenn er sich ohne gezielte Überprüfungen darauf verlässt, dass Gefahren nicht auftreten, weil bislang Arbeiten hierzu in der wissenschaftlichen Literatur nicht veröffentlicht worden sind. Es ist geboten den Prozess zu beobachten und geeignete Messungen durchzuführen.

967 Helte, Anforderungen an die Produktsicherheit, S. 90.

968 Ohne dies so klar zu benennen OLG Karlsruhe, VersR 1978, 550.

969 In diese Richtung auch *Schucht*, PHi 2023, 148 (156).

in der aktiven Produktbeobachtung führt. Denn bisher war diese lediglich als mittelbare Marktbeobachtung ausgestaltet, betraf aber nicht die unmittelbare Beobachtung der jeweiligen Produktexemplare.⁹⁷⁰ Ein anlassloses und engmaschiges Überprüfen eines einzelnen Produkts auf dem Markt konnte nämlich technisch in zumutbarem Maße bisher gar nicht geleistet werden.⁹⁷¹ In Anbetracht der technischen Möglichkeiten und der damit einhergehenden Weiterentwicklung des Standes von Wissenschaft und Technik, an welchem die Produktbeobachtungspflicht als Verkehrspflicht auszurichten ist, lässt sich aber auch eine Weiterentwicklung der aktiven Produktbeobachtungspflicht hin zu einer „aktivistischen“ Produktbeobachtung annehmen.⁹⁷² Die damit einhergehende Veränderung des Charakters der Produktbeobachtungspflicht ist lediglich eine Folge des technischen Fortschritts. Führen technische Möglichkeiten dazu, dass Hersteller nach dem Inverkehrbringen ein umfassenderes Bild ihrer Produkte erhalten, als dies durch Stichproben und Prüfpflichten möglich ist, darf dieses Potential nicht ungenutzt bleiben.⁹⁷³

b) Allgemeine Erwägungen der Zumutbarkeit

Einer gesonderten Betrachtung bedarf dagegen das Kriterium der Zumutbarkeit. Hier stellt sich schon allgemein und noch losgelöst von der individuellen Produktgattung die Frage, ob sich dieses aufgrund der Leichtigkeit, mit welcher Daten von den Produkten erlangt werden können und vor dem Hintergrund leistungsfähiger Analyseverfahren, die auch große Datenmengen sichten und bewerten können, zu Lasten der Hersteller verschiebt.⁹⁷⁴

970 Schmid, IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme, S. 206; Schmid, CR 2019, 141 (142); Schreck, Fahrzeugdaten, S. 227 weist darauf hin, dass sich Sensor-Daten stets auf das konkrete Gerät beziehen und daher viel präziser sind als abstrakte Fachliteratur.

971 So Chibanguza/Schubmann, GmbHR 2019, 313 (315); vgl. auch Grützmacher, CR 2021, 433 (435).

972 I.E. auch Chibanguza, in: Buck-Heeb/Oppermann (Hg.), Automatisierte Systeme, S. 407 (412).

973 Eine Pflicht zur Auswertung von Sensor-Daten wird in der Literatur häufig pauschal angenommen, vgl. nur Droste, CCZ 2015, 105 (110); Thöne, Autonome Systeme, S. 212; Piltz/Reusch, BB 2017, 841 (841); Gomille, JZ 2016, 76 (80).

974 Dazu Klindt, DAR 2023, 7 (8); Chibanguza/Schubmann, GmbHR 2019, 313 (315 f.); v. Bodungen/Hoffmann, NZV 2016, 503 (506); Chibanguza, in: Chibanguza/Kuß/Steeger (Hg.), Künstliche Intelligenz, § 5, K., Rn. 22; Chibanguza, in: Buck-Heeb/Op-

aa) Übergang zum Äquivalenzinteresse

Es wird angeführt, dass sich eine allgemeine Unzumutbarkeit einer solchen Produktbeobachtungspflicht daraus ergeben könne, dass die Grenze zwischen Produkthaftung und Sachmangelrecht verwische. Denn faktisch würden die gewonnenen Daten nicht lediglich zu Zwecken der deliktsrechtlich gebotenen Gefahrenabwehr genutzt, sondern vielmehr auch zur Implementierung eines Verschleiß-Frühwarnsystems, welches dann allein das vertragliche Äquivalenzinteresse betreffe.⁹⁷⁵ Dieses Argument gegen die Zumutbarkeit der Erhebung von Sensor-Daten kann indes schon im Ansatz nicht verfangen. Denn es besteht freilich keine Verpflichtung, die Daten für andere Zwecke als die Produktbeobachtung zu verwenden. Möchte der Hersteller den Nutzern die gewonnenen Daten gleichwohl aufbereitet zur Verfügung stellen, steht es ihm frei, dies als zusätzliche Serviceleistung (und ggfs. gegen Entgelt) anzubieten. Der mit dieser anderweitigen Nutzung der Daten anfallende zusätzliche Aufwand ist dann aber nicht mehr Folge der Produktbeobachtungspflicht, sondern der freien wirtschaftlichen Entscheidung des Unternehmers.

bb) Endlose Flut theoretisch verfügbarer Daten

Dagegen muss im Rahmen der Zumutbarkeit Berücksichtigung finden, dass sich die Hersteller mit einer nahezu endlosen Flut theoretisch verfügbarer Daten konfrontiert sehen. Zwar sollte die Speicherung dieser Daten keine Probleme bereiten. Denn während die Rechenleistungen und Speicherkapazitäten der Geräte selbst begrenzt sind, sodass umfassende Protokollspeicher in den Geräten an ihre Grenzen stoßen können,⁹⁷⁶ verfügen die Backendserver der Hersteller über die entsprechenden Kapazitäten.⁹⁷⁷ Vergewagt man sich allerdings, dass beim autonomen Fahren künftig

permann (Hg.), *Automatisierte Systeme*, S. 407 (411); Droste, CCZ 2015, 105 (110); Thöne, *Autonome Systeme*, S. 212.

975 Zu dieser Argumentation, wenn auch i.E. ablehnend, Grünvogel/Dörrenbächer, ZVertriebsR 2019, 87 (89).

976 Reichwald/Pfisterer, CR 2016, 208 (211); Grützmaker, CR 2016, 695 (697).

977 Vgl. Chibanguza, in: Buck-Heeb/Oppermann (Hg.), *Automatisierte Systeme*, S. 407 (412).

von einem Fahrzeug etwa 4 Terabyte Daten am Tag verarbeitet werden,⁹⁷⁸ sind insbesondere bei der Übermittlung und Auswertung der Daten gewisse Umsetzungsprobleme zu erwarten.⁹⁷⁹

Nicht vergessen werden darf an diesem Punkt allerdings, dass es für die Produktbeobachtung allein auf die Erhebung von sicherheitstechnisch relevanten Daten ankommt. Nicht aus allen Daten, die von einem IoT-Gerät verarbeitet werden, lassen sich Rückschlüsse auf sicherheitskritische Eigenschaften ziehen. Aber auch bei alleiniger Betrachtung der sicherheitsrelevanten Daten darf nicht übersehen werden, dass der Hersteller auch mit den erweiterten technischen Möglichkeiten im Rahmen der Produktbeobachtung weder in der Lage noch verpflichtet ist, eine absolute Sicherheit zu gewährleisten oder jede Produktgefahr zu erkennen. Eine umfassende und permanente Erfassung aller anfallenden Daten würde daher selbst für Zwecke der Produktbeobachtung zu weit gehen.⁹⁸⁰ Allein aus der technischen Möglichkeit zur Übermittlung von Daten folgt daher nicht, dass der theoretisch mögliche Erkenntnisgewinn aus allen anfallenden Daten zur Grundlage der Produktbeobachtungspflicht gemacht werden muss.⁹⁸¹

Es wird daher angeführt, dass eine Pflicht zur Datenerhebung lediglich dann anzunehmen sei, wenn ein ganz konkreter Anlass bestünde und der Hersteller die Daten temporär benötige, um eine konkrete Gefahrenursache zu ermitteln.⁹⁸² Damit wird aber schon die Reaktion auf eine im Verdachtsstadium erkannte Gefahr angesprochen. Eine Beschränkung der aktiven Erfassung von Sensor-Daten auf diese Phase würde jedoch lediglich das Potential nutzen, bereits aus anderen Quellen der Produktbeobachtung gewonnene Informationen zu verifizieren. Das „aktivistische“ Potential, nämlich die Informationen aus den Sensor-Daten zu nutzen, um eigene Erkenntnisse zu gewinnen und damit Produktfehler möglichst vor der Schadensverursachung zu erkennen, bliebe gänzlich ungenutzt. Daher

978 Vgl. die Aussage des ehemaligen CEO von Intel, Brian Krzanich, unter <https://download.intel.com/newsroom/2021/archive/2016-11-15-editorials-krzanich-the-future-of-automated-driving.pdf> (zuletzt abgerufen am 23.09.2024).

979 *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 152; *Wende*, in: Sassenberg/Faber (Hg.), *Industrie 4.0 und Internet of Things*, § 4, Rn. 23.

980 So auch *Raith*, *Das vernetzte Automobil*, S. 152; *Hartl*, in: Kühne/Nack (Hg.), *Connected Cars*, S. 108.

981 *Wende*, in: Sassenberg/Faber (Hg.), *Industrie 4.0 und Internet of Things*, § 4, Rn. 23; *Xylander*, *Die Verantwortlichkeit des Herstellers automatisierter PKW*, S. 152; zurückhaltend auch *Haagen*, *Verantwortung für Künstliche Intelligenz*, S. 273.

982 So *Hartl*, in: Kühne/Nack (Hg.), *Connected Cars*, S. 108; wohl auch *Piovanolo/Schucht/Wiebe*, *Produktbeobachtung in der Digitalisierung*, S. 110.

kann dieser Ansicht jedenfalls in ihrer Pauschalität unabhängig vom Gefährdungspotential des Produkts nicht zugestimmt werden. Vielmehr sind pragmatische Lösungen zu finden, um die anfallenden Daten in zumutbarer Weise für die Produktbeobachtung nutzbar zu machen.

cc) Stichprobenerhebung sicherheitsrelevanter Daten

Eine Möglichkeit zur Erfüllung der erweiterten Produktbeobachtungspflicht könnte die stichprobenartige Erhebung sicherheitsrelevanter Daten sein.⁹⁸³ Dabei kann die stichprobenartige Überwachung sowohl in zeitlicher Hinsicht als auch in Bezug auf die Anzahl der überwachten Produkte abgestuft und nach einem individuell für die Produktgattung zu bestimmendem Muster erfolgen. Bei einer ausreichenden Anzahl an Produkten auf dem Markt kann sich aufgrund der daraus resultierenden Menge an Daten ein recht detailliertes Bild von der Bewährung der Produkte im Feld ergeben.⁹⁸⁴

dd) Integrierte Produktbeobachtung

Aussagekräftiger ist freilich die Datenerhebung bei jedem einzelnen Produkt. Vor diesem Hintergrund wird der selbständigen Systemfehleranalyse entscheidende Bedeutung zukommen.⁹⁸⁵ Letztlich handelt es sich dabei um eine Weiterentwicklung der insbesondere aus der Automobilbranche bekannten Fehlerspeicher. Bereits aktuell können sich Systeme selbst überwachen, indem Abweichungen des Ist- vom definierten Soll-Zustand erfasst werden und so Systemfehlerereignisse und sonstige atypische Systemzustände automatisch erkannt werden.⁹⁸⁶ Allerdings ist zu berücksichtigen, dass sich diese automatische Überwachung des Systemzustandes darin erschöpft, vorher festgelegte Werte und deren Beziehungen auf Grenzwertüberschreitungen und Anomalien zu prüfen. Fehlermeldungen sind daher lediglich in dem vorher definierten Umfang zu erwarten. Das Ausbleiben einer Fehlermeldung kann daher eine trügerische Sicherheit suggerieren,

983 Hierfür plädiert *Raith*, Das vernetzte Automobil, S. 152; ähnlich *Haagen*, Verantwortung für Künstliche Intelligenz, S. 274.

984 So *Raith*, Das vernetzte Automobil, S. 152.

985 *Voigt*, in: BeckOGK, BGB, § 823, Rn. 780.

986 Vgl. *Schmid*, CR 2019, 141 (143).

die möglicherweise gar nicht vorhanden ist, da neue, nicht antizipierte Fehlerbilder nicht erkannt werden.

Die sich im Zuge der Vernetzung bietende Neuerung liegt nun darin, dass die Zustandsmeldungen nicht mehr lediglich intern gespeichert und erst bei einer nächsten Inspektion ausgelesen werden, sondern unmittelbar an den Hersteller übermittelt werden können.⁹⁸⁷ Damit ist die Datenauswertung nicht mehr nur Geräten vorbehalten, die regelmäßigen Wartungszyklen unterliegen, sondern kann bei sämtlichen IoT-Produkten erfolgen. Modellcharakter können in diesem Zusammenhang die bereits bekannten Fehlermeldungen bei Softwareprogrammen haben, wenn etwa bei einer ungeplanten Beendigung des Programms gefragt wird, ob die Fehlfunktion samt Metadaten an den Hersteller übermittelt werden soll.⁹⁸⁸ Eine Echtzeitübermittlung dieser Daten zum Zwecke der Produktbeobachtung ist aber regelmäßig nicht erforderlich. Ausreichend erscheint eine Übermittlung der angefallenen Daten an den Hersteller bei nächster Gelegenheit, d.h. insbesondere bei Verfügbarkeit einer entsprechenden Datenübertragungsrate. Da eine solche Selbstüberwachung in die Systeme implementiert werden muss, hat sich hierfür der Terminus der „integrierten Produktbeobachtung“ etabliert.⁹⁸⁹

ee) Zwischenfazit

Die vorstehenden Ausführungen haben gezeigt, dass eine Pflicht zur Erhebung und Übermittlung von angefallenen Sensor-Daten im Allgemeinen geeignet, aufgrund der latenten Produktgefahren und ausgemachten Unsicherheiten nach Inverkehrgabe auch erforderlich und unter Berücksichtigung individueller Ausgestaltungsmöglichkeiten zumutbar ist, um die Produktbeobachtungspflicht zu erfüllen. Gegenstand der Produktbeobachtungspflicht bilden damit auch Daten, die zwar nicht zu anderen Zwecken

987 Vgl. *Günther*, Roboter und rechtliche Verantwortung, S. 159 f.

988 *Schrader*, DAR 2018, 314 (317). Ob eine solche Mitwirkung des Nutzers erforderlich ist oder die Daten auch unabhängig davon automatisch an den Hersteller übermittelt werden können, stellt eine Frage des Datenschutzrechts dar und wird sogleich behandelt.

989 Geprägt wurde die Begrifflichkeit von *Schmid*, IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme, S. 205; *Wende*, in: Sassenberg/Faber (Hg.), Industrie 4.0 und Internet of Things, § 4, Rn. 23 spricht von „Produktgedächtnis“.

gesammelt und ausgewertet werden, aber ohne Weiteres – aufgrund der entsprechenden Konnektivität – erhoben werden können.

c) Individuelle Erwägungen der Zumutbarkeit

Die konkrete Ausgestaltung hängt dann maßgeblich von der individuellen Gefährlichkeit des Produkts sowie dem individuell zu betreibenden Aufwand ab. Zur Bestimmung der individuellen Gefährlichkeit eines smarten Produkts als maßgebliche Kenngröße der Erforderlichkeit und Zumutbarkeit ist zunächst dessen herkömmliche Gefährlichkeit losgelöst von seiner Digitalisierung und damit seiner smarten Funktionen zu betrachten. Hierbei kommt es eben auf die Eintrittswahrscheinlichkeit eines Schadens, bestimmt durch die Gefahreneigtheit des Produkts und die Schadenshöhe an. Sodann ist bei dieser Betrachtung einzustellen, dass schon die allgemein erhöhte Gefahreneigtheit smarter Produkte aufgrund der bestehenden Unsicherheiten nach dem Inverkehrbringen zu einer erhöhten Eintrittswahrscheinlichkeit von Schädigungen führt, die zu der individuellen und produktspezifischen Gefahreneigtheit tritt. Neben dieser so ermittelten Gefährlichkeit muss der Tatsache Rechnung getragen werden, dass bei CPS der Einsatzbereich, also deren Mobilität und der Grad der Strukturiertheit der Umgebung sowie deren Lernfähigkeit, weitere gewichtige Einflussfaktoren zur Beurteilung des Schadenspotentials darstellen.⁹⁹⁰ Speziell im Rahmen der Zumutbarkeit ist noch zu berücksichtigen, dass diese auch von der Unternehmensgröße beeinflusst wird.⁹⁹¹

Betrachtet man die integrierte Produktbeobachtung, so ist Voraussetzung dafür, dass der Hersteller Mechanismen vorsieht, die es einem System ermöglichen, sich kontinuierlich selbst zu beobachten, Systemfehler automatisch zu erkennen und diese dem Hersteller zu melden.⁹⁹² Der für die Frage der Zumutbarkeit allein ausschlaggebende Mehraufwand, also der Aufwand, der zur Umsetzung der konkreten Verkehrssicherungspflicht nicht

990 Vgl. Zech, DJT 2020 Gutachten, A S.29; mit graphischer Darstellung Lohmann, AJP/PJA 2017, 152 (153 f.).

991 Gomille, JZ 2016, 76 (80); Piovano/Schucht/Wiebe, Produktbeobachtung in der Digitalisierung, S. 72; Mayrhofer, Außervertragliche Haftung für fremde Autonomie, S. 308 f.; in diese Richtung schon BGH, NJW 1981, 1606 (1608); rechtsfortbildend weitergehend Sommer, Haftung für autonome Systeme, S. 237 ff.

992 Schmid, IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme, S. 181; Xylander, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 152.

ohnehin aufgrund technischer Erfordernisse oder anderweitig rechtlicher Pflichten notwendig ist, kann dabei als gering beurteilt werden.⁹⁹³ Dies gilt jedenfalls, wenn die anfallenden Daten aus Gründen der Funktionalität ohnehin verarbeitet werden. Dann stellt die Implementierung der integrierten Produktbeobachtung lediglich ein „Add-on“ bereits bestehender Prozesse dar.⁹⁹⁴ Zurückhaltung ist dagegen angezeigt, wenn es darum geht, eine solche Sensorik allein zu Zwecken der nachfolgenden Produktbeobachtung zu verbauen.⁹⁹⁵ Mit Blick darauf, dass bereits im Rahmen der Konstruktion in kostenaufwendige Technik zur Erhebung und Auswertung der Daten investiert werden müsste, würde dadurch die unternehmerische Freiheit der Hersteller stark eingeschränkt.⁹⁹⁶ Freilich hängt dies auch davon ab, um welches Produkt es sich konkret handelt und welche Gefahren von diesem ausgehen können.

Weiter ist zu konstatieren, dass gerade unter Softwareherstellern viele kleinere Unternehmen oder Start-ups am Markt sind, deren Wirtschaftskraft z.B. nicht mit Herstellern aus der Automobilindustrie vergleichbar ist.⁹⁹⁷ Dies betrifft insbesondere die Möglichkeit, über entsprechende Backendserver eine umfassende Speicherung und Analyse der übermittelten Daten zu betreiben. Sofern es hier die Gefahrengeneigntheit und der Einsatzbereich des Produkts zulassen, ist eine lediglich stichprobenartige Erhebung sicherheitsrelevanter Daten gerechtfertigt.⁹⁹⁸

d) Beispiel Automotiv-Sektor und selbstlernende KI-Systeme

Bleibt man beispielhaft beim Automotive-Sektor und dem autonomen Fahren, gestaltet sich zwar die Einschätzung der Eintrittswahrscheinlichkeit mangels qualifizierter Unfallstatistiken als äußerst schwierig.⁹⁹⁹ Allerdings kann sowohl die Schadenshöhe aufgrund der potenziellen Verletzungen

993 Vgl. Schmid, CR 2019, 141 (145).

994 So ausdrücklich Schmid, IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme, S. 223.

995 So auch Piovano/Schucht/Wiebe, Produktbeobachtung in der Digitalisierung, S. 72, 110.

996 So auch Piovano/Schucht/Wiebe, Produktbeobachtung in der Digitalisierung, S. 73.

997 Dazu Schmid, IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme, S. 223.

998 Ähnlich Chibanguza, in: Buck-Heeb/Oppermann (Hg.), Automatisierte Systeme, S. 407 (411), der für weniger sensible und hochwertige Rechtsgüter die Möglichkeit zur Selbstdiagnose nicht verlangt.

von Leib und Leben und der regelmäßigen hohen Intensität dieser Verletzungen als auch die Mobilität und Komplexität der Umgebung sowie die Lernfähigkeit als sehr hoch beurteilt werden. Vor diesem Hintergrund wird hier die Implementierung einer integrierten Produktbeobachtung in jedem Fall zu fordern sein.¹⁰⁰⁰ So sieht Nr. 7.2.2.4 lit. b UN-Regelung Nr. 155 bereits jetzt vor, dass das vom Hersteller zu betreibende Cybersecurity-Managementsystems („CSMS“) in der Lage sein muss, Cyberbedrohungen, Schwachstellen und Cyberangriffe anhand von Fahrzeugdaten und Fahrzeugprotokollen zu analysieren und zu erkennen. Für den Bereich der Cybersicherheit ist die Implementierung der integrierten Produktbeobachtung damit schon normativ verankert.¹⁰⁰¹

Bei Systemen, die nach dem Inverkehrbringen weiter aus ihrer Umgebung lernen und bei denen der Lernfortschritt ohne vorherige Verifikation durch den Hersteller automatisch umgesetzt werden soll, kann eine integrierte Produktbeobachtung dazu führen, dass die Risiko-Nutzen-Abwägung, die das Inverkehrbringen überhaupt erst erlaubt, positiv ausfällt.¹⁰⁰² Da Fehlentwicklungen im Lernen bei jedem Einsatz denkbar sind, wird auch der zeitlichen Ausgestaltung der Zustandsmeldungen eine entscheidende Bedeutung zukommen und werden diese mehrmals täglich zu for-

999 Zu diesem Problem auch *Schmid*, IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme, S. 215.

1000 So auch *Chibanguza*, in: Buck-Heeb/Oppermann (Hg.), *Automatisierte Systeme*, S. 407 (411), der die Implementierung auch im sensiblen Bereich der Medizinprodukte für denkbar hält. Denkt man an einen Herzschrittmacher kommt dieser zwar in einer strukturierten Umgebung und ohne sonderliche Lernfähigkeit zum Einsatz. Allerdings ist ein Versagen des Produkts regelmäßig mit einem letalen Ausgang verbunden. Vor dem Hintergrund der Schadenshöhe verdient die Ansicht daher Zustimmung.

1001 Vgl. *Kahl/Behrendt*, RAW 2020, 82 (84); zur technischen Ausgestaltung *Simo/Waidner/Gemmin*, in: Roßnagel/Hornung (Hg.), *Grundrechtsschutz im Smart Car*, S. 311 (314) und *Wurm*, *Automotive Cybersecurity*, S. 77.

1002 Vgl. auch *Eichelberger*, in: Ebers et al., (Hg.), *Künstliche Intelligenz und Robotik*, S. 186; Die Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) plädiert in diesem Zusammenhang als Verkehrsfähigkeitsvoraussetzung für die Implementierung eines Produktbegleitkonzepts. Dieses soll sowohl das Sammeln von Informationen im Betrieb des Produkts und deren Auswertung als auch das Ergreifen von Maßnahmen umfassen. In Abgrenzung zur herkömmlichen Produktbeobachtung wurde jedoch der Begriff der „Produktbegleitung“ gewählt, vgl. BAuA, *Rechtliche Rahmenbedingungen für die Bereitstellung autonomer und KI-Systeme*, 2021, S. 189 ff.

dern sein.¹⁰⁰³ Hinzu kommt, dass das Defizit ausgeglichen werden muss, dass Zustandsmeldungen nur vorab definierte Fehlerbilder abgleichen können. Mit einer zusätzlich stichprobenartigen Kontrolle sämtlicher sicherheitsrelevanten Daten können von den Fehlermeldungen nicht erfasste Auffälligkeiten erkannt werden. In diesem Zusammenhang sieht Art. 12 Abs. 1 KI-VO vor, dass Hochrisiko-KI-Systeme so konzipiert und entwickelt sein müssen, dass eine automatische Aufzeichnung von Vorgängen und Ereignissen („Protokollierung“) während des Betriebs der Hochrisiko-KI-Systeme möglich ist. Dadurch soll insbesondere die Beobachtung nach dem Inverkehrbringen erleichtert werden (vgl. Art. 12 Abs. 2 lit. b KI-VO). Zwar sieht Art. 12 Abs. 3 KI-VO nur die Protokollierung bestimmter Daten als Mindestanforderung vor, gleichwohl ergibt sich auch hier eine normative Anknüpfung der integrierten Produktbeobachtung. Um den engen Zusammenhang zwischen den Produktsicherheitsvorschriften und den Haftungsvorschriften zu stärken, sieht Art. 10 Abs. 2 lit. b ProdHaftRL vor, dass von der Fehlerhaftigkeit eines Produkts ausgegangen wird, dass verbindliche Anforderungen des Produktsicherheitsrechts, die einen Schutz gegen das Risiko des der geschädigten Person entstandenen Schadens bieten sollen, nicht eingehalten wurden. Ausweislich Erwägungsgrund (46) ProdHaftRL schließt dies Fälle mit ein, in denen ein Produkt nicht mit einer Vorrichtung ausgestattet ist, mit der Informationen über die Verwendung des Produkts gemäß dem Unionsrecht oder dem nationalen Recht aufgezeichnet werden können. Das Fehlen vorgeschriebener Dokumentations- bzw. Aufzeichnungsvorrichtungen führt damit produkthaftungsrechtlich zu einer Vermutung der Fehlerhaftigkeit des Produkts.¹⁰⁰⁴

4. Beweislastverteilung unter Berücksichtigung des Data Acts

Im Rahmen der Produzentenhaftung nach § 823 Abs. 1 BGB muss der Geschädigte beweisrechtlich lediglich nachweisen, dass das Produkt zum Zeitpunkt des Inverkehrbringens fehlerhaft und für die eingetretene Rechts-

1003 So für autonome Fahrzeuge *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 152 f.; für intelligente Medizinprodukte *Droste*, MPR 2018, 109 (111); allgemein auch *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 73 und *Gauger/Hartmannsberger*, NJW 2014, 1137 (1140); *Spindler*, in *Hornung/Schallbruch* (Hg.), IT-Sicherheitsrecht, § 11, Rn. 31 „laufende Produktbeobachtungspflicht“.

1004 Vgl. auch *Spindler*, CR 2022, 689 (698).

gutsverletzung kausal war. Der objektive Verstoß gegen die Verkehrssicherungspflicht und das Verschulden des Herstellers werden dann vermutet.¹⁰⁰⁵ Dem liegt die Erwägung zugrunde, dass Vorgänge, die sich im Betrieb des Herstellers abspielen, dem Beweis einer Sorgfaltspflichtverletzung durch den Geschädigten kaum zugänglich sind. Vielmehr ist der Hersteller „näher daran“, den Sachverhalt aufzuklären, da er die Produktionssphäre und den Herstellungsprozess überblickt.¹⁰⁰⁶ Die Produktbeobachtungspflicht wurde jedoch von der Beweislastumkehr ausgenommen, da es sich bei den Erkenntnissen und Erfahrungen mit dem Produkt in der Regel um Informationen handele, die nicht nur dem Bereich des Herstellers, sondern allgemein und damit auch dem Nutzer zugänglich seien.¹⁰⁰⁷ In der Tat ist die Begründung für den Ausschluss der Beweislastumkehr bei der Produktbeobachtungspflicht nicht überzeugend, wenn die Informationen ausschließlich auf die Erkenntnisquellen des Herstellers beschränkt sind und dem Nutzer nicht zugänglich sind und daher verschlossen bleiben.¹⁰⁰⁸

Indes sieht der am 11.01.2024 in Kraft getretenen und ab 12.09.2025 geltende Data Act¹⁰⁰⁹ in Art. 3 Abs. 1 vor, dass vernetzte Produkte so konzipiert und hergestellt werden müssen, dass Produktdaten und relevante Metadaten standardmäßig für den Nutzer einfach, sicher, unentgeltlich in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format zugänglich sein müssen. Insoweit wird herstellerseitig ein Datenzugang by design zu berücksichtigen sein. Für diese Verpflichtung ist allerdings in Art. 50 Data Act eine Übergangsfrist vorgesehen, sodass sie erst ab dem 12.9.2026 gilt. Daneben regelt Art. 4 Abs. 1 Data Act, dass soweit der Nutzer nicht direkt vom vernetzten Produkt auf die Daten zugreifen kann, die Dateninhaber die ohne Weiteres verfügbaren Daten unverzüglich, einfach, sicher, unentgeltlich, in einem umfassenden, gängigen und maschinenlesbaren Format und kontinuierlich und in Echtzeit bereitzustellen haben. Dies hat auf einfaches Verlangen auf elektronischem Wege zu geschehen. Insoweit erhält der Nutzer ab Geltungsbeginn des Data Acts einen Zugangsanspruch zu den generierten Daten. Mangels abweichender Regelung steht den Nutzern das Datenzugangsrecht auch bezüglich vor dem Geltungsbe-

1005 Grundlegend BGH, NJW 1969, 269 (274).

1006 BGH, NJW 1969, 269 (274 f.).

1007 BGH, NJW 1981, 1603 (1605).

1008 Schrader, in: Buck-Heeb/Oppermann (Hg.), *Automatisierte Systeme*, S. 333 (360).

1009 Verordnung (EU) 2023/2854.

ginn erworbener Produkte zu.¹⁰¹⁰ Jedenfalls mit Geltungsbeginn des Data Acts fehlt es den Nutzern damit in Bezug auf die erhobenen Sensor-Daten nicht an einer entsprechenden Einsichtsmöglichkeit, sodass eine Neuordnung der Beweislastverteilung im Rahmen der Produktbeobachtungspflicht nicht erforderlich ist.

Daneben sieht künftig die neue Produkthaftungsrichtlinie in Art. 9 Abs. 1 ProdHaftRL vor, dass die Mitgliedsstaaten sicherzustellen haben, dass die nationalen Gerichte auf Antrag der geschädigten Person anordnen können, dass der Hersteller in seiner Verfügungsgewalt befindliche relevante Beweismittel offenlegen muss. Hierunter ließen sich dann auch Erkenntnisse aus den angefallenen Sensor-Daten zum Zwecke der Produktbeobachtung subsumieren.¹⁰¹¹ Auch durch diese Offenlegung kann einer beweisrechtlich schlechteren Ausgangslage des Geschädigten begegnet werden.

V. Aspekte des Datenschutzes

Sowohl das Social-Media-Monitoring als auch die Erhebung und Auswertung von Sensor-Daten können datenschutzrechtliche Implikationen aufweisen und zu Überschneidungen zwischen den Anforderungen der Produktbeobachtung und den datenschutzrechtlichen Beschränkungen führen.¹⁰¹² Neben der Erforderlichkeit und Zumutbarkeit kann die Produktbeobachtung damit auch durch (datenschutz-)rechtliche Rahmenbedingungen begrenzt sein.¹⁰¹³ So birgt die Erfassung von Sensor-Daten zum Zwecke der Produktbeobachtung aufgrund des fehlenden Einblicks in die tatsächlich generierten und erfassten Daten sowie die fehlende Kontrolle über den Datenfluss das Risiko, dass die Nutzer weniger selbstbestimmt und stetig mit dem Blick auf die Folgen ihrer Gerätenutzung handeln könnten.¹⁰¹⁴

1010 Etzkorn, RDi 2024, 116 (123).

1011 So auch Kapoor/Sedlmaier, RAW 2023, 8 (13).

1012 Reusch, in: Kaulartz/Braegelman (Hg.), Artificial Intelligence und Machine Learning, S. 143; Piltz/Reusch, BB 2017, 841 (841).

1013 Chibanguza, in: Buck-Heeb/Oppermann (Hg.), Automatisierte Systeme, S. 407 (414).

1014 Hartl, in: Kühne/Nack (Hg.), Connected Cars, S. 85.

1. Anwendbarkeit des Datenschutzrechts – Personenbezug

Die Anwendbarkeit des Datenschutzrechts setzt nach § 2 Abs. 1 DS-GVO voraus, dass personenbezogene Daten verarbeitet werden (vgl. auch § 1 Abs. 1 DS-GVO). Nach § 4 Nr. 1 DS-GVO sind darunter Informationen zu verstehen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Fraglich ist damit, ob es sich bei den zum Zwecke der Produktbeobachtung erhobenen sicherheitsrelevanten Daten auch um personenbezogene Daten handelt. Zum einen dürfte es sich dann um keine reinen Sachdaten handeln („auf eine natürliche Person beziehen“), zum anderen müsste die Information auch einer konkreten natürlichen Person zugeordnet werden können („identifizierte oder identifizierbare natürliche Person“).¹⁰¹⁵

a) Abgrenzung zum reinen Sachdatum

Da es sich bei den anfallenden Sensor-Daten jedenfalls im Ausgangspunkt um technische Daten handelt,¹⁰¹⁶ ist zunächst eine Abgrenzung zum reinen Sachdatum vorzunehmen. Ein solches sagt nichts über eine natürliche Person aus und unterfällt daher nicht dem Anwendungsbereich des Datenschutzrechts.¹⁰¹⁷ Enthalten die technischen Daten damit völlig unabhängig vom individuellen Nutzungsverhalten oder den Eigenschaften des Nutzers lediglich Informationen über den Zustand einer Sache, so sind sie dadurch rein technischer Natur. Sie sind dann als anonym zu betrachten und weisen keinen Personenbezug auf.

Im Kontext der Produktbeobachtung wären hier physikalische Werte wie die ermittelte Außentemperatur oder das Einspritzverhalten eines Motors zu nennen.¹⁰¹⁸ Werden technische Zustandsdaten nicht vom individuellen Nutzungsverhalten beeinflusst, besteht keine Gefahr, dass die Daten auch

1015 Zu diesem „Prüfschema“ *Hartl*, in: Kühne/Nack (Hg.), *Connected Cars*, S. 87; vgl. allgemein zur Differenzierung *Klar/Kühling*, in: Kühling/Buchner (Hg.), *DS-GVO*, Art. 4, Rn. 11 und *Arning/Rothkegel*, in: Taeger/Gabel (Hg.), *DSGVO*, Art. 4, Rn. 10.

1016 *Forgó*, in: Oppermann/Stender-Vorwachs (Hg.), *Autonomes Fahren*, 2. Aufl., S. 353 (357); *Buchner*, *DuD* 2015, 372 (373).

1017 *Mantz/Spittka*, in: Sassenberg/Faber (Hg.), *Industrie 4.0 und Internet of Things*, § 6, Rn. 17.

1018 *Hartl*, in: Kühne/Nack (Hg.), *Connected Cars*, S. 89; *Eul*, in: Leupold/Wiebe/Glossner (Hg.), *IT-Recht*, Teil 10.2, Rn. 29.

zur Beurteilung des Verhaltens der Person herangezogen werden können oder sich deren Verwendung auf die Rechte und Interessen einer bestimmten Person auswirken.¹⁰¹⁹ Auch wenn die Auswertung dieser Daten konkret personenbezogene Folgen haben kann, indem ein Hersteller bspw. ein Produkt zurückruft, ändert dies nichts daran, dass sich das bloße Datum an sich nicht auf einen Nutzer bezieht.¹⁰²⁰ Wenn technische Daten aber auch Rückschlüsse auf den Nutzer zulassen, wie bspw. der Bremsenverschleiß auf das individuelle Fahrverhalten, sind die Daten nicht mehr rein sach-, sondern personenbezogen.¹⁰²¹ Gerade solche Rückschlüsse werden aber bei von IoT-Geräten produzierten Daten der Regelfall sein.¹⁰²²

b) Bestimmbarkeit einer natürlichen Person

Kann eine Information entsprechend generell mit einer natürlichen Person in Verbindung gebracht werden, ist in einem zweiten Schritt zu fragen, ob auch wirklich eine konkrete Person hinter der Information identifiziert werden kann. Hierfür muss eine Information für sich genommen aber noch nicht direkt auf eine bestimmte natürliche Person bezogen werden können. Es ist ausreichend, wenn eine solche Zuordnung aufgrund der Verknüpfung mit weiteren Informationen möglich ist.¹⁰²³ Zu untersuchen ist damit, ob sich anhand der technischen Daten unter Hinzunahme weiterer Identifikatoren eine spezifische Person bestimmen lässt.¹⁰²⁴

1019 Dazu *Rücker/Dienst*, in: Bräutigam/Kraul (Hg.), *Internet of Things*, § 6, Rn. 154 ff.

1020 Hierauf weisen *Daute/Sütthoff*, *EuZW* 2023, 500 (504) hin.

1021 *Weisser/Färber*, *MMR* 2015, 506 (508); *Buchner*, *DuD* 2015, 372 (373); *Hartl*, in: Kühne/Nack (Hg.), *Connected Cars*, S. 89; *Forgó*, in: *Oppermann/Stender-Vorwachs* (Hg.), *Autonomes Fahren*, 2. Aufl., S. 353 (357); *Weichert*, *NZV* 2017, 507 (510); zu den allgemeinen Abgrenzungskriterien Art.-29-Datenschutzgruppe, Stellungnahme 4/2007, WP 136, S. 10 ff. und EuGH, *NJW* 2018, 767 (768).

1022 *Arning/Rothkegel*, in: Taeger/Gabel (Hg.), *DSGVO*, Art. 4, Rn. 14; *Klar/Kühling*, in: Kühling/Buchner (Hg.), *DS-GVO*, Art. 4, Rn. 14.

1023 Vgl. *Klar/Kühling*, in: Kühling/Buchner (Hg.), *DS-GVO*, Art. 4, Rn. 19.

1024 Vgl. auch *Hartl*, in: Kühne/Nack (Hg.), *Connected Cars*, S. 87; *Eul*, in: Leupold/Wiebe/Glossner (Hg.), *IT-Recht*, Teil 10.2, Rn. 29.

aa) Identifikatoren

Selbst wenn die Datenauswertung der Hersteller für die Produktbeobachtung nicht dezidiert personenbezogen, sondern mit Blick auf das Erfahrungswissen über die Produkte im Feld gerätebezogen erfolgt, kommt es darauf an, ob diese Informationen personenbezogene Daten enthalten.¹⁰²⁵ Hierbei ist zu berücksichtigen, dass die Hersteller bei der Erhebung der technischen Daten für die Produktbeobachtung regelmäßig auch eindeutige, dauerhaft mit dem Gerät bzw. der SIM-Karte verbundene Kennungen (bspw. IMEI, UDID, IMSI, MAC-Adresse)¹⁰²⁶ erheben,¹⁰²⁷ um die Daten strukturiert auswerten und mit anderen Erkenntnissen zusammenführen zu können. Denn der bloße technische Wert an sich wird regelmäßig nicht zu einem geeigneten Erkenntnisgewinn im Rahmen der Produktbeobachtung führen, sondern bedarf der Zuordnung zu einem bestimmten Produkt. Diese Individualisierung des Produkts ist auch angezeigt, um in einem weiteren Schritt individuelle und zielgerichtete Gefahrenabwehrmaßnahmen ergreifen zu können.¹⁰²⁸

Eine solche Kennung stellt isoliert betrachtet aber auch kein personenbezogenes Datum dar, da sie lediglich die Identifizierung eines einzelnen Produkts ermöglicht, aber allein noch keine eindeutige Zuordnung zu einer natürlichen Person zulässt.¹⁰²⁹ Haben sich die Nutzer allerdings vor der Verwendung des Produkts registriert oder ein Benutzerkonto angelegt, lassen sich die erhobenen technischen Daten samt Kennung aus der Verknüpfung mit den hinterlegten Stammdaten einer konkreten Person zuordnen, woraus sich der Personenbezug ohne Weiteres ergibt.¹⁰³⁰ Gleiches gilt, wenn

1025 Vgl. *Roßnagel*, ZD 2013, 562 (565).

1026 Vgl. Düsseldorf Kreis, Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter, Stand 16.06.2014, S. 5.

1027 Vgl. bereits Erwägungsgrund (30) DS-GVO. Werden Fahrzeugdaten erhoben, erfolgt dies stets in Kombination mit der Fahrzeug-Identifizierungsnummer (FIN), welche aus dem Welt-Hersteller-Code, der Baureihe und dem Motortyp sowie einer fortlaufenden Nummer besteht und daher eine eindeutige Identifizierung eines bestimmten Fahrzeugs ermöglicht, vgl. dazu *Raith*, Das vernetzte Automobil, S. 100 f. und *Kahl*, RAW 2019, 70 (71).

1028 Vgl. *Hartmann*, DAR 2015, 122 (125); *Hartmann*, PHi 2017, 42 (45); *Raith*, Das vernetzte Automobil, S. 150.

1029 So EuGH, MMR 2016, 842 (843) in Bezug auf dynamische IP-Adressen; verallgemeinernd *Moos/Rothkegel*, MMR 2016, 842 (846).

1030 *Hartl*, in: Kühne/Nack (Hg.), Connected Cars, S. 88; *Steege/Stender-Vorwachs*, in: Chibanguza/Kuß/Steege (Hg.), Künstliche Intelligenz, § 3, K., Rn. 11; *Eul*, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 10.2, Rn. 30.

die Kennung in den Kaufvertrag aufgenommen wurde und dieser mit den Käuferdaten an den Hersteller übermittelt wurde.¹⁰³¹

bb) Berücksichtigung von Zusatzwissen

Aber auch wenn der Hersteller selbst nicht über dieses Zusatzwissen der Stammdaten verfügt, kann die Kombination aus der Kennung und den technischen Daten für einen Personenbezug ausreichen. Dies ist dann der Fall, wenn das Zusatzwissen der Stammdaten bei einem Dritten vorhanden ist und dem Hersteller als verarbeitender Stelle Mittel zur Verfügung stehen, die vernünftigerweise genutzt werden, um das entsprechende Zusatzwissen von dem Dritten zu erlangen.¹⁰³² Entsprechende Mittel stellen insbesondere rechtliche Auskunftsansprüche direkt gegenüber dem Dritten dar.¹⁰³³ Ferner ist es ausreichend, wenn die verarbeitende Stelle das Zusatzwissen über eine zwischengeschaltete Behörde erlangen kann, etwa wenn die verarbeitende Stelle selbst nicht, wohl aber eine zuständige Behörde über einen Auskunftsanspruch verfügt und die Behörde zur Geltendmachung des Auskunftsanspruchs veranlasst werden kann.¹⁰³⁴ Nach Erwägungsgrund (26) DS-GVO ist allerdings der zur Identifizierung erforderliche Aufwand einschränkend zu beachten und sind lediglich solche Mittel zu berücksichtigen, die nach allgemeinem Ermessen wahrscheinlich genutzt werden. Hinsichtlich der erhobenen technischen Daten von IoT-Geräten samt Kennung ist damit anhand des Bestehens rechtlicher Auskunftsansprüche und des tatsächlich erforderlichen Aufwands der Identifizierung zu prüfen, ob diese Daten einer konkreten natürlichen Person zugeordnet werden können.¹⁰³⁵

Die gerade dargelegten Grundsätze hat der EuGH hinsichtlich dynamischer IP-Adressen entwickelt, bei denen lediglich der Access-Provider den Namen des Surfenden kennt. Da die verarbeitende Stelle jedoch durch die Angabe der IP-Adresse über eine Strafanzeige gegen einen mutmaßlichen Täter ein staatsanwaltschaftliches Verfahren in Gang setzen bzw. bei drohendem Schaden die zuständige Behörde zur Gefahrenabwehr einschalten kann und hierüber die entsprechende Auskunft erhalten kann, verfügt sie

1031 Hartl, in: Kühne/Nack (Hg.), *Connected Cars*, S. 87.

1032 EuGH, MMR 2016, 842 (843); EuGH, GRUR-RS 2023, 30962 (Rn. 45).

1033 EuGH, MMR 2016, 842 (843).

1034 EuGH, MMR 2016, 842 (843); instruktiv Moos/Rothkegel, MMR 2016, 842 (846).

1035 So Mantz/Spittka, in: Sassenberg/Faber (Hg.), *Industrie 4.0 und Internet of Things*, § 6, Rn. 18.

über ein rechtliches Mittel zur Bestimmung der Person.¹⁰³⁶ Bezieht man diese Rechtsprechung auf zum Zwecke der Produktbeobachtung erhobene Daten, ist es nach allgemeinem Ermessen auch „wahrscheinlich“ i.S.d. Erwägungsgrunds (26) DS-GVO, dass sich ein Hersteller des Wissens und der Mittel staatlicher Stellen zur Informationserlangung bedient, um etwa bei einer erkannten Produktgefahr effektive Gefahrengegenmaßnahmen ergreifen zu können.¹⁰³⁷ Damit handelt es sich bei erhobenen technischen Daten samt IP-Adresse um personenbezogene Daten.

Auch bei von vernetzten Fahrzeugen erhobenen Daten handelt es sich regelmäßig um personenbezogene Daten. Zwar stellt die miterhobene Fahrzeug-Identifizierungsnummer (FIN) als alphanumerischer Code, den der Hersteller einem Fahrzeug zu dem Zweck zuweist, dass es einwandfrei identifiziert werden kann, für sich genommen kein personenbezogenes Datum dar. Gleichwohl wird sie für denjenigen, der bei vernünftiger Betrachtung über Mittel verfügt, die es ermöglichen, sie einer bestimmten Person zuzuordnen, zu einem personenbezogenen Datum.¹⁰³⁸ Da die FIN gem. § 59 Abs. 1 Nr. 4 StVZO an allen Kfz anzubringen ist und gem. § 33 Abs. 1 Nr. 1 StVG im Zentralen Fahrzeugregister zu speichern ist, ermöglicht diese über den Auskunftsanspruch gegenüber der Zulassungsbehörde oder des Kraftfahrt-Bundesamts nach § 39 Abs. 1 StVG nicht nur die Identifizierung des Kfz, sondern auch des Halters.¹⁰³⁹

Bei anderen Gerätekennungen wie Smartphone-IDs, Smart-TV-IDs oder MAC-Adressen wird dem Hersteller dagegen regelmäßig schon mangels entsprechender Zuordnungstabellen kein rechtliches Mittel zu den Identifikationsdaten des Nutzers offenstehen, sodass der Personenbezug hier regelmäßig abzulehnen sein wird.¹⁰⁴⁰ Anders sieht dies freilich dort aus,

1036 EuGH, MMR 2016, 842 (843); BGH, NJW 2017, 2416 (2418).

1037 Auf den Streit, ob die Tatbestandsvoraussetzungen von etwaigen Auskunftsansprüchen tatsächlich vorliegen müssen oder nicht, was etwa dann nicht der Fall wäre, wenn Informationen zu Zwecken erhoben werden, die eine Einschaltung der zuständigen Behörden nicht nach sich ziehen können (z.B. reine Nutzungsanalysezwecke), kommt es damit nicht an, vgl. dazu *Arning/Rothkegel*, in: *Taeger/Gabel* (Hg.), DSGVO, Art. 4, Rn. 37 f. m.w.N.; *Moos/Rothkegel*, MMR 2016, 842 (846); *Klar/Kühling*, in: *Kühling/Buchner* (Hg.), DS-GVO, Art. 4, Rn. 30.

1038 EuGH, GRUR-RS 2023, 30962 (Rn. 46).

1039 Hierzu *Weichert*, NZV 2017, 507 (509); *Raith*, Das vernetzte Automobil, S. 107; *Eul*, in: *Leupold/Wiebe/Glossner* (Hg.), IT-Recht, Teil 10.2, Rn. 30; vom EuGH, GRUR-RS 2023, 30962 (Rn. 49), der Prüfung durch das vorliegende Gericht überlassen.

1040 So *Moos/Rothkegel*, MMR 2016, 842 (846); *Mantz/Spittka*, in: *Sassenberg/Faber* (Hg.), Industrie 4.0 und Internet of Things, § 6, Rn. 18.

wo verschiedene Stellen solche Kennungen einer Person zuordnen.¹⁰⁴¹ Hier kann möglicherweise über den Umweg einer Behörde das Zusatzwissen erlangt werden.

cc) Auswirkungen von Big Data

Fraglich ist allerdings, ob nicht auch personenbezogene Daten vorliegen können, wenn entsprechende Zuordnungstabellen fehlen, keine Auskunftrechte bestehen oder die technischen Daten gänzlich ohne Kennung erhoben wurden. Ein Personenbezug könnte sich vor dem Hintergrund von Big Data ergeben.¹⁰⁴² Kennzeichnend für Big Data ist die schnelle Analyse einer großen Menge unstrukturierter Daten aus unterschiedlichsten Datenquellen, wobei Zusammenhänge automatisiert erkannt werden.¹⁰⁴³ Aufgrund der großen Menge an vorhandenen Daten und der Kombination einzelner Daten kann sich aus deren Verkettung regelmäßig ein Personenbezug ergeben.¹⁰⁴⁴ Entscheidend dabei ist, ob in der Fülle der Daten ausreichende Merkmale vorhanden sind, um den Betroffenen zu individualisieren.¹⁰⁴⁵ Dies ist dann der Fall, wenn in der Datenfülle eine einzigartige Kombination an Informationen vorliegt, die eine eindeutige Zuordnung zu einer natürlichen Person ermöglicht.¹⁰⁴⁶

Führt der Hersteller unterschiedliche Informationen zusammen, um ein ausführliches Bild über die Bewährung des Produkts im Feld zu erlangen, wird automatisch nach entsprechenden Zusammenhängen gesucht. Je detaillierter dann aber ein solches Profil ist, desto wahrscheinlicher ist es, dass über die Verkettung von Informationen auch der letzte Schritt der Zuordnung des Profils zu einer konkreten Person möglich wird.¹⁰⁴⁷

1041 In diese Richtung Düsseldorf Kreis, Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter, Stand 16.06.2014, S. 5; undifferenziert dagegen *Piltz/Reusch*, BB 2017, 841 (841).

1042 *Bräutigam/Klindt*, NJW 2015, 1137 (1140); *Rücker/Dienst*, in: *Bräutigam/Kraul* (Hg.), *Internet of Things*, § 6, Rn. 170.

1043 *Schefzig*, DSRITB 2014, 103 (109).

1044 Vgl. nur *Steege/Stender-Vorwachs*, in: *Chibanguza/Kuß/Steege* (Hg.), *Künstliche Intelligenz*, § 3, K., Rn. 9; *Schefzig*, DSRITB 2014, 103 (109); *Krügel/Pfeiffenbring*, in: *Ebers et al.*, (Hg.), *Künstliche Intelligenz und Robotik*, S. 417; v. *Bodungen*, in: *Specht/Mantz* (Hg.), *Handbuch Datenschutzrecht*, § 16, Rn. 6.

1045 *Roßnagel*, ZD 2013, 562 (563).

1046 *Schefzig*, DSRITB 2014, 103 (111).

1047 So *Mantz/Spittka*, in: *Sassenberg/Faber* (Hg.), *Industrie 4.0 und Internet of Things*, § 6, Rn. 18.

Big Data macht auch eine Anonymisierung der Daten, welche zwar die grundsätzliche Anwendbarkeit des Datenschutzes nach Anfall der Daten ausschließen könnte (vgl. Erwägungsgrund (26) DS-GVO), zunehmend schwieriger. Denn selbst wenn Daten in Aggregation aufgelöst werden, indem Merkmale durch Gruppenbildung generalisiert werden, scheint es im Rahmen von Big Data immer noch möglich, die anonymisierten Daten einer Person zuzuordnen zu können.¹⁰⁴⁸ Darüber hinaus kann eine Anonymisierung im Rahmen der Produktbeobachtung gerade vor dem Hintergrund der sich anschließenden und möglichst individuell und zielgerichtet zu gestaltenden Gefahrenabwehrmaßnahmen wenig zweckdienlich sein.¹⁰⁴⁹

c) Fazit

Auch wenn stets eine einzelfallabhängige Betrachtung vorzunehmen ist, lässt sich festhalten, dass bei der Datenerhebung zum Zwecke der Produktbeobachtung im IoT-Kontext gerade auch vor dem Hintergrund von Big Data regelmäßig ein Personenbezug vorliegen kann.

Auch beim Social-Media-Monitoring wird regelmäßig ein Personenbezug der erhobenen Daten vorliegen. Dieser ergibt sich, sobald Beiträge der Nutzer samt deren Namen erfasst werden. Dies muss jedenfalls dann gelten, wenn die Nutzer auf der Social-Media-Plattform mit ihrem Klarnamen auftreten.¹⁰⁵⁰ Für die Betroffenen kann ein umfassendes Social-Media-Monitoring das Risiko bergen, dass durch die Verarbeitung ihrer Daten neue Kontexte und Bedeutungen entstehen, die ihnen vorher nicht bewusst waren und die daher ihren Interessen zuwiderlaufen. Eine solche Zweckänderung hat das Potential, die informationelle Selbstbestimmung, die Kontrollmöglichkeiten und das Vertrauen in das digitale Umfeld zu beeinträchtigen.

1048 Vgl. *Buchner*, DuD 2015, 372 (374); *Roßnagel*, ZD 2013, 562 (565 f.); *Forgó*, in: *Oppermann/Stender-Vorwachs* (Hg.), *Autonomes Fahren*, 2. Aufl., S. 353 (358 f.).

1049 Vgl. auch *May/Gaden*, InTer 2018, 110 (115); a.A. wohl *Raith*, *Das vernetzte Automobil*, S. 153 und *Droste*, CCZ 2015, 105 (110), welche darauf hinweisen, dass zur Gefahrenanalyse Daten über das IoT-Gerät selbst ausreichen. Auch für eine Warnung sei die Verbindung zum Produkt ausreichend. Gleiches dürfte auch für aufgespielte Updates gelten. Diese „anonymen“ Gefahrenabwehrmaßnahmen können aber an ihre Grenzen stoßen. Dies schon dann, wenn es an einem Display am Produkt für eine entsprechende Kommunikation fehlt oder die Produktgefahr eine weitere Kommunikation mit dem Nutzer erforderlich macht.

1050 *Solmecke/Wahlers*, ZD 2012, 550 (552).

Zudem kann ein Gefühl der Überwachung entstehen, das Menschen davon abhalten kann, sich im Internet frei zu äußern.¹⁰⁵¹

2. Rechtmäßigkeit der Datenverarbeitung

Wurde in einem ersten Schritt die Anwendbarkeit des Datenschutzrechts aufgrund der Verarbeitung von personenbezogenen Daten festgestellt, muss in einem zweiten Schritt untersucht werden, ob eine solche Verarbeitung rechtmäßig ist. Nach dem im Datenschutzrecht geltenden Verbotsprinzip ist dies nur dann der Fall, wenn die Verarbeitung durch einen Erlaubnistatbestand ausdrücklich gerechtfertigt ist (vgl. Art. 6 Abs. 1 DS-GVO, Art. 8 Abs. 2 S. 1 GRCh).

a) Einwilligung

Zuvorderst sei hier an die Einwilligung in die Verarbeitung der personenbezogenen Daten nach Art. 6 Abs. 1 lit. a DS-GVO gedacht. Auch wenn eine solche Lösung den Datenschutzinteressen der Betroffenen am besten Rechnung trägt, ist sie doch mit praktischen Unwägbarkeiten verbunden. So kann die Einwilligung regelmäßig nicht bei Abschluss des Kaufvertrages miteingeholt werden kann, da der Hersteller, welcher die Daten später verarbeitet, nur in den seltensten Fällen Vertragspartner ist und es daher am Kontakt zwischen datenschutzrechtlich Verantwortlichem und Betroffenen fehlt.¹⁰⁵² Sofern das jeweilige Produkt über ein Display verfügt, erscheint eine Information und Einwilligung hierüber zwar denkbar, jedoch gehen auch hiermit praktische Probleme einher.¹⁰⁵³ Zum einen werden IoT-Produkte häufig nicht nur von einer, sondern von mehreren Personen genutzt,

1051 Zum Ganzen *Gilga*, ZD-Aktuell 2020, 07022 in Bezug auf eine Stellungnahme des Europäischen Datenschutzbeauftragten zu einer Praxis des Social-Media-Monitoring des Europäischen Unterstützungsbüros für Asylfragen.

1052 *Forgó*, in: Oppermann/Stender-Vorwachs (Hg.), *Autonomes Fahren*, 2. Aufl., S. 353 (361).

1053 Vgl. *Piltz/Reusch*, BB 2017, 841 (842 f.); Die Einwilligung als Willensbekundung kann in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung vorgenommen werden (Art. 4 Nr. 11 DS-GVO; anders sah § 4a Abs. 1 S. 3 BDSG a.F. noch die Schriftform vor).

sodass grundsätzlich jede dieser Personen einwilligen müsste.¹⁰⁵⁴ Denn die Einwilligung rechtfertigt einen Grundrechtseingriff und kann daher nur vom Betroffenen erteilt werden.¹⁰⁵⁵ Zum anderen setzt die Einwilligung eine vorangegangene Informiertheit voraus, zu welchem Zweck welche Daten verwendet werden (vgl. Art. 4 Nr. 11 DS-GVO). Diese Transparenz über ein – wenn überhaupt vorhandenes – kleines Display am Produkt herzustellen erscheint kaum möglich.¹⁰⁵⁶

Da die Einwilligung aber überhaupt zunächst einmal erteilt werden muss und sodann auch jederzeit widerrufen werden kann (vgl. Art. 7 Abs. 3 S. 1 DS-GVO), ist sie für den Hersteller mit Unsicherheiten verbunden.¹⁰⁵⁷ Auch wenn die Rechtmäßigkeit der bisherigen Verarbeitung nach Art. 7 Abs. 3 S. 2 DS-GVO von einem Widerruf unberührt bleibt, sind sämtliche personenbezogenen Daten, die ausschließlich auf der Einwilligung des Betroffenen beruhen, nach deren Widerruf zu löschen.¹⁰⁵⁸ Damit läuft aber die Angewiesenheit auf die Mitwirkung des Nutzers der Effektivität der Produktbeobachtung zuwider.¹⁰⁵⁹ Denn die Produktbeobachtung dient nicht nur der Sicherheit des Produktnutzers, sondern auch den durch das Produkt gefährdeten Dritten.¹⁰⁶⁰

b) Erfüllung eines Vertrags

Weiter wird mehrheitlich darauf hingewiesen, dass eine Datenerhebung zur Erfüllung der Produktbeobachtungspflicht nicht im Hinblick auf den abgeschlossenen (Kauf)Vertrag i.S.d. Art. 6 Abs. 1 lit. b DS-GVO erfolge, da diese lediglich der Einhaltung deliktsrechtlicher Sorgfaltspflichten diene.¹⁰⁶¹ Berücksichtigt man jedoch, dass Art. 6 Abs. 1 lit. b DS-GVO neben

1054 Als Frage auch von Schmid, CR 2019, 141 (146) aufgeworfen; Daute/Sütthoff, EuZW 2023, 500 (505) halten es bei lebensnaher Betrachtung für zweifelhaft, dass jeder Nutzer ein eigenes Konto anlegt und nicht das eines anderen nutzt.

1055 Lüdemann, ZD 2015, 247 (252); Eul, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 10.2, Rn. 35.

1056 Steege/Stender-Vorwachs, in: Chibanguza/Kuß/Steege (Hg.), Künstliche Intelligenz, § 3, K., Rn. 63.

1057 So auch Forgó, in: Oppermann/Stender-Vorwachs (Hg.), Autonomes Fahren, 2. Aufl., S. 353 (362).

1058 Steege/Stender-Vorwachs, in: Chibanguza/Kuß/Steege (Hg.), Künstliche Intelligenz, § 3, K., Rn. 60.

1059 Piltz/Reusch, BB 2017, 841 (843).

1060 Hierauf weist zu Recht Schmid, CR 2019, 141 (146) hin.

der Erfüllung des geschuldeten Leistungserfolgs auch Nebenpflichten, insbesondere auch nachvertragliche Rücksichtnahme- und Schutzpflichten umfasst,¹⁰⁶² könnte eine andere Beurteilung angezeigt sein. Zwar handelt es sich bei der Produktbeobachtungspflicht in erster Linie um eine deliktsrechtliche Verkehrspflicht, allerdings können sich Verkehrspflichten auch mit vertraglichen Schutzpflichten decken.¹⁰⁶³ Der BGH hat noch vor der Anerkennung einer deliktsrechtlichen Produktbeobachtungspflicht im Rahmen eines gegen einen Kfz-Hersteller geltend gemachten Schadensersatzanspruchs von diesem den Nachweis verlangt, dass „er die nötigen Anstalten getroffen hat, um von der praktischen Bewährung oder etwaigen Betriebsunfällen unterrichtet zu werden, die mit dem Versagen der Vorrichtungen [des Kfz] zusammenhängen können“ und damit die Produktbeobachtungspflicht auch als vertragliche Schutzpflicht anerkannt.¹⁰⁶⁴ Für den freilich eher seltenen Fall, dass ein Vertragsverhältnis unmittelbar zwischen Hersteller und Nutzer besteht, ließe sich die Datenerhebung für die Produktbeobachtung damit durchaus auf diesen Erlaubnistatbestand stützen.¹⁰⁶⁵

c) Rechtliche Verpflichtung

Da der Hersteller mit der Erhebung und Auswertung der Daten seiner Produktbeobachtungspflicht aus § 823 Abs. 1 BGB nachkommt, kommt eine Rechtfertigung unter dem Gesichtspunkt einer rechtlichen Verpflichtung nach Art. 6 Abs. 1 lit. c DS-GVO in Betracht.¹⁰⁶⁶ Allerdings handelt es sich bei Art. 6 Abs. 1 lit. c DS-GVO lediglich um eine sog. Scharniernorm, sodass der eigentliche Erlaubnistatbestand gem. Art. 6 Abs. 3 DS-GVO

1061 So *Piltz/Reusch*, BB 2017, 841 (843); *Chibanguza*, in: Chibanguza/Kuß/Steege (Hg.), Künstliche Intelligenz, § 4, E., Rn. 20; *Schantz*, in: NK-DatenschutzR, Art. 6, Rn. 37; zurückhaltender *Schmid*, CR 2019, 141 (146).

1062 *Buchner/Petri*, in: Kühling/Buchner (Hg.), DS-GVO, Art. 3, Rn. 33.

1063 *Sprau*, in: Grüneberg, BGB, § 823, Rn. 45; dies verkennend *Piltz/Reusch*, BB 2017, 841 (843).

1064 BGH, BeckRS 1970, 30404653.

1065 Wohl auch *Forgó*, in: Oppermann/Stender-Vorwachs (Hg.), Autonomes Fahren, 2. Aufl., S. 353 (363), wenn er darauf abstellt, dass Daten, mit denen die Funktionsweise des Produkts überwacht werden unter die Norm fallen könnten. Dagegen seien Verschleißdaten lediglich nützlich, aber häufig nicht erforderlich.

1066 Vgl. *Schmid*, CR 2019, 141 (146); *Kahl*, RAW 2019, 70 (72).

aus dem europäischen oder nationalen Recht kommen muss.¹⁰⁶⁷ Dabei ist es erforderlich, dass es sich bei der Vorschrift um eine normierte Verpflichtung handelt, die sich unmittelbar auf die Datenverarbeitung bezieht. Dass der Verantwortliche, um irgendeine rechtliche Verpflichtung erfüllen zu können, auch personenbezogene Daten verarbeiten muss, ist dagegen nicht ausreichend.¹⁰⁶⁸ Bei der deliktsrechtlichen Produktbeobachtungspflicht handelt es sich zum einen aber nur um eine richterrechtlich entwickelte Ausprägung des § 823 Abs. 1 BGB und nicht selbst um eine niedergeschriebene Vorschrift.¹⁰⁶⁹ Zum anderen weist § 823 Abs. 1 BGB schon keinen bestimmten Bezug zu einer Datenverarbeitung auf.¹⁰⁷⁰ Damit liegt in der Produktbeobachtungspflicht kein datenschutzrechtlicher Erlaubnistatbestand.¹⁰⁷¹ Anderes könnte im Automotive-Sektor aufgrund Nr. 7.2.2.4 lit. b UN-Regelung Nr. 155 gelten, da diese Vorschrift bereits in einer gewissen Detailtiefe Datenverarbeitungsvorgänge beschreibt.¹⁰⁷²

d) Wahrung lebenswichtiger Interessen

Eine Rechtfertigung unter dem Gesichtspunkt der Wahrung lebenswichtiger Interessen nach Art. 6 Abs. 1 lit. d DS-GVO ist ebenfalls nicht einschlägig. Denn die Beschränkung auf lebenswichtige Interessen einer Person macht deutlich, dass eine konkrete Gefahrensituation vorliegen muss und eine allgemeine Vorsorge zur Abwehr lebensbedrohlicher Risiken nicht von der Norm erfasst ist. Die Norm umfasst gerade Ausnahmesituationen, in denen lebenswichtige Interessen unmittelbar bedroht werden.¹⁰⁷³ Mangels

1067 Schantz, in: NK-DatenschutzR, Art. 6, Rn. 52.

1068 Buchner/Petri, in: Kühling/Buchner (Hg.), DS-GVO, Art. 3, Rn. 76.

1069 Chibanguza, in: Chibanguza/Kuß/Steege (Hg.), Künstliche Intelligenz, § 4, E., Rn. 20; Daute/Sütthoff, EuZW 2023, 500 (504).

1070 Daute/Sütthoff, EuZW 2023, 500 (504).

1071 i.E. auch Hartl, in: Kühne/Nack (Hg.), Connected Cars, S. 108; in diese Richtung auch Kahl/Behrendt, RAW 2020, 82 (86); a.A. Steinrötter, ZD 2021, 513 (515) und Piovano/Schucht/Wiebe, Produktbeobachtung in der Digitalisierung, S. 142; Daute/Sütthoff, EuZW 2023, 500 (505) weisen darauf hin, dass dies de lege ferenda im Rahmen des Art. 61 KI-VO anders zu beurteilen sein könnte. Denn Abs. 2 hebt direkt darauf ab, dass gesammelten Daten zur Leistung der Hochrisiko-KI-Systeme über deren gesamte Lebensdauer hinweg aktiv und systematisch erfasst, dokumentiert und analysiert werden müssen.

1072 Vgl. Kahl/Behrendt, RAW 2020, 82 (86).

1073 Schantz, in: NK-DatenschutzR, Art. 6, Rn. 62; vgl. auch Erwägungsgrund (46) S. 3 DS-GVO.

einer solchen konkreten Gefahrenlage ist die anlasslose Produktbeobachtung nicht von der Norm erfasst.¹⁰⁷⁴ Die Datenerhebung im Rahmen der Produktbeobachtung dient regelmäßig erst dazu, eine konkrete Gefahrenlage zu entdecken. Erst wenn ein anderweitig bestehender Verdacht hinsichtlich einer potenziell lebensbedrohlichen Produktgefahr vorliegt, wären weitere Datenerhebungen nach Art. 6 Abs. 1 lit. d DS-GVO gerechtfertigt.

e) Berechtigtes Interesse – Interessenabwägung

Die Produktbeobachtungspflicht des Herstellers könnte aber als berechtigtes Interesse eine Datenerhebung rechtfertigen, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, vgl. Art. 6 Abs. 1 lit. f DS-GVO. Zu den berechtigten Interessen zählt Erwägungsgrund (49) DS-GVO ausdrücklich die Gewährleistung der Informationssicherheit, jedenfalls wenn die Verarbeitung personenbezogener Daten unbedingt notwendig und verhältnismäßig ist. Zur Gewährleistung der Informationssicherheit, muss eine Sicherheitslücke zunächst erkannt werden. Auch hierzu kann die Erhebung und Auswertung von Sensor-Daten Aufschluss geben, sodass in diesem Fall schon aufgrund der Wertung des Erwägungsgrunds von einem berechtigten Interesse auszugehen ist.¹⁰⁷⁵ Aber auch im Übrigen ist bei der Datenverarbeitung im Rahmen der Produktbeobachtung von einem berechtigten Interesse auszugehen. Denn diese dient der Erfüllung der herstellerseitigen Sorgfaltspflicht und hat damit den Zweck, die von dem Produkt ausgehenden Gefahren zu reduzieren und Haftungsfälle des Herstellers zu vermeiden.¹⁰⁷⁶ Hinzu kommt, dass durch die Produktbeobachtung die Produktsicherheit im Allgemeinen erhöht wird und folglich auch die Rechte und Rechtsgüter der Verkehrsteilnehmer, aber auch der Nutzer selbst geschützt werden.¹⁰⁷⁷ Die obigen Betrachtungen haben einer-

1074 Schmid, CR 2019, 141 (146); Chibanguza, in: Chibanguza/Kuß/Steege (Hg.), Künstliche Intelligenz, § 4, E., Rn. 21; Kahl/Behrendt, RAW 2020, 82 (86).

1075 So auch Raith, Das vernetzte Automobil, S. 147.

1076 In diese Richtung auch Chibanguza, in: Buck-Heeb/Oppermann (Hg.), Automatisierte Systeme, S. 407 (416); Kahl/Behrendt, RAW 2020, 82 (87) räumen einer bestehenden rechtlichen Verpflichtung gar Indizwirkung für eine positive Interessenabwägung ein.

1077 Dazu Piltz/Reusch, BB 2017, 841 (844); v. Bodungen, in: Specht/Mantz (Hg.), Handbuch Datenschutzrecht, § 16, Rn. 39; Chibanguza, in: Buck-Heeb/Oppermann (Hg.), Automatisierte Systeme, S. 407 (415).

seits gezeigt, wie effektiv eine Produktbeobachtung über die Erfassung von Sensor-Daten sein kann, andererseits aber auch, welche Unsicherheiten und Gefahren bei smarten Produkten nach dem Inverkehrbringen bestehen, sodass von der datenschutzrechtlichen Erforderlichkeit der Datenverarbeitung ausgegangen werden kann.¹⁰⁷⁸ Auch im Rahmen der gebotenen Interessenabwägung ist die besondere Konstellation der Produktbeobachtung zu berücksichtigen. Denn die Abwehr von Produktgefahren liegt nicht nur im Interesse des Herstellers, sondern gerade auch im Interesse des datenschutzrechtlich betroffenen Produktnutzers, so dass im Umkehrschluss auch kein schutzwürdiges Interesse des Produktnutzers am Ausschluss der Verarbeitung oder Nutzung zum Zwecke der Gefahren- und Schadensabwehr besteht, sondern eine Interessengleichheit gegeben ist.¹⁰⁷⁹

In der Praxis wird die Datenerhebung jedoch häufig durch wirtschaftliche Überlegungen der Hersteller motiviert sein, und die Erfüllung der Produktbeobachtungspflicht ist möglicherweise nicht das primäre Interesse.¹⁰⁸⁰ So ergibt sich der Wert der Daten gerade daraus, dass sie auch für andere Zwecke verwendet werden können, als für die Zwecke, für die sie erhoben wurden.¹⁰⁸¹ Vor dem Hintergrund, dass die produkthaftungsrechtlichen Verpflichtungen der Hersteller lediglich mit wirtschaftlichen Interessen an der Datennutzung einhergehen, könnte das produkthaftungsrechtliche Gefahrsteuerungsinteresse daher einen zu unbestimmten Zweck darstellen, um für sich allein die Datenverarbeitung zu rechtfertigen.¹⁰⁸² Diese Argumentation spricht allerdings bereits einen weiteren Aspekt an, nämlich die Zweckbindung der Datenverarbeitung nach Art. 5 Abs. 1 lit. b DS-GVO. Die Befürchtung einer nicht mit den Zwecken der Erhebung in Einklang stehenden Weiterverarbeitung der Daten ist eine Folgefrage, welche die Erhebung der Daten für den rechtmäßigen Zweck nicht in Frage stellt. Entscheidend für die rechtmäßige Erhebung der Daten zur Erfüllung der Produktbeobachtungspflicht ist, dass sich die Datenverarbeitung lediglich auf die Produktbeobachtung und damit auf sicherheitsrelevante Funk-

1078 Ohne ausdrücklich das Kriterium der Erforderlichkeit zu nennen *Eul*, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 10.2, Rn. 36.

1079 *Raith*, Das vernetzte Automobil, S. 150 f.; *Hartmann*, DAR 2015, 122 (126), allerdings nicht auf die Datenerhebung, sondern lediglich auf die Gefahrenabwehrmaßnahmen bezogen.

1080 *Hartmann*, DAR 2015, 122 (125).

1081 *Forgó*, in: Oppermann/Stender-Vorwachs (Hg.), Autonomes Fahren, 2. Aufl., S. 353 (364).

1082 *Hartmann*, DAR 2015, 122 (125 f.) verlangt daher zusätzlich eine Einwilligung.

tionen beschränkt und die Daten nicht zu einer allgemeinen Verarbeitung herangezogen werden.¹⁰⁸³ Zu Produktbeobachtungszwecken berechtigterweise erhobene Daten dürfen eben nicht unter denselben Gesichtspunkten gleichzeitig zu absatzpolitischen Bestrebungen eingesetzt werden. Insoweit stellen Gefahrenabwendungsinteressen und weitergehende wirtschaftliche Intentionen keine austauschbaren Verwendungsgründe dar.¹⁰⁸⁴ Sind die Daten aber für die Produktbeobachtung tatsächlich erforderlich, liegt deren Erhebung für die Gefahrenanalyse auch im Interesse des Betroffenen.¹⁰⁸⁵ Erforderlich sind die Daten für die Produktbeobachtung, soweit die Hersteller verpflichtet sind, diese Daten zu erheben.¹⁰⁸⁶ Hier ist auf die oben dargestellten Lösungen zu verweisen. Da diese eine permanente und anlasslose Datenübertragung an das Backend der Hersteller zu Produktbeobachtungszwecken nicht vorsehen, ist auch der datenschutzrechtliche Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) gewahrt.¹⁰⁸⁷

f) Fazit

In den weit überwiegenden Konstellationen, in denen kein Vertragsverhältnis zwischen Hersteller und Nutzer besteht, rechtfertigt Art. 6 Abs. 1 lit. f DS-GVO eine Datenverarbeitung zum Zwecke der Produktbeobachtung. Damit ist ein datenschutzrechtlicher Gleichlauf mit den Anforderungen der Produktbeobachtungspflicht hergestellt.¹⁰⁸⁸ Auf das Institut der Einwilligung braucht dann nicht zurückgegriffen werden.¹⁰⁸⁹

1083 *Ensthaler/Gollrad*, Rechtsgrundlagen des automatisierten Fahrens, S. 145; *Raith*, in: Roßnagel/Hornung (Hg.), Grundrechtsschutz im Smart Car, S. 89 (104).

1084 So zu der Vorgängernorm des § 28 Abs. 1 Nr. 2 BDSG a.F. *Simitis*, in: NK-BDSG, § 28, Rn. 113; in diese Richtung auch *Ensthaler/Gollrad*, Rechtsgrundlagen des automatisierten Fahrens, S. 144 f.

1085 *Raith*, Das vernetzte Automobil, S. 151.

1086 So *Hartl*, in: Kühne/Nack (Hg.), Connected Cars, S. 108.

1087 Vgl. dazu *Raith*, in: Roßnagel/Hornung (Hg.), Grundrechtsschutz im Smart Car, S. 89 (104); *Ensthaler/Gollrad*, Rechtsgrundlagen des automatisierten Fahrens, S. 145; *Hartl*, in: Kühne/Nack (Hg.), Connected Cars, S. 108; *Böck/Theurer*, BB 2021, 520 (524).

1088 So auch *v. Bodungen*, in: Specht/Mantz (Hg.), Handbuch Datenschutzrecht, § 16, Rn. 39.

1089 A.A. ohne nähere Begründung *Wiebe*, InTer 2020, 66 (69) und *Droste*, CCZ 2015, 105 (110).

3. Bedeutung der E-Privacy-RL und des TTDSG

Weitere Beachtung muss dem Verhältnis der DS-GVO und Art. 5 Abs. 3 S. 1 E-Privacy-RL und deren Umsetzung in § 25 TTDSG geschenkt werden. Sinn und Zweck der Regelung ist es, die Integrität von Endeinrichtungen unabhängig vom Vorliegen personenbezogener Daten umfassend gegen den Zugriff durch Dritte zu schützen.¹⁰⁹⁰ Hierzu statuiert § 25 Abs. 1 S. 1 TTDSG, dass sowohl die Speicherung von Informationen in Endeinrichtungen des Endnutzers als auch ein Zugriff auf dort gespeicherte Informationen von einer Einwilligung des Endnutzers abhängen. Eine Einwilligung ist nur in engen Ausnahmefällen entbehrlich, nämlich insbesondere dann, wenn der Zugriff oder die Speicherung nach § 25 Abs. 2 Nr. 2 zwingend erforderlich ist, um einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen zu können. Die Rechtfertigungsgründe sind damit deutlich restriktiver formuliert als im Rahmen des Art. 6 Abs. 1 DS-GVO.

a) Anwendungsbereich und Verhältnis zur DS-GVO

Der Anwendungsbereich der Norm erstreckt sich auch auf die Produktbeobachtung durch den Hersteller. Nach § 2 Abs. 2 Nr. 6 TTDSG ist unter einer Endeinrichtung jede Einrichtung zum Aussenden, Verarbeiten oder Empfangen von Nachrichten erfasst, die direkt oder indirekt an die Schnittstelle eines öffentlichen Telekommunikationsnetzes angeschlossen ist. Aufgrund dieser weiten Fassung fallen hierunter eine Vielzahl von IoT-Geräten, die bspw. über einen WLAN-Router an das öffentliche Kommunikationsnetz angeschlossen sind.¹⁰⁹¹ Werden nun im Rahmen der Produktbeobachtung Sensor-Daten ausgelesen, ist hierin ohne Weiteres ein Zugriff auf in Endeinrichtungen gespeicherte Informationen zu sehen. Daneben kann auch in aufgespielten Updates als Gefahrengegenmaßnahmen ein Speichern von Informationen auf dem Endgerät gesehen werden.¹⁰⁹²

Das Verhältnis zur DS-GVO wird in Art. 95 DS-GVO angesprochen und überwiegend dahingehend verstanden, dass sich der Zugriff auf personenbezogene Daten nach der spezielleren E-Privacy-RL und damit nach § 25

1090 *Ettig*, in: Taeger/Gabel (Hg.), DSGVO, § 25 TTDSG, Rn. 3.

1091 Hierzu BT-Drs. 19/27441, S. 38.

1092 DSK, Orientierungshilfe der Aufsichtsbehörden Telemedien 2021, S. 7.

TTDSG richtet.¹⁰⁹³ Da das TTDSG allerdings lediglich den Zugriff auf Informationen regelt, kommt es zu einem Nebeneinander mit der DS-GVO, sodass sich der Zugriff auf die Information nach § 25 TTDSG beurteilt, während sich die Verarbeitung der Daten nach der DS-GVO richtet.¹⁰⁹⁴ Damit aber haben die restriktiven Rechtfertigungsgründe für den Zugriff auf die Information auch reflexartig Auswirkungen auf die anschließende Datenverarbeitung nach Art. 6 Abs. 1 DS-GVO und schränken diese ein.¹⁰⁹⁵ Denn der Verantwortliche könnte für die Verarbeitung der Daten zwar auf die flexibleren Rechtfertigungsgründe des Art. 6 Abs. 1 DS-GVO zurückgreifen, dies hilft ihm allerdings wenig, wenn er das Einfallstor und damit die strengen Rechtfertigungsgründe für die nachgelagerte Verarbeitung erst gar nicht überwinden kann und ein Zugriff auf die Daten schon nicht möglich ist.¹⁰⁹⁶ Für die Produktbeobachtung bedeutet dies, dass die erhobenen Sensor-Daten zwar einwilligungsfrei nach Art. 6 Abs. 1 lit. f DS-GVO aufgrund eines berechtigten Interesses verarbeitet werden dürften, allerdings der vorgelagerte Zugriff auf diese Daten nach § 25 Abs. 1 S. 1 TTDSG an die Einwilligung gebunden wäre.

b) Auslegung der Rechtfertigungsgründe des § 25 Abs. 2 TTDSG

Ob dieses Ergebnis so tragbar ist, ist noch nicht abschließend geklärt.¹⁰⁹⁷ Teilweise wird in dieser im Vergleich zu Art. 6 Abs. 1 DS-GVO restriktiven Fassung der Rechtfertigungsgründe gerade eine bewusste Entscheidung des Gesetzgebers gesehen.¹⁰⁹⁸ Möglicherweise kann aber über eine Auslegung dieser strengen Rechtfertigungsgründe des § 25 Abs. 2 TTDSG eine sachgerechte Lösung erreicht werden.

1093 Kühling/Raab, in: Kühling/Buchner (Hg.), DS-GVO, Art. 95, Rn. 1; i.E. auch Golland, in: Taeger/Gabel (Hg.), DSGVO, Art. 95, Rn. 4 ff. m.w.N.; Hartl, in: Kühne/Nack (Hg.), Connected Cars, S. 67.

1094 Hartl, in: Kühne/Nack (Hg.), Connected Cars, S. 104; Grages, CR 2021, 834 (837); DSK, Orientierungshilfe der Aufsichtsbehörden Telemedien 2021, S. 6.

1095 So auch Grages, CR 2021, 834 (837).

1096 Vgl. DSK, Orientierungshilfe der Aufsichtsbehörden Telemedien 2021, S. 31.

1097 So auch Hartl, in: Kühne/Nack (Hg.), Connected Cars, S. 109; offen gelassen auch von Grages, CR 2021, 834 (837).

1098 DSK, Orientierungshilfe der Aufsichtsbehörden Telemedien 2021, S. 21; wohl auch Hense, in: Taeger/Pohle (Hg.), Computerrechts-Handbuch, Teil 33.2, Rn. 108; angedeutet bei Grages, CR 2021, 834 (836).

Es ließe sich argumentieren, dass dem Hersteller die zur Verfügungstellung des Telemediendienstes nur unter Erfüllung seiner deliktsrechtlichen Produktbeobachtungspflicht nach § 823 Abs. 1 BGB möglich ist, sodass der entsprechende Zugriff auf die Informationen unbedingt erforderlich i.S.d. § 25 Abs. 2 Nr. 2 TTDSG wäre. Jedenfalls ließe sich in der Verwendung des entsprechenden IoT-Geräts in Kenntnis der Netzanbindung ein Nutzerwunsch in diese Richtung sehen.¹⁰⁹⁹ Die unbedingte Erforderlichkeit würde in diesem Fall weit ausgelegt und erfasste nicht nur Technologien, die technisch erforderlich sind, um den gewünschten Dienst bereitzustellen. Um den praktischen Notwendigkeiten gerecht werden zu können, dürften nicht nur technische, sondern auch rechtliche, vertragliche und wirtschaftliche Aspekte berücksichtigt werden.¹¹⁰⁰ Für den Fall, dass der Zugriff auf personenbezogene Daten einer anschließenden Datenverarbeitung dient, welche nach Art. 6 Abs. 1 lit. b-f DS-GVO ohne Einwilligung erlaubt ist, sei auch der vorherige Zugriff i.S.d. § 25 Abs. 2 Nr. 2 TTDSG für den späteren Verarbeitungszweck erforderlich.¹¹⁰¹ Andererseits wird angeführt, dass die Ausnahmenvorschrift restriktiv auszulegen sei und dass insbesondere die Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO nicht automatisch geeignet sei, die Voraussetzungen von § 25 Abs. 2 Nr. 2 TTDSG zu erfüllen.¹¹⁰² Allerdings betonte der EuGH zu der Vorgängernorm des § 15 TMG a.F., dass die Verarbeitung personenbezogener Daten nicht kategorisch und ohne Raum für eine Abwägung der im konkreten Einzelfall einander gegenüberstehenden Rechte und Interessen ausgeschlossen werden darf.¹¹⁰³ Dieser herausgearbeitete Grundsatz, dass immer eine Interessenabwägung als Rechtfertigung für eine Datenverarbeitung in Betracht zu ziehen sei, habe allgemeine Gültigkeit und sei auch im Rahmen der E-Privacy-Richtlinie zu beachten.¹¹⁰⁴ Vor diesem Hintergrund sei § 25 TTDSG richtlinienkonform und im Einklang mit Art. 6 DS-GVO, um die dort genannten Erlaubnistatbestände und insbesondere um den Abwägungstatbestand des Art. 6 Abs. 1 lit. f DS-GVO zu ergänzen, wobei bei den entgegenstehenden Interessen des Nutzers die Wertung des Art. 5 Abs. 3 E-Privacy-RL zu berücksichtigen sei, wodurch eine Beschränkung auf besondere Anwendungsfälle erreicht werde.¹¹⁰⁵ Es

1099 Hanloser, ZD 2021, 399 (401 f.).

1100 Schonhofen, ZD 2023, 326 (328).

1101 Hanloser, ZD 2021, 399 (401).

1102 DSK, Orientierungshilfe der Aufsichtsbehörden Telemedien 2021, S. 21 f.

1103 EuGH, MMR 2016, 842 (844).

1104 Schmitz, MMR 2022, 735 (736).

1105 Schmitz, MMR 2022, 735 (737).

muss jedenfalls konstatiert werden, dass nicht ersichtlich ist, warum der reine Endgerätezugriff nach § 25 TTDSG strenger behandelt werden soll als eine Verarbeitung von personenbezogenen Daten.¹¹⁰⁶ Allerdings bedarf es auch bei einer weiten Auslegung des Kriteriums der Erforderlichkeit einiger juristischer Kreativität, das bloße Funktionieren des Produkts als vom Nutzer gewünschten „Telemediendienst“ einzuordnen.¹¹⁰⁷ Hier zeigt sich die Friktion, dass § 25 TTDSG zwar alle Endeinrichtungen schützt, aber nicht alle dazu bestimmt sind, im klassischen Sinne Nachrichten zu übermitteln oder einen Telemediendienst anzubieten.¹¹⁰⁸

Selbst wenn man die Erfüllung der Produktbeobachtungspflicht nicht als von § 25 Abs. 2 Nr. 2 TTDSG gedeckt ansieht, bleibt ein anderer Weg, um in diesem Fall nicht an der Einwilligungsschranke stehen bleiben zu müssen. Denn selbst der EDSA geht davon aus, dass nicht strikt an den Rechtfertigungsgründen des § 25 TTDSG festgehalten werden kann. Dieser hat für den automatischen Notruf nach der eCall-VO¹¹⁰⁹ eine Ausnahme von der grundsätzlich erforderlichen Einwilligung anerkannt. Begründet wurde dies damit, dass der Verantwortliche gerade einer rechtlichen Verpflichtung unterliege und die betroffenen Personen aus diesem Grund gar keine echte oder freie Wahl haben, die Verarbeitung ihrer Daten zu verweigern.¹¹¹⁰ Da man bei einem automatisch ausgelösten Notruf kaum von einem ausdrücklich gewünschten Telemediendienst i.S.d. § 25 Abs. 2 Nr. 2 TTDSG sprechen kann, liegt es nahe, einen Zugriff verallgemeinernd zur Erfüllung einer vorrangigen rechtlichen Verpflichtung über § 25 Abs. 2 TTDSG hinaus zu erlauben.¹¹¹¹ Es würde auch der Logik des Art. 5 Abs. 3 E-Privacy-Richtlinie widersprechen, wenn der Nutzer einen Diensteanbieter an der Erfüllung seiner Pflicht hindern und einen Gesetzesverstoß des Anbieters provozieren könnten, indem sie ihre Einwilligung in den Zugriff auf das von ihnen genutzte Gerät verweigern.¹¹¹²

Durch die Anerkennung der Erfüllung der Produktbeobachtungspflicht als Ausnahme vom Einwilligungserfordernis kann folglich ein Gleichlauf

1106 *Schonhofen*, ZD 2023, 326 (328).

1107 So auch *Grages*, CR 2021, 834 (836).

1108 *Grages*, CR 2021, 834 (836).

1109 Verordnung (EU) 2015/758.

1110 EDSA, Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen, S. 36.

1111 *Hanloser*, ZD 2021, 399 (401); *Wiesemann*, MMR 2022, 343 (345) „overriding legal obligation“.

1112 So auch *Piltz*, CR 2021, 555 (562).

mit den Anforderungen der Produktbeobachtungspflicht und eine Kohärenz mit dem Datenschutzrecht hergestellt werden.

4. Bedeutung des Data Acts

Hinsichtlich nicht-personenbezogener Daten sieht Art. 4 Abs. 13 Data Act vor, dass der Dateninhaber diese Daten nur auf der Grundlage eines Vertrags mit dem Nutzer nutzen darf (Lizenzvertrag). Zwar werden zum Zwecke der Produktbeobachtung genutzte Daten regelmäßig einen Personenbezug aufweisen, indes ist im Rahmen der im Einzelfall vorzunehmenden Betrachtung nicht ausgeschlossen, dass Daten keinen Personenbezug haben.¹¹¹³ Mangels Ausnahmetatbestand ist in diesem Fall eine vertragliche Abrede zwingend erforderlich, sodass prima facie nicht-personenbezogene Daten strenger geschützt werden als personenbezogene Daten.¹¹¹⁴ Indes eröffnet eine vertragliche Abrede einen weiteren Gestaltungsspielraum als eine einzuholende Einwilligung nach der DS-GVO. Nach Erwägungsgrund (25) Data Act kann ein solcher Vertrag Teil einer Vereinbarung über die Erbringung des verbundenen Dienstes sein und zusammen mit dem Kaufvertrag über das Produkt getroffen werden. Auch wenn Hersteller und Verkäufer auseinanderfallen, kann der Hersteller die Nutzung des Dienstes von der Einräumung entsprechender Nutzungsrechte abhängig machen.¹¹¹⁵ Auch wenn entsprechende Klauseln einer AGB-Kontrolle standhalten müssen,¹¹¹⁶ ist es den Herstellern so möglich, sich die entsprechende Rechte vom Nutzer übertragen zu lassen.

VI. Fazit zur Herstellerverantwortung bei zunehmender Datenverfügbarkeit

Im Rahmen der passiven Produktbeobachtung hat der Hersteller sämtliche Informationen, die ihn erreichen, auch auszuwerten. Dies gilt ungeachtet des konkreten Kommunikationsweges und damit unterschiedslos für ihn erreichende Social-Media-Inhalte und Sensor-Daten. Insoweit gilt, dass eine erhöhte Datenkenntnis auch zu einer gesteigerten Produktverantwortung führt. Hinsichtlich der aktiven Produktbeobachtung führen automa-

1113 Vgl. unter D.V.I.c).

1114 So *Bomhard/Merkle*, RD 2022, 168 (174).

1115 Vgl. auch *Wiebe*, GRUR 2023, 1569 (1571).

1116 Vgl. auch Erwägungsgrund (28) Data Act.

tisierte Prozesse und KI-gestützte Big Data-Auswertungen sowie die Möglichkeit der Auslagerung an externe Dienstleister zu einer Verschiebung der Kriterien der Erforderlichkeit und Zumutbarkeit zu Lasten des Herstellers. Daneben führen technische Zugriffsmöglichkeiten auf Daten vernetzter Produkte dazu, dass die Hersteller zunehmend selbst Daten aktivistisch generieren müssen. Die Reichweite und konkrete Ausgestaltung dieser Pflicht kann produktspezifisch stark variieren und nur im Einzelfall bestimmt werden. Weder das Datenschutzrecht noch der Schutz der Integrität von Endeinrichtungen gegen den Zugriff Dritter nach dem TTDSG stellen insoweit Hemmnisse dar. Denn die Erfüllung der Produktbeobachtungspflicht zur Abwehr von Gefahren vom Nutzer und der Allgemeinheit stellt eine Rechtfertigung dar.

E. Smarte Reaktionspflichten des Herstellers

Wurde im vorangegangenen Kapitel festgestellt, dass ein durch die Digitalisierung zur Verfügung stehender erhöhter Datenbestand auch mit einer verstärkten Verantwortung des Herstellers im Rahmen seiner Produktbeobachtungspflicht einhergeht, sollen nun die durch die Digitalisierung der Produktlandschaft erweiterten Reaktionsmöglichkeiten auf eine erkannte Produktgefahr und sich daraus ergebenden Verantwortlichkeiten des Herstellers untersucht werden. Da smarte Produkte aufgrund ihrer Vernetzung die Möglichkeit einer unmittelbaren Kommunikation und Interaktion zwischen Hersteller und Nutzer ermöglichen, können die entsprechenden Maßnahmen individuell und zielgerichtet erfolgen, sodass von smarten Reaktionsmaßnahmen bzw. Reaktionspflichten gesprochen werden kann.

I. Bedeutung der Reaktionspflichten

Die bloße Produktbeobachtung i.e.S. verhindert noch keinen Schadensfall und würde für sich genommen der Verantwortung des Herstellers nach der Inverkehrgabe nicht gerecht. Umgekehrt führt eine Verletzung der Produktbeobachtung i.e.S. zu keiner Haftung des Herstellers, sollte dieser, weil er etwa zufällig von der Gefahr Kenntnis genommen hat, angemessen reagieren.¹¹¹⁷ Mit Blick auf die Haftungsbegründung kommt damit den Reaktionspflichten maßgebliche Bedeutung zu. Diese schließen sich an die gewonnenen Erkenntnisse des Herstellers an und sollen eine effektive Gefahrenabwehr und den Schutz des Nutzers und Dritter sicherstellen.

Dabei ist zwischen noch nicht ausgelieferten und bereits in Verkehr gebrachten Produkten zu unterscheiden. Von den noch nicht in den Verkehr gebrachten Produkten gehen keine Gefahren für Dritte aus, sodass es hier ausreichend ist, die Auslieferung zu stoppen und abhängig vom konkreten Sicherheitsdefizit die Konstruktion, Fabrikation oder Instruktion anzupassen.¹¹¹⁸ Denn aufgrund der auf den Zeitpunkt des Inverkehrbrin-

1117 Dazu *Wagner*, VersR 2014, 905 (907).

1118 *Förster*, in: BeckOK, BGB, § 823, Rn. 743; BGH, NJW 1994, 3349 (3350); BGH, NJW 1990, 906 (908).

gens konkretisierten Sorgfaltspflichtbestimmung führt eine erkannte Gefahr zur Fehlerhaftigkeit der später noch in Verkehr gebrachten Produkte. Mit der Anpassung des Herstellungsprozesses soll einem diesbezüglichen Fehlervorwurf entgegengewirkt werden.¹¹¹⁹ Dagegen erweist sich die Gefahrenabwehr bei bereits ausgelieferten Produkten als schwieriger, da diese die unmittelbare Einwirkungssphäre des Herstellers verlassen haben und im Feld eine fortwährende Gefahr für Dritte darstellen.¹¹²⁰ Im Ausgangspunkt muss es darum gehen, den Wissensvorsprung, den der Hersteller aufgrund der erlangten Informationen über den Sicherheitszustand des Produkts hat, an den nichtsahnenden und folglich ungeschützten Produktnutzer heranzutragen.¹¹²¹ Die bisherige Fokussierung der Gefahrenabwendungsmaßnahmen auf die Warnung und den Rückruf, beruht dabei weniger auf rechtlichen Erwägungen als mehr auf den tatsächlichen Gegebenheiten analoger Produkte.¹¹²² Auch hier muss gelten, dass die Produktbeobachtungspflicht die Weiterentwicklung des Standes von Wissenschaft und Technik zu berücksichtigen hat.¹¹²³ So sind aufgrund der Vernetzung der Produkte Maßnahmen wie zielgerichtete Warnungen, fehlerbehebende Updates oder gar die Deaktivierung eines Produkts per Fernzugriff möglich.¹¹²⁴

II. Herkömmliche Reaktionspflichten

Um beurteilen zu können, unter welchen Voraussetzungen diese neuartigen Reaktionsmöglichkeiten in Betracht kommen und in welchem Verhältnis sie zueinanderstehen, müssen zunächst die herkömmlichen bzw. analogen Reaktionspflichten beleuchtet werden. Allerdings fehlt es bereits bei einer begrifflichen Abgrenzung der Gefahrenabwendungsmaßnahmen an einer

1119 Ausführlich zur Auswirkung wissenschaftlich-technischen Fortschritts für die Herstellerpflichten bereits aufgelegter Produkte *Helte*, Anforderungen an die Produktsicherheit, S. 167 ff.

1120 So auch *Förster*, in: BeckOK, BGB, § 823, Rn. 744.

1121 *Klindt*, DAR 2023, 7 (7).

1122 Vgl. auch *Meents/Obradovic*, ZfPC 2022, 13 (14) und *Meents*, in: FS Taeger, S. 13 (19).

1123 Vgl. nochmals *Wende*, in: Sassenberg/Faber (Hg.), Industrie 4.0 und Internet of Things, § 4, Rn. 22 und *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 70.

1124 Vgl. *Hartmann*, in: Knappertsbusch/Gondlach (Hg.), Arbeitswelt und KI 2030, S. 63 (68 f., 71); *Klindt*, DAR 2023, 7 (8).

einheitlichen Terminologie.¹¹²⁵ Für eine leichtere Unterscheidung bietet es sich aber an, zwischen der Warnung auf der einen Seite und den Reaktionspflichten jenseits der Warnung auf der anderen Seite zu unterscheiden.¹¹²⁶ Während bei einer Warnung lediglich Informationen übermittelt werden, zielen weitergehende Reaktionsmaßnahmen auf die herstellerseitige Einwirkung auf das Produkt ab.¹¹²⁷

1. Ausgangspunkt: Pflegebetten-Entscheidung des BGH

Gerade der Umfang und die Reichweite der herstellerseitigen Reaktionspflichten gehört aber zu den strittigsten Bereichen der Produkthaftung. In den „Apfelschorf“-Fällen¹¹²⁸, in denen die Produktbeobachtungspflicht gewissermaßen aus der Taufe gehoben wurde, schwieg der BGH noch hinsichtlich der Reaktionspflichten des Herstellers, die über eine Warnung der Verbraucher hinausgehen.¹¹²⁹ Ergangene Entscheidungen der Instanzgerichte divergierten in der Sache oder ließen eine Auseinandersetzung mit den Voraussetzungen und dem Verhältnis der jeweiligen Reaktionsmaßnahmen vermissen.¹¹³⁰ Zwar hat der BGH bereits in der strafrechtlichen „Lederspray“-Entscheidung eine Rückrufflicht des Herstellers bejaht,¹¹³¹ jedoch offengelassen, welche Maßnahmen als „Rückruf“ in Betracht kommen, wie sich dieser zur Warnung verhält und wie die Frage der Kostentragung zu beurteilen ist.¹¹³² Bereits aufgrund der fehlenden Herleitung und

1125 Teilweise wird der Begriff „Rückruf“ ohne weitere Differenzierung als Maßnahmen zur Gefahrenabwehr jeglicher Art verstanden, welcher auch die Warnung umfassen soll, so *Lenz*, in: *Lenz*, Produkthaftung, § 4, Rn. 2 und *Stöhr*, in: FS Müller, S. 173 (Fn. 1).

1126 Eine Differenzierung zwischen Warnung und weitergehenden Sicherungspflichten wird auch vom BGH in der Pflegebetten-Entscheidung vorgenommen, vgl. BGH NJW 2009, 1080 (1081, Rn. 11).

1127 Vgl. *Lüftenegger*, Die Rückrufflicht des Herstellers, S. 26 f.; *Lüftenegger*, DAR 2016, 122 (122); *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 162; ähnlich auch *Huber*, Rechtsfragen des Produktrückrufs, S. 12.

1128 BGH, NJW 1981, 1606 und BGH, NJW 1981, 1603.

1129 So auch *Wagner*, in: MüKo, BGB, § 823, Rn. 1122.

1130 Vgl. die Auflistung bei *Lenz*, in: *Lenz*, Produkthaftung, § 4, Rn. 5 ff. und *Lüftenegger*, Die Rückrufflicht des Herstellers, S. 169 ff. sowie *Stöhr*, in: FS Müller, S. 173 (175 ff.); *Burckhardt*, VersR 2007, 1601 „Die bisherige Rechtsprechung [...] zeigt keine einheitliche Linie“.

1131 BGH, NJW 1990, 2560.

1132 Vgl. *Wagner*, in: MüKo, BGB, § 823, Rn. 1122; *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), Produkthaftungshandbuch, § 24, Rn. 331 „auf geradezu irritierende

der generellen Schwierigkeit der Übertragung auf die zivilrechtliche Dogmatik musste eine Bezugnahme auf diese Entscheidung zur Begründung einer zivilrechtlichen Rückrufpflicht als Überinterpretation angesehen werden.¹¹³³ Ebenso zeichnete sich in der juristischen Literatur ein breites und uneinheitliches Meinungsspektrum ab.¹¹³⁴ Mit der Pflegebetten-Entscheidung aus dem Jahr 2008 bezog der BGH erstmalig in der Sache Stellung zu den deliktsrechtlichen Warn- und Rückrufpflichten der Hersteller.¹¹³⁵ Auch wenn in der Entscheidung die Frage nach dem Umfang der Reaktionspflichten nicht abschließend beantwortet wurde,¹¹³⁶ hat der BGH doch Leitplanken für eine entsprechende Prüfung vorgegeben. Im Folgenden sollen daher die höchstrichterlichen Aussagen aus der Pflegebetten-Entscheidung dargestellt und untersucht werden, inwieweit sie einer kohärenten Dogmatik folgen und daher auch auf die smarten Reaktionspflichten übertragbar sind.

2. Effektivität der Gefahrenabwehr als Maxime

Bei den Reaktionspflichten handelt es sich wie bei den übrigen Herstellerpflichten um eine Konkretisierung der allgemeinen Verkehrspflichten, sodass sich der Pflichtenumfang danach richtet, was zur Gefahrenabwehr objektiv erforderlich und zumutbar ist.¹¹³⁷

Auch der BGH geht in seiner Pflegebetten-Entscheidung im Sinne dieses Zweiklangs vor,¹¹³⁸ rückt aber das Kriterium der Erforderlichkeit in den Mittelpunkt.¹¹³⁹ Bei der Auslegung des Kriteriums der Erforderlichkeit ist indes zu berücksichtigen, dass bei den Reaktionspflichten eine andere Ausgangslage als bei den übrigen Produzentenpflichten besteht. Denn es geht nicht um die präventive Vermeidung einer Gefahr im Rahmen des Produktionsprozesses, sondern um die Abwehr einer bereits bestehenden Produktgefahr im Feld. In dieser Konstellation liegt aber eine „rechtsdog-

Weise übergangen“ und „daher wenig hilfreich bei der Klärung der Rückruf-Problematik“; *Lüftenegger*, Die Rückrufpflicht des Herstellers, S. 168.

1133 So *Molitoris*, NJW 2009, 1049 (1051).

1134 Vgl. die Nachweise bei *Lenz*, in: *Lenz*, Produkthaftung, § 4, Rn. 39.

1135 BGH, NJW 2009, 1080.

1136 Vgl. dazu *Wagner*, in: *MüKo*, BGB, § 823, Rn. 1122; *Lüftenegger*, Die Rückrufpflicht des Herstellers, S. 206.

1137 *Lüftenegger*, Die Rückrufpflicht des Herstellers, S. 154.

1138 BGH, NJW 2009, 1080 (1081, Rn. 12; 1082, Rn. 20).

1139 So auch *Lüftenegger*, Die Rückrufpflicht des Herstellers, S. 212.

matische Grenzsituation¹¹⁴⁰ vor, denn der deliktsrechtliche Schutz ist auf die in § 823 Abs. 1 BGB aufgezählten Rechte und Rechtsgüter beschränkt. Damit sind primäre Vermögensschäden nur ausnahmsweise im Falle einer vorsätzlichen sittenwidrigen Schädigung nach § 826 BGB oder nach § 823 Abs. 2 BGB i.V.m. einem vermögensschützenden Schutzgesetz ersatzfähig. Es entspricht dem Sinn und Zweck des Deliktsrechts, den Interessen des Geschädigten am Erhalt der Unversehrtheit seiner Rechtsgüter (status quo) Rechnung zu tragen und dort eingetretene Schäden zu kompensieren (Integritätsinteresse). Dagegen soll es keinen Ausgleich für das durch eine mangelhafte Lieferung gestörte Austauschverhältnis zwischen Sachleistung und Kaufpreiszahlung schaffen (Äquivalenzinteresse). Dies ist dem vertraglichen Gewährleistungsrecht vorbehalten.¹¹⁴¹ Qualitätsmängel am Produkt ohne Sicherheitsrelevanz können dem Hersteller deliktsrechtlich daher nicht entgegengehalten werden.¹¹⁴²

Da das Deliktsrecht nicht das Nutzungs- oder Äquivalenzinteresse, sondern ausschließlich das Integritätsinteresse schützt, kann im Rahmen der Erforderlichkeit aber nicht maßgeblich auf die objektive Verkehrserwartung abgestellt werden, sondern muss das Kriterium eigenständig ausgelegt werden.¹¹⁴³ Maßgebliche Bedeutung erlangt dabei die Effektivität der Gefahrenabwehr.¹¹⁴⁴ Vor diesem Hintergrund bestimmt sich die Erforderlichkeit daher ergebnisorientiert danach, wie die Gefahr tatsächlich abgewehrt werden kann und weniger nach dem dafür eingesetzten Mittel.¹¹⁴⁵

In diesem Sinne stellt der BGH gleich zu Beginn seiner Pflgebetten-Entscheidung klar, dass die „Sicherungspflichten des Herstellers nach Inverkehrbringen seines Produkts [...] nicht notwendig auf die Warnung vor etwaigen Gefahren beschränkt“ sind und erkennt damit erstmalig ausdrücklich¹¹⁴⁶ die Existenz weitergehender deliktsrechtlicher Sicherungspflichten an.¹¹⁴⁷ Dies gilt jedenfalls für Fälle, in denen eine solche Maßnahme „im konkreten Fall erforderlich ist, um Produktgefahren [...] effektiv abzuwehren“.¹¹⁴⁸ Maßgeblich für die Annahme solcher weitergehender Si-

1140 So Kettler, VersR 2009, 272 (275).

1141 Vgl. nur BGH NJW 2009, 1080 (1082, Rn. 19) m.w.N.

1142 Wagner, Deliktsrecht, Kap. 9, Rn. 4.

1143 Feststellung bei Lüftenegger, Die Rückrufflicht des Herstellers, S. 154.

1144 BGH, NJW 2009, 1080 (1081 f., Rn. 11 f., 16 ff.).

1145 Lüftenegger, Die Rückrufflicht des Herstellers, S. 213.

1146 Zur Bedeutung vorangegangener Nichtannahmebeschlüsse des BGH im Zusammenhang mit Rückruf-Entscheidungen vgl. Stöhr, in: FS Müller, S. 173 (179 f.).

1147 BGH, NJW 2009, 1080 (1081, Rn. 11).

1148 BGH, NJW 2009, 1080 (1081, Rn. 12).

cherungspflichten ist damit die Effektivität der Gefahrbeseitigung für die bedrohten Rechtsgüter sowie das Vorhandensein gleich effizienter Alternativenmaßnahmen.¹¹⁴⁹ Die Reichweite der Gefahrenabwehrungsmaßnahmen kann daher immer nur unter Berücksichtigung aller Umstände des Einzelfalls entschieden werden.¹¹⁵⁰ Auch wenn der BGH in der Pflegebetten-Entscheidung dezidiert offen ließ, welche Konsequenzen sich aus seinen Grundsätzen für die Reaktionspflichten der Hersteller im Allgemeinen ergeben,¹¹⁵¹ lassen sich doch Orientierungen entnehmen, wann eine bloße Warnung nicht mehr ausreichend ist.

3. Verhältnis von Warnung und Rückruf

a) Ausgangslage

Die Warnung der Produktnutzer kann als Mindeststandard der Reaktion angesehen werden.¹¹⁵² Hierdurch wird die eingangs beschriebene Informationsasymmetrie zwischen Hersteller und Nutzer ausgeglichen und Letzterer zur eigenen Gefahrensteuerung befähigt. Dies gilt insbesondere bei einem anfänglichen Instruktionsfehler. Versäumnisse im Rahmen der Instruktionspflicht können durch weitere Warnungen, Ergänzungen oder den Austausch der Betriebsanleitung korrigiert werden.¹¹⁵³ Weitergehende Sicherungsmaßnahmen scheiden hier schon deshalb aus, weil bei angemessener Handhabung vom Produkt selbst keine Gefahren ausgehen.¹¹⁵⁴ Aber auch im Übrigen befähigt die Warnung den Produktnutzer im Ausgangspunkt zu einer eigenverantwortlichen Gefahrensteuerung. Es verwundert daher nicht, dass der BGH in seiner Pflegebetten-Entscheidung gleich zu Beginn seiner Ausführungen die Warnung in den Vordergrund rückt.¹¹⁵⁵ Aus Gründen der Effektivität der Gefahrenabwehr kann der Hersteller aber über die Warnung hinaus verpflichtet sein, dafür Sorge zu tragen, dass

1149 Burckhardt, VersR 2007, 1601.

1150 BGH, NJW 2009, 1080 (1081, Rn. 13).

1151 Vgl. BGH, NJW 2009, 1080 (1082, Rn. 20).

1152 Wagner, VersR 2014, 905 (907 f.).

1153 Allgemeine Meinung, vgl. nur BGH NJW 1986, 1863 (1864); Ackermann, in: NK-ProdR, § 823 BGB, Rn. 131; Schwenger, JZ 1987, 1059 (1061); Klindt, BB 2009, 792 (795); Michalski, BB 1998, 961 (965).

1154 Schwenger, JZ 1987, 1059 (1061).

1155 BGH, NJW 2009, 1080 (1081, Rn. 10): „insbesondere Reaktionspflichten zur Warnung“.

ein bereits ausgeliefertes gefährliches Produkt aus dem Verkehr gezogen wird oder nicht mehr benutzt wird.¹¹⁵⁶ In diesem Sinne wird die Warnung vom Rückruf abgegrenzt.¹¹⁵⁷ Der Rückruf zielt gerade auf die Erwirkung der Rückgabe eines bereits in den Verkehr gebrachten Produkts ab, vgl. § 2 Nr. 24 ProdSG.¹¹⁵⁸

b) Fallgruppen einer Rückrufflicht

Wurde festgestellt, dass ein Rückruf neben der Warnung in Betracht kommt, ist zu untersuchen, in welchen Fallgruppen dies möglich ist. Die Marschroute ist dabei nach oben Gesagtem bereits vorgegeben. Erst wenn eine Warnung im Einzelfall aus Gründen der Effektivität der Gefahrenabwehr nicht ausreichend ist, das Integritätsinteresse zu schützen, kommt ein Rückruf als ultima ratio in Betracht.¹¹⁵⁹ Die zu diesem Zweck vom BGH vorgenommene Fallgruppenbildung, die sich allerdings nicht als abschließend versteht, soll im Folgenden untersucht werden.¹¹⁶⁰

aa) Warnung nicht ausreichend zur Gefahren einschätzung und Verhaltensanpassung

Voraussetzung einer hinreichend effektiven Warnung muss sein, dass diese beim Produktnutzer eine ausreichende Gefahrenkenntnis schafft und ihm die Gefahrensteuerung ermöglicht. Daher können Sicherungspflichten des Herstellers dann über eine Warnung hinausgehen, wenn Grund zur Annahme besteht, dass auch eine hinreichend deutliche und detaillierte

1156 BGH, NJW 2009, 1080 (1081, Rn. 11).

1157 BGH, NJW 2009, 1080 (1081, Rn. 11); vgl. auch *Handorn*, MPR 2009, 37 (39).

1158 Der BGH verweist noch auf die Vorgängernorm des § 2 Abs. 17 GPSG.

1159 Vgl. *Voigt*, in: BeckOGK, BGB, § 823, Rn. 682; *Förster*, in: BeckOK, BGB, § 823, Rn. 751; *Kettler*, VersR 2009, 272 (275); *Pieper*, BB 1991, 985 (988); *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 166; in der Wortwahl zurückhaltender, in der Sache aber wohl identisch *Lenz*, in: *Lenz*, Produkthaftung, § 4, Rn. 52; *Xia*, Die Pflicht zum Produktrückruf, S. 46 weist darauf hin, dass die Argumentation juristisch zu verstehen ist und sich in der Praxis ein umgekehrtes Bild zeigen kann; in tatsächlicher Hinsicht anders auch *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 280.

1160 BGH, NJW 2009, 1080 (1081, Rn. 11): „können etwa dann weiter gehen“.

Warnung den Produktnutzern nicht ausreichend ermöglicht, die Gefahr einzuschätzen und ihr Verhalten darauf einzurichten.¹¹⁶¹

Schon im Ausgangspunkt kann eine Warnung beim Verwender kein Gefahrenbewusstsein schaffen, wenn der Hersteller bereits weder die Gefahr noch wirksame Maßnahmen zu ihrer Beseitigung darstellen kann, etwa weil er selbst den Produktfehler und seine Auswirkungen noch nicht hinreichend beurteilen kann.¹¹⁶² Eine Warnung, die aufgrund mangelnden Erkenntniswissens beim Hersteller über die Gefahr nicht hinreichend deutlich und detailliert erfolgen kann, versetzt den Produktnutzer schon nicht in die Lage, die drohenden Gefahren und mögliche Folgen zu erkennen und sein Verhalten daran auszurichten.¹¹⁶³

Welche Konstellationen der BGH darüber hinaus selbst im Blick hatte, ergibt sich aus den in den Entscheidungsgründen angeführten Belegen. Dabei sind zunächst Sonderfälle gemeint, in denen die bloße Warnung die zunächst bestehende Informationsasymmetrie hinsichtlich der Gefahrenträchtigkeit des Produkts zwischen Hersteller und Nutzer nicht hinreichend effizient ausgleichen kann. Dies ist zum einen dann der Fall, wenn bereits aufgrund konstruktiver Schwächen des Produkts Gefahren trotz deutlicher und wahrgenommener Warnung leicht und immer wieder in der Verwendung übersehen werden können,¹¹⁶⁴ das Produkt also so beschaffen ist, dass die Warnung nur schwer Gefahrenbewusstsein schaffen kann.¹¹⁶⁵ Zum anderen wird die gefährdete Personengruppe in den Fokus genommen und weitergehende Pflichten für möglich gehalten, sollten diese – man denke an Kinder, welche die Produkte nutzen – nur eingeschränkt in der Lage sind, die Gefahr auf die Warnung hin selbst zu steuern.¹¹⁶⁶

1161 BGH, NJW 2009, 1080 (1081, Rn. 11).

1162 Zwar vom BGH nicht aufgegriffen, so aber *Lüftenegger*, Die Rückruffpflicht des Herstellers, S. 219.

1163 Dies entspricht der Linie des BGH zur komplementär zu beurteilenden Instruktionspflicht (vgl. dazu *Ackermann*, in: NK-ProdR, § 823 BGB, Rn. 133), wo „jedenfalls in den Fällen, in denen erhebliche Körper- oder Gesundheitsschäden durch eine Fehlanwendung des Produkts entstehen können, auch die Funktionszusammenhänge klar gemacht werden [müssen], so daß erkennbar wird, warum das Produkt gefährlich ist“ (BGH, NJW 1992, 560 (561)); vgl. auch *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 255 f.

1164 Insoweit wird auf BGH NJW 1994, 3349 verwiesen, wo konstruktiv ein Stecker versehentlich leicht in eine falsche Steckdose gesteckt werden konnte.

1165 Dazu *Lüftenegger*, Die Rückruffpflicht des Herstellers, S. 220.

1166 Ein Hinweis hierzu findet sich auch in der zitierten Rspr. BGH NJW 1994, 3349 (351), ergibt sich aber v.a. aus den zitierten Literaturfundstellen, insbesondere

Ferner soll es Konstellationen geben, in denen eine Warnung zwar die Informationsasymmetrie ausgleichen kann, der Benutzer aber trotzdem nicht in der Lage ist, die Gefahr zu vermeiden oder zu entscheiden, ob er sich ihr aussetzt.¹¹⁶⁷ In der Literatur wird versucht, diese Konstellation mit Leben zu füllen, indem auf Fälle abgehoben wird, in denen die Gefahr trotz Nichtbenutzens des Produkts fortbesteht oder das Nichtbenutzen als Selbstschutzmaßnahme schlicht nicht möglich ist und der Produktnutzer der Gefahr daher nicht ausweichen kann.¹¹⁶⁸ Bereits hier zeigt sich aber eine schwierige Grenzziehung. Denn dass eine Nichtbenutzung die Gefahr nicht beseitigt, dürfte in den allerseltensten Konstellationen der Fall sein.¹¹⁶⁹ Regelmäßig kann der ausreichend gewarnte Nutzer durch die schlichte Nichtnutzung selbst verhindern, dass sich das identifizierte Risiko im Schadensereignis realisiert.¹¹⁷⁰ In diesem Zusammenhang wird etwa angeführt, dass man nicht aus seiner Wohnung ausziehen könne, wenn von der Baustoffsubstanz aufgrund verwendeter giftiger Materialien Gefahren ausgingen.¹¹⁷¹ Allerdings ist es auch hier möglich, seinem Grundstück schlicht fernzubleiben, um einen Schadenseintritt zu verhüten.¹¹⁷² Ein aus der Nichtbenutzung für den Nutzer resultierender Schaden ist nämlich unbeachtlich, da dieser allein auf die Mangelhaftigkeit des Produkts bei Erwerb zurückzuführen ist und daher allein die enttäuschte Vertragserwartung betrifft.¹¹⁷³ Damit rücken aber Fallkonstellationen in den Vordergrund, in denen die Nichtbenutzung des gefährlichen Produkts zwar möglich, für den Gewarnten aber unzumutbar erscheint. Indes hat die Warnung in diesen Fällen in tatsächlicher Hinsicht für eine hinreichende Gefahrenkenntnis und Gefahrensteuerungsmöglichkeit gesorgt. Damit ist die Warnung aber nicht aus sich heraus als Informationsmedium unzureichend, vielmehr ergibt sich ihre Ineffektivität aus Gründen, die in der Sphäre des Nutzers liegen. Die

Bodewig, Der Rückruf fehlerhafter Produkte, S. 268, vgl. *Lüftenegger*, Die Rückrufpflicht des Herstellers, S. 220.

1167 Auch diese Fallgruppe ergibt sich aus einem Verweis auf *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 257, 268.

1168 *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 257; *Lüftenegger*, Die Rückrufpflicht des Herstellers, S. 220; *Voigt*, in: BeckOGK, BGB, § 823, Rn. 681; *Reusch*, BB 2017, 2248 (2252) sieht sogar alleinig hier eine Warnung für nicht ausreichend an.

1169 Vgl. ausführlicher unter E.II.6.a).

1170 *Klindt*, BB 2009, 792 (793).

1171 So *Hager*, in: Staudinger, BGB, § 823, Rn. F 25.

1172 Krit. daher *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), Produkthaftungshandbuch, § 24, Rn. 336, 346.

1173 BGH, NJW 2009, 1080 (1083, Rn. 25).

für den Nutzer unzumutbare Gefahrensteuerung kann damit nicht mit Fällen der tatsächlich unmöglichen Gefahrensteuerung gleichgestellt werden.¹¹⁷⁴ Gleichwohl kann die unzumutbare Gefahrensteuerung als eigene Fallgruppe unter weiteren Voraussetzungen Berücksichtigung finden.

bb) Hinwegsetzen über eine Warnung

Auch wenn eine Warnung ausreichende Gefahrenkenntnis schafft und dem Nutzer die Gefahrensteuerung ermöglicht, kann sie zur Gefahrenabwehr nicht hinreichend effektiv sein. Denn es kann Konstellationen geben, in denen sich der informierte Produktnutzer über eine Warnung hinwegsetzt, sodass weiterhin Gefahren von dem Produkt und seiner Verwendung ausgehen. So kommen weitergehende Sicherungspflichten in Betracht, wenn Grund zur Annahme besteht, dass sich die Produktnutzer – auch bewusst – über die Warnung hinwegsetzen und dadurch Dritte gefährden.¹¹⁷⁵

Allerdings ist zum einen die Tragweite dieser Konstellation schwer zu ermessen,¹¹⁷⁶ da offen bleibt, anhand welcher Kriterien zu beurteilen ist, in welchen Situation sich ein Produktnutzer nachvollziehbarerweise über eine verstandene Warnung hinwegsetzen wird. Zum anderen bestehen auch dogmatische Bedenken, bei einem solchen Fehlverhalten des Nutzers von einer weitergehenden Verantwortung des Herstellers auszugehen.¹¹⁷⁷

(1) Drittgefährdung als zentrale Voraussetzung

Zunächst kommt bei einem Hinwegsetzen über eine Warnung der Drittgefährdung maßgebliche Bedeutung zu.

1174 So wohl auch der BGH, der das Hinwegsetzen über eine Warnung als eigene Fallgruppe bei vorhandener Gefahrensteuerungsmöglichkeit diskutiert, vgl. BGH, NJW 2009, 1080 (1081, Rn. 11).

1175 BGH, NJW 2009, 1080 (1081, Rn. 11); anders noch LG Frankfurt a.M., BeckRS 2008, 2795, wonach „die aus der Weiternutzung resultierende Gefährdungshaftung aufgrund der von der Klägerin [=Herstellerin] ergriffenen Maßnahmen auf den Nutzer übergehen“, zustimmend *Handorn*, MPR 2009, 37 (42).

1176 So *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), *Produkthaftungsbandbuch*, § 24, Rn. 338.

1177 *Lüftenegger*, *Die Rückrufpflicht des Herstellers*, S. 230 nennt dies „[b]emerkenswert“.

Denn in Fällen der Drittgefährdung bestehen gerade unzureichende Selbstschutzmöglichkeiten der Dritten. Hierin besteht der Grund der erweiterten Sicherungspflichten. Denn Dritte werden von einer Warnung regelmäßig nicht erreicht bzw. haben auch bei einer öffentlichen Warnung¹¹⁷⁸ regelmäßig keinen Einfluss darauf, die Gefahr zu verhindern oder ihr auszuweichen.¹¹⁷⁹ Die Annahme weitergehender Sicherungspflichten steht in diesem Fall ganz im Zeichen der Effektivität der Gefahrenabwendung. Zwar mag auch der über die Produktgefahren informierte Nutzer eigene Pflichten der Allgemeinheit gegenüber haben. Ein solch nachträglicher Haftungsübergang kann allerdings bei der Beurteilung präventiver Gefahrenabwehrmaßnahmen nur nachgelagerte Bedeutung zukommen.¹¹⁸⁰ Ein dem unbeteiligten Geschädigten gegen den Nutzer zugebilligter Schadensersatz verhindert den Schaden nämlich nicht, sondern liquidiert ihn lediglich.¹¹⁸¹ In diesen Fällen darf sich der Hersteller nicht auf die Gefahrensteuerung durch den Nutzer verlassen, sondern muss unmittelbar selbst auf den Gefahrenherd einwirken.¹¹⁸² Mit einem größeren – weil über das alleinige Integritätsinteresse des Produktnutzers hinausgehenden – Gefährdungspotential geht auch ein erweiterter Pflichtenumfang des Herstellers einher.¹¹⁸³

Von einer Unterbrechung des Kausal- bzw. Zurechnungszusammenhangs durch die weitere Verwendung des gefährlichen Produkts durch den gewarnten Produktnutzer ist damit nicht auszugehen.¹¹⁸⁴ Andernfalls bliebe eine Verletzung der über die Warnung hinausgehenden Sicherungspflicht des Herstellers unberücksichtigt.¹¹⁸⁵ Dies stellt sich auch vor dem Hinter-

1178 Eine solche aber hält *Handorn*, MPR 2009, 37 (42) in dieser Konstellation für ausreichend.

1179 *Lüftenegger*, Die Rückrufpflicht des Herstellers, S. 222; *Lüftenegger*, NJW 2018, 2087 (2090); *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 266 f.; *Meents/Obradovic*, ZfPC 2022, 13 (17 f.); auch *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), *Produkthaftungshandbuch*, § 24, Rn. 358 hält daher in dieser Konstellation eine Rückrufpflicht für „am ehesten denkbar“; ähnlich *Burckhardt*, VersR 2007, 1601 (Fn. 40).

1180 *Burckhardt*, VersR 2007, 1601.

1181 In diese Richtung auch *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 267; diesem Umstand schenken *Pieper*, BB 1991, 985 (989) und *Molitoris*, NJW 2009, 1049 (1051) indes zu wenig Bedeutung.

1182 So schon v. *Bar*, in: *Lieb* (Hg.), *Produktverantwortung und Risikoakzeptanz*, S. 29 (41).

1183 *Lüftenegger*, NJW 2018, 2087 (2090).

1184 Sehr krit. *Klindt*, BB 2009, 792 (794, Fn. 21).

1185 Konsequente Folgerung bei *Kettler*, VersR 2009, 272 (275).

grund der allgemeinen Dogmatik als konsequent dar.¹¹⁸⁶ Denn durch das Inverkehrbringen eines gefährlichen Produkts schafft der Hersteller erst die entscheidende Ursache für den Schadensverlauf, auf den der unbeteiligte Dritte keinen Einfluss nehmen kann, sodass eine gänzliche Verlagerung der Verantwortung auf den Produktnutzer ausscheiden muss.¹¹⁸⁷ Es lässt sich eben von einer besonderen Gefahrenlage sprechen, die der Hersteller geschaffen hat und die es dem Produktnutzer erst ermöglicht, eine nachträgliche Warnung in den Wind zu schlagen. Hinzu kommt, dass beim Hinwegsetzen über die Warnung ohnehin nur solche Fälle berücksichtigt werden, bei denen dieses Verhalten noch dem entspricht, was nach der allgemeinen Lebenserfahrung vorhersehbar ist.

Dagegen kommt dem Kriterium des Hinwegsetzens über eine Warnung bei alleiniger Gefährdung des Produktnutzers keine Bedeutung zu.¹¹⁸⁸ Der entscheidende Unterschied bei der Beurteilung der Frage nach der Unterbrechung des Kausalzusammenhangs liegt dabei in der Perspektive. Während sich das Hinwegsetzen des Nutzers über eine Warnung aus der Sicht anderer Geschädigter als Fehlverhalten eines Dritten darstellt, handelt es sich gegenüber dem Nutzer selbst um einen vorsätzlichen – wenn auch häufig vorhersehbaren – Missbrauch.¹¹⁸⁹ Nach allgemeinen Grundsätzen sind Sicherungsmaßnahmen gegenüber sich selbst schädigenden Personen allerdings nur zur Abwendung eines vorhersehbaren und nahe liegenden Fehlverhaltens geboten, während zum Schutz unbeteiligter Dritter auch vorsätzlich-missbräuchliches Fehlverhalten zu berücksichtigen ist.¹¹⁹⁰ Eben diese unterschiedlichen Sorgfaltsanforderungen zeichnet auch der BGH bei seiner Fallgruppenbildung hinsichtlich der Rückruffpflichten nach. Er differenziert zwischen Rückruffpflichten zu Gunsten des Nutzers bei fehlender Möglichkeit zur Gefahreinschätzung und Verhaltensanpassung durch eine Warnung einerseits und Rückruffpflichten zu Gunsten Dritter beim Hinwegsetzen über eine Warnung durch den Produktnutzer anderer-

1186 Anders Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 360 f.

1187 Stöhr, in: FS Müller, S. 173 (185); Lüftenegger, NJW 2018, 2087 (2090); in diese Richtung auch Schwenzler, JZ 1987, 1059 (1061); i.E. auch Huber, Rechtsfragen des Produktrückrufs, S. 47 ff. und Xia, Die Pflicht zum Produktrückruf, S. 37.

1188 Dogmatisch stellt sich dabei die Frage, ob die entsprechende Selbstschutzmöglichkeit des Nutzers die Verkehrspflicht entfallen lässt oder lediglich im Rahmen des Mitverschuldens nach § 254 BGB zu berücksichtigen ist, vgl. allgemein Larenz/Canaris, Lehrbuch des Schuldrechts II/2, S. 414 f.

1189 Dies gerade aber verkennt Schmidt, Produktrückruf und Regress, S. 80.

1190 Vgl. oben C.III.2.d)bb)(2)α).

seits.¹¹⁹¹ Dass allein das Hinwegsetzen über eine Warnung für die Annahme von Rückruffpflichten nicht ausreichend ist, macht der BGH sprachlich deutlich, indem er die Gefährdung Dritter gerade als kumulative Voraussetzung („und dadurch Dritte gefährden“) formuliert.¹¹⁹² Hier bestehen die weitergehenden Sicherungspflichten nicht zum Schutz des selbst zur Gefahrensteuerung in der Lage befindlichen Produktnutzers, sondern mit dem Ziel, unbeteiligte Dritte zu schützen. Umgekehrt entstehen folglich weitergehende Pflichten des Herstellers regelmäßig nicht, wenn der Produktnutzer sich durch das Hinwegsetzen über die Warnung alleinig selbst gefährdet.¹¹⁹³ Hierin spiegelt sich der produkthaftungsrechtliche Grundsatz wider, dass der Produktnutzer grundsätzlich für die Beherrschung der Gefahren in der Nutzungsphase gegenüber sich selbst verantwortlich ist.¹¹⁹⁴

(2) Übereinstimmung mit Systematik des Produkthaftungsrechts

Damit hat der Hersteller im Rahmen seiner Reaktionspflichten ein voraussichtlich nicht konformes Verhalten des Produktnutzers zu berücksichtigen. Inwieweit sich dies in die Systematik des Produkthaftungsrechts einfügt, soll im Folgenden untersucht werden.

α) Vergleich mit Instruktionspflicht

Betrachtet man die Warnung, so drängt sich ein struktureller Vergleich mit der Instruktionspflicht vor der Inverkehrgabe auf. In beiden Fällen geht von dem Produkt eine Gefahr aus und besteht hinsichtlich der Gefahrenkenntnis eine Informationsasymmetrie zwischen Hersteller und Nutzer, die durch die Warnung bzw. Instruktion ausgeglichen werden soll. Der Pro-

1191 Vgl. BGH, NJW 2009, 1080 (1081, Rn. 11).

1192 BGH, NJW 2009, 1080 (1081, Rn. 11).

1193 So bereits *Tamme*, Rückrufkosten, S. 77 ff.; anders noch *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 257, 268 ff., der nachfolgende Fallgruppen auch bei der bloßen Gefährdung des Nutzers für relevant hält; wie hier *Lüftenegger*, Die Rückruffpflicht des Herstellers, S. 215; wohl auch *Stöhr*, in: FS Müller, S. 173 (184); anders, allerdings ohne Auseinandersetzung mit dem Wortlaut des BGH *Schmidt*, Produktrückruf und Regress, S. 83 und *Xia*, Die Pflicht zum Produktrückruf, S. 81 f., die im Fall der Drittgefährdung zwar eher zu Rückruffpflichten kommen, diese aber nicht als fallentscheidend ansehen.

1194 Vgl. *Lüftenegger*, Die Rückruffpflicht des Herstellers, S. 215.

duktnutzer wird dabei durch die Information zur eigenverantwortlichen Gefahrensteuerung befähigt.¹¹⁹⁵

Auch im Rahmen der Instruktionspflicht erweitert sich der Pflichtenkreis des Herstellers mit Blick auf ein Fehlverhalten des Nutzers bei der Verwendung. So hat der Hersteller den Nutzer auch hinsichtlich eines naheliegenden Fehlgebrauchs – sollte dieser nicht schon (zumutbar) konstruktiv ausgeschlossen werden können – zu instruieren. Eine Ausnahme vom Prinzip, dass der Produktnutzer nicht vor selbstverschuldeten Gefahren geschützt werden muss, ist also keine Neuschöpfung der Pflegebetten-Entscheidung.¹¹⁹⁶ Allerdings sind die Herstellerpflichten beim bestimmungswidrigen Gebrauch begrenzt. Der Hersteller hat weder vor Schadensrisiken zu warnen, die so offensichtlich zu Tage treten, dass sie zum allgemeinen Gefahrenwissen der Produktnutzer gehören, noch vor missbräuchlicher Verwendung des Produkts. Nach oben hin endet damit die Herstellerverantwortung bei der Überschreitung des naheliegenden Fehlgebrauchs. Stellt sich der Fehlgebrauch als äußert leichtfertig oder vorsätzlich dar,¹¹⁹⁷ wird der Hersteller nicht mehr als Verantwortlicher betrachtet, sondern wird die eigentliche Gefahrenquelle im Verhalten des Produktnutzers gesehen.¹¹⁹⁸ Erst recht missbräuchlich handelt ein Nutzer, der sich über eine Warnung hinsichtlich des naheliegenden Fehlgebrauchs hinwegsetzt und das Produkt instruktionswidrig verwendet. Auch hier trifft den Hersteller keine Verantwortlichkeit. Anders geht der BGH in seiner Pflegebetten-Entscheidung vor, indem er bei einem bewussten Hinwegsetzen über eine Warnung dem Hersteller weitere Sicherungspflichten aufgibt, obwohl dieses Fehlverhalten des Nutzers die anfängliche herstellereitige Instruktionsverantwortung nicht auslösen würde, sondern als missbräuchliches Verhalten gewertet werden würde.¹¹⁹⁹ Insoweit wirkt sich ein missbräuchliches Fehlverhalten des Nutzers trotz der strukturellen Vergleichbarkeit von anfänglicher Instruktion und Warnung als Reaktionspflicht unterschiedlich auf den Pflichtenkreis des Herstellers aus. Eine Widersprüchlichkeit mag man auch mit Blick auf einen anfänglichen Instruktionsfehler ausmachen. Dieser kann

1195 Zur Vergleichbarkeit *Lüftenegger*, Die Rückrufpflicht des Herstellers, S. 232.

1196 *Xia*, Die Pflicht zum Produktrückruf, S. 53; vgl. auch *Lüftenegger*, Die Rückrufpflicht des Herstellers, S. 231.

1197 Vgl. BGH, NJW 1999, 2815 (2816).

1198 *Oechsler*, in: Staudinger, BGB, § 3 ProdHaftG, Rn. 64; OLG Bamberg, NJW-RR 2010, 902 (903).

1199 Plakativ *Klindt*, BB 2009, 792 (794 f.); *Lüftenegger*, Die Rückrufpflicht des Herstellers, S. 232 ff.

durch die schlichte Nachholung der Information korrigiert werden, ohne dass ein mögliches Hinwegsetzen über eine solche nachgelieferte Warnung überhaupt diskutiert wird.¹²⁰⁰ Schon gar nicht werden in diesem Fall weitergehende Reaktionsmaßnahmen in Betracht gezogen, sondern reicht es aus, dass eine Warnung deutlicher erfolgt oder prominenter platziert wird.¹²⁰¹ Indes war bei einem Instruktionsfehler anfänglich eben auch nur die Instruktion geschuldet, sodass ein nachträgliches Mehr an Reaktion nicht sachgerecht wäre.

Aber auch im Übrigen greift es zu kurz, einen Bruch mit der Systematik des Produkthaftungsrechts auszumachen.¹²⁰² Denn die Vergleichbarkeit dürfte sich gerade auf die strukturelle Natur erschöpfen. Hinsichtlich der unterschiedlichen Berücksichtigung des Missbrauchs durch den Produkt-nutzer divergieren schon die Ausgangslagen. Eine anfängliche Instruktion gibt dem Nutzer zumindest die Möglichkeit, einen erfolgten Warnhinweis in seine Kaufentscheidung einzubeziehen und vom Erwerb abzusehen, sollte sich die von ihm beabsichtigte Verwendung nicht innerhalb der Grenzen der allgemeinen Zweckbestimmung des Produkts halten und daher gefährlich sein.¹²⁰³ Dagegen soll eine nachträgliche Warnung den Nutzer gerade davon abhalten, das Produkt entsprechend seiner allgemeinen Zweckbestimmung zu benutzen. Aufgrund seiner Gefährlichkeit soll der Nutzer das Produkt gar nicht mehr benutzen. Selbst im Rahmen der anfänglichen Instruktion ist die Herstellerverantwortung umso eher angesprochen, je näher der Fehlgebrauch am eigentlichen bestimmungsgemäßen Gebrauch erfolgt.¹²⁰⁴ Zudem wird die psychologische Hemmschwelle, ein bereits erworbenes Produkt ersatzlos nicht mehr zu benutzen, regelmäßig höher sein, als ein Produkt von vorneherein gar nicht zu erwerben.¹²⁰⁵ Darüber hinaus ist auch die Schutzrichtung, warum der Hersteller ein pflichtwidriges Verhalten des Nutzers berücksichtigen muss, eine Unterschiedliche. Die Instruktion beim naheliegenden Fehlgebrauch dient in erster Linie dem

1200 Vgl. *Klindt*, BB 2009, 792 (795).

1201 Vgl. *Lüftenegger*, Die Rückruffpflicht des Herstellers, S. 233.

1202 So aber *Lüftenegger*, Die Rückruffpflicht des Herstellers, S. 234.

1203 *Xia*, Die Pflicht zum Produktrückruf, S. 54; *Klindt*, BB 2009, 792 (Fn. 18) weist dagegen darauf hin, dass nachträgliche Warnungen (wenn denn gelesen) sogar wohl eine größere Wahrnehmungsintensität als eine beigelegte Instruktion haben.

1204 Vgl. dazu mit Beispielen aus der Rspr. *Taeger*, in: NK-ProdR, § 3 ProdHaftG, Rn. 42.

1205 *Xia*, Die Pflicht zum Produktrückruf, S. 54; auf der anderen Seite weist *Klindt*, BB 2009, 792 (Fn. 18) darauf hin, dass nachträgliche Warnungen wohl sogar eine größere Wahrnehmungsintensität als eine beigelegte anfängliche Instruktion haben.

Schutz des Produktnutzers bei der Verwendung des Produkts und schützt die Allgemeinheit nur reflexartig dadurch, dass der Nutzer das Produkt auch nicht in drittgefährdender Weise verwendet. Dagegen zielen die weitergehenden Reaktionspflichten des Herstellers bei einem vermuteten Hinwegsetzen über eine Warnung gerade ausschließlich auf den Schutz Dritter ab,¹²⁰⁶ wo eben auch vorsätzlich-missbräuchliches Fehlverhalten zu berücksichtigen ist (s.o.). Vor diesem Hintergrund lässt sich eine Ausweitung der Herstellerverantwortung auch bei einem missbräuchlichen Hinwegsetzen des Nutzers über eine Warnung rechtfertigen.

β) Objektiv zu bestimmende Sorgfaltsanforderungen

Dem Kriterium des Hinwegsetzens über eine Warnung Bedeutung bei der Bemessung des Pflichtenumfangs zukommen zu lassen, wird eine systemwidrige Subjektivierung objektiver Sorgfaltsanforderungen nachgesagt.¹²⁰⁷ Zu einer solchen Subjektivierung mag es zwar kommen, wenn man die Sorgfaltspflicht des Herstellers tatsächlich an der subjektiven Lustlosigkeit oder Ignoranz des individuellen Produktnutzers ausrichtet, eine nachträgliche Warnung zu befolgen.¹²⁰⁸ Einer Subjektivierung kann indes dadurch begegnet werden, dass die Fälle, in denen ein „Grund zu der Annahme besteht“, nach objektivierten Kriterien bestimmt werden. Insoweit ist die richtige Perspektive einzunehmen. Es kommt nicht maßgeblich auf ein möglicherweise unvernünftiges Verhalten eines individuellen Nutzers an, sondern darauf, ob der Hersteller anhand objektiver Kriterien damit rechnen muss, dass eine Warnung missachtet wird.¹²⁰⁹ Insoweit ist es auch

1206 Diese unterschiedliche Schutzrichtung sieht auch *Lüftenegger*, Die Rückrufpflicht des Herstellers, S. 234, ohne aber daraus eine Rechtfertigung für eine unterschiedliche Behandlung der Konstellationen zu ziehen.

1207 Deutlich *Klindt*, BB 2009, 792 (795) bei der „richterrechtlich entwickelte Figur der Verkehrssicherungspflicht – geht es immer um verobjektivierbare Pflichten, nicht um subjektive Bequemlichkeiten“; ähnlich *Lüftenegger*, Die Rückrufpflicht des Herstellers, S. 236 f.

1208 Dies unterstellt jedenfalls *Klindt*, BB 2009, 792 (794 f.) der Pflegebetten-Entscheidung; auch *Handorn*, MPR 2009, 37 (42) lehnt die Fallgruppe des BGH dagegen ab; dagegen aber *Lüftenegger*, Die Rückrufpflicht des Herstellers, S. 223 und *Lüftenegger*, NJW 2018, 2087 (2090).

1209 In diese Richtung auch *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 168 und *Xia*, Die Pflicht zum Produktrückruf, S. 55.

gerade Aufgabe der objektiv zu bestimmenden Sorgfaltspflichten, einer in der Praxis eingerissenen Nachlässigkeit entgegenzuwirken.¹²¹⁰

Entscheidend ist damit, in welchem Ausmaß sich der Hersteller berechtigterweise auf die Gefahrensteuerung durch andere verlassen darf.¹²¹¹ Mit der Wahl dieser Perspektive kann auch dem Argument begegnet werden, dass im Ergebnis unvernünftiges Verhalten prämiert werde, indem Nutzer, die eine Warnung bewusst ignorieren, besser gestellt werden als diejenigen, die einer Warnung Folge leisten und die Nutzung einstellen.¹²¹² Nicht die Gruppe der Nutzer, die sich irrational und ignorant darstellt, soll mit einem Rückruf bedacht werden, sondern die Gruppe, bei der aufgrund objektiver Kriterien davon auszugehen ist, dass sie sich über eine Warnung hinwegsetzt.¹²¹³ So verstanden wird es auch weniger um Ignoranz als vielmehr um aner kennenswerte Gründe gehen, einer Warnung nicht Folge zu leisten. Mit der hier dargestellten Auslegung entsteht auch kein Missbrauchspotential oder eine Anreizwirkung dahingehend, dass Nutzer bewusst eine Weiternutzung anstreben könnte, um den Pflichtenkreis des Herstellers hin zu einem Rückruf zu erweitern.¹²¹⁴ Die Objektivität der Verkehrspflichten anzuerkennen, bedeutet demnach nicht, die Geeignetheit des vom BGH gewählten Maßstabs generell in Zweifel zu ziehen, sondern ist lediglich bei der Ausfüllung zu berücksichtigen.

(3) „Grund zu der Annahme“

Bereits aufgezeigt wurde, dass irrationale Motive der Produktnutzer, die Warnung zu ignorieren, nicht zu weitergehenden Handlungspflichten des Herstellers führen können. Insoweit ist es nicht Sache des Herstellers, seine Gefahrenabwehrmaßnahme so attraktiv wie möglich auszugestalten, um einem bewussten Fehlverhalten des Nutzers entgegenzuwirken.¹²¹⁵ Es stellt sich daran anschließend aber die Frage, nach welchen objektiven Kriterien

1210 Allgemein *Grundmann*, in: MüKo, BGB, § 276, Rn. 38.

1211 So auch *v. Bar*, in: Lieb (Hg.), Produktverantwortung und Risikoakzeptanz, S. 29 (42).

1212 So aber *Wagner*, JZ 2009, 905 (910); angedeutet auch bei *Thürmann*, NVersZ 1999, 145 (146).

1213 In diese Richtung auch *Lüftenegger*, NJW 2018, 2087 (2091).

1214 Aufgeworfen, wenn gleich in der Sache relativiert von *Eichelberger*, in: *Ebers et al.*, (Hg.), Künstliche Intelligenz und Robotik, S. 190 und *Lüftenegger*, Die Rückrufpflicht des Herstellers, S. 238 ff.

1215 So auch *Lüftenegger*, Die Rückrufpflicht des Herstellers, S. 222 f.

zu bestimmen ist, ob sich ein Produktnutzer über eine Warnung hinwegsetzen wird. Denn jedenfalls im Ausgangspunkt wird ein Eigeninteresse des Nutzers bestehen, sich durch die Verwendung eines gefährlichen Produkts nicht eigenen Schadensrisiken auszusetzen und sich nicht durch eine gefährliche Weiterverwendung Dritten gegenüber schadensersatzpflichtig zu machen.¹²¹⁶

Erkennt man mit dem BGH an, dass das Hinwegsetzen über eine Warnung als Missbrauch durch den Produktnutzer die Reaktionspflichten des Herstellers erweitert, liegt es nahe, dies jedenfalls nur bei einem naheliegenden bzw. vorhersehbaren Hinwegsetzen über die Warnung zu tun. Das Kriterium der Vorhersehbarkeit wird auch im Rahmen des bestimmungswidrigen Gebrauchs herangezogen, um eine Ausnahme von dem Prinzip, dass der Produktnutzer vor selbstverschuldeten Gefahren nicht geschützt werden muss, zu begründen. Es liegt daher nahe, die Herstellerverantwortung beim Missbrauch als gesteigerter Form des Fehlgebrauchs auch davon abhängig zu machen, ob mit diesem billigerweise noch gerechnet werden muss, er also vorhersehbar oder üblich ist.¹²¹⁷ Mit der Warnung nimmt der Hersteller zwar eine Entwidmung des Produkts für den allgemeinen Verwendungszweck vor, sodass eine Weiternutzung als Missbrauch einzuordnen ist.¹²¹⁸ Dies sagt aber noch nichts darüber aus, ob eine Weiternutzung und damit ein Missbrauch aufgrund bestimmter Faktoren naheliegend sein kann und daher mit Blick auf die Drittfährdung eine Warnung nicht mehr ausreichend ist.

α) Verkenntung der Produktgefahr

Ein vorhersehbares Hinwegsetzen über eine Warnung kommt zunächst bei einer drohenden Verkenntung der Produktgefahr in Betracht.¹²¹⁹ Gemeint sind Fälle, in denen die Warnung zwar die bestehende Informationsasymmetrie hinreichend ausgleicht und den Nutzer zur eigenen Gefahrensteue-

1216 Arbeitsgruppe „Digitaler Neustart“, Bericht vom 15. April 2019, S. 198.

1217 Dass sich Missbrauch und Vorhersehbarkeit nicht zwangsläufig ausschließen, zeigt die Sniffing-Entscheidung des BGH, vgl. BGH, NJW 1981, 2514 (2516); vgl. zum naheliegenden Missbrauch auch BGH, NJW 1972, 2217 (2221).

1218 Ähnlich Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 345, 361.

1219 Lüftenegger, Die Rückrufflicht des Herstellers, S. 224 f.; Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 360.

rung befähigt, in denen es gleichwohl zu befürchten gilt, dass der Produkt-
nutzer die Gefahr herunterspielen wird.¹²²⁰

Ein solches Verhalten liegt insbesondere dann nahe, wenn für den Nutzer keine Anhaltspunkte gegeben sind, dass gerade sein individuelles Produkt fehlerhaft ist.¹²²¹ Dies ist insbesondere bei Produkten möglich, die bereits über längere Zeit einwandfrei funktioniert haben und bei denen zudem kein Konstruktions-, sondern ein Fabrikationsfehler vorliegt.¹²²² Ob einem solchen Herunterspielen der Gefahr tatsächlich mit einer deutlich oder gar drastisch formulierten Warnung entgegengewirkt werden kann, darf bezweifelt werden.¹²²³ Insoweit ist nämlich zwischen dem vorhandenen Gefahrenbewusstsein und der falschen Gefahreinschätzung zu trennen. Ein Gefahrenbewusstsein liegt bei den Nutzern in diesen Fällen vor. Allerdings schätzen sie die individuelle Eintrittswahrscheinlichkeit einer Rechtsverletzung als gering ein. Einem solchen Verständnis wird aber auch mit einer noch so drastischen Warnung nicht begegnet werden können, da der Hersteller schon darlegen müsste, warum gerade das Produkt des individuellen Nutzers betroffen sein sollte und er daher gerade bei sich mit einer Verwirklichung der Produktgefahr zu rechnen hat. Eine solch eindeutige Identifizierung der fehlerhaften Produkte ist ihm aber gerade bei einem Fabrikationsfehler regelmäßig nicht möglich.

β) Unzumutbare Gefahrensteuerung

In diesem Zusammenhang ist auch eine für den Produktnutzer unzumutbare Gefahrensteuerung zu diskutieren. Kommt für den Nutzer im Rahmen der Gefahrensteuerung lediglich die Nichtbenutzung des Produkts in Betracht und stellt sich diese für den Nutzer als unzumutbar heraus, mag er geneigt sein, sich über eine Warnung hinwegzusetzen.¹²²⁴ Die entscheidende Frage wird daher sein, anhand welcher Kriterien die Unzumutbarkeit der Nichtnutzung objektiviert werden kann, um eine Weiternutzung als naheliegend einstufen zu können, mit der der Hersteller rechnen muss.

1220 Vgl. auch Bodewig, Der Rückruf fehlerhafter Produkte, S. 271.

1221 Lüftenegger, Die Rückrufpflicht des Herstellers, S. 224.

1222 Stöhr, in: FS Müller, S. 173 (183); Lüftenegger, Die Rückrufpflicht des Herstellers, S. 224; Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 360.

1223 So aber Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 360.

1224 Vgl. auch Bodewig, Der Rückruf fehlerhafter Produkte, S. 271.

Ausgangspunkt der Überlegung ist, dass es Fälle geben kann, in denen dem Nutzer eine eigenständige Behebung der Produktgefahr kaum oder nur äußerst schwierig möglich ist, er also bei der Fehlerbehebung auf Angebote des Herstellers angewiesen ist. Lässt sich die Sicherheit des Produkts aber auf eine Warnung des Herstellers hin nicht durch den Nutzer selbst und auch nicht unter Zuhilfenahme Dritter als Fachleute herstellen, lässt sich der Warnung eine Ineffektivität attestieren, wenn das Produkt in Betrieb bleiben soll.¹²²⁵ Denn in solchen Konstellationen verbleibt dem Nutzer keine andere Möglichkeit, als im Rahmen der Gefahrensteuerung auf die Nutzung des Produkts zu verzichten. Ist das Produkt aber gleichermaßen von zentraler Bedeutung für die Lebensführung¹²²⁶ und eine Ersatzbeschaffung aufgrund eines hohen Produktpreises für die Nutzer nicht tragbar, ist es für den Hersteller erwartbar, dass eine Vielzahl der Nutzer den Gebrauch nicht einstellen werden.¹²²⁷ Ein Hinwegsetzen über die Warnung kommt dann nicht unter dem Aspekt der als gering eingestuft individuellen Eintrittswahrscheinlichkeit in Betracht, sondern aufgrund einer ausgeblendeten Eintrittswahrscheinlichkeit.¹²²⁸ Die Angewiesenheit bei der Fehlerbeseitigung auf den Hersteller sowie die Angewiesenheit auf die Nutzung des Produkts und ein hoher Produktpreis sind demnach Faktoren, die ein Hinwegsetzen über eine Warnung als naheliegend erscheinen lassen. Dabei ist es dem Produkthaftungsrecht nicht fremd, die überlegenen Gefahrensteuerungsmöglichkeiten des Herstellers im Vergleich zum Produktnutzer als Rechtfertigung für weitergehende Pflichten anzunehmen; dies geschieht auch im Rahmen des bestimmungswidrigen Gebrauchs.¹²²⁹ Außerdem wird die typische Angewiesenheit für die eigenwirtschaftliche Lebensführung in der Rechtsprechung bereits herangezogen; nämlich bei der Anerkennung einer abstrakten Nutzungsausfallentschädigung.¹²³⁰ Auch im hiesigen Kontext trägt das Kriterium zur notwendigen Objektivierung bei.

1225 Vgl. *Gomille*, JZ 2016, 76 (80); *Lüftenegger*, NJW 2018, 2087 (2090).

1226 Diesen Aspekt betonen auch *Rudkowski*, VersR 2018, 65 (72) und *Lüftenegger*, NJW 2018, 2087 (2090); *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 271.

1227 *Hammel*, Haftung und Versicherung bei Pkw, S. 440; *Xyländer*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 166.

1228 So auch *Huber*, Rechtsfragen des Produktrückrufs, S. 258 f.

1229 Vgl. *Lüftenegger*, NJW 2018, 2087 (2090; Fn. 28).

1230 Hierauf weisen *Rudkowski*, VersR 2018, 65 (72, Fn. 79) und *Hammel*, Haftung und Versicherung bei Pkw, S. 440 (Fn. 2245) hin; vgl. zur Nutzungsausfallentschädigung *Grüneberg*, in: *Grüneberg*, BGB, § 249, Rn. 49.

4. Ausgestaltung der Rückrufpflicht

Steht anhand der dargestellten Kriterien fest, dass eine Warnung zur Gefahrenabwehr nicht ausreichend ist, stellt sich die Frage, wie der Rückruf des Produkts auszugestalten ist.

Nun kommt der bloßen Rückführung des Produkts an den Hersteller jedenfalls bei herkömmlichen Reaktionsmaßnahmen kaum eigenständige Bedeutung zukommt.¹²³¹ Denn sowohl bei der Erwirkung der Rückgabe als auch bei der Stilllegung ist der Hersteller herkömmlicherweise auf die Mitwirkung des Produktnutzers angewiesen. Sie sind beide nicht gegen oder ohne den Willen des Nutzers möglich. Es ist aber nicht ersichtlich, warum der Nutzer eine Warnung nicht befolgen sollte, wohl aber eine Aufforderung das Produkt zurückzugeben oder stillzulegen. Der eng verstandene Rückruf wäre damit kaum einmal effektiver als die Warnung.¹²³² Es verwundert daher nicht, dass der BGH gleich im nächsten Absatz darauf eingeht, dass es auch zum deliktsrechtlich geschuldeten Pflichtenumfang des Herstellers gehören kann, die Produkte nicht nur im eng verstandenen Sinne zurückzurufen, sondern das Sicherheitsrisiko durch Nachrüstung oder Reparatur zu beseitigen.¹²³³ In diesem Zusammenhang sind künftig auch die in Art. 37 GPSR eingeführten Abhilfemaßnahmen zu sehen. Sie sollen den Verbraucher gerade dazu bringen, auf einen Rückruf zu reagieren, vgl. Erwägungsgrund (88) GPSR. Daher kann ein Rückruf nicht für sich alleinstehen, sondern zieht nach Art. 37 Abs. 1 GPSR weitere Abhilfemaßnahmen nach sich.

1231 Vgl. *Huber*, Rechtsfragen des Produktrückrufs, S. 12.

1232 Vgl. auch *Klindt*, NVwZ 2008, 1073 (1074 f.).

1233 BGH, NJW 2009, 1080 (1081, Rn. 12); in der Literatur wird der Begriff des Rückrufs ohnehin regelmäßig weitergehend verwendet und soll sämtliche Maßnahmen zur Rückführung des Produkts an den Hersteller, den Austausch oder die Ersatzlieferung eines fehlerfreien Produkts sowie Reparaturen umfassen, vgl. *Lüftenegger*, Die Rückrufpflicht des Herstellers, S. 26 f.; *Lüftenegger*, DAR 2016, 122 (122); *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 162; *Huber*, Rechtsfragen des Produktrückrufs, S. 12.

a) Abgrenzung des Äquivalenz- vom Integritätsinteresse

Insgesamt liest sich die Entscheidung jedoch dahingehend, dass weitergehende Sicherungspflichten Ausnahmecharakter haben sollen.¹²³⁴ Dieses Verständnis wird vor dem Hintergrund der Abgrenzung des Äquivalenz- vom dem Integritätsinteresse entwickelt¹²³⁵ und ist angesichts des Ziels der deliktsrechtlichen Verkehrspflichten nur konsequent. Denn diese haben nicht zum Inhalt, die Vertragserwartung des Nutzers an einem mangelfreien und in jeder Hinsicht gebrauchstauglichen Produkt sowie sein Interesse an einer ungestörten Nutzung und seine Werterwartung zu schützen (Nutzungs- und Äquivalenzinteresse). Vielmehr sind sie einzig auf das Interesse gerichtet, dass die absoluten Rechtsgüter i.S.d. § 823 Abs.1 BGB nicht durch das vom Hersteller in den Verkehr gegebenen Produkt verletzt werden (Integritätsinteresse).¹²³⁶ Die Produkthaftung dient eben nur dem Schutz der Sicherheitserwartungen an das Produkt und nicht der Gebrauchstauglichkeit.¹²³⁷ Gelingt es dem Hersteller, dieses Ziel der deliktsrechtlichen Verkehrspflichten zu erreichen, sind seine Pflichten erfüllt. Über diese rechtliche Obergrenze des Pflichtenkatalogs beginnt dann das Kulanzverhalten.¹²³⁸ Wehrt ein Hersteller nun aber eine von seinem Produkt ausgehende Gefahr für diese absoluten Rechtsgüter durch Austausch bzw. Ersatzlieferung eines fehlerfreien Produkts oder Reparatur ab, dient dies nicht nur dem Integritätsinteresse des Nutzers, sondern auch seinem Äquivalenzinteresse.¹²³⁹

Eine entsprechende Verpflichtung des Herstellers aber nur deshalb auszuschließen, weil andernfalls das Gewährleistungsrecht und damit das Recht des Herstellers (als Verkäufer), nur während der Gewährleistungsfrist

1234 So auch *Lüftenegger*, Die Rückruffpflicht des Herstellers, S. 211; *Xia*, Die Pflicht zum Produktrückruf, S. 46; *Wagner*, JZ 2009, 905 (909) spricht daher davon, dass „die Anhänger deliktischer Rückruffpflichten einen herben Dämpfer bekommen“ haben.

1235 Vgl. BGH, NJW 2009, 1080 (1081 f., Rn. 12; 1082, Rn. 19 f.).

1236 Auch außerhalb der Rückruf-Problematik allg. Meinung, vgl. *Sprau*, in: Grünberg, BGB, § 823, Rn. 181; *Förster*, in: BeckOK, BGB, § 823, Rn. 674; speziell zum Rückruf: *Stöhr*, in: FS Müller (2009) und *Klindt*, BB 2009, 792 (793).

1237 Plakativ *Müller*, VersR 2004, 1073.

1238 *Klindt*, BB 2009, 792 (793); ähnlich *Wagner*, JZ 2009, 905 (910); gerade im Automobilsektor wird die Reparatur regelmäßig freiwillig als Marketinginstrument eingesetzt, auch wenn keine gesetzliche Verpflichtung dazu besteht, vgl. *Lüftenegger*, DAR 2016, 122 (122).

1239 Vgl. *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 163.

nach § 438 BGB für das Äquivalenzinteresse einzustehen, konterkariert werden könnte, überzeugt nicht.¹²⁴⁰ Denn deliktsrechtliche und vertragliche Ansprüche stehen schon aufgrund ihrer unterschiedlichen Zielrichtungen in echter Anspruchskonkurrenz nebeneinander und sind in Voraussetzungen, Inhalt und Durchsetzung eigenständig zu beurteilen.¹²⁴¹ Besteht die Produktgefahr neben dem Erwerber und Nutzer auch gegenüber Dritten, greift das Argument des Vorrang des Vertragsrechts ohnehin nicht, da in diesem Verhältnis weitergehende Sicherungsmaßnahmen nicht der Kompensation eines Mangels, sondern der Gefahrenabwehr dienen.¹²⁴² Ferner lässt sich nicht der Schluss ziehen, dass es keine deliktsrechtliche Pflicht geben kann, die identisch mit dem Erfüllungsinteresse ist.¹²⁴³

Richtig ist allerdings, dass sich eine weitergehende Sicherungspflicht nie allein aus dem Äquivalenzinteresse des Nutzers ergeben kann, sondern immer nur daraus, dass die von einem Produkt ausgehenden Gefahren für die von § 823 Abs. 1 BGB geschützten Rechte und Rechtsgüter effektiv und zumutbar auszuschalten sind.¹²⁴⁴ Führt nun die deliktsrechtliche Pflicht zum Schutz des Integritätsinteresses dazu, dass auch das Äquivalenzinteresse (teilweise) gewahrt wird, ist dies zwar nicht Sinn der Pflicht, aber eine hinzunehmende Reflexwirkung.¹²⁴⁵ Geht damit von einem Produkt auch eine Gefahr für das Integritätsinteresse aus, ist eine weitergehende Sicherungspflicht zumindest nicht von vorneherein ausgeschlossen.¹²⁴⁶ Stellt andererseits ein Hersteller bereits mit einer Warnung oder Rückgabeaufforderung sicher, dass das gefahrenträchtige Produkt keine absolut geschützten Rechtsgüter der Nutzer oder Dritter mehr verletzen kann, sind weiter-

1240 Vgl. Stöhr, in: FS Müller, S. 173 (181 f.); Staudinger/Czaplinski, JA 2008, 401 (404); anders aber Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 349 f.

1241 St. Rspr., vgl. nur BGH, NJW 1977, 379 (380); BGH, NJW 1992, 1039 (1041); Wagner, in: MüKo, BGB, § 823, Rn. 1035 f.

1242 Stöhr, in: FS Müller, S. 173 (182); Xylander, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 164.

1243 So auch Hager, in: Staudinger, BGB, § 823, Rn. F 2.

1244 Dies wird gerade von BGH, NJW 2009, 1080 (1082, Rn. 19) herausgestellt.

1245 Faust, JuS 2009, 377 (379); Eichelberger, in: Ebers et al. (Hg.), Künstliche Intelligenz und Robotik, S. 190; ähnlich Produkthaftung Reusch, in: Kaulartz/Braegelmann (Hg.), Artificial Intelligence und Machine Learning, S. 146.

1246 Dies erkennt auch der BGH an, vgl. BGH, NJW 2009, 1080 (1081, Rn. 12); Staudinger/Czaplinski, JA 2008, 401 (404); Xylander, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 163 f.; vgl. auch Wagner, JZ 2009, 905 (909); a.A. Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 350 (Fn. 1156).

gehende Maßnahmen nach den deliktsrechtlichen Verkehrspflichten nicht geschuldet. Denn wird ein gefährliches Produkt eigenverantwortlich nicht mehr benutzt oder der Rückgabeaufforderung Folge geleistet, kann dieses Produkt das Integritätsinteresse ebenso wenig berühren wie ein nachgerüstetes Produkt.¹²⁴⁷ Ein hieraus für den Nutzer resultierender Schaden wäre allein auf die Mangelhaftigkeit des Produkts bei Erwerb zurückzuführen und betrifft daher allein die enttäuschte Vertragserwartung.¹²⁴⁸

b) Relevante Kriterien des Einzelfalls

Vor diesem Hintergrund kommen weitergehende Pflichten des Herstellers, das bereits im Verkehr befindliche fehlerhafte Produkte nicht nur zurückzurufen, sondern das Sicherheitsrisiko durch Nachrüstung oder Reparatur zu beseitigen nur in Betracht, wenn eine solche Maßnahme im konkreten Fall erforderlich ist, um Produktgefahren, die den in § 823 Abs.1 BGB geschützten Rechtsgütern der Benutzer oder unbeteiligter Dritter drohen, effektiv abzuwehren.¹²⁴⁹ In diesem Sinne benennt der BGH mit der Identifikationsmöglichkeit der Produktnutzer und dessen eigenen Pflichten gegenüber Dritten weitere Einflussfaktoren auf die Effektivität der Gefahrenabwehr und nimmt neben der nachgezeichneten Fallgruppenbildung weiter zum Verhältnis der Sicherungspflichten Stellung.¹²⁵⁰ Gerade bei diesen Faktoren handelt es sich aber nicht um absolute Kriterien, sondern um Tendenzen in der Einzelfallentscheidung.¹²⁵¹

Bereits das Kriterium des Hinwegsetzens über eine Warnung lässt sich darauf zurückführen, dass in diesen Fällen eine zuverlässige Gefahrensteuerung nicht gewährleistet ist und aus Gründen der Effektivität der Gefahrenabwehr bei Gefährdung für die Allgemeinheit eine weitreichendere Pflicht des Herstellers besteht. Umgekehrt scheiden damit aber weitergehende Sicherungsmaßnahmen des Herstellers aus, wenn hinreichende Gewähr

1247 So schon LG Frankfurt a.M., BeckRS 2008, 2795.

1248 BGH, NJW 2009, 1080 (1083, Rn. 25).

1249 So BGH, NJW 2009, 1080 (1081, Rn. 12).

1250 BGH, NJW 2009, 1080 (1081, Rn. 13; 1082, Rn. 16).

1251 Für beide Kriterien weist der BGH explizit darauf hin, dass die Umstände des jeweiligen Falles zu beachten sind; vgl. auch *Lüftenegger*, Die Rückrufpflicht des Herstellers, S. 279.

dafür besteht, dass die Nutzer eine entsprechende Produktwarnung oder Rückgabeaufforderung nicht in den Wind schlagen werden.¹²⁵²

aa) Eigene Pflichten des Nutzers zum Schutz Dritter

Fortgezeichnet sollen eigene Pflichten des Nutzers zum Schutz Dritter die Erforderlichkeit und damit die Effektivität der Gefahrenabwehr beeinflussen.¹²⁵³ Im konkreten Fall waren die Pflegekassen als Nutzer der gefährlichen Betten aufgrund ihrer sozialversicherungsrechtlichen Leistungsverpflichtungen angehalten, die Pflegebedürftigen zu versorgen und vor drohenden Gefahren zu schützen. Dies umfasst nach § 40 Abs. 3 S. 3 SGB XI auch einen Anspruch der Pflegebedürftigen hinsichtlich notwendiger Änderungen, Instandsetzungen und Ersatzbeschaffungen von Pflegehilfsmitteln und betrifft damit auch die fehlerbehafteten Pflegebetten.¹²⁵⁴ Vor dem Hintergrund ihrer öffentlich-rechtlichen Rechtspflichten waren die Pflegekassen zu einem rechtskonformen und sicherheitsbewussten Verhalten gezwungen,¹²⁵⁵ sodass der BGH eine hinreichende Gewähr für ein rechtskonformes Verhalten annahm. Wenn der BGH weiter darauf abstellt, dass im konkreten Fall keine Anhaltspunkte dafür vorlagen, dass die Pflegekassen ihren Pflichten nicht nachkommen würden,¹²⁵⁶ wird deutlich, dass das Bestehen eigener gesetzlicher Pflichten aber kein absoluter Maßstab für die Beurteilung der Gewährleistung einer zuverlässigen Gefahrenabwehr ist.¹²⁵⁷ Vielmehr ist hierin ein Indiz dafür zu sehen, dass der Produktnutzer eine Warnung oder Rückgabeaufforderung befolgen wird, dem aber im Sinne einer effektiven Gefahrenabwehr keine gegenteiligen Anhaltspunkte entgegenstehen dürfen.¹²⁵⁸

1252 Vgl. auch *Wagner*, JZ 2009, 905 (910); *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), *Produkthaftungshandbuch*, § 24, Rn. 359.

1253 BGH, NJW 2009, 1080 (1081, Rn. 16).

1254 BGH, NJW 2009, 1080 (1081, Rn. 16).

1255 So auch *Klindt*, BB 2009, 792 (794).

1256 BGH, NJW 2009, 1080 (1081, Rn. 16).

1257 Strenger aber *Klindt*, BB 2009, 792 (794) „Eine herstellerseitige Warnung muss immer dort ausreichen dürfen, wo ihr auf Betreiberseite eine genuine Rechtspflicht korrespondierend gegenübersteht, die eine Ignoranz der Sicherheitswarnung eigenständig sanktioniert“.

1258 Zu Recht *Lüftenegger*, Die Rückruffpflicht des Herstellers, S. 214 f.; ähnlich *Xia*, Die Pflicht zum Produktrückruf, S. 62; auch *Burckhardt*, BB 2009, 630 (630); *Wagner*, JZ 2009, 905 (910) misst dagegen eigenen gesetzlichen Pflichten keine tragende Rolle im System des BGH bei.

(1) Indizwirkung bei kodifizierten Pflichten

Eine solche Indizwirkung dürfte dabei aber lediglich bei genuin kodifizierten Pflichten bestehen.¹²⁵⁹ Zwar treffen alle Nutzer eines Produkts gegenüber Dritten aufgrund der Ausübung der tatsächlichen Sachherrschaft die allgemeinen deliktsrechtlichen Verkehrspflichten aus § 823 Abs. 1 BGB.¹²⁶⁰ Sie haben bei hinreichenden Anhaltspunkten für einen Sicherheitsmangel des Produkts – was insbesondere nach einer Produktwarnung des Herstellers der Fall ist – alle erforderlichen und zumutbaren Maßnahmen zu ergreifen, um eine Gefährdung Dritter durch das Produkt zu verhindern.¹²⁶¹ Eine herstellerseitige Warnung oder Rückgabeaufforderung aktiviert damit auch ohne das Bestehen spezieller kodifizierter Pflichten eigene (Verkehrs)plichten der Nutzer.¹²⁶² Der BGH stellt indes nicht entscheidend auf das Bestehen einer eigenen Pflicht des Nutzers ab, sondern zieht diese lediglich zur Begründung einer hinreichenden Gewähr für eine zuverlässige Gefahrenabwehr heran. Im Sinne der Effektivität der Gefahrenabwehr ist es eben entscheidend, in welchem Ausmaß sich der Hersteller auf die Gefahrenabwehr durch andere verlassen darf,¹²⁶³ mithin wie der Erfolg der Gefahrenabwehrmaßnahme zu beurteilen ist.¹²⁶⁴ Mit der Annahme, dass sich Nutzer gerade auch bewusst über eine Warnung hinwegsetzen können,¹²⁶⁵ zeigt der BGH aber Skepsis, dass jenseits von sonderrechtlich kodifizierten Pflichten die allgemeinen Verkehrspflichten der Endabnehmer eine hinreichend zuverlässige Gefahrenabwehr gewährleisten.¹²⁶⁶ Für den Hersteller lassen erst kodifizierte Schutzpflichten des Nutzers erwarten, dass dessen Gefahrensteuerung auf sachgerechter Bewertung und pflichtgemäß erfolgt.¹²⁶⁷ Andernfalls ist aus Sicht des Herstellers eine effektive Gefahrenabwehr nicht gewährleistet. Insoweit kann eine hohe Produktver-

1259 So auch *Huber*, Rechtsfragen des Produktrückrufs, S. 234.

1260 *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), *Produkthaftungshandbuch*, § 24, Rn. 340; speziell in Bezug auf IT-Produkte *Riehm/Meier*, MMR 2020, 571 (573 f.).

1261 *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), *Produkthaftungshandbuch*, § 27, Rn. 17 f.

1262 *Molitoris*, NJW 2009, 1049 (1050 f.); *Klindt*, BB 2009, 792 (795); *Handorn*, MPR 2009, 37 (43).

1263 Vgl. nochmals *v. Bar*, in: *Lieb* (Hg.), *Produktverantwortung und Risikoakzeptanz*, S. 29 (42); so wohl auch *Wagner*, JZ 2009, 905 (910).

1264 *Kettler*, VersR 2009, 272 (275).

1265 BGH, NJW 2009, 1080 (1081, Rn. 11).

1266 In diese Richtung auch *Kettler*, VersR 2009, 272 (275); ähnlich *Stöhr*, in: FS Müller, S. 173 (180); krit. aber *Klindt*, BB 2009, 792 (795).

antwortung des Nutzers beim Gebrauch zu einem verringerten Pflichten-
umfang des Herstellers führen.¹²⁶⁸

(2) Bedeutung der Adressatenkreise

Diese Betrachtung führt aber fast zwangsläufig zu einer Differenzierung nach Adressatenkreisen.¹²⁶⁹ Bei gewerblicher Nutzung der Produkte (B2B-Belieferungen) wird der Hersteller regelmäßig davon ausgehen dürfen, dass die Warnung auch beachtet oder der Rückgabeaufforderung nachgekommen wird.¹²⁷⁰ Dies sollte dabei weniger an der Fachkunde des gewerblichen Nutzers festgemacht werden als mehr an eigenen Gefahrenbeseitigungspflichten. Das Argument, dass Fachkräften eher der ordnungsgemäße Umgang mit einer Gefahr zugetraut werden darf als Laien,¹²⁷¹ verfängt in diesem Zusammenhang nicht. Denn sofern eine Warnung ausreichend Gefahrenbewusstsein schafft – und dies ist Grundvoraussetzung, dass eine Warnung überhaupt als ausreichend in Betracht gezogen werden kann – bedarf es für das Befolgen der Warnung und die Nichtbenutzung des Produkts keines weiteren technischen Fachwissens.¹²⁷² Dagegen bestehen sonderrechtliche Pflichten¹²⁷³ oder eigene vertragliche Verantwortlichkeiten¹²⁷⁴

1267 Huber, Rechtsfragen des Produktrückrufs, S. 234 „aktive Schutzpflicht“; wohl auch Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 359.

1268 Vgl. Lüftenegger, NJW 2018, 2087 (2089).

1269 So Lenz, in: Lenz, Produkthaftung, § 4, Rn. 49; für eine Gleichbehandlung von professionellen und privaten Endnutzern aufgrund gleichermaßen bestehender allgemeiner Verkehrspflichten aber Molitoris, NJW 2009, 1049 (1050 f.); Klindt, BB 2009, 792 (795); Handorn, MPR 2009, 37 (43).

1270 Klindt, BB 2009, 792 (794); Kettler, VersR 2009, 272 (275); Burckhardt, VersR 2007, 1601; insoweit werden in der Pflegebetten-Entscheidung (BGH, NJW 2009, 1080 (1081; Rn. 13) für das Ausreichen von Sicherungsmaßnahmen unterhalb der Schwelle des Rückrufs mit kostenloser Reparatur durchgängig Entscheidungen zitiert, in denen der Adressat der Warnung kein privater Endverbraucher war, vgl. dazu Kettler, VersR 2009, 272 (275).

1271 So v. Bar, in: Lieb (Hg.), Produktverantwortung und Risikoakzeptanz, S. 29 (42); Voigt, in: BeckOGK, BGB, § 823, Rn. 683.

1272 Eine Parallele mit den anfänglichen Instruktionspflichten, die bei Fachkräften reduziert sein können, besteht folglich schon von der Interessenlage her nicht, daher zu Recht krit. Klindt, BB 2009, 792 (794; Fn. 18).

1273 Klindt, BB 2009, 792 (794) und Lüftenegger, Die Rückruffpflicht des Herstellers, S. 280 ff. listen einige Betreiberpflichten in Spezialgesetzen auf.

1274 Hierauf weist zu Recht Stöhr, in: FS Müller, S. 173 (180) hin.

regelmäßig nur bei professionell fachkundigen Nutzern, nicht aber bei privaten Endverbrauchern.¹²⁷⁵ Daneben ist auch bei Behörden oder staatlich beaufsichtigten Stellen eine zuverlässige Gefahrenabwehr nach einer Warnung oder Rückgabeaufforderung zu erwarten.¹²⁷⁶ Bei gewerblichen Nutzern wird daher, insbesondere beim Bestehen sonderrechtlicher Pflichten, eine Warnung oder Rückgabeaufforderung eher ausreichend sein. Dass dies aber keinesfalls immer so sein muss, zeigt eine dem Pflegebetten-Fall des BGH zeitlich nachfolgende Entscheidung des OLG Nürnberg.¹²⁷⁷ Der Senat nahm trotz des Bestehens entsprechender öffentlich-rechtlicher Pflichten weitergehende Sicherungspflichten an, da insbesondere bei privaten Betreibern, anders als bei öffentlicher Trägerschaft weder die Kenntnis noch die Einhaltung der Verpflichtung zwingend erwartet werden könne.¹²⁷⁸ Die Zurückhaltung hinsichtlich der Gewähr für eine zuverlässige Gefahrenabwehr trotz bestehender Sonderpflichten wird nicht weiter begründet,¹²⁷⁹ dürfte aber der besonderen Fallkonstellation geschuldet sein. Denn während die spezifische Produktgefahr durch einfache Nichtbenutzung beseitigt werden konnte, bedeutete diese Stilllegung die Schaffung neuer Gefahren, da das Produkt eine Sicherungsfunktion erfüllte und daher zwingend nachgerüstet werden musste. Diesen über die Nichtbenutzung hinausgehenden Schritt der Nachrüstung traute der Senat den Betreibern im Sinne eines effektiven Drittschutzes wohl nicht zu.

bb) Identifizierbarkeit der Produktnutzer

Der BGH weist darauf hin, dass auch in Fällen erheblicher (!) Gefahren für Dritte (!) vielfach Maßnahmen unterhalb einer kostenfreien Nachrüstung ausreichen, sofern die Produktnutzer bekannt oder zumindest ermittelbar sind.¹²⁸⁰ Dem dürfte zunächst die Überlegung zu Grunde liegen, dass bei einem identifizierbaren Abnehmerkreis die Warnung oder die Rückgabeaufforderung jeden Produktnutzer erreichen kann und die Rücklaufquote,

1275 So *Kettler*, VersR 2009, 272 (275), der zusätzlich darauf hinweist, dass Unternehmen einem „Geflecht von (Compliance-)Regeln und Strukturen zur wechselseitigen Kontrolle der Einhaltung dieser Regeln“ unterliegen.

1276 *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), *Produkthaftungshandbuch*, § 24, Rn. 359.

1277 So auch *Huber*, *Rechtsfragen des Produktrückrufs*, S. 231.

1278 OLG Nürnberg, BeckRS 2013, 6837.

1279 Krit. insoweit auch *Lüftenegger*, *Die Rückruffpflicht des Herstellers*, S. 260 f.

1280 BGH, NJW 2009, 1080 (1081, Rn. 13).

also das Verhältnis der von der Aktion erreichten Nutzer und der Gesamtzahl der betroffenen Produkte,¹²⁸¹ nahezu 100 % erreichen kann.¹²⁸² Vor diesem Hintergrund normiert auch Art. 35 Abs. 1 GPSR künftig die Pflicht, dass alle ermittelbaren Nutzer direkt und unverzüglich zu unterrichten sind und hierzu auch alle erhobenen Kundendaten zu nutzen sind. Der direkte Kontakt sei nach Erwägungsgrund (85) GPSR die wirksamste Methode, das Bewusstsein des Nutzers zu erhöhen und ihn zum Handeln zu ermutigen.¹²⁸³ Indes ist die Erreichbarkeit des Produktnutzers noch nicht mit einer effektiven Gefahrenabwehr gleichzusetzen.¹²⁸⁴ Denn ob der gezielt erreichte Produktnutzer der Warnung oder der Rückgabeaufforderung tatsächlich Folge leisten wird, ist eine andere Frage.¹²⁸⁵

(1) Bedeutung des marktüberwachungsrechtlichen Tätigwerdens

Gleichwohl scheint der BGH in diesen Fällen die Effektivität der Gefahrenabwehr vor dem Hintergrund für gewährleistet zu halten, dass bei identifizierbaren Produktnutzern die zuständigen Behörden eingeschaltet werden können und ihrerseits die notwendigen Maßnahmen ergreifen können.¹²⁸⁶ Dabei dürften allerdings die Eingriffsbefugnisse der Marktüberwachungsbehörden überschätzt worden sein. Denn das Marktüberwachungsrecht sieht vor, dass behördliche Maßnahmen gegen andere Personen als die Wirtschaftsakteure und damit auch gegen den Verwender¹²⁸⁷ nur bei einem gegenwärtig ernstem Risiko, das nicht auf andere Weise abgewehrt werden kann, zulässig sind (vgl. § 9 S. 2 Marktüberwachungsgesetz, im Folgenden „MüG“). Bevor es zu einem marktüberwachungsrechtlichen Tätigwerden gegen die Nutzer kommen kann, dürfen also keine anderen erfolgsversprechenden Gefahrenabwehrmöglichkeiten existieren und haben sich die

1281 Vgl. auch zur Bedeutung der Rücklaufquote *Klindt/Wende*, Rückrufmanagement, S. 95 ff.

1282 Vgl. auch *Lüftenegger*, NJW 2018, 2087 (2089); zustimmend daher *Voigt*, in: BeckOGK, BGB, § 823, Rn. 683.

1283 Krit. *Hartmann/Klindt*, ZfPC 2022, 73 (75).

1284 Hierauf weist *Lüftenegger*, RDt 2021, 293 (294 f.) hin.

1285 Zu Recht *Xia*, Die Pflicht zum Produktrückruf, S. 58.

1286 BGH, NJW 2009, 1080 (1081, Rn. 13); so auch *Burckhardt*, VersR 2007, 1601.

1287 Vgl. noch zur Vorgängernorm des § 27 Abs. 1 S. 2 ProdSG LASI LV 46, S. 32 und *Schucht*, in: *Klindt*, ProdSG, § 27, Rn. 25.

Marktüberwachungsbehörden vorrangig an den Hersteller zu wenden.¹²⁸⁸ Insofern ist eher zu erwarten, dass eine Behörde den Hersteller zur Ergreifung von Korrekturmaßnahmen nach Art. 16 Abs. 2 Marktüberwachungsverordnung (im Folgenden „MÜ-VO“)¹²⁸⁹ auffordert oder den Rückruf nach Art. 16 Abs. 5 MÜ-VO anordnet.¹²⁹⁰ Ein direktes marktüberwachungsrechtliches Vorgehen gegen einen sich der Maßnahme verweigernden Nutzer kommt nur in Ausnahmefällen in Betracht.¹²⁹¹ Die maßgebliche Verantwortung für das Ergreifen der effektiven Reaktionsmaßnahmen verbleibt beim Hersteller.¹²⁹²

(2) Geringe Bedeutungskraft des Kriteriums

Allerdings führt die Identifizierbarkeit der Nutzer dazu, dass bei einer Verweigerung der Mitwirkung weitere, individualisierte Maßnahmen des Herstellers getroffen werden können.¹²⁹³ Insbesondere im Rahmen einer zweiten Maßnahmenaktion kann der Hersteller versuchen, durch individuelle und drastische Warnungen und gezielte Anreize¹²⁹⁴ ein Umdenken beim Nutzer zu erreichen. Ob die durch die Identifizierbarkeit mögliche Individualisierung der Ansprache die Compliance des Produktnutzers aber tatsächlich erhöht, ist zu bezweifeln.¹²⁹⁵ Es drängt sich der Verdacht auf,

1288 Zur Subsidiarität *Schucht*, in: Klindt, ProdSG, § 27, Rn. 26; *Giesberts/Gayger*, in: NK-ProdR, § 9 MüG, Rn. 46.

1289 Verordnung (EU) 2019/1020.

1290 So auch im hiesigen Kontext *Stöhr*, in: FS Müller, S. 173 (182 f.); vgl. auch *Lenz*, in: *Lenz*, Produkthaftung, § 4, Rn. 53, welcher darauf hinweist, dass in produktsicherheitsrechtlicher Hinsicht für den Hersteller stets die Anordnung eines belastenden Verwaltungsakts drohe.

1291 Vgl. *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), Produkthaftungshandbuch, § 24, Rn. 324 f. mit Verweis auf die Fallkonstellation in BGH, VersR 1960, 856; anders hat die Kfz-Zulassungsbehörde die Möglichkeit, eine Betriebsuntersagung für betroffene Fahrzeuge zu erlassen, wenn der Halter einem Sicherheitsaufruf nicht nachkommt (§ 5 Abs. 1 FZV), vgl. *Klindt/Wende*, Rückrufmanagement, S. 97 und *Lüftenegger*, NJW 2018, 2087 (2089 f.); *Wiesemann/Mattheis/Wende*, MMR 2020, 139 (141); *Schrader*, NZV 2018, 489 (493).

1292 I.E. auch *Xia*, Die Pflicht zum Produktrückruf, S. 58; *Stöhr*, in: FS Müller, S. 173 (182).

1293 *Burckhardt*, BB 2009, 630 (630).

1294 Vgl. hierzu *Klindt/Wende*, Rückrufmanagement, S. 97; *Lenz*, in: *Lenz*, Produkthaftung, § 4, Rn. 51 spricht von „Draufgaben“ und „goodies“.

1295 Skeptisch auch *Klindt/Wende*, Rückrufmanagement, S. 97; *Lenz*, in: *Lenz*, Produkthaftung, § 4, Rn. 51, 71.

dass der BGH bei der Identifizierbarkeit der Nutzer gerade Fallkonstellationen der B2B-Belieferung professioneller Nutzer mit spezialisierten Produkten vor Augen hatte, bei denen der Abnehmerkreis übersichtlich ist oder ohnehin eine Auftragsdokumentation stattfindet bzw. eine Kundendatei vorliegt.¹²⁹⁶ Innerhalb einer solchen individuellen Geschäftsbeziehung mag das Befolgen einer Maßnahme tatsächlich eher angenommen werden können als bei einem anonymisierten Massengeschäft. Für sich allein genommen mag das Kriterium der Identifizierbarkeit aber nicht recht überzeugen. Ausgehend von dieser vom BGH vorgenommenen negativen Abgrenzung – nämlich wann eine kostenlose Nachrüstung nicht in Betracht kommt – lässt sich daher auch ein Umkehrschluss für Massenprodukte, bei denen die Nutzer kaum zu identifizieren sind, schwerlich ziehen.¹²⁹⁷

Selbst wenn man die Identifizierbarkeit der Produktnutzer als Kriterium für die Beurteilung der Effektivität der Gefahrenabwehr anerkennt, muss berücksichtigt werden, dass der BGH diese Frage gerade im Kontext der Kostentragungspflicht behandelt. Bei einem identifizierbaren Abnehmerkreis könne es vielfach genügen, dass der Hersteller seine Hilfe anbietet, um die Nutzer in die Lage zu versetzen, die erforderlichen Nachrüstungs- oder Reparaturmaßnahmen auf ihre Kosten durchzuführen.¹²⁹⁸ Insoweit kann aber auch bei einem identifizierbaren Abnehmerkreis eine bloße Warnung oder Rückgabepflicht zur effektiven Gefahrenabwehr nicht ausreichen, sondern wird ein Rückrufangebot des Herstellers erforderlich sein.

cc) Fehlertypen

Nach einer verbreiteten Ansicht im Schrifttum sollen weitergehende Pflichten des Herstellers nur dann bestehen, wenn der Hersteller im Zeitpunkt der Inverkehrgabe des Produkts bereits sorgfaltswidrig gehandelt hat und folglich ein Konstruktions- oder Fabrikationsfehler vorliegt, nicht aber bei

1296 Solche Konstellationen nennt auch *Lüftenegger*, Die Rückrufpflicht des Herstellers, S. 279 als Beispiele; einen ähnlichen Konnex nimmt *Lenz*, in: *Lenz*, Produkthaftung, § 4, Rn. 71 vor; auch der BGH verweist in der an dieser Stelle (Rn. 13) zitierten Rechtsprechung allein auf B2B-Konstellationen.

1297 Ähnlich zurückhaltend auch *Burckhardt*, BB 2009, 630 (631) und *Lüftenegger*, Die Rückrufpflicht des Herstellers, S. 226.

1298 Vgl. BGH, NJW 2009, 1080 (1081, Rn. 13).

Entwicklungsrisiken.¹²⁹⁹ Dogmatisch wird dies damit begründet, dass ohne Pflichtverletzung im Zeitpunkt der Inverkehrgabe der Unrechtstatbestand des § 823 Abs. 1 BGB nicht erfüllt sein könne, da die Rechtsgutsgefährdung nicht auf ein rechtswidriges Verhalten des Herstellers zurückgeführt werden könne.¹³⁰⁰ Zudem sei es in diesem Fall inkonsistent, einem Hersteller, der seine Sorgfaltspflichten bei der Konstruktion verletzt hat, zu gestatten, sich durch eine nachträgliche Warnung seiner Haftung zu entziehen und die Verantwortung auf den Produktnutzer abzuwälzen. Denn dadurch könnten Fehlanreize entstehen und Fehler beim Inverkehrbringen in Kauf genommen werden, von denen der Hersteller letztlich sogar profitiert, wenn er eine kostenpflichtige Reparatur anbieten kann.¹³⁰¹

Indes dürften diese Fehlanreize wohl nur theoretischer Natur sein und nicht der wirtschaftlichen Realität entsprechen. Hersteller haben auch andere Anreize – nicht zuletzt den drohenden Imageverlust –, ihren Kunden kein fehlerbehaftetes Produkt bereitzustellen.¹³⁰² Hinzu kommt, dass der Hersteller zumindest im Rahmen der Gewährleistungsfristen von seinem Vertragspartner (ggf. im Regresswege, vgl. § 445a BGB ggf. i.V.m. § 478 BGB) in Anspruch genommen werden kann.¹³⁰³ Im Übrigen mag auch die dogmatische Begründung nicht zu verfangen. Denn das Unterlassen des nachträglich gebotenen Einschreitens begründet unabhängig von einer vorgelagerten Sorgfaltspflichtverletzung für sich ein rechtswidriges Verhalten.¹³⁰⁴ Insoweit stellt die Pflicht weitergehender Sicherungspflichten im Rahmen der Produktbeobachtungspflicht eine eigene Verkehrspflicht dar, die bei rechtswidriger Nichtbeachtung zu einem Schadensersatz führen kann und nicht eine bloße Rechtsfolge einer vorangegangenen rechtswidrigen Verletzung einer eigenen Verkehrspflicht ist.¹³⁰⁵ Folglich ist schon die eingenommene Perspektive unzutreffend. Bei der Produktbeobachtungs-

1299 Vgl. *Wagner*, in: MüKo, BGB, § 823, Rn. 1124; *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), *Produkthaftungshandbuch*, § 24, Rn. 341; *Schwenzer*, JZ 1987, 1059 (1061); ähnlich auch *Hager*, in: *Staudinger*, BGB, § 823, Rn. F 26.

1300 *Wagner*, in: MüKo, BGB, § 823, Rn. 1124; *Schwenzer*, JZ 1987, 1059 (1061).

1301 *Hager*, VersR 1984, 799 (800); *Schwenzer*, JZ 1987, 1059 (1061); *Hager*, in: *Staudinger*, BGB, § 823, Rn. F 26; *Wagner*, JZ 2009, 905 (911).

1302 *Lenz*, in: *Lenz*, *Produkthaftung*, § 3, Rn. 231; *Xylander*, *Die Verantwortlichkeit des Herstellers automatisierter PKW*, S. 171f; *Xia*, *Die Pflicht zum Produktrückruf*, S. 66.

1303 *Faust*, JuS 2009, 377 (379).

1304 *So v. Bar*, in: *Lieb* (Hg.), *Produktverantwortung und Risikoakzeptanz*, S. 29 (41).

1305 *So Schmid*, *IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme*, S. 236; ähnlich auch *Wilhelmi*, in: *Erman*, BGB, § 823, Rn. 119.

pflcht steht eben die Gefahrenabwehr im Vordergrund und nicht die Verschuldensverursachung.¹³⁰⁶ Die Frage des Verschuldens bei der Gefahrenschaffung ändert weder etwas am nunmehrigen Vorhandensein der vom Hersteller veranlassten objektiven Gefahr noch an einer möglichen Erforderlichkeit eines Rückrufs.¹³⁰⁷

Auch der BGH hat einer vorgeschlagenen Differenzierung nach der Fehlerhaftigkeit bei Inverkehrgabe eine Absage erteilt.¹³⁰⁸ Denn eine pauschale Nachrüstungspflicht bei Konstruktions- oder Fabrikationsfehlern könnte über das erforderliche Maß zur effektiven Gefahrenabwehr hinausgehen und das Äquivalenzinteresse betreffen, sollte nämlich eine Warnung ausreichen. Umgekehrt kann bei Entwicklungsrisiken eine Nachrüstungspflicht aber auch nicht pauschal ausgeschlossen werden. Es kommt insoweit immer auf die Erforderlichkeit im Einzelfall an.¹³⁰⁹

dd) Gefährlichkeit

Teilweise wird in der juristischen Literatur die erforderliche Reaktionsmaßnahme vom jeweils gefährdeten Rechtsgut und der Größe der Gefahr abhängig gemacht.¹³¹⁰ Dies dürfte seinen Grund darin haben, dass die Gefährlichkeit im Rahmen der Verkehrspflichten allgemein zur Bestimmung der Erforderlichkeit und Zumutbarkeit herangezogen wird und die Intensität der zu ergreifenden Sicherungspflichten beeinflusst.

Die Auswahl der richtigen Reaktionsmaßnahme folgt indes der Maxime der Effektivität der Gefahrenabwehr. Weitergehende Sicherungspflichten sind nur dort erforderlich, wo eine Warnung oder Rückgabeaufforderung eine effektive Gefahrenabwehr nicht gewährleistet.¹³¹¹ Gerade bei Gefahren für Leib und Leben bei einer hohen Eintrittswahrscheinlichkeit der Rechts-

1306 Lenz, in: Lenz, Produkthaftung, § 3, Rn. 231; § 4, Rn. 39, 54; vgl. auch Sommer, Haftung für autonome Systeme, S. 284.

1307 Förster, in: BeckOK, BGB, § 823, Rn. 751.

1308 BGH, NJW 2009, 1082 (1081, Rn. 18, 19).

1309 Vgl. auch Lüftenegger, Die Rückruffpflicht des Herstellers, S. 244; Xyländer, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 172; Xia, Die Pflicht zum Produktrückruf, S. 66, 70.

1310 Xyländer, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 170; Burckhardt, BB 2009, 630 (631); gerade bei Personengefahren wird regelmäßig eher eine Rückruffpflicht angenommen, vgl. Voigt, in: BeckOGK, BGB, § 823, Rn. 682 und Wagner, AcP 217 (2017), 707 (754).

1311 Vgl. auch Tamme, Rückrufkosten, S. 179.

gutsverletzung dürfte aber schon aus dem Eigeninteresse eher damit zu rechnen sein, dass der Produktnutzer der Maßnahme des Herstellers Folge leistet.¹³¹² Der BGH geht in seiner Pflegebetten-Entscheidung zwar auch auf das jeweils gefährdete Rechtsgut und die Größe der Gefahr ein,¹³¹³ allerdings nicht um die Maßnahmen voneinander abzugrenzen, sondern um innerhalb der Reaktionsmaßnahme der Warnung dessen Inhalt und Umfang zu bestimmen.¹³¹⁴ Allein das Vorliegen einer großen Gefahr zwingt nicht zu weitergehenden Sicherungspflichten, es sei denn, dieser ist zur effektiven Gefahrenabwehr erforderlich.¹³¹⁵ Dieses Verständnis wird auch unmittelbar aus der Pflegebetten-Entscheidung deutlich, wenn der BGH anführt, dass selbst in Fällen erheblicher (!) Gefahren eine kostenlose Nachrüstung vielfach nicht erforderlich sei.¹³¹⁶ Vor diesem Hintergrund und der stets angeführten Einzelfallabhängigkeit kann eine Nachrüstungsspflicht auch bei anzunehmenden bloßen Sachgefahren nicht von vorneherein ausgeschlossen werden.¹³¹⁷ Hinzu kommt, dass eine Differenzierung nach dem Umfang der Gefahr oder der geschützten Rechtsgüter aufgrund fließender Grenzen angesichts der Vielzahl praktischer Kombinationsmöglichkeiten letztendlich zusätzliche Bewertungsschwierigkeiten schafft.¹³¹⁸ Gleichwohl kann unter dem Gesichtspunkt der Zumutbarkeit eine Rückrufflicht bei bloßen drohenden Sachschäden aufgrund des im Vergleich zum Integritätsinteresse hohen wirtschaftlichen Aufwands des Herstellers abzulehnen sein.¹³¹⁹ Dies betrifft aber eine der Erforderlichkeit nachgelagerte Frage.

1312 In diese Richtung in anderem Zusammenhang *Rudkowski*, VersR 2018, 65 (71).

1313 BGH, NJW 2009, 1080 (1081, Rn. 10).

1314 Dies verkennen *Ackermann*, in: NK-ProdR, § 823 BGB, Rn. 136 und *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 170, wenn sie insoweit den BGH zitieren; mindestens missverständlich *Wagner*, AcP 217 (2017), 707 (754).

1315 So auch *Thöne*, Autonome Systeme, S. 214; ähnlich *Hager*, in: Staudinger, BGB, § 823, Rn. F 25.

1316 BGH, NJW 2009, 1080 (1081, Rn. 13).

1317 So aber *Schwenzer*, JZ 1987, 1059 (1062); in diese Richtung auch *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 274 ff.; zurückhaltender: *Michalski*, BB 1998, 961 (964); *Lenz*, in: Lenz, Produkthaftung, § 4, Rn. 46; *Lüftenegger*, Die Rückrufflicht des Herstellers, S. 244; *Xia*, Die Pflicht zum Produktrückruf, S. 84; *Schmidt*, Produktrückruf und Regress, S. 74; *Tamme*, Rückrufkosten, S. 178 f.

1318 So *Förster*, in: BeckOK, BGB, § 823, Rn. 751.

1319 *Huber*, Rechtsfragen des Produktrückrufs, S. 214 ff.

5. Kostentragung

Kommt man anhand der dargelegten Kriterien zu dem Ergebnis, dass eine Warnung oder Rückgabeaufforderung zur effektiven Gefahrenabwehr nicht mehr ausreichend ist und den Hersteller eine Nachrüstungspflicht trifft, stellt sich die anschließende Frage, wer die Kosten hierfür zu tragen hat. Dadurch dass die Rückrufrkosten mit einer hohen finanziellen Belastung einhergehen können und den Kern der Abgrenzung des Äquivalenz- vom Integritätsinteresse betreffen, kommt dieser Frage zentrale Bedeutung bei der Bewertung der Reaktionsmaßnahmen zu.¹³²⁰ Dabei ist sich aber stets zu vergegenwärtigen, dass den Hersteller eine Nachrüstungspflicht nur unter den oben genannten strengen Voraussetzungen trifft und sich auch nur dann die Frage nach der Kostentragung des Rückrufs stellt.

a) Effektivität der Gefahrenabwehr als Maxime

In der juristischen Literatur wird bei Vorliegen der nach der jeweiligen Ansicht erforderlichen Voraussetzungen für eine Nachrüstung regelmäßig auch von einer Kostentragungspflicht des Herstellers ausgegangen.¹³²¹ Begründet wird dies auch mit der sonst fehlenden Abgrenzbarkeit von Warnung, Rückgabeaufforderung und Nachrüstung. Bei einem Rückruf ist der Hersteller herkömmlicherweise auf die Mitwirkung des Nutzers angewiesen, er kann ihn nicht zur Rückgabe des Produktes zwingen.¹³²² Erfolgt ein Rückruf dann aber ohne Übernahme der Kosten durch den Hersteller, wird argumentiert, dass der Nutzer nicht anders stünde als im Rahmen einer Warnung. Er werde über die Gefahrenträchtigkeit des Produkts informiert, müsse aber in beiden Fällen eine Gefahrensteuerung auf eigene Kosten unternehmen.¹³²³ Dies werde der Effektivität der Gefahrenabwehr regelmäßig nicht gerecht, da nicht genügend Anreize für den Nutzer bestünden, das

1320 Vgl. auch Xia, Die Pflicht zum Produktrückruf, S. 89.

1321 Hager, in: Staudinger, BGB, § 823, Rn. F 26; Hager, VersR 1984, 799 (804); Schwenzer, JZ 1987, 1059 (1063); im Ausgangspunkt auch Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 326 „der echte Rückruf ist das lockende Versprechen kostenloser Abhilfe“.

1322 Vgl. Xia, Die Pflicht zum Produktrückruf, S. 95; Bodewig, Der Rückruf fehlerhafter Produkte, S. 281.

1323 Dazu Xylander, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 165; Bodewig, Der Rückruf fehlerhafter Produkte, S. 283.

schlichte Rücknahmeangebot des Herstellers zu befolgen.¹³²⁴ Ablehnende Stimmen sehen dagegen mit einem kostenfreien Rückruf die Grenze des vom Deliktsrecht geschützten Integritätsinteresses überschritten.¹³²⁵

Indes kann auch die Frage der Kostentragungspflicht nur vor dem Hintergrund der Effektivität der Gefahrenabwehr gesehen werden. Eine Kostenübernahme des Herstellers ist nur dort geschuldet, wo die Umstände des Einzelfalls dies aus Gründen der Effektivität der Gefahrenabwehr fordern.¹³²⁶ In diesem Zusammenhang listet auch der BGH Maßnahmen auf, die je nach Einzelfall unterhalb der Schwelle eines kostenlosen Rückrufs ausreichend sein können. So mag es vielfach genügen, dass die Abnehmer über die Notwendigkeit der Nachrüstung oder Reparatur informiert werden und der Hersteller seine Hilfe anbietet, sodass die Nutzer diese Maßnahmen auf eigene Kosten durchführen können. Auch eine Stilllegungsaufforderung unter Einschaltung der zuständigen Behörden wird dabei angesprochen.¹³²⁷ Die Frage der Kostentragung hat sich auch am Kriterium der Effektivität der Gefahrenabwehr auszurichten. Ist die völlige Kostenübernahme durch den Hersteller daher mit Blick auf die Gefahrenabwehr erforderlich, kann diese nicht mit Verweis auf das zugleich gewährte Äquivalenzinteresse abgelehnt werden.¹³²⁸ Andererseits erfordert eine effektive Gefahrenabwehr auch nicht immer einen kostenfreien Rückruf. Zwischen der Warnung und dem kostenlosen Rückruf gibt es Maßnahmen, die je nach Einzelfall genügend Anreiz für die Produktnutzer bieten, das Sicherheitsniveau des Produkts wiederherzustellen und damit auch eine effektive Gefahrenabwehr gewährleisten.¹³²⁹

1324 Xia, Die Pflicht zum Produktrückruf, S. 96, 99; für den Regelfall auch Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 367 und Bodewig, Der Rückruf fehlerhafter Produkte, S. 283 f.

1325 Förster, in: BeckOK, BGB, § 823, Rn. 752; Dietborn/Müller, BB 2007, 2358 (2361); tendenziell auch Burckhardt, VersR 2007, 1601.

1326 BGH, NJW 2009, 1080 (1081, Rn. 12 f.); vgl. dazu auch Lüftenegger, Die Rückruffpflicht des Herstellers, S. 246; so schon Staudinger/Czaplinski, JA 2008, 401 (405 f.).

1327 BGH, NJW 2009, 1080 (1081, Rn. 13).

1328 Vgl. die Argumentation unter E.I.3.a); daneben Xia, Die Pflicht zum Produktrückruf, S. 99; Huber, Rechtsfragen des Produktrückrufs, S. 273; Rosenberger, Die außervertragliche Haftung für automatisierte Fahrzeuge, S. 425.

1329 Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 367 spricht von einem „bedingte[n] Rückruf“; vgl. auch Ackermann/Golling, ZfPC 2022, 67 (71).

b) Bedeutung für die Fallgruppen der Rückrufflicht

So sind Fälle denkbar, in denen bereits das bloße Reparaturangebot auch ohne Kostenübernahme durch den Hersteller einen erheblichen Mehrwert für den Nutzer haben kann.¹³³⁰ Dabei ist gerade die Fallgruppe des Hinwegsetzens über eine Warnung aufgrund der Unzumutbarkeit der Gefahrensteuerung angesprochen. Ist der Nutzer bei der Fehlerbehebung vom Hersteller abhängig und gleichzeitig auf das Produkt angewiesen, ist ihm oft schon geholfen, wenn der Hersteller ihm die Reparatur auf eigene Kosten ermöglicht, so dass er nicht vor der Wahl steht, das gefährliche Produkt weiter zu benutzen oder ein teures Ersatzprodukt kaufen zu müssen.¹³³¹

Anders ist dies, wenn die individuelle Eintrittswahrscheinlichkeit einer Rechtsgutsverletzung als gering eingeschätzt und die Produktgefahr verkannt wird. Ein kostenpflichtiges Reparaturangebot mag hier aus den gleichen Gründen in den Wind geschlagen werden wie die Warnung.¹³³² Da es sich aber regelmäßig um Fabrikationsfehler handeln wird, ist es denkbar, dass der Hersteller eine kostenlose Überprüfung des einzelnen Produkts auf Fehlerhaftigkeit anbietet, die Kosten einer eventuellen Reparatur aber vom Nutzer zu tragen sind.¹³³³

Kann eine Warnung nicht ausreichend Gefahrenbewusstsein schaffen und wird ein Rückruf deshalb erforderlich, muss einzelfallabhängig entschieden werden, ob ein bloßes Reparaturangebot genügend Anreiz beim Produktnutzer schaffen kann, sich an der Rückrufaktion zu beteiligen.

Interessant sind die Fälle, in denen eine Warnung nicht ausreicht, also ein Rückruf erforderlich ist, der Hersteller dem Nutzer aber nicht einmal ein Reparaturangebot machen kann, weil die Reparatur schlicht unmöglich ist. Dass eine Warnung hier gerade keine wirksame Maßnahme zur Gefahrenabwehr darstellt,¹³³⁴ steht außer Frage, denn sonst würde ein Rückruf gar nicht in Betracht kommen. Ist das Produkt dagegen allein wegen seiner Gefährlichkeit wertlos oder wegen des Sicherheitsmangels nicht mehr funktionsfähig, stellt sich die Frage eines Rückrufs regelmäßig nicht, weil eine gefährliche Weiterbenutzung nicht in Betracht kommt und

1330 In diese Richtung auch *Huber*, Rechtsfragen des Produktrückrufs, S. 274f. „erhöhte[r] Motivationsdruck“ im Vergleich zur Warnung.

1331 Dies verkennt aber gerade *Xia*, Die Pflicht zum Produktrückruf, S. 96 f.

1332 Vgl. *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 165.

1333 So *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 284.

1334 Anders aber *Lüftenegger*, NJW 2018, 2087 (2090), der die einzig effektive Gefahrenabwehr darin sieht, auf den Gebrauch zu verzichten.

eine Warnung ausreicht.¹³³⁵ Vor diesem Hintergrund wird in diesen Fällen eine effektive Gefahrenbeseitigung nur durch eine Rückgabe des Produkts gegen Erstattung des Kaufpreises oder das Angebot eines Ersatzprodukts gewährleistet werden können.¹³³⁶

c) Weitere Differenzierungsansätze

In der juristischen Literatur werden daneben weitere Differenzierungskriterien vertreten. Insbesondere soll der Hersteller die Kosten für den Ausbau gefährlicher Teile, nicht aber die Materialkosten und die Kosten für den Einbau neuer Teile zu tragen haben.¹³³⁷ Teilweise soll diese Einschränkung nur für Sach-, nicht aber für Personengefahren Dritter gelten, sondern dort insgesamt eine hälftige Kostenteilung erfolgen.¹³³⁸ Die Beschränkung auf die Ausbaukosten soll eine schärferer Abgrenzung des Integritäts- vom Äquivalenzinteresse ermöglichen.¹³³⁹ Denn die Produktsicherheit werde bereits mit dem Ausbau der gefährlichen Teile sichergestellt, während der Einbau neuer Teile lediglich der Wiederherstellung der Gebrauchstauglichkeit diene und daher dem Nutzer auferlegt werden sollte.¹³⁴⁰ Daneben wird mit Erwägungen der Verhältnismäßigkeit angesichts der eigenen Produktverantwortung des Nutzers argumentiert.¹³⁴¹ Zwar wird mit dem Ausbau der fehlerhaften Teile die Gefahr rein technisch beseitigt. Zu dieser Gefahrenbeseitigung kommt es allerdings nur, wenn der Nutzer dem Hersteller das Produkt dafür zur Verfügung stellt.¹³⁴² Werden aber lediglich die Ausbaukosten vom Hersteller übernommen, die angesichts der Materialkosten des Ersatzteils und den Einbaukosten regelmäßig eher einen kleinen Teil der Gesamtkosten ausmachen dürften, ist der Anreiz für den Nutzer kaum einmal größer als bei einer gänzlich eigenen Kostentragung

1335 Vgl. dazu Hager, VersR 1984, 799 (804 f.); Hager, in: Staudinger, BGB, § 823, Rn. F 25; Tamme, Rückruftkosten, S. 157 f.

1336 Schwenger, JZ 1987, 1059 (1063 f.); Huber, Rechtsfragen des Produktrückrufs, S. 277; Bodewig, Der Rückruf fehlerhafter Produkte, S. 286 f.

1337 So Voigt, in: BeckOGK, BGB, § 823, Rn. 684; Staudinger/Czaplinski, JA 2008, 401 (405); Pieper, BB 1991, 985 (988).

1338 Staudinger/Czaplinski, JA 2008, 401 (405 f.).

1339 Voigt, in: BeckOGK, BGB, § 823, Rn. 684; Staudinger/Czaplinski, JA 2008, 401 (405).

1340 Staudinger/Czaplinski, JA 2008, 401 (405).

1341 Staudinger/Czaplinski, JA 2008, 401 (405).

1342 So auch Xia, Die Pflicht zum Produktrückruf, S. 96 f.

der Reparatur.¹³⁴³ Aus diesem Grund hat die Kostenverteilung zwischen Hersteller und Nutzer so zu erfolgen, dass noch ausreichend Anreize für den Nutzer bestehen, an der Rückrufaktion des Herstellers mitzuwirken.¹³⁴⁴ Dass im Rahmen der Gefahrenabwehr auch das Äquivalenzinteresse mitverwirklicht wird, ist unerheblich, wenn dies aus Gründen der Effektivität erforderlich ist. Verhältnismäßigkeitsgesichtspunkte spielen dagegen bei der Gefahrenabwehr von vornherein keine Rolle, da diese allein auf die Effektivität im Hinblick auf den Rechtsgüterschutz ausgerichtet ist. Eine Beschränkung der herstellerseitigen Kostentragung auf die Ausbaukosten verliert aber die Effektivität der Gefahrenabwehr aus den Augen und ist daher nicht überzeugend.

Die Kostentragungspflicht des Herstellers dagegen durch den Abzug „neu für alt“ zu begrenzen, entspricht einem allgemeinen schadensrechtlichen Grundsatz und dürfte die Effektivität der Gefahrenabwehr regelmäßig nicht in Frage stellen und auch vom Produktnutzer mitgetragen werden.¹³⁴⁵

6. Bedeutung der Boston Scientific-Entscheidung

Auf Vorlage des BGH äußerte sich der EuGH in seiner Boston Scientific-Entscheidung zu der Frage, ob die mit dem Austausch verbundenen Kosten implantierter und fehleranfälliger Herzschrittmacher bzw. Kardioverter-Defibrillatoren (ICD) nach § 1 Abs. 1 S. 1 ProdHaftG erstattungsfähig sind.¹³⁴⁶ Da die implantierten Herzschrittmacher selbst noch keine Körper- oder Gesundheitsverletzung verursacht haben und Streitgegenstand ausschließlich die Ausbaukosten des alten und die Einbaukosten des neuen Geräts sind,¹³⁴⁷ ist die Entscheidung auch im Zusammenhang mit der Rückrufproblematik zu sehen.

1343 Xia, Die Pflicht zum Produktrückruf, S. 96 f.

1344 Xia, Die Pflicht zum Produktrückruf, S. 95 f.

1345 Hierfür auch *Schwenzer*, JZ 1987, 1059 (1063); *Tamme*, Rückrufkosten, S. 144 f.; *Xia*, Die Pflicht zum Produktrückruf, S. 98 f.; *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 287.

1346 EuGH, NJW 2015, 1163. Die Vorgaben der Vorabentscheidung setzte der BGH dann in zwei Entscheidungen um, BGH, NJW 2015, 3096 und BGH, NJW 2015, 2507.

1347 Vgl. *Brügemeier*, MedR 2014, 537 (538).

a) Berücksichtigung der Pflegebetten-Entscheidung

Wendet man die Rückrufrechtsprechung des BGH nach den in der Pflegebetten-Entscheidung aufgestellten Grundsätzen auf den vorliegenden Fall an, ist zweifelhaft, ob sich eine Rückrufpflicht des Herstellers ergibt. Im vorliegenden Fall kann zwar eine auf die Warnung des Herstellers vorgenommene nutzerseitige Stilllegung des Geräts die unmittelbar von ihm ausgehende Gefahr beheben, dies kann aber zugleich dazu führen, dass der auf den Herzschrittmacher angewiesene Patient Gesundheitsschäden erst erleidet. Gerade wenn ein Produkt eine Sicherheitsfunktion erfüllt, können durch seine Außerbetriebnahme oder Nichtnutzung neue Gefahren entstehen, nämlich genau die, vor denen das Produkt eigentlich schützen soll. Teilweise wird in solchen Fallkonstellationen das Paradebeispiel dafür gesehen, dass ein Nutzungsverzicht nicht möglich und eine Warnung daher nicht ausreichend ist.¹³⁴⁸

Indes kann zwar die Nutzung des Produkts nicht einfach eingestellt werden, da sich hieraus gerade eine Rechtsgutsverletzung ergeben kann. Allerdings ist davon auszugehen, dass sich die Nutzer auf eine Warnung des Herstellers hin bei einem so lebenswichtigen Produkt wie einem Herzschrittmacher umgehend eigenständig um dessen Überprüfung und gegebenenfalls um dessen Austausch bemüht hätten.¹³⁴⁹ Ist der Nutzer daher bei der Fehlerbehebung nicht auf die Mitwirkung des Herstellers angewiesen, kann von einer fehlenden Möglichkeit zur Gefahrensteuerung regelmäßig keine Rede sein.¹³⁵⁰ Versetzt eine Warnung den Produktnutzer damit in die Lage hinreichender Gefahrenkenntnis und hat dieser auch die tatsächliche Möglichkeit der Gefahrensteuerung, ist nicht ersichtlich, warum eine Warnung nicht zur effektiven Gefahrenabwehr ausreichen soll. Anders kann dies in Fällen sein, in denen die fehlende Sicherungsfunktion des Produkts durch die Stilllegung auch zu einer Gefährdung Dritter führen kann. Hier ist eine Warnung nur ausreichend, wenn vom Nutzer nicht nur die Außerbetriebnahme des Produkts erwartet werden kann, sondern auch die Nachrüstung, dass die ursprüngliche Sicherungsfunktion des Pro-

1348 Lüftenegger, Die Rückrufpflicht des Herstellers, S. 260, 262; vgl. auch Hager, VersR 1984, 799 (806).

1349 So Rudkowski, VersR 2018, 65 (71).

1350 Handorn, MPR 2009, 37 (42) schränkt daher hier wohl die Rückrufpflicht auf Fallkonstellationen ein, in denen „der Betreiber in absehbarer Zeit kein Ersatzgerät anderweitig anschaffen kann“.

dukts wieder erfüllt wird.¹³⁵¹ Die Fallgruppe des Hinwegsetzens über eine Warnung durch die möglicherweise ausfallenden Herzschrittmacher war mangels Drittfährdung aber schon nicht einschlägig.

b) Argumentationslinien des EuGH

In der Boston Scientific-Entscheidung stellte der EuGH fest, dass der Schadensersatz im Rahmen von § 1 Abs. 1 ProdHaftG auch den Austausch der fehlerhaften Produkte beinhalten könne. Denn der Schadensersatz umfasse alles, was erforderlich sei, um die Schadensfolgen zu beseitigen und das notwendige Sicherheitsniveau wiederherzustellen.¹³⁵² Auch wenn die Produkthaftungsrichtlinie eine Haftung des Herstellers an einen Produktfehler im Zeitpunkt der Inverkehrgabe knüpft und den Hersteller nicht zu einer Produktbeobachtung nach diesem Zeitpunkt und damit auch nicht zur Wiederherstellung eines bestimmten Sicherheitsniveaus verpflichtet, wird die Ersatzfähigkeit der Austauschkosten vom EuGH als Schaden hergeleitet.¹³⁵³ Allerdings haftet der Hersteller nicht für jeden Schaden, der durch sein fehlerhaftes Produkt verursacht wurde, sondern nur bei einer Verletzung der tatbestandlich geschützten Rechtsgüter. Reine Vermögensschäden sind insoweit nicht ausreichend. Gerade bei der Benennung der relevanten Rechtsgutsverletzung blieb der EuGH aber vage.¹³⁵⁴ Insoweit argumentierte die Kammer, „dass es sich bei dem durch eine chirurgische Operation zum Austausch eines fehlerhaften Produkts [...] verursachten Schaden um einen „durch Tod und Körperverletzungen verursachten Schaden“ handelt, für den der Hersteller haftet, wenn diese Operation erforderlich ist, um den Fehler des betreffenden Produkts zu beseitigen.“¹³⁵⁵ Abgestellt wird damit weder auf einen durch die Operationskosten verursachten reinen Vermögensschaden noch auf eine bloße Rechtsgutsgefährdung¹³⁵⁶ durch die Implantation eines potenziell fehlerbehafteten Geräts, sondern auf die durch die Austauschoperation verursachte Körperverletzung.¹³⁵⁷

1351 So die Fallkonstellation in OLG Nürnberg, BeckRS 2013, 6837.

1352 EuGH, NJW 2015, 1163 (1164 f., Rn. 49 f.).

1353 Vgl. Wagner, JZ 2016, 292 (300 f.).

1354 Mäsch, JuS 2015, 556 (558); Oeben, Der potenzielle Produktfehler, S. 140, 143.

1355 EuGH, NJW 2015, 1163 (1165, Rn. 55).

1356 Krit. hierzu schon BGH, NJW 2009, 1080 (1083, Rn. 23).

1357 Krit. Brügge, MedR 2014, 537 (538) und Mäsch, JuS 2015, 556 (558); zustimmend Oeben, Der potenzielle Produktfehler, S. 144 f.; argumentativ Wagner, JZ 2016, 292 (300) und Reich, EuZW 2014, 898 (899).

Dabei kommt die Anerkennung eines solchen Ersatzanspruchs im Rahmen des ProdHaftG „der Selbsterfüllung von Rückruffpflichten des Herstellers gefährlich nahe“.¹³⁵⁸ Prima facie geht die Entscheidung mit der Anerkennung der Austauschoperation als durch den Fehler verursachte Körperverletzung über die Grundsätze der Pflegebetten-Entscheidung des BGH hinaus. Ein über das Integritätsinteresse hinausgehender Schutz des Äquivalenzinteresses, welcher auch der Produkthaftungsrichtlinie fremd ist, klingt auch durch die Formulierung an, wonach der Hersteller „das Sicherheitsniveau wiederherzustellen [hat], das man nach Art. 6 Abs. 1 der Richtlinie zu erwarten berechtigt ist.“¹³⁵⁹ Indes verdeutlicht auch der EuGH, dass das Produkthaftungsrecht allein dem Schutz des Integritätsinteresses dient. Denn die Kammer führt aus, dass ein Schadensersatz nicht verlangt werden kann, falls das vom Hersteller empfohlene Ausschalten des Magnetschalters geeignet gewesen wäre, den potenziellen Produktfehler der ICDs und damit das mit dem Ausfall verbundene Schadensrisiko zu beseitigen.¹³⁶⁰ Dann nämlich wären die Kosten der präventiven Austauschoperation nicht erforderlich gewesen und damit als Äquivalenzschaden nicht ersatzfähig.¹³⁶¹ Die Tatsache, dass nicht mehr alle Funktionen des Geräts hätten genutzt werden können, ist dem Äquivalenzinteresse zuzuordnen und kann demnach keine Rolle spielen.¹³⁶² Folglich scheidet die Ersatzfähigkeit von Fehlerbeseitigungskosten aus, sollten weniger einschneidende Maßnahmen zur Verfügung stehen, die keine Rechtsgutsverletzung beim Produktnutzer erfordern und das von dem Produkt ausgehende Risiko beseitigen.¹³⁶³

c) Bewertung der Boston Scientific-Entscheidung

Eine Erweiterung der Rückruffpflichten und die Anerkennung der Kostentragung bei Austausch, Reparatur oder Ersatzlieferung geht mit der Boston Scientific-Entscheidung damit nur in eng umgrenzten Fallgruppen einher. Denn regelmäßig wird sich die Gefährdung der Produktnutzer auf andere

1358 So *Wagner*, JZ 2016, 292 (300 f.).

1359 So EuGH, NJW 2015, 1163 (1164, Rn. 49); dazu *Handorn*, MPR 2015, 91 (96 f.); *Moelle/Dockhorn*, NJW 2015, 1163 (1165); *Wagner*, JZ 2016, 292 (300 f.); *Oeben*, Der potenzielle Produktfehler, S. 140.

1360 EuGH, NJW 2015, 1163 (1164, Rn. 54 f.).

1361 *Handorn*, MPR 2015, 91 (97); *Oeben*, Der potenzielle Produktfehler, S. 144.

1362 *Moelle/Dockhorn*, NJW 2015, 1163 (1165).

1363 *Handorn*, MPR 2015, 91 (97); *Wagner*, JZ 2016, 292 (301); *Oeben*, Der potenzielle Produktfehler, S. 144.

Weise als durch Eingriff in deren Rechtsgüter beseitigen lassen, insbesondere durch eine Warnung verbunden mit der Aufforderung, den Gebrauch des Produkts einzustellen.¹³⁶⁴ Bei einem Herzschrittmacher, sollte dieser nicht durch technische Maßnahmen von außen deaktiviert werden können – und hier liegt die Besonderheit des Falles – kommt eine Stilllegung ohne rechtsgutsverletzende Operation aber gerade nicht in Betracht. Auch eine Warnung zieht hier eine Operation und damit eine Körperverletzung mit entsprechendem Schaden nach sich. Die Produktgefahr lässt sich in jedem Fall nur durch die Verletzung der körperlichen Integrität des Nutzers beheben.¹³⁶⁵ Anders als im Rahmen der Produktbeobachtungspflicht spielt es keine Rolle, ob der Produktnutzer einer Warnung Folge leisten wird und diese damit aus Gründen der Effektivität der Gefahrenabwehr also gerade ausreichend ist. Es kommt allein auf die eingetretene Rechtsgutsverletzung und den daraus resultierenden Schaden an. Insoweit sind die Anknüpfungstatsachen bei der Produktbeobachtungspflicht und beim Schadensersatzanspruch aus § 1 Abs. 1 S. 1 ProdHaftG andere. Dass Gefahrenabwendungsmaßnahmen aber zwangsläufig zu Rechtsgutsverletzungen des Nutzers mit einhergehendem Schaden führen, ist bei kaum einer anderen Produktgattung als bei implantierten Medizinprodukten denkbar.¹³⁶⁶ Die Haftung des Herstellers für solche Ausbaukosten wird sich folglich nur dort stellen, wo die Gefahrenabschirmung des Nutzers allein und notwendigerweise mit einer Rechtsgutsverletzung einhergeht.¹³⁶⁷ Insofern sollte die Boston Scientific-Entscheidung des EuGH im Hinblick auf die Rückrufproblematik nicht als Widerspruch zur Pflegebetten-Entscheidung des BGH begriffen, sondern als spezieller Teilaspekt aufgegriffen werden.

III. Smarte Reaktionspflichten

Nachdem die Reichweite der herkömmlichen Reaktionspflichten analysiert wurde, ist nun zu untersuchen, inwieweit diese Grundsätze auch auf die smarten Reaktionsmöglichkeiten übertragen werden können.

1364 So auch *Wagner*, in: MüKo, BGB, § 3 ProdHaftG, Rn. 59.

1365 Vgl. *Wagner*, JZ 2016, 292 (301); *Mayrhofer*, Außervertragliche Haftung für fremde Autonomie, S. 289.

1366 *Handorn*, MPR 2015, 91 (96); *Wagner*, JZ 2016, 292 (301).

1367 *Moelle/Dockhorn*, NJW 2015, 1163 (1165).

1. Updatepflichten

Zunächst soll der Frage nachgegangen werden, ob bzw. unter welchen Voraussetzungen den Hersteller smarter Produkte Updatepflichten zur Gefahrenabwehr treffen können.

a) Gefahrenabwehr durch Updates

Dabei muss zunächst geklärt werden, in welchen unterschiedlichen Ausprägungen Gefahrenabwehrmaßnahmen als Updates möglich sind.

In Betracht kommt zunächst die bloße Bereitstellung eines Updates, das die bestehende Sicherheitsgefahr behebt. Ein solches müsste der Nutzer dann nach einem entsprechenden Hinweis des Herstellers eigenverantwortlich durchführen. Daneben kann die Behebung einer Sicherheitslücke oder eines sonstigen Softwarefehlers auch durch ein automatisches Sicherheitsupdate erfolgen; dies beispielsweise, wenn die automatische Installation von Updates als Standardkonfiguration voreingestellt ist oder ein solches Vorgehen vom Nutzer gewünscht wird. Dabei kann der Nutzer eine (voreingestellte) automatische Update-Funktion jederzeit deaktivieren.¹³⁶⁸ Daneben ist aber auch möglich, dass eine entgegenstehende Willensäußerung des Nutzers durch ein Zwangsupdate „überspielt“ wird.¹³⁶⁹ In allen Fällen sind solche Sicherheitsupdates möglich, wenn nicht die physischen Komponenten eines Produkts betroffen sind, sondern Gefahren von der verwendeten Software ausgehen.¹³⁷⁰ Ist dagegen die Hardware betroffen, bleibt es regelmäßig bei den beschriebenen Kriterien, da sich solche Mängel kaum einmal mittels eines Softwareupdates beheben lassen.¹³⁷¹ Der Unterschied zu einer herkömmlichen Nacherfüllung oder Reparatur liegt nun darin, dass Updates regelmäßig „Over-the-Air“ („OTA“) erfolgen und so der Gang in die Werkstatt zur Fehlerbehebung entfällt;¹³⁷² dies freilich nur wenn das Produkt dafür ausgelegt ist, also über eine Internetanbindung verfügt und von seiner Hard- und Software für OTA-Updates ausgerüstet

1368 Vgl. *Riehm*, in: Schmidt-Kessel/Kramme (Hg.), *Geschäftsmodelle in der digitalen Welt*, S. 201 (221).

1369 Vgl. *Duden*, *Digitale Sachherrschaft*, S. 59.

1370 Vgl. *Sommer*, *Haftung für autonome Systeme*, S. 279.

1371 *Thöne*, *Autonome Systeme*, S. 215 (Fn. 127).

1372 *Wittig*, *Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten*, S. 236.

ist („updateable“)¹³⁷³ sowie die Sicherheitsgefahr durch Software beseitigt werden kann.

Ferner ist über ein Update und die darin enthaltenen Steuerbefehle auch die vollständige oder teilweise Deaktivierung der Geräte aus der Ferne möglich. Daneben kommt eine faktische Deaktivierung durch die Einstellung notwendiger Serverdienste in Betracht, auf die das Produkt angewiesen ist.¹³⁷⁴ Gerade bei Geräten, deren Funktionalität in hohem Maße von solchen externen Diensten abhängt, führt die Einstellung dieser Dienste dazu, dass das Produkt nur noch eine „nutzlose Hülle“ darstellt und aufgrund der Funktionslosigkeit vom Nutzer nicht mehr verwendet wird.¹³⁷⁵ In beiden Fällen weist die Fernstilllegung des Produkts durch den Hersteller eine inhaltliche Parallele zum Produktrückruf als Maßnahme auf, mit der das gefährliche Produkt aus dem Verkehr gezogen wird.¹³⁷⁶ Zwar geht es nicht um die Rückgabe des Produkts an den Hersteller, sondern um die direkte Stilllegung beim Nutzer.¹³⁷⁷ Allerdings dient auch die Rückführung an den Hersteller keinem Selbstzweck, sondern ist darauf

1373 Zu dieser Anforderung als Konstruktionspflicht nach Deliktsrecht schon *Reusch*, BB 2019, 904 (906); *Hartmann*, PHi 2017, 42 (46); *Wiesner*, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 10.6, Rn. 41; *Wagner*, in: MüKo, BGB, § 823, Rn. 1130; ausführlich *Brenner et al.*, RDt 2024, 252 (254 ff.).

1374 Vgl. die einleitend genannte Schlagzeile, wonach Samsung im Jahr 2017 bei seinem Galaxy Note 7 ein Softwareupdate durchführte, wodurch die Batteriekapazität auf Null gesetzt wurde und ein Aufladen des Akkus nicht mehr möglich war, damit Nutzer, die einem herkömmlichen Rückruf nicht nachkamen, das explosionsgefährdete Gerät nicht mehr nutzen konnten, vgl. den Bericht der EU-Kommission über die Auswirkungen Künstlicher Intelligenz, des Internets der Dinge und der Robotik im Hinblick auf Sicherheit und Haftung, COM (2020) 64 final, S. 3 und <https://www.golem.de/news/samsung-galaxy-note-7-wird-per-update-endgueltig-lahmgelegt-1703-126934.html> (zuletzt abgerufen am 23.09.2024); vgl. zum Ganzen nur *Regenfus*, JZ 2018, 79 (79); *Grünvogel/Dörrenbächer*, ZVertriebsR 2019, 87 (90); *Schrader*, DAR 2018, 314 (317); *Wittig*, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 231 f.; *Wagner*, in: MüKo, BGB, § 823, Rn. 320, 1133; *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 102; *Ackermann*, in: NK-ProdR, § 823 BGB, Rn. 138; *Sedlmaier*, in: Kühne/Nack (Hg.), Connected Cars, S. 44; *Fida*, Updates, Patches & Co, S. 162; *Burrer*, in: Bräutigam/Kraul (Hg.), Internet of Things, § 8, Rn. 101.

1375 *Solmecke/Vondrlík*, MMR 2013, 755 (758); vgl. auch *Kuschel*, AcP 220 (2020), 98 (102).

1376 *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 103; *Regenfus*, JZ 2018, 79 (82); *Sommer*, Haftung für autonome Systeme, S. 284.

1377 Daher spricht *Sedlmaier*, in: Kühne/Nack (Hg.), Connected Cars, S. 44 von „Vorstufe zum Produktrückruf“.

angelegt, das Produkt aus dem Verkehr zu ziehen.¹³⁷⁸ Die Deaktivierung durch den Hersteller ist im Gegensatz zu der bei herkömmlichen Produkten erforderlichen Rückgabeaufforderung an den Benutzer aber jedenfalls technisch nur insoweit von der Mitwirkung des Nutzers abhängig, dass er die Schnittstellenkonnektivität nicht unterbindet oder die Schnittstelle selbst nicht blockiert. Vor diesem Hintergrund erlangt diese Maßnahme als Mittel der Gefahrenabwehr gerade neben der Warnung eigenständige Bedeutung.

Damit lassen sich Updates unterscheiden, die zum einen eine durch einen Softwarefehler oder eine Sicherheitslücke ausgelöste Gefahr beheben (Sicherheitsupdates), und Updates, die zum anderen das Produkt über enthaltene Steuerbefehle oder die Einstellung notwendiger Serverdienste ganz oder teilweise deaktivieren (Fernstilllegung).

b) Verhältnis von Warnung und Updates

In Anknüpfung an die Pflegebetten-Entscheidung kommen Updatepflichten – ungeachtet ihrer konkreten Ausgestaltung – als weitergehende Sicherungsmaßnahmen aber erst in Betracht, wenn eine Warnung zur Gefahrenabwehr nicht hinreichend effektiv ist.

Eine Updatepflicht aber allein aus der im Vergleich zur Warnung größeren Effektivität bei der Gefahrenabwehr herzuleiten, greift jedoch zu kurz.¹³⁷⁹ Zwar stellt sich ein Sicherheitsupdate als effizienteres Mittel der Gefahrenabwehr dar, da es mit einer flächendeckenden Ursachenbekämpfung einhergeht, während eine Warnung lediglich auf eine Gefahr hinweist, diese aber noch nicht beseitigt.¹³⁸⁰ Indes ist die Ausgangslage bei der klassischen Reparatur oder Nachrüstung keine andere.¹³⁸¹ Auch eine Fernstilllegung des Geräts durch den Hersteller unter Umgehung des Nutzers ist prima facie effektiver als eine Warnung. Immerhin können von einem derart stillgelegten Gerät regelmäßig keine Gefahren mehr für die Rechte und Rechtsgüter der Nutzer oder Dritten ausgehen, sodass der Hersteller da-

1378 Dazu BGH, NJW 2009, 1080 (1081, Rn. 11).

1379 In diese Richtung aber *Reusch*, BB 2019, 904 (909); ähnlich *Eichelberger*, in: Ebers et al., (Hg.), Künstliche Intelligenz und Robotik, S. 189.

1380 Vgl. *Hinze*, Haftungsrisiken des automatisierten und autonomen Fahrens, S. 162; *Eichelberger*, in: Ebers et al. (Hg.), Künstliche Intelligenz und Robotik, S. 189.

1381 *Huber*, Rechtsfragen des Produktrückrufs, S. 204; *Hinze*, Haftungsrisiken des automatisierten und autonomen Fahrens, S. 162.

mit seiner Gefahrensteuerungspflicht in vollem Umfang nachkäme.¹³⁸² Allerdings lässt sich aus der Maxime der Effektivität der Gefahrenabwehr nicht folgern, dass der Hersteller gerade die bestmögliche Maßnahme zur Gefahrenabwehr umzusetzen hat.¹³⁸³ Denn seine Verantwortung ist durch die Verantwortung des Produktnutzers begrenzt.¹³⁸⁴ Damit bestehen weitergehende Sicherungspflichten über die Warnung hinaus nur, wenn die Gefahr nicht auf anderem Wege effektiv beseitigt werden kann.¹³⁸⁵ Folglich kann eine Warnung auch dann ausreichend sein und die Produktbeobachtungspflicht erfüllt werden, wenn technisch die Möglichkeit besteht, die Gefahr durch Updates abzuwenden.¹³⁸⁶

Bei der Abgrenzung, ob Updatepflichten bei smarten Produkten zur Gefahrenabwehr erforderlich sein können, soll an die vom BGH entwickelten Fallgruppen angeknüpft werden, in denen eine Warnung nicht mehr ausreichend ist und eine Rückrufpflicht in Betracht kommt.

aa) Geeignetheit der Warnung

Hinsichtlich einer Warnung ist bei smarten Produkten eine Besonderheit zu beachten, die bereits die Geeignetheit einer Warnung als Gefahrenabwehrmaßnahme in Frage stellen kann. Führen Softwarefehler zu Sicherheitslücken, kann eine öffentliche Warnung vor der Schwachstelle gerade zu einer Erhöhung der Gefahr für die betroffenen Rechtsgüter führen. Denn durch die Warnung werden nicht nur die Produktnutzer über die Schwachstelle informiert, sondern auch potenzielle Angreifer. Diese könnten durch eine öffentliche Warnung erst auf die Schwachstelle aufmerksam gemacht werden, sodass eine solche Warnung die Gefahr birgt, dass An-

1382 *Regenfus*, JZ 2018, 79 (83) auch mit dem Hinweis in Fn. 41 auf die Boston-Scientific-Entscheidung, in der der EuGH die Deaktivierung des Geräts bzw. einer gefährlichen Funktion als grundsätzlich ausreichend angesehen hat, vgl. EuGH, NJW 2015, 1163 (1164 f., Rn. 54); ähnlich *Wittig*, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 232.

1383 Allgemein schon *Lüftenegger*, Die Rückrufpflicht des Herstellers, S. 242; im hiesigen Kontext *Meents*, in: FS Taeger, S. 13 (19 f.) und *Meents/Obradovic*, ZfPC 2022, 13 (15 f.); *Lüftenegger*, RD i 2021, 293 (300).

1384 *Lüftenegger*, Die Rückrufpflicht des Herstellers, S. 242; anmahndend auch *Klindt*, BB 2009, 792 (795).

1385 *Kipker/Walkusz*, DuD 2019, 513 (517).

1386 *Meents*, in: FS Taeger, S. 13 (20) und *Meents/Obradovic*, ZfPC 2022, 13 (16).

griffswellen erst hervorgerufen oder vergrößert werden.¹³⁸⁷ Anders ist dies freilich, wenn die Schwachstelle ohnehin bereits breiten Kreisen bekannt geworden ist.¹³⁸⁸

Allerdings ermöglichen smarte Produkte vielfach eine individuelle Kommunikation mit dem Nutzer.¹³⁸⁹ Eine Warnung kann zielgerichtet bspw. über ein Bediendisplay am Produkt via Datenverbindung eingespielt werden und den Nutzer individuell auf die Gefahr aufmerksam machen.¹³⁹⁰ Vergleichbares gilt bei Produkten ohne Display, die über eine zugehörige App verfügen und mit dem Smartphone verbunden sind.¹³⁹¹ Besteht die Möglichkeit einer derart individuellen und zielgerichteten Warnung, ist sie jedenfalls bei von Hackern ausnutzbaren Sicherheitslücken einer öffentlichen Warnung vorzuziehen.¹³⁹² Aber auch eine individuelle und zielgerichtete Warnung des Nutzers kann Hacker über Umwege erreichen. Spätestens wenn sich Nutzer in Internet-Foren über die Sicherheitslücke austauschen oder beschweren, ist die Information öffentlich. Ist eine gezielte Warnung der Nutzer dagegen schon nicht möglich, sind Updates aber technisch möglich, ist von einer öffentlichen Warnung vor der Sicherheitslücke abzugehen, da diese sonst die Gefahrenlage verschärfen würde. Insoweit ist nämlich zu berücksichtigen, dass eine öffentliche Warnung mit einer erheblichen zeitlichen Verzögerung beim Nutzer ankommen kann, wenn sie ihn denn überhaupt erreicht und Angreifer diese Zeitspanne bereits ausgenutzt haben können. Vor diesem Hintergrund ist auch bei einer Warnung ledig-

1387 Vgl. nur *Raue*, NJW 2017, 1841 (1844); *Wittig*, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 229 f.; *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), *Produkthaftungshandbuch*, § 24, Rn. 175; *Spindler*, NJW 2004, 3145 (3147); *Wiebe*, NJW 2019, 625 (629); *Rockstroh/Kunkel*, MMR 2017, 77 (81); *Wiesemann/Mattheis/Wende*, MMR 2020, 139 (140); *May/Gaden*, InTer 2018, 110 (113); *Droste*, CCZ 2015, 105 (108).

1388 *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), *Produkthaftungshandbuch*, § 24, Rn. 175.

1389 *Klindt*, DAR 2023, 7 (8) „Target-genaue Ansprache“.

1390 Vgl. *Hartmann*, DAR 2015, 122 (124 f.); *Chibanguza/Schubmann*, GmbHR 2019, 313 (316); *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 162; *Lüftenegger*, RDt 2021, 293 (294).

1391 *Lüftenegger*, RDt 2021, 293 (294).

1392 *Spindler*, NJW 2004, 3145 (3147); *Spindler*, in: *Hornung/Schallbruch* (Hg.), *IT-Sicherheitsrecht*, § 11, Rn. 31; *Raue*, NJW 2017, 1841 (1844); *Hey*, Die außervertragliche Haftung des Herstellers autonomer Fahrzeuge, S. 94; allgemein *Dötsch*, Außervertragliche Haftung für KI, S. 258 „für den passenden Kommunikationsweg entscheiden“; *Piovano/Schucht/Wiebe*, *Produktbeobachtung in der Digitalisierung*, S. 101 weisen darauf hin, dass kein besonderes Formerfordernis existiert.

lich über eine zugehörige App oder ein entsprechendes Nutzerkonto im Einzelfall abzuwägen, ob diese den Nutzer erreichen wird.¹³⁹³

Insgesamt birgt bei ausnutzbaren Sicherheitslücken eine Warnung stets die Gefahr, Angriffe erst zu ermöglichen. Im Regelfall werden Updates daher schon aufgrund der mangelnden Eignung einer Warnung zur Gefahrenabwehr Vorrang haben.

bb) Warnung nicht ausreichend zur Gefahreneinschätzung und Verhaltensanpassung

Daneben versetzt eine Warnung den Produktnutzer bei Softwaregefahren möglicherweise nicht ausreichend in die Lage, die Gefahr einzuschätzen und sein Verhalten dementsprechend auszurichten. Immerhin sind softwarebedingte Sicherheitsmängel für die Produktnutzer kaum erkennbar, weil sie weder haptisch noch visuell greifbar sind.¹³⁹⁴

Es greift aber zu kurz, weitergehende Sicherungspflichten allein deshalb anzunehmen, weil Software für den Massenmarkt, aber auch smarte Produkte häufig von Nutzern mit begrenzten IT-Kenntnissen genutzt werden, die regelmäßig nicht das gesamte Gefahrenpotential einer Schwachstelle einschätzen können und daher ein geringes Gefahrenverständnis im Umgang mit dieser haben.¹³⁹⁵ Zum einen entwickelt sich zunehmend eine veränderte Beziehung der Nutzer zur Technik. Mit der zunehmenden Durchdringung des Alltags mit Technik und der immer leichteren Bedienbarkeit und Konfigurierbarkeit werden auch die IT-spezifischen Gefahren immer besser von den Nutzern einschätzbar und beherrschbar.¹³⁹⁶ Zum anderen spielt die eigene Fachkenntnis beim Befolgen einer Warnung nur eine untergeordnete Rolle.¹³⁹⁷ Es ist gerade Aufgabe der Warnung ein hinreichendes Gefahrenbewusstsein zu schaffen. Dabei ist es aber nicht

1393 Krit. *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 162, der die Einrichtung einer speziellen Empfangsvorrichtung nicht mehr von der Mitwirkungspflicht des Nutzers bei der Gefahrenabwehr umfasst sieht.

1394 *Wiebe*, NJW 2019, 625 (625); *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 176.

1395 So aber *Wittig*, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 229; *Wiebe*, InTer 2020, 66 (69); *Grapentin*, Vertragsschluss und vertragliches Verschulden beim Einsatz von KI, S. 178; in diese Richtung auch *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 98.

1396 Hierzu *Riehm/Meier*, MMR 2020, 571 (574).

1397 Vgl. schon E.II.4.b)aa)(2).

notwendig, dass der Nutzer die technischen Hintergründe im Einzelnen nachvollziehen kann. Dies wird ihm regelmäßig auch bei komplexeren analogen Produkten nicht möglich sein. Entscheidend ist vielmehr, dass er eine Vorstellung vom Gefährdungspotential erlangt und ausgehend von den potenziellen Schadensfolgen sein Verhalten darauf einstellen kann. Sicherlich kann sich ein Hersteller dabei nicht auf die Nennung des Sicherheitsproblems beschränken. Wird vor einem „buffer overflow“¹³⁹⁸ gewarnt, ist bei einem Laien nicht davon auszugehen, dass die Warnung bei ihm ein hinreichendes Gefahrenbewusstsein schafft. Anders verhält es sich aber, wenn der Zusatz erfolgt, dass hierdurch Hacker-Angriffe möglich sind und die weiteren Folgen dieser Angriffe verdeutlicht werden.¹³⁹⁹ Es wird daher nur selten Konstellationen geben, in denen das fehlende technische Verständnis der Nutzer dazu führt, dass auch eine hinreichend deutliche und detaillierte Warnung kein ausreichendes Gefahrenbewusstsein schaffen kann.

cc) Hinwegsetzen über eine Warnung

Weitere Sicherungspflichten in Form einer Updatepflicht könnten sich aber aus einem vorhersehbaren Hinwegsetzen der Nutzer über eine Warnung bei gleichzeitiger Drittgefährdung ergeben.

Da Software in smarten Produkten regelmäßige Steuerungsfunktionen zukommt, sind Drittgefährdungen bei softwarebedingten Sicherheitsmängeln ebenso denkbar wie bei physischen Teilprodukten.¹⁴⁰⁰ Daneben geht auch von Sicherheitslücken – gerade bei verbreiteter Standardsoftware – eine große Streuwirkung aus.¹⁴⁰¹ Zwar erfolgt der Zugriff der Hacker zunächst nur auf das System des individuellen Nutzers. Werden dann aber mehrere infizierte Systeme zusammengeschlossen, können über DDoS-Angriffe auch Dritte angegriffen und ganze Server zum Absturz gebracht werden.¹⁴⁰² Sicherheitslücken können sich damit auf die gesamte digitale Infrastruktur

1398 Bei einem „buffer overflow“ werden durch Fehler im Programm zu große Datenmengen in einen dafür zu kleinen reservierten Speicherbereich geschrieben. Diese Schwachstelle kann von Angreifern ausgenutzt werden.

1399 Ausführlich zu den Anforderungen *Marly*, Praxishandbuch Softwarerecht, Rn. 1824.

1400 Vgl. *Klindt*, DAR 2023, 7 (9) zur fußgängerbezogenen Schutzfunktion der Aufprall-Abbremsung im Vergleich zur softwaregesteuerten Auslösung des Fahrer-Airbags.

1401 *Raue*, NJW 2017, 1841 (1844).

1402 Im hiesigen Kontext *Grünvogel/Dörrenbächer*, ZVertriebsR 2019, 87 (89).

auswirken und haben das Potential, das Vertrauen in vernetzte IT-Systeme insgesamt zu beeinträchtigen.¹⁴⁰³

(1) Verkenntung der Produktgefahr bei Sicherheitslücken

Zunächst scheint es möglich, dass die Gefahren von den Nutzern schlicht verkannt werden und die Nutzer trotz vorhandenen Gefahrenbewusstseins eine falsche Gefahreneinschätzung vornehmen und sich deshalb über eine Warnung hinwegsetzen.

Dies drängt sich gerade bei Sicherheitslücken auf. Auch wenn bei den Nutzern ein abstraktes Problembewusstsein für Cybersicherheit vorhanden ist und durch die Warnung ein konkretes Gefahrenbewusstsein geschaffen wird, lässt sich ein Hinwegsetzen über entsprechende Warnungen beobachten. Prominentes Beispiel ist hier das veraltete Betriebssystem Windows XP. Auch ein Jahr nach der Ankündigung von Microsoft, keinen Support in Form von Sicherheitsupdates mehr zu leisten, hatte das Betriebssystem noch einen Marktanteil von knapp 15 %.¹⁴⁰⁴ Ob ein solches Hinwegsetzen über eine Warnung zu weitergehenden Sicherungspflichten führt, hängt nach den unter E.II.3.b)bb) gefundenen Ergebnissen entscheidend davon ab, ob sich dieses Nutzerverhalten nach objektiven Kriterien als naheliegend darstellt.

Eine individuell gering einzuschätzende Eintrittswahrscheinlichkeit der Rechtsgutsverletzung lässt sich aber nicht damit begründen, dass das eigene Produkt möglicherweise nicht von der Sicherheitslücke betroffen ist. Denn bei ausnutzbaren Sicherheitslücken handelt es sich um Konstruktionsfehler, die jedem der vertriebenen Softwareprodukte anhaften und somit auch die Software des Nutzers betreffen. Die Tatsache, dass die Software bisher einwandfrei funktionierte, lässt in diesem Zusammenhang auch keine anderen Schlüsse zu. Denn eine Sicherheitslücke wird regelmäßig erst mit ihrer Entdeckung gefährlich.

Die Tatsache, dass Warnungen trotz vorhandenen oder geschaffenen Problembewusstseins nicht befolgt werden, lässt sich aber regelmäßig auf eine rationale Abwägung der Nutzer zurückführen,¹⁴⁰⁵ bei der die Nutzer zu dem Ergebnis kommen, dass die Kosten der Nutzungsaufgabe im Ver-

1403 *Raue*, NJW 2017, 1841 (1844).

1404 Dieses Beispiel nennt *Raue*, NJW 2017, 1841 (1843).

1405 Aus techniksoziologischer Sicht *Herley*, NSPW 2009, 133 (134).

hältnis zu den Risiken überwiegen.¹⁴⁰⁶ Zum einen bedingen gefahrbezüglichen Sicherheitslücken in der Regel keine Nutzungsbeeinträchtigung.¹⁴⁰⁷ Zum anderen gingen bisher von Sicherheitslücken kaum physische Gefahren aus. Die Möglichkeiten der Datenkompromittierung oder des Datenverlusts sind den Nutzern zwar bewusst,¹⁴⁰⁸ dennoch handelt es sich um Rechtsgutverletzungen, die eher in Kauf genommen werden als physische Gefahren. Hinzu kommt, dass die Sicherheitslücke selbst noch nicht zu einer Rechtsgutverletzung führt, sondern es zusätzlich des vorsätzlichen Einschreitens eines Cyberkriminellen bedarf. Diese Aspekte treffen auf ein Phänomen, das in der Techniksoziologie als „security fatigue“ diskutiert wird. Die Vielzahl der Warnungen, mit denen ein Nutzer in seinem digitalen Alltag konfrontiert wird, führt zu einer gewissen Ermüdung, sich mit diesen Warnungen zu befassen und entsprechend zu handeln.¹⁴⁰⁹ Dies gilt insbesondere für Bedrohungen, vor denen zwar wiederholt gewarnt wird, von denen der Nutzer aber nach bisheriger eigener Erfahrung nicht betroffen war.¹⁴¹⁰ Gerade bzgl. Cyberbedrohungen besteht eine solche Diskrepanz zwischen der Häufigkeit von Warnungen und der subjektiv wahrgenommenen Realität.¹⁴¹¹ Diese subjektiv wahrgenommene Realität wurde auch durch in Unternehmen durchgeführte Cybersicherheitsschulungen der Mitarbeiter unterstützt. Diese Kampagnen haben zwar dazu beigetragen, das Risikobewusstsein der Arbeitnehmer auf Unternehmensebene zu schärfen, gleichzeitig führten sie aber auch dazu, dass aufgrund des Fehlens spezifischer Aufklärungsmaßnahmen im Alltag und im Privatleben der Eindruck entstanden ist, dass Unternehmen eher von Cyberangriffen betroffen sein werden als private Nutzer. Da es gerade im privaten Sektor nur wenige Daten über die Häufigkeit und Schwere der Angriffe gibt, ist auch objektiv das durch das Befolgen der Warnung verringerte Risiko spekulativ.¹⁴¹² Das von der Warnung adressierte Worst-Case-Szenario wird

1406 Piovano/Schucht/Wiebe, Produktbeobachtung in der Digitalisierung, S. 98.

1407 Meents, in: FS Taeger, S. 13 (17) weist darauf hin, dass gefahrbezügliche Sicherheitslücken meist keine Nutzungsbeeinträchtigung bedingen.

1408 Vgl. in Bezug auf Smartphones Benenson et al., FedCSIS 2012, 1179 (1181).

1409 Furnell, in: Jajodia/Samarati/Yung (Hg.), Encyclopedia of Cryptography, Security and Privacy, Kap. S.

1410 Herley, NSPW 2009, 133 (141).

1411 Furnell, in: Jajodia/Samarati/Yung (Hg.), Encyclopedia of Cryptography, Security and Privacy, Kap. S.

1412 Herley, NSPW 2009, 133 (134); auch das BSI spricht lediglich davon, dass aufgrund „der Verbreitung der schwachstellenbehafteten Produkte [...] von einer sehr großen Zahl von Betroffenen auszugehen“ ist, vgl. BSI, Sicherheitsbericht 2022, S. 11.

von der gefühlten und empirischen Realität damit nicht abgebildet und führt zu der Einstellung der Nutzer, dass sie schon nicht selbst Opfer eines solchen Angriffs werden. Damit aber haben Nutzer erkannt, dass das Ignorieren von Warnungen wenige Konsequenzen nach sich zieht, während die Nutzungsaufgabe für sie mit erheblichen Einbußen verbunden ist.¹⁴¹³ Bei der Entscheidung, eine Software trotz Warnung aufgrund der gering eingeschätzten eigenen Gefahren weiter zu nutzen, handelt es sich demnach um eine nachvollziehbare Abwägung, sodass auch nicht der Irrationalität des Produktnutzers und damit subjektiver Kriterien Berücksichtigung geschenkt wird.¹⁴¹⁴

Dieser Zusammenhang ändert sich aber, sobald die Gefahren auch auf Seiten des Produktnutzers größer werden. Dies wird aber bei allen CPS der Fall sein, da Cyberangriffe hier auch zu physischen Schäden führen können. Dann aber kann nicht mehr von einer nachvollziehbaren Abwägung gesprochen werden, sondern beruht das Hinwegsetzen über die Warnung auf irrationalen Gründen. Während also bei Sicherheitslücken reiner Software das Verkennen der Produktgefahr zu einem vorhersehbaren Hinwegsetzen über eine Warnung führen und Updatepflichten nach sich ziehen kann, wird dies bei CPS deutlich seltener der Fall sein.

(2) Unzumutbarkeit der Gefahrensteuerung jenseits von Sicherheitslücken und bei CPS

Auch jenseits von Sicherheitslücken bzw. auch bei CPS könnte sich ein Hinwegsetzen über eine Warnung aber unter dem Gesichtspunkt der für den Produktnutzer unzumutbaren Gefahrensteuerung ergeben.

α) Angewiesenheit auf den Hersteller

Bei softwarebedingten Sicherheitsmängeln sind die Reaktionsmöglichkeiten der Nutzer eingeschränkt. Denn eine eigenständige oder durch einen

1413 Vgl. auch Herley, NSPW 2009, 133 (141); allgemein Eckhardt/Feist/Herrmann, in: Jahrbuch Konsum und Verbraucherwissenschaften 2023 (im Erscheinen): „Menschen handeln genuin eigensinnig und aus Gründen, die für regulierende Akteure [...] nicht immer nachvollziehbar sind.“

1414 Vgl. allgemein zu dieser Fallkonstellation Lüftenegger, Die Rückrufpflicht des Herstellers, S. 223.

Dritten vorgenommene Behebung der Softwarefehler kommt in den seltensten Fällen in Betracht.¹⁴¹⁵ Zwar kann die zur Fehlerbehebung erforderliche Dekompilierung nach § 69d Abs. 1 UrhG entsprechend neuerer EuGH-Entscheidung auch ohne Zustimmung des Rechteinhabers i.S.d. § 69c Nr. 2 S.1 UrhG zulässig sein.¹⁴¹⁶ Allerdings versteht allein der Hersteller den Aufbau und die Konzeption der Software in Gänze, sodass er regelmäßig der einzige Akteur ist, der die Software fehlerärmer und sicherer machen kann.¹⁴¹⁷ Da der Kauf einer neueren oder alternativen Softwareversion bei älteren Computern oder insbesondere bei softwaregesteuerten Gegenständen nicht möglich ist, kann die eigene Gefahrensteuerung des Nutzers auf eine Warnung hin nur durch die Stilllegung des Produkts in Gänze erfolgen.¹⁴¹⁸ Bei der Gefahrenbeseitigung durch eine originäre Fehlerbehebung ist der Nutzer dagegen auf den Hersteller und von ihm bereitgestellte Sicherheitsupdates angewiesen.¹⁴¹⁹ Bleiben diese Updates aus, bestehen für den Nutzer nur zwei Möglichkeiten auf die Warnung zu reagieren. Entweder er befolgt die Warnung und stellt die Verwendung des gefährlichen Produkts ein oder er verwendet das Produkt trotz seiner Gefährlichkeit weiter.

β) Angewiesenheit auf das Produkt

Aufgrund der fehlenden Möglichkeit, die Sicherheitsmängel selbst zu beheben, stellt die Warnung in diesen Fällen ein wenig effektives Mittel der Gefahrenabwehr dar,¹⁴²⁰ jedenfalls bei Produkten, die für die Lebensführung von zentraler Bedeutung sind und bei denen ein Nutzungsverzicht daher nicht unbedingt zu erwarten ist. Genau das wird aber bei vielen smarten Produkten der Fall sein. Denn diese sind häufig keine Luxusgüter

1415 Huber, Rechtsfragen des Produktrückrufs, S. 204; Reusch, BB 2019, 904 (905); Wittig, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 239; Oechsler, in: Staudinger, BGB, § 1 ProdHaftG, Rn. 60a.

1416 EuGH, GRUR 2021, 1508; zu Einschränkungen Kaboth, ZUM 2022, 126 (127 f.); vgl. zur alten Rechtslage Raue, NJW 2017, 1841 (1842) und Wittig, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 239 f.

1417 Etzkorn, MMR 2020, 360 (365); Deusch/Eggendorfer, in: Taeger/Pohle (Hg.), Computerrechts-Handbuch, Teil 5, Rn. 460; Regenfus, JZ 2018, 79 (80).

1418 Raue, NJW 2017, 1841 (1842 f.).

1419 So auch Wittig, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 241; Sommer, Haftung für autonome Systeme, S. 280.

1420 Gomille, JZ 2016, 76 (80); Raue, NJW 2017, 1841 (1842) sieht eine korrespondierende Verkehrspflicht des Nutzers zur Stilllegung gar als unzumutbar an.

oder Spielereien, sondern ersetzen herkömmliche Produkte, bei denen die zentrale Bedeutung der ständigen Verfügbarkeit für die eigenwirtschaftliche Lebensführung anerkannt ist. Dies gilt gerade für Geräte der Haushaltselektronik wie Waschmaschinen, Kühlschränke, Fernseher und ohnehin für PCs und Laptops.¹⁴²¹ Es gibt keinen Grund, von dieser Sichtweise abzuweichen, nur weil das Produkt nun noch „smart“ ist. Hinzu kommt, dass Software aufgrund ihrer erhöhten Fehleranfälligkeit regelmäßig auch kritische Softwarefehler aufweist und der Nutzer daher jederzeit und insbesondere vor Ablauf der mechanischen Lebensdauer des Produkts mit einer Warnung verbunden mit einer Stilllegungsaufforderung rechnen muss.¹⁴²² Da eine Annäherung der Lebensdauer von Software an die der Hardware gerade bei teureren Produkten nicht der Realität entspricht, wird es dem Nutzer unverständlich sein, ein Produkt, dessen Hardware noch eine beträchtliche Lebenszeit hätte, wegen sicherheitskritischer Softwarefehler auszusortieren.¹⁴²³ Dies gilt umso mehr, als sich der Produktnutzer aufgrund der Allgegenwärtigkeit von Softwarefehlern bei all seinen Produkten mit der Gefahr einer Stilllegungsaufforderung konfrontiert sieht und ihm dieses Schicksal auch bei der Vornahme einer Ersatzbeschaffung droht. Hinzu kommt, dass die Erwartung des Nutzers an ein in jeder Hinsicht ausgereiftes Produkt zum Zeitpunkt des Inverkehrbringens durch die Erwartung abgelöst wurde, dass das einmal erworbene Produkt später mit Sicherheitsupdates versorgt wird.¹⁴²⁴

Einem Nutzer, der auf die Verwendung des Produkts angewiesen ist und nicht die Möglichkeit hat, das Sicherheitsrisiko ohne Hilfe des Herstellers selbst zu beseitigen, wird ein Nutzungsverzicht damit regelmäßig unzumutbar sein. Bei ihm ist daher zu erwarten, dass er die Eintrittswahrscheinlichkeit einer Rechtsgutsverletzung ausblenden und sich über eine Warnung hinwegsetzen wird.

1421 Vgl. die Auflistung m.w.N. von *Grüneberg*, in: *Grüneberg*, BGB, § 249, Rn. 49; *Oechsler*, in: *Staudinger*, BGB, § 1 ProdHaftG, Rn. 60a „Gebrauchsgegenstand der Alltagswelt“.

1422 Ähnlich auch *Raue*, NJW 2017, 1841 (1842 f.).

1423 Anders aber *Schrader/Engstler*, MMR 2018, 356 (361); wie hier *Wiesemann/Mattheis/Wende*, MMR 2020, 139 (Fn. 20); *Raue*, NJW 2017, 1841 (1843) „weder aus individueller noch aus volkswirtschaftlicher Sicht eine gangbare Lösung“; *Oster*, in: *Foerste/Graf v. Westphalen* (Hg.), *Produkthaftungshandbuch*, § 57, Rn. 26 sieht in einer Updatepflicht gerade die „Kehrseite“ für die Fehleranfälligkeit von Software.

1424 Zu dieser im Tatsächlichen geänderten Erwartungshaltung *Riehm*, in: *Schmidt-Kessel/Kramme* (Hg.), *Geschäftsmodelle in der digitalen Welt*, S. 201 (204).

γ) Erhöhte Einflussmöglichkeit des Herstellers

Außerdem korrespondiert die Angewiesenheit des Nutzers bei der Fehlerbehebung vom Hersteller mit gesteigerten Einflussmöglichkeiten des Herstellers auf das Produkt auch noch nach der Inverkehrgabe.¹⁴²⁵ Bei herkömmlichen Produkten knüpft die Abgrenzung der Risikosphären zwischen Hersteller und Nutzer gerade an den Kontrollverlust des Herstellers über das Produkt mit dem Zeitpunkt des Inverkehrbringens an.¹⁴²⁶ Zwar kann der Hersteller über eine Warnung oder einen Produktrückruf die Gefahrensteuerung initiieren, für weitergehende Sicherungsmaßnahmen ist allerdings die physische Zugriffsmöglichkeit auf das Produkt erforderlich, indem der Nutzer es zum Hersteller oder in eine Werkstatt bringt.¹⁴²⁷ Da smarte Produkte aber ständig über das Internet verbunden sind, können die Hersteller hier jederzeit aus der Ferne auf ihre Produkte zugreifen und auf die sicherheitsrelevanten Eigenschaften per Update Einfluss nehmen, sodass diese weiterhin der Kontrolle des Herstellers unterliegen.¹⁴²⁸

Der Hersteller ist damit im Vergleich zum Produktnutzer besser in der Lage, auf Produktfehler zu reagieren.¹⁴²⁹ Kann dies zudem mit geringem Aufwand und geringen Kosten erfolgen, spricht dies für eine Erweiterung des Pflichtenumfangs des Herstellers.¹⁴³⁰ Denn die Abgrenzung der Verantwortungssphären ist allgemein dadurch geprägt, dass die Risiken demjenigen zugewiesen werden, der sie am besten beherrschen kann.¹⁴³¹ Ungeachtet der konkreten Ausgestaltung ist die Bereitstellung von Updates im Vergleich zu großangelegten Rückrufaktionen mit einem geringeren

1425 Schrader, in: Buck-Heeb/Oppermann (Hg.), Automatisierte Systeme, S. 333 (334).

1426 Vgl. B.I.3.

1427 Vgl. Sedlmaier, in: Kühne/Nack (Hg.), Connected Cars, S. 45.

1428 Riehm, DJT 2022 Referat, K S. 56; Thöne, Autonome Systeme, S. 215; v. Bodungen, in: Chibanguza/Kuß/Steege (Hg.), Künstliche Intelligenz, § 3, I., Rn. 30; Beierle, Die Produkthaftung im Zeitalter des Internet of Things, S. 207 f.; Mayrhofer, Außervertragliche Haftung für fremde Autonomie, S. 291 f.; ansatzweise auch Haf-
tenberger, Die Produkthaftung für künstlich intelligente Medizinprodukte, S. 131;
Sommer, Haftung für autonome Systeme, S. 280.

1429 So auch Oster, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 57, Rn. 25.

1430 So allgemein bzw. im Kontext von herkömmlichen Kfz-Rückrufen Lüftenegger, NJW 2018, 2087 (2090).

1431 Vgl. allgemein Spindler, MMR 2008, 7 (8); ähnlich Klindt et al., in: Bräutigam/Klindt (Hg.), Digitalisierte Wirtschaft/Industrie 4.0, S. 76 (89); im hiesigen Kontext Oster, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 57, Rn. 25.

Aufwand für den Hersteller verbunden.¹⁴³² Dabei sollen noch gar nicht die für das Update anfallenden Kosten in den Fokus genommen werden.¹⁴³³ Denn nach der hier vertretenen Auffassung ist die Frage der weitergehenden Sicherungspflichten von der Frage der Kostentragung zunächst zu trennen. Außerdem betonte der BGH in seiner Pflegebetten-Entscheidung, dass Rückrufspflichten nicht allein aus Zumutbarkeitsgesichtspunkten – ohne Rücksicht darauf, ob diese überhaupt erforderlich sind – hergeleitet werden können.¹⁴³⁴ Festzuhalten ist aber, dass für das Bereitstellen eines Updates keine Werkstatt-, sondern lediglich Serverkapazitäten bereitgestellt werden müssen.¹⁴³⁵ Speziell im Hinblick auf Sicherheitsupdates ist weiter zu konstatieren, dass diese ohnehin bereits mit Blick auf die weitere Vermarktung des Produkts oder seiner Nachfolgemodelle entwickelt werden müssen, um der Konstruktionspflicht gerecht zu werden und das Produkt so ohne Sicherheitsrisiken in den Verkehr zu bringen.¹⁴³⁶

Diese überlegenen Gefahrensteuerungsmöglichkeiten des Herstellers gegenüber dem Nutzer bei gleichzeitig geringem Mehraufwand führen dazu, dass bei einem naheliegenden Hinwegsetzen des Nutzers über eine Warnung Updatepflichten des Herstellers anzunehmen sind.¹⁴³⁷

1432 Grünvogel/Dörrenbächer, ZVertriebsR 2019, 87 (89); Oster, in: Foerste/Graf v. Westphalen (Hg.), ProdukthaftungsHandbuch, § 57, Rn. 25.

1433 In der Literatur wird die Nachrüstungspflicht z.T. jedoch maßgeblich mit den im Vergleich zur Reparatur geringen Kosten begründet, vgl. nur Wagner, AcP 217 (2017), 707 (756); Wagner, in: MüKo, BGB, § 823, Rn. 1130, 1132; Hinze, Haftungsrisiken des automatisierten und autonomen Fahrens, S. 162 f.; Leupold/Wiesner, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 9.6.4, Rn. 75; Eichelberger, in: Ebers et al. (Hg.), Künstliche Intelligenz und Robotik, S. 189; Haagen, Verantwortung für Künstliche Intelligenz, S. 276.

1434 BGH, NJW 2009, 1080 (1082, Rn. 20); im hiesigen Kontext Schmid, IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme, S. 241.

1435 Raue, NJW 2017, 1841 (1844); Wittig, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 237.

1436 Wagner, AcP 217 (2017), 707 (756); Grünvogel/Dörrenbächer, ZVertriebsR 2019, 87 (89); Hinze, Haftungsrisiken des automatisierten und autonomen Fahrens, S. 162 f.; Eichelberger, in: Ebers et al. (Hg.), Künstliche Intelligenz und Robotik, S. 189; Wittig, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 238; Lüftenegger, RD 2021, 293 (298).

1437 So auch Thöne, Autonome Systeme, S. 216 und Raue, NJW 2017, 1841 (1846).

dd) Identifizierbarkeit der Produktnutzer

Fraglich ist aber, wie sich auswirkt, dass im Rahmen einer Warnung über Displays etc. 100 % der Produktnutzer erreicht werden können.¹⁴³⁸ Immerhin wurde in der Pflegebetten-Entscheidung angemerkt, dass auch bei erheblichen Gefahren für Dritte bei bekanntem oder ermittelbarem Abnehmerkreis eine kostenfreie Nachrüstung oder Reparatur vielfach nicht erforderlich sei.¹⁴³⁹ Selbst wenn man aber die Identifizierbarkeit der Abnehmer als Kriterium für die Beurteilung der Effektivität der Gefahrenabwehr anerkennt, sollte die unmittelbare Erreichbarkeit der Produktnutzer nicht mit der Bekanntheit der Abnehmer gleichgesetzt werden. Die Tatsache, dass über das Produkt selbst ein Kommunikationskanal zu den Nutzern besteht, bedeutet nämlich noch nicht, dass dem Hersteller die Nutzer auch bekannt wären. Da die Identifizierbarkeit nämlich insbesondere dazu führen soll, dass der Hersteller bei Nichtbeachtung der Warnung durch die Produktnutzer die zuständigen Behörden einschalten kann, sind hierfür die Kundendaten erforderlich. Ist aber für die Nutzung des smarten Produkts nicht gerade die Erstellung eines individuellen Accounts erforderlich, führt die unmittelbare Kommunikationsmöglichkeit über das Produkt nicht zu einer diesbezüglichen herstellerseitigen Kenntnis.

Daneben spricht die Identifizierbarkeit der Produktnutzer allenfalls gegen die Kostenfreiheit der Updates, nicht aber gegen eine grundsätzliche Pflicht des Herstellers. Der BGH selbst weist darauf hin, dass bei einem identifizierbaren Abnehmerkreis der Hersteller erforderlichenfalls seine Hilfe anbieten muss, um die Nutzer in die Lage zu versetzen, eine Nachrüstung auf eigene Kosten vorzunehmen.¹⁴⁴⁰ Gerade Sicherheitsupdates scheinen der Paradefall für diese Konstellation zu sein. Denn wie kaum woanders ist hier der Nutzer auf die Hilfe des Herstellers angewiesen, um in der Lage zu sein, einen sicherheitsrelevanten Fehler überhaupt beheben zu können. Die bloße Information über die Notwendigkeit der Nachrüstung ist eben nicht ausreichend (s.o.).

1438 Hierzu *Lüftenegger*, RDi 2021, 293 (294); *Klindt*, DAR 2023, 7 (8).

1439 BGH, NJW 2009, 1080 (1081, Rn. 13).

1440 BGH, NJW 2009, 1080 (1081, Rn. 13).

c) Fazit

Anders als bei herkömmlichen Produkten wird die vorzunehmende Einzelfallbetrachtung bei Software und bei smarten Produkten regelmäßig zu einer Updateverpflichtung des Herstellers führen. Aufgrund der tatsächlichen Gegebenheiten wird hier vielfach ein Hinwegsetzen über eine Warnung erwartet werden müssen. Bei reiner Software folgt dies aus dem Verkennen des Gefahrenpotentials von Sicherheitslücken, bei smarten Produkten aus der unzumutbaren Gefahrensteuerung aufgrund der fehlenden eigenen Fehlerbeseitigungsmöglichkeit bei gleichzeitiger gesteigerter Einflussmöglichkeit des Herstellers in Kombination mit der Angewiesenheit auf das Produkt.

2. Ausgestaltung der Updatepflicht

Wurde geklärt, dass die Hersteller von Software und smarten Produkten regelmäßig Updatepflichten treffen, muss in einem zweiten Schritt das Verhältnis der unterschiedlichen Updatemaßnahmen, insbesondere von Sicherheitsupdates und Fernstilllegungen, untersucht werden.

a) Bedeutung der vertraglichen Aktualisierungspflicht aus § 327f BGB

Innerhalb einer Vertragsbeziehung mit einem Verbraucher ist eine Aktualisierungspflicht zum Erhalt der Vertragsmäßigkeit des digitalen Produkts mittlerweile nach § 327f Abs. 1 BGB¹⁴⁴¹ geltendes Recht. Erfasst sind insbesondere auch Sicherheitsaktualisierungen (S. 2). Diese Kodifizierung der Aktualisierungspflicht stellt aber die deliktsrechtliche Pflicht zur Vornahme von Sicherheitsupdates als solche nicht in Frage.¹⁴⁴² Bereits Erwägungsgrund (47) Digitale-Inhalte-RL stellt nämlich klar, dass sich aus anderen Gründen ergebende gesetzliche Aktualisierungspflichten unberührt blei-

1441 § 327f BGB beruht auf der Richtlinie (EU) 2019/770 über die Bereitstellung digitaler Inhalte.

1442 So aber *Gansmeier/Kochendörfer*, JuS 2022, 704 (707 f.); in diese Richtung wohl auch *Voigt*, in: BeckOGK, BGB, § 823, Rn. 782; *Haftenberger*, Die Produkthaftung für künstlich intelligente Medizinprodukte, S. 131 folgert dagegen einen Trend hin zur Update-Verpflichtung auch des Herstellers nach Inverkehrgabe; ähnlich *Oechsler*, NJW 2022, 2713 (2715), der von einem „Leitbildcharakter“ spricht.

ben.¹⁴⁴³ Darüber hinaus wäre ein auf Verbraucherverträge beschränkter Schutz des Integritätsinteresses vor durch Updates behebbaren Gefahren schlicht unzureichend. Weder Unternehmern noch am Vertrag nicht beteiligten Dritten stünden Schadensersatzansprüche zu, wenn sie aufgrund unterlassener Updates einen Schaden erlitten.¹⁴⁴⁴ Vielmehr muss es beim grundsätzlichen Nebeneinander von Vertrags- und Deliktsrecht bleiben.¹⁴⁴⁵

b) Abgrenzung zwischen Äquivalenz- und Integritätsinteresse

Gerade bei der Frage nach der konkreten Ausgestaltung der Updatepflicht im Rahmen der Produktbeobachtungspflicht setzt sich die Abgrenzung zwischen deliktsrechtlich geschütztem Integritätsinteresse und nicht geschütztem Äquivalenzinteresse fort.¹⁴⁴⁶

Allein vom Standpunkt der Gefahrenabwehr gehen von einem zwangsweise aus der Ferne deaktivierten Gerät regelmäßig keine Gefahren mehr für die Rechte und Rechtsgüter der Nutzer oder Dritten aus, sodass der Hersteller damit seiner Gefahrensteuerungspflicht in vollem Umfang nachkäme.¹⁴⁴⁷ Dass die Nutzer dann kein funktionsfähiges Produkt mehr haben, ist aus produkthaftungsrechtlicher Perspektive unerheblich, weil es insoweit nur darauf ankommt, dass von dem Produkt keine Gefahren für geschützte Rechtsgüter mehr ausgehen. Deliktsrechtlich geschützt ist eben nur das Integritäts- und nicht das Äquivalenzinteresse, weshalb der Verlust der weiteren Nutzungsmöglichkeit bei der Gefahrenabwehr keine Rolle spielt.¹⁴⁴⁸ Im Hinblick auf die mangelnde Funktionsfähigkeit müssen sich die Nutzer allein mit ihrem Vertragspartner auseinandersetzen und beispielsweise Gewährleistungsrechtliche Rechtsbehelfe geltend machen, sofern diese noch nicht verjährt sind.

1443 Vgl. auch *Schmidt-Kessel*, ZfPC 2022, 117 (119); *Wagner*, JZ 2023, 1 (6).

1444 *Meents/Obradovic*, ZfPC 2022, 13 (16); *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 98 f.

1445 *Wagner*, JZ 2023, 1 (6).

1446 *Lüftenegger*, RDt 2021, 293 (299).

1447 *Regenfus*, JZ 2018, 79 (83) auch mit dem Hinweis in Fn. 41 auf die Boston-Scientific-Entscheidung, in der der EuGH die Deaktivierung des Geräts bzw. einer gefährlichen Funktion als grundsätzlich ausreichend angesehen hat, vgl. EuGH, NJW 2015, 1163 (1164 f., Rn. 54); ähnlich *Wittig*, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 232.

1448 Vgl. auch BGH, NJW 2009, 1080 (1083, Rn. 25).

Ebenso wenig wie bei der Rückruffrage überzeugt es jedoch auch bei der Updatepflicht nicht, Sicherheitsupdates pauschal mit dem Hinweis auf das lediglich vertraglich geschützte Äquivalenzinteresse abzulehnen.¹⁴⁴⁹ Eine deliktsrechtliche Nachrüstung durch Updates kommt freilich von vornherein nicht in Bezug auf lediglich funktionserhaltende Updates ohne Sicherheitsrelevanz in Betracht, da ansonsten tatsächlich nur das Äquivalenzinteresse betroffen wäre. Eine ständige Pflege der Software, um diese funktionell auf dem aktuellen Stand zu halten oder gar zu optimieren, ist deliktsrechtlich nicht geschuldet.¹⁴⁵⁰ Erwächst aus der unzureichenden Programmierung allein eine fehlerhafte oder fehlende Funktionalität, ergibt sich aus der deliktsrechtlichen Produktbeobachtungspflicht gerade keine Aktualisierungspflicht.¹⁴⁵¹ Zwar wird dem Nutzer auch bei der Bereitstellung von sicherheitsrelevanten Aktualisierungen wieder ein vertragsgemäßes Produkt zur Verfügung gestellt und somit ebenfalls seinem Äquivalenzinteresse entsprochen.¹⁴⁵² Allerdings beschränkt sich hier die Fehlerbeseitigung mittels Updates nicht auf das Äquivalenzinteresse, sondern berührt in gleicher Weise das Integritätsinteresse, wenn von dem Produkt Gefahren für die nach § 823 Abs.1 BGB geschützten Rechte und Rechtsgüter ausgehen.¹⁴⁵³ Insoweit bestehen keine Unterschiede zur Gefahrenbeseitigung bei analogen Produkten.

Auch die Möglichkeit, Aktualisierungen auf die rein deliktsrechtlich geschuldeten sicherheitsrelevanten Updates zu beschränken, führt nicht dazu, dass sich die Abgrenzungsfrage zwischen dem vertraglich geschützten Äqui-

1449 So aber *Schmid*, IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme, S. 241 f.; in diese Richtung auch *Rockstroh/Kunkel*, MMR 2017, 77 (81); *Spindler*, in: Hilgendorf (Hg.), Robotik im Kontext von Recht und Moral, S. 63 (75); *Spindler*, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, Rn. 141; Arbeitsgruppe „Digitaler Neustart“, Bericht vom 15. April 2019, S. 197 f.; *Heydn* in: Schuster/Grützmaker (Hg.), IT-Recht, § 3 ProdHaftG, Rn. 23; zurückhaltend auch *Chibanguza*, in: Buck-Heeb/Oppermann (Hg.), Automatisierte Systeme, S. 407 (418) und *Wende*, in: Sassenberg/Faber (Hg.), Industrie 4.0 und Internet of Things, § 4, Rn. 59.

1450 Mindestens missverständlich aber *Ebers*, in: Oppermann/Stender-Vorwachs (Hg.), Autonomes Fahren, 1. Aufl., S. 93 (114); wie hier *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 174 und *Spindler*, in: Hornung/Schallbruch (Hg.), IT-Sicherheitsrecht, § 11, Rn. 41 f.

1451 *Reusch*, BB 2019, 904 (908).

1452 *Gless/Janal*, JR 2016, 561 (569 f.).

1453 *Hinze*, Haftungsrisiken des automatisierten und autonomen Fahrens, S. 163 und *Spindler*, in: Hornung/Schallbruch (Hg.), IT-Sicherheitsrecht, § 11, Rn. 42; vgl. auch *Sommer*, Haftung für autonome Systeme, S. 280.

valenzinteresse und dem deliktsrechtlich geschützten Integritätsinteresse weniger dringlich stellt.¹⁴⁵⁴ Gleiches gilt für die Tatsache, dass die Funktionalität eines Produkts von Softwarefehlern häufig zunächst gar nicht betroffen ist und Unsicherheiten vom Produktnutzer nicht wahrgenommen werden.¹⁴⁵⁵ Denn bei genauerer Betrachtung handelt es sich dabei um keine Besonderheiten smarter Produkte. Auch im Rahmen eines herkömmlichen Rückrufs ist eine Nachrüstung allein auf das sicherheitsgefährdende Teil beschränkt. Zudem wirken sich Produktfehler bei analogen Produkten regelmäßig auch erst mit Eintritt des Schadens funktionsbeeinträchtigend aus. Entscheidender Punkt – und dies gilt sowohl für analoge als auch für smarte Produkte – ist vielmehr, dass mit einer Einstellung der Nutzung des Produkts der Schutzfunktion des Deliktsrechts Genüge getan ist und weitergehende Maßnahmen, welche die weitere Nutzbarkeit des Produkts ermöglichen, jedenfalls auch dem Äquivalenzinteresse zuzuordnen sind.¹⁴⁵⁶ Bei der Überlegung, wie der Hersteller das Integritätsinteresse des Nutzers zu wahren hat, ist daher der Nachrüstung durch Updates nicht allein deshalb der Vorzug zu geben, weil dadurch die Nutzbarkeit des Gegenstandes erhalten werden kann.¹⁴⁵⁷

c) Effektivität der Gefahrenabwehr als Maxime

Die Verpflichtung, ein Produkt nicht nur zurückzurufen und damit aus dem Verkehr zu ziehen, sondern weitergehende Sicherheitsmaßnahmen zu ergreifen, kommt aber immer dann in Betracht, wenn dies aus Gründen einer effektiven Gefahrenabwehr erforderlich ist.¹⁴⁵⁸ Die zentrale Frage hinsichtlich der Ausgestaltung der Updatemaßnahme lautet demnach: Unter welchen Umständen erweist sich eine vom Hersteller aus der Ferne vorgenommene aufgedrängte Sicherheitsbereicherung, die eine weitere (gefährliche) Nutzung gerade ausschließt, dennoch als nicht hinreichend effektiv bei der Gefahrenabwehr?

1454 So aber Thöne, *Autonome Systeme*, S. 217 und Dötsch, *Außervertragliche Haftung für KI*, S. 261.

1455 In diese Richtung aber Reusch, *BB* 2019, 904 (908).

1456 Ähnlich auch Arbeitsgruppe „Digitaler Neustart“, Bericht vom 15. April 2019, S. 198; Spindler, in Hornung/Schallbruch (Hg.), *IT-Sicherheitsrecht*, § 11, Rn. 41 f.

1457 Meents, in: FS Taeger, S. 13 (20).

1458 BGH, *NJW* 2009, 1080 (1081, Rn. 12).

Anders als das in der Pflegebetten-Entscheidung zugrunde gelegte Verständnis eines Rückrufs als mitwirkungsbedürftiger Maßnahme, ist eine solche aufgedrängte Sicherheitsbereicherung dem Grunde nach nicht von der Mitwirkung des Nutzers abhängig.¹⁴⁵⁹ Unterbindet der Nutzer die Schnittstellenkonnektivität nicht, wozu er regelmäßig keinen Anlass haben wird, und blockiert er die Schnittstelle nicht, wozu dem Laien regelmäßig die hinreichende Sachkunde fehlen wird, kann die Maßnahme ohne weiteres Zutun durch den Hersteller erfolgen. Gerade deshalb ist die Maßnahme zwar sehr effektiv, indes führt dies dazu, dass nicht bei diesem Ergebnis stehen geblieben werden kann.¹⁴⁶⁰ Denn jeglicher nachträgliche Eingriff des Herstellers in das Produkt steht potenziell in Konflikt mit dem Eigentumsrecht des Nutzers. Diese Konfliktlage hat nun Rückwirkungen auf die Präventionspflichten des Herstellers: Eine Maßnahme zur Vermeidung von Rechtsgutsverletzungen genügt eben nur dann den Anforderungen der Produktbeobachtungspflicht, wenn sie auch praktisch wirksam ist.¹⁴⁶¹ Dies ist aber dann nicht der Fall, wenn eine Maßnahme das Eigentumsrecht des Nutzers verletzt, weil es an der Einwilligung zu der entsprechenden Maßnahme fehlt und auch kein anderer Rechtfertigungsgrund besteht. Dann ist die Maßnahme nicht geeignet, um Rechtsgutsverletzungen durch das Produkt effektiv zu verhindern. Maßgeblich für die Beurteilung der Effektivität der Gefahrenabwehr einer aufgedrängten Sicherheitsbereicherung ist damit die Frage, ob eine entsprechende Maßnahme das Eigentumsrecht des Nutzers in rechtswidriger Weise verletzt.

aa) Aufgedrängte Sicherheitsbereicherung als Rechtseingriff

Hierzu ist zunächst zu betrachten, inwiefern eine solche Maßnahme einen Rechtseingriff darstellt. Dabei ist nach der Art des digitalen Eingriffs¹⁴⁶² durch den Hersteller zu unterscheiden.¹⁴⁶³

1459 Vgl. *Duden*, Digitale Sachherrschaft, S. 59.

1460 Vgl. auch *Grünvogel/Dörrenbächer*, ZVertriebsR 2019, 87 (90); *Wittig*, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 232.

1461 Vgl. BGH, NJW 2009, 1080 (1082, Rn. 19).

1462 Diesen Begriff verwendet *Kuschel*, AcP 220 (2020), 98 (102).

1463 So auch *Duden*, Digitale Sachherrschaft, S. 57 und S. 159.

(1) Schutz des softwarebasierten Gebrauchs

Ein Update – unabhängig davon, ob es lediglich einen Fehler behebt oder eine Sperre der integrierten Software auslöst und das Gerät damit stilllegt – geht mit einer Veränderung oder Löschung der Softwaredaten¹⁴⁶⁴ auf dem Produkt einher, sodass es zu einer Veränderung der Software kommt.¹⁴⁶⁵ Die Speicherung der Software erfolgt nämlich über Speicherzellen, in denen jeweils ein Bit des Programmcodes hinterlegt ist. Da diese Speicherung durch Magnetisierung oder durch Steuerung der elektronischen Leitfähigkeit mittels Transistoren dargestellt wird, schlägt sich diese auch körperlich nieder.¹⁴⁶⁶ Werden folglich durch die Löschung, Veränderung und Speicherung der Softwaredaten die materiellen Eigenschaften der einzelnen Speicherzellen beeinflusst, so wird auch auf den Körper des Datenträgers eingewirkt und damit eine Substanzverletzung durch die physikalische Veränderung des Produkts als Datenträger herbeigeführt, sodass eine Eigentumsverletzung vorliegt.¹⁴⁶⁷

Führt das Update bzw. die darin enthaltenen Steuerbefehle zu einer vollständigen Deaktivierung des Gerätes, liegt neben der Substanzverletzung zugleich eine Eigentumsverletzung in Form einer Nutzungsbeeinträchtigung vor.¹⁴⁶⁸ Die Nutzungsbeeinträchtigung erfolgt in diesem Fall durch eine Störung der Funktionsfähigkeit der Sache selbst (als Folge der Substanzverletzung) und nicht nur durch eine Beeinträchtigung von Faktoren der Umwelt, auf die die Sache angewiesen ist. Die letztere Fallgruppe entwickelten einschränkenden Kriterien zur Bestimmung einer relevanten

1464 Auch Softwareinstallationen bestehen aus gespeicherten Daten, welche den Objektcode der Software enthalten, vgl. Heydn in: Schuster/Grützmaker (Hg.), IT-Recht, § 823 BGB, Rn. 29.

1465 Duden, Digitale Sachherrschaft, S. 160.

1466 Ausführlich Duden, Digitale Sachherrschaft, S. 93 f.

1467 Im hiesigen Kontext Kuschel, AcP 220 (2020), 98 (103); Ausführlich Duden, Digitale Sachherrschaft, S. 161 f.; allgemein schon OLG Karlsruhe, NJW 1996, 200 (201); h.M. vgl. nur Wagner, in: MüKo, BGB, § 823, Rn. 286 und Hager, in: Staudinger, BGB, § 823, Rn. B 60 jeweils m.w.N.; Faustmann, VuR 2006, 260 (260); Riehm, VersR 2019, 714 (717).

1468 Einer vorprogrammierten Funktionssperre, die beim Eintritt einer vorgegebenen Bedingung eine weitere Ausführung der Software verhindert und damit ohne Update und Substanzverletzung eine Stilllegung des Geräts auslösen kann, kommt dagegen im Rahmen der Gefahrenabwehr keine praktische Bedeutung zu, da die Gefahr kaum einmal als Bedingung hinreichend antizipiert und in der Programmierung berücksichtigt werden kann; vgl. allgemein dazu Duden, Digitale Sachherrschaft, S. 59 f. und S. 169 ff.

Nutzungsbeeinträchtigung sind daher nicht einschlägig. Die Eigentumsverletzung ergibt sich bereits daraus, dass es sich um eine sachinterne Störung handelt und unmittelbar die Funktionsfähigkeit des Geräts selbst betroffen ist.¹⁴⁶⁹ Nichts anderes kann dann bei einer Abschaltung lediglich einzelner gefährlicher Gerätefunktionen¹⁴⁷⁰ gelten.¹⁴⁷¹

(2) Schutz des netzbasierten Gebrauchs

Anders könnte der Fall allerdings liegen, wenn der Hersteller lediglich Serverdienste oder Leistungen von außerhalb einstellt, auf die das Produkt angewiesen ist. Die entscheidende Frage ist hier, wie weit der Eigentumschutz außerhalb von Eingriffen in die Sachsubstanz bei Beeinträchtigungen der Gebrauchstauglichkeit des vernetzten Systems geht.¹⁴⁷²

α) Parallele zur Versorgungssperre

Im Ausgangspunkt stellt eine „Versorgungssperre“, bei der der Vermieter die Versorgung des Mieters mit Strom, Wasser und Wärme einstellt, keine Besitzstörung durch verbotene Eigenmacht i.S.d. § 858 Abs.1 BGB dar.¹⁴⁷³ Auch wenn der Zufluss von Versorgungsleistungen Voraussetzung für den vertragsgemäßen Gebrauch sein kann, wird durch deren Einstellung nicht die aus dem bloßen Besitz folgende Nutzungsmöglichkeit eingeschränkt.¹⁴⁷⁴ Denn Versorgungsleistungen führen lediglich dazu, dass die im Besitz liegende Gebrauchsmöglichkeit erweitert wird. Ein entsprechendes Recht auf zusätzliche Leistungen folgt aber nicht aus dem Besitz an einer Sache, sondern kann sich allenfalls unter vertraglichen Gesichtspunkten ergeben.¹⁴⁷⁵ Aus dem Besitz kann daher nicht die Verpflichtung anderer hergeleitet

1469 Duden, Digitale Sachherrschaft, S.170, S.202; ohne Weiteres auch Wagner, in: MüKo, BGB, § 823, Rn. 320; wohl auch Regenfus, JZ 2018, 79 (83).

1470 Vgl. das in der Einleitung erwähnte Beispiel von Tesla, Fn. 4.

1471 Magnus, Fernkontrolle im Internet der Dinge, S. 221 f.; a.A. Regenfus, JZ 2018, 79 (83), der sich bereits hier auf die Rechtsprechung zu den Auswirkungen von Beeinträchtigungen von Umweltfaktoren bezieht.

1472 Wiesner, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 10.6, Rn. 25.

1473 BGH NJW 2009, 1947 (1948).

1474 BGH NJW 2009, 1947 (1948).

1475 Vgl. BGH NJW 2009, 1947 (1948); dazu auch Riehm, in: Fries/Paal (Hg.), Smart Contracts, S. 85 (96).

werden, für den Eigentümer Aufwendungen zu tätigen, damit dieser die Sache nach Belieben gebrauchen kann.¹⁴⁷⁶ Da der Schutz des Eigentums nicht hinter dem Schutz des Besitzes zurücksteht,¹⁴⁷⁷ können die Aussagen über das Vorliegen einer Beeinträchtigung des Besitzes auch für eine mögliche Beeinträchtigung des Eigentums herangezogen werden.¹⁴⁷⁸ Damit berechtigt aber auch das Eigentum an einer Sache lediglich dazu, diese so zu nutzen, wie es die physischen Eigenschaften „aus sich heraus“ erlauben.¹⁴⁷⁹ Reichen diese Eigenschaften demnach nicht aus, um ein Produkt ordnungsgemäß zu nutzen, sondern sind hierfür weitere Leistungen von außen nötig, erstreckt sich der Zuweisungsgehalt des Eigentums aus § 903 S. 1 BGB nicht hierauf.¹⁴⁸⁰

Wird folglich ein notwendiger Server vom Hersteller eingestellt, liegt darin lediglich die Realisierung einer von Anfang an bestehenden Schwäche des Produkts und wird die deliktsrechtlich nicht geschützte Erwartung des Nutzers enttäuscht, dass die Serverdienste aufrechterhalten bleiben und das Produkt voll einsatzfähig bleibt.¹⁴⁸¹ Das Ausbleiben netzbasierter Gebrauchsvoraussetzungen bleibt damit für sich genommen deliktsrechtlich ohne Bedeutung.¹⁴⁸²

β) Bedeutung des Entzugs des gebrauchsnötigen Netzzugangs

Allerdings entspricht es der ständigen Rechtsprechung, dass eine Eigentumsverletzung auch durch eine die sonstigen Eigentümerbefugnisse betreffende tatsächliche Einwirkung auf die Sache selbst erfolgen kann,¹⁴⁸³ die zu einer nicht unerheblichen Beeinträchtigung der bestimmungsgemäßen Verwendung der betreffenden Sache führt.¹⁴⁸⁴ Wird die Benutzung der Sache objektiv verhindert, die Verwendungsfähigkeit also vorübergehend praktisch aufgehoben, wirkt eine derartige Beeinträchtigung der Eigentümerbefugnisse wie eine zeitweilige Wegnahme der Sache und ist als Eigen-

1476 Kuschel, AcP 220 (2020), 98 (123).

1477 Wagner, in: MüKo, BGB, § 823, Rn. 303; BGH, NJW 2015, 1174 (1175).

1478 Duden, Digitale Sachherrschaft, S. 254 f.

1479 Regenfus, JZ 2018, 79 (84).

1480 Regenfus, JZ 2018, 79 (84).

1481 Regenfus, JZ 2018, 79 (84); Wagner, in: MüKo, BGB, § 823, Rn. 320; Magnus, Fernkontrolle im Internet der Dinge, S. 225 f.

1482 Duden, Digitale Sachherrschaft, S. 259 f.

1483 Vgl. nur BGH, NJW-RR 2017, 219 (221).

1484 Stehende Formulierung, vgl. BGH, NJW 2015, 1174 (1175).

tumsverletzung zu qualifizieren.¹⁴⁸⁵ Handelt es sich um ein Cloud-basiertes Gerät, das in seiner Funktionsfähigkeit auf eine kontinuierliche Verbindung zur Cloud des Anbieters angewiesen ist, führt die Einstellung des Cloud-Servers oder die Verweigerung des Zugangs zu diesem dazu, dass die Nutzungsmöglichkeit des Geräts insgesamt aufgehoben ist. Vor diesem Hintergrund könnte die bestimmungsgemäße Verwendung des Produkts aufgehoben und eine Eigentumsverletzung gegeben sein.¹⁴⁸⁶ Prima facie liegt der Fall nicht anders als bei einem „Einsperren“ von Schiffen in einem Hafen.¹⁴⁸⁷ Dem Eigentümer wird das Einsatzpotential seiner Sache in Gänze genommen.¹⁴⁸⁸ Anders als bei der vollständigen Aufhebung der Verwendungsfähigkeit einer Sache liegt eine Eigentumsverletzung von vorneherein dagegen nicht vor, wenn lediglich eine bestimmte Verwendungsmodalität bzw. eine Mehrzahl von Verwendungszwecken, die das Einsatzpotential der Sache nicht erschöpfen, ausgeschlossen wird.¹⁴⁸⁹ Die zeitweilige Verhinderung lediglich einer spezifischen Verwendungsabsicht des Eigentümers führt nur zu einer vorübergehenden Einengung der wirtschaftlichen Nutzungsmöglichkeit¹⁴⁹⁰ und rechtfertigt daher keine Behandlung als Eigentumsverletzung.¹⁴⁹¹ Vor diesem Hintergrund liegt jedenfalls keine Eigentumsverletzung vor, wenn das Gerät lediglich hinsichtlich einzelner Funktionen nicht mehr auf einen Cloud-Server zugreifen kann, im Übrigen aber offline weiter bestimmungsgemäß nutzbar bleibt.¹⁴⁹² Vergleichbar mit einem „ausgesperrten“ Schiff, das ein bestimmtes Gewässer nicht mehr befahren kann,¹⁴⁹³ ist es dem vernetzten System lediglich nicht möglich, einen digitalen Ort anzusteuern.¹⁴⁹⁴ Insoweit eröffnet § 903 BGB dem Eigentümer

1485 BGH, NJW-RR 2017, 219 (221); zustimmend Förster, in: BeckOK, BGB, § 823, Rn. 132, mit Nachweisen zu krit. Stimmen in Rn. 131; im Wesentlichen auch Hager, in: Staudinger, BGB, § 823, Rn. B 97.

1486 Als eindeutig sehen dies etwa Solmecke/Vondrlik, MMR 2013, 755 (758) an.

1487 Vgl. den sog. „Fleet-Fall“ BGH, NJW 1971, 886 und BGH, NJW-RR 2017, 219; diesen Vergleich zieht auch Regenfus, JZ 2018, 79 (83).

1488 Vgl. Larenz/Canaris, Lehrbuch des Schuldrechts II/2, S. 388 f.

1489 Ständige Rspr., vgl. nur BGH, NJW-RR 2017, 219 (221) und h.M., vgl. Förster, in: BeckOK, BGB, § 823, Rn. 132; Voigt, in: BeckOGK, BGB, § 823, Rn. 137.

1490 Vgl. insbesondere BGH, NJW 2015, 1174 (1176).

1491 Vgl. Förster, in: BeckOK, BGB, § 823, Rn. 132; Voigt, in: BeckOGK, BGB, § 823, Rn. 137.

1492 Weiter aber Solmecke/Vondrlik, MMR 2013, 755 (759).

1493 Vgl. erneut BGH, NJW 1971, 886 (888).

1494 Vgl. Wiesner, in: Leupold/Wiebe/Glossner (Hg.), IT-Recht, Teil 10.6, Rn. 25; ähnlich Duden, Digitale Sachherrschaft, S. 237 f.

zwar das Recht, mit seiner Sache nach Belieben zu verfahren, nicht aber auch das Recht, dafür auf Sachen Dritter zurückzugreifen.¹⁴⁹⁵

Aber selbst wenn das Gerät seine bestimmungsgemäße Nutzungsmöglichkeit durch die Unterbrechung des Server-Zugangs gänzlich verliert, ist zu berücksichtigen, dass das Gerät – anders als bei einem im Hafen eingesperrten Schiff – zu keinem Zeitpunkt fähig war, ohne den externen Server zu funktionieren. Während es bei dem eingeschlossenen Schiff genügte, die Blockade zu beseitigen, ist ein solch vernetztes Produkt dauerhaft auf die Bereitstellung des externen Dienstes bzw. des externen Servers angewiesen.¹⁴⁹⁶ Die Möglichkeit der bestimmungsgemäßen Verwendung ist dem Produkt nicht inhärent, sondern ergibt sich erst aufgrund zusätzlicher Leistungen.¹⁴⁹⁷ Anders könnte dies zu beurteilen sein, wenn bereits der Zugang zu einem externen Server verhindert wird. Denn dies betrifft nicht lediglich die Versorgung der Sache, sondern bereits die Versorgbarkeit der Sache.¹⁴⁹⁸ Die Versorgbarkeit mit einer Leistung ist aber in der Sache angelegt und kann als Teil der in der Sache vorhandenen Gebrauchsmöglichkeiten angesehen werden.¹⁴⁹⁹ Während folglich die Verhinderung des Zugangs¹⁵⁰⁰ zum entsprechenden Server oder Dienst jedenfalls im Ausgangspunkt eigentumsrechtlich relevant sein könnte, ist dies dagegen bei der bloße Einstellung eines externen Servers oder Dienstes zweifelhaft.

Allerdings ist zu berücksichtigen, dass der externe Server oder Dienst im Eigentum des Anbieters steht. Damit darf dieser frei darüber entscheiden, wer sein Eigentum nutzen darf. Auch wenn der Nutzer sein Gerät nur über den Zugang zum Server des Anbieters nutzen kann, ist der Anbieter nicht verpflichtet, diesem den Zugang auch zu gewähren. Insoweit endet der Zuweisungsgehalt des Eigentums des Nutzers am Zuweisungsgehalt des Eigentums des Serveranbieters.¹⁵⁰¹ Die Beeinträchtigung der bestimmungsgemäßen Nutzung stellt sich somit lediglich als Reflex der Ausübung des

1495 Vgl. *Larenz/Canaris*, Lehrbuch des Schuldrechts II/2, S. 388.

1496 *Magnus*, Fernkontrolle im Internet der Dinge, S. 224.

1497 Vgl. dazu in anderem Kontext *Riehm*, in: Fries/Paal (Hg.), *Smart Contracts*, S. 85 (96).

1498 *Duden*, Digitale Sachherrschaft, S. 263.

1499 *Duden*, Digitale Sachherrschaft, S. 239.

1500 Technisch kann dies durch sog. Blacklisting umgesetzt werden. Dabei wird die Identifikationsnummer des Geräts oder des Nutzers auf einer Sperrliste vermerkt. Diese Liste wird abgefragt, sobald sich ein Gerät für einen Serverzugriff authentifizieren möchte, dazu *Duden*, Digitale Sachherrschaft, S. 57 f.

1501 *Duden*, Digitale Sachherrschaft, S. 249, S. 266.

Eigentumsrechts des Serveranbieters dar.¹⁵⁰² Dabei spielt es keine Rolle, ob der Hersteller der Anbieter des Servers ist oder ob es sich um die Serverinfrastruktur eines Dritten handelt, der im Auftrag des Herstellers handelt.¹⁵⁰³ Solange der private Server keiner öffentlichen Regulierung unterliegt, kann der Anbieter aufgrund seines Eigentums frei über den Zugang des Nutzers entscheiden.

(3) Zwischenfazit

Updates – ob zur Fehlerbehebung, zur Deaktivierung einzelner Funktionen oder zur Fernstilllegung – führen stets zu einer Substanzverletzung am Produkt. Geht eine solche Substanzverletzung mit einer Nutzungsbeeinträchtigung einher, liegt hierin ein zweiter Anknüpfungspunkt für eine Eigentumsverletzung des Nutzers. Kommt es dagegen zu einer faktischen Stilllegung des Produkts, weil notwendige Serverdienste gesperrt oder nicht mehr bereitgestellt werden, verwirklicht sich lediglich ein im Produkt von vorneherein angelegtes Risiko, ohne dass dies eigentumsrechtlich relevant wäre.

bb) Interessenlage im Rahmen der aufgedrängten Sicherheitsbereicherung

Der Hersteller kann gerade an der Durchführung von Sicherheitsupdates – ungeachtet einer hierauf gerichteten deliktsrechtlichen Pflicht – ein erhebliches Eigeninteresse haben. Zum einen wächst der Hersteller gem. § 6 Abs. 2 S. 1 ProdHaftG bei einem anfänglichen Fehler seines Produkts auch dann in die Haftung gegenüber einem geschädigten Dritten hinein, wenn der Nutzer nicht in die Installation des bereitgestellten Updates einwilligt. Zwar ist es ihm hier möglich, im Innenverhältnis Regress beim Nutzer zu nehmen (§ 426 BGB), gleichwohl trägt er dessen Insolvenzrisiko.¹⁵⁰⁴ Wichtiger aus Sicht des Herstellers dürfte jedoch die negative Berichterstattung und der damit verbundene Vertrauensverlust sein, der nach einem Schadensfall aufgrund einer nicht geschlossenen Sicherheitslücke oder eines sonstigen

1502 Dazu *Raff*, in: MüKo, BGB, § 1004, Rn. 126.

1503 *Duden*, Digitale Sachherrschaft, S. 266.

1504 Dies übersieht *Meents*, in: FS Taeger, S. 13 (22); zu apodiktisch auch *Wagner*, AcP 217 (2017), 707 (757).

Softwarefehlers zu erwarten ist.¹⁵⁰⁵ Für den Imageverlust dürfte es im Ausgangspunkt unerheblich sein, ob der Schaden darauf zurückzuführen ist, dass der Nutzer ein bereitgestelltes Sicherheitsupdate nicht eingespielt hat. Der Schaden wird immer mit dem Namen des Herstellers in Verbindung gebracht werden. Während der Hersteller damit sein Risiko minimiert, liegt die Fehlerbehebung aber grundsätzlich auch im Interesse des Nutzers, der dadurch ein sichereres Produkt erhält.¹⁵⁰⁶ Dies jedenfalls dann, wenn die Durchführung der Updates auf die Behebung des Sicherheitsrisikos gerichtet ist. Gerade mit Blick auf Sicherheitsupdates kann darüber hinaus ein Interesse des Herstellers bestehen, diese ohne Kenntnis des Nutzers durchzuführen. Denn auf diese Weise kann die Gefährlichkeit des Produkts beseitigt werden, ohne dass der Nutzer davon erfährt und ohne dass der Hersteller allein durch diese Sicherheitsgefährdung einen Reputationsschaden erleidet. Auch in Fällen, in denen eine Warnung vor dem Produkt daher ausnahmsweise ausreichend sein kann, etwa weil eine Gefährdung allein des Nutzers droht, kann ein Hersteller daher geneigt sein, die Gefahr durch ein Sicherheitsupdate zu beseitigen.¹⁵⁰⁷ Dagegen wird eine Fernstilllegung für den Hersteller nur eine Notlösung in absoluten Ausnahmefällen sein, weil eine solche Komplettabschaltung für seine Reputation desaströs wäre.¹⁵⁰⁸

cc) Schuldvertragliche Gestattung der aufgedrängten Sicherheitsbereicherung

Möglicherweise kann sich der Hersteller vorab vertraglich das Recht einräumen lassen, Updates mit den damit verbundenen Rechtseingriffen vornehmen zu dürfen.¹⁵⁰⁹ Da eine schuldrechtliche Gestattung grundsätzlich

1505 Zu Recht *Meents*, in: FS Taeger, S. 13 (22).

1506 So auch *Wendehorst*, Besitz- und Eigentumsverhältnisse beim Internet der Dinge – Rechtsgutachten, S. 23.

1507 Es entspricht auch bisher – gerade im Automotive-Sektor – der gängigen Praxis, dass Fehler von Werkstätten im Rahmen eines planmäßigen Werkstattbesuchs behoben werden, ohne dass der Nutzer hiervon etwas mitbekommt (sog. stiller Rückruf), vgl. <https://www.zeit.de/auto/2010-10/auto-maengel-rueckruf> (zuletzt abgerufen am 23.09.2024).

1508 Vgl. auch *Riehm/Leithäuser/Brenner*, in: Raue (Hg.), Digitale Resilienz, S. 5 (10).

1509 *Wendehorst*, Besitz- und Eigentumsverhältnisse beim Internet der Dinge – Rechtsgutachten, S. 81 spricht von antizipierter Einwilligung.

unwiderruflich ausgestaltet sein kann,¹⁵¹⁰ würde sie dem Hersteller Rechtssicherheit bieten.¹⁵¹¹ Dabei können auch Eingriffe in das Eigentumsrecht grundsätzlich unwiderruflich gestattet werden.¹⁵¹² Dies zeigt bereits die gesetzlich breit angelegt Dispositionsbefugnis, die von der schuldrechtlichen und dinglichen Belastung bis hin zur unwiderruflichen Übertragung des Eigentums reicht.¹⁵¹³ Da ein Nutzer eine eigenständige Einwilligungserklärungen in Nutzungsbeeinträchtigungen aber kaum einmal abgeben wird und bereits eine entsprechende Anfrage des Herstellers zu Reputationsschäden führen dürfte, kommt einer formularmäßigen antizipierten Einwilligung erhebliche praktische Bedeutung zu.¹⁵¹⁴

(1) Vertragsverhältnis zwischen Hersteller und Eigentümer

Allerdings ist bereits die schuldrechtliche Begründung einer entsprechenden Gestattung mit Schwierigkeiten verbunden; dies jedenfalls, wenn der Nutzer das Produkt wie regelmäßig nicht unmittelbar vom Hersteller erwirbt. Der Hersteller muss folglich mit dem Eigentümer einen separaten Vertrag schließen. Problematisch ist dabei, inwieweit ein solcher Vertragsschluss durch konkludentes Verhalten angenommen werden kann. Dem Nutzer wird es dabei regelmäßig am Erklärungsbewusstsein fehlen. Dies gilt sowohl für das Aufreißen der Verpackung eines smarten Produkts, auf der die entsprechenden Vertragsbedingungen vom Hersteller aufgedruckt sind, als auch für das bloße Akzeptieren einer entsprechenden Vertragsbedingung, die vor der Inbetriebnahme auf einem Display angezeigt wird.¹⁵¹⁵ Auch muss sich der Nutzer eine entsprechende Erklärung nicht zurechnen lassen. Insoweit ist zu berücksichtigen, dass der Nutzer darauf vertraut, durch den Abschluss des entgeltlichen Vertrags mit dem Händler eine umfassende Nutzungsmöglichkeit der Sache eingeräumt zu bekommen und ein obligatorischer zweiter Vertragsschluss mit dem Hersteller gar überraschend für diesen ist. Ohne einen Hinweis hierauf bereits bei Vertrags-

1510 Vgl. *Ohly*, GRUR 2012, 983 (986).

1511 Vgl. auch *Magnus*, Fernkontrolle im Internet der Dinge, S. 226.

1512 Anders bspw. im Hinblick auf eine Körperverletzung im Rahmen des ärztlichen Heileingriffs, vgl. dazu § 630d Abs. 3 BGB.

1513 Vgl. *Magnus*, Fernkontrolle im Internet der Dinge, S. 227.

1514 Dazu *Duden*, Digitale Sachherrschaft, S. 276.

1515 *Marly*, Praxishandbuch Softwarerecht, Rn. 999; *Redeker*, in: *Redeker*, IT-Recht, Rn. 605 f.

schluss mit dem Händler kann dieser Vertrauenstatbestand nicht zerstört werden und eine Zurechnung der Erklärung nicht erfolgen.¹⁵¹⁶ Einen Vertragsschluss mit dem Hersteller wird man daher regelmäßig nur bei einer eigens vorzunehmenden Registrierung annehmen können.¹⁵¹⁷ Problematisch bei der Einholung einer schuldrechtlichen Gestattung bereits bei der Registrierung ist indes, dass es bis zur tatsächlichen Vornahme des Updates zu einem Auseinanderfallen der registrierten Person und des Eigentümers kommen kann, insbesondere wenn das Produkt bis dahin weiterveräußert wurde.¹⁵¹⁸ Damit fallen aber Rechtsgutsinhaber und einwilligende Person auseinander.

(2) AGB-Kontrolle

Abgesehen von diesen tatsächlichen Unsicherheiten für den Hersteller muss eine entsprechende Klausel auch der AGB-Kontrolle standhalten und wirksam sein.

α) Fernstilllegung als überraschende Klausel

Gerade vor dem Hintergrund, dass der Vertrag mit dem Hersteller erst nach dem Erwerb des Geräts geschlossen wird, dürfte eine Fernstilllegung oder die Deaktivierung einzelner Funktionen durch ein Update eine überraschende Klausel i.S.d. § 305c Abs. 1 BGB darstellen.¹⁵¹⁹ Denn anders als bei einer Fernstilllegung zur technischen Bewehrung der Vertragsdurchführung rechnet der Eigentümer des Geräts nach dem Erwerb nicht mit einer

1516 Ausführlich zum Ganzen *Marly*, Praxishandbuch Softwarerecht, Rn. 1000 ff.; i.E. zu Verkaufsbedingungen, die der Hersteller seinen Geräten beilegt auch *Wiesemann/Mattheis/Wende*, MMR 2020, 139 (141); nach *Redeker*, in: *Redeker*, IT-Recht, Rn. 606 können durch einen entsprechenden Hinweis zwar dingliche Einschränkungen wirksam sein, aber keine eigenen Rechte des Herstellers abgeleitet werden.

1517 *Marly*, Praxishandbuch Softwarerecht, Rn. 1007; dazu auch *Wiesemann/Mattheis/Wende*, MMR 2020, 139 (141).

1518 So auch *Magnus*, Fernkontrolle im Internet der Dinge, S. 231.

1519 In diese Richtung auch *Duden*, Digitale Sachherrschaft, S. 297; auch das LG München I, DAR 2021, 633 (634) nannte ein Update (allerdings nicht im Zusammenhang mit einer AGB-Kontrolle), das im Rahmen einer Mangelbeseitigung zu einer Funktionseinschränkung führte, überraschend, sodass man hiermit nicht rechnen müsse.

Einschränkung der sich aus dem Gerät ergebenden Nutzungsmöglichkeit durch eine herstellerseitige Fernstilllegung. Insoweit wird es sich bei dem Vertrag mit dem Hersteller regelmäßig um einen Dienst- oder typen gemischten Vertrag handeln, der im Zusammenhang mit dem verkauften Gerät steht und deren Zweck auf die Erbringung von Serviceleistungen bzw. darauf gerichtet ist, den Betrieb des Produkts in tatsächlicher Hinsicht zu ermöglichen.¹⁵²⁰ Unter einem entsprechenden Service wird sich aber kaum die Deaktivierung verstehen lassen. Der Erwerber geht davon aus, dass er das, was er erlangt und bezahlt hat, behalten darf.¹⁵²¹ Anders ist damit aber die Situation hinsichtlich der Durchführung von Updates zur Fehlerbehebung zu beurteilen. Ein solcher Service entspricht möglicherweise sogar der Nutzererwartung. Gleichwohl darf die Klausel auch in diesem Zusammenhang nicht zu allgemein gehalten werden, da andernfalls ein Verstoß gegen § 307 Abs. 1 S. 2 BGB in Betracht kommt.¹⁵²²

β) Unangemessene Benachteiligung bei funktionsändernden Updates

Eine Klausel, die dem Hersteller das Recht einräumt, Sicherheitsupdates automatisch durchzuführen, könnte den Nutzer allerdings unangemessen benachteiligen und gem. § 307 Abs. 1 S. 1 BGB unwirksam sein. Zunächst soll der Fall betrachtet werden, dass das Sicherheitsupdate – wie regelmäßig in der Praxis – mit Funktionsänderungen verbunden wird.¹⁵²³ Dann aber kann das Produkt nach dem Update neue und von dem Verbraucher unerwünschte Eigenschaften aufweisen.¹⁵²⁴ Beispielsweise seien das Verbrauchen von Speicherplatz, eine neue Menüführung, veränderte Shortcuts für Eingabebefehle, ein neues Design der Bildschirmoberfläche, neues Kompatibilitäts- und Interoperabilitätsverhalten, neue Funktionalitäten

1520 Dazu *Wiesemann/Mattheis/Wende*, MMR 2020, 139 (141 f.); *Magnus*, Fernkontrolle im Internet der Dinge, S. 232 f.

1521 So LG Frankfurt a.M., MMR 2013, 645 (646) allerdings im Rahmen von § 308 Nr. 4 BGB.

1522 Dazu *Magnus*, Fernkontrolle im Internet der Dinge, S. 232.

1523 Vgl. dazu *Schreiber/Esser*, RDt 2022, 317 (317); *Duden*, Digitale Sachherrschaft, S. 164 f; *Riehm*, in: Schmidt-Kessel/Kramme (Hg.), Geschäftsmodelle in der digitalen Welt, S. 201 (219 f.).

1524 Die Gründe dafür, dass Nutzer Updates nicht immer von sich aus installieren, liegen insbesondere in der Zufriedenheit mit der aktuellen Softwareversion und in negativen Erfahrungen mit funktionsverändernden Updates, vgl. *Vaniea/Rader/Wash*, CHI 2014, 2671 (2671 ff.); ferner BR-Drs. 60/21, S. 85 bzgl. § 327r BGB.

oder Möglichkeiten der Verarbeitung personenbezogener Daten und damit verbundene Überwachungsmöglichkeiten genannt.¹⁵²⁵ Eine Klausel, die auch solche Funktionsänderungen erlaubt, könnte dem Rechtsgedanken des § 308 Nr. 4 BGB entsprechend unwirksam sein.¹⁵²⁶ Hiernach ist eine Klausel unzulässig, die es dem Verwender erlaubt, die versprochene Leistung zu ändern oder von ihr abzuweichen, wenn nicht die Vereinbarung der Änderung oder Abweichung unter Berücksichtigung der Interessen des Verwenders für den anderen Vertragsteil zumutbar ist. Eine unmittelbare Anwendung des Klauselverbots scheitert allerdings, da eine antizipierte Einwilligung nicht dazu führt, dass der Hersteller sein Leistungsversprechen ändern kann. Vielmehr ermöglicht es ihm nach erfolgter Leistungserbringung in bereits gelieferte Inhalte einzugreifen.¹⁵²⁷ Während das Klauselverbot auf den Erhalt der Äquivalenz von Leistung und Gegenleistung abzielt,¹⁵²⁸ greift ein funktionsänderndes Update gar in das Integritätsinteresse des Eigentümers ein. Damit stellt sich die Frage der Zumutbarkeit aber sogar in verschärfter Form.¹⁵²⁹ Der Hersteller hat regelmäßig ein Interesse daran, Sicherheits- und Funktionsupdates miteinander zu verbinden, um nicht verschiedene Updatepfade für die unterschiedlichen im Feld befindlichen Versionen entwickeln zu müssen.¹⁵³⁰ Indes führt eine entsprechende Klausel dazu, dass dem Eigentümer automatisch und ohne sein Wissen Programmänderungen aufgespielt werden, deren Funktion er nicht kennt und gegen die er sich nicht wehren kann.¹⁵³¹ Damit aber stellt eine Klausel, die auch funktionsändernde Updates – ohne konkrete Beschreibung der möglichen Änderungen oder entsprechender Beschränkung – einer antizipierten Einwilligung unterstellt, eine unangemessene Benachteiligung des Verbrauchers dar.¹⁵³² Ferner würde eine entsprechende Klausel zumindest künftig auch vom gesetzlichen Leitbild abweichen und gem. § 307 Abs. 2

1525 Beispiele nach *Wendehorst*, Besitz- und Eigentumsverhältnisse beim Internet der Dinge – Rechtsgutachten, S. 23.

1526 So auch *Magnus*, Fernkontrolle im Internet der Dinge, S. 233; für eine direkte Anwendung bei einem App-Store für Smartphones LG Frankfurt a.M., MMR 2013, 645 (646).

1527 *Wendehorst*, Besitz- und Eigentumsverhältnisse beim Internet der Dinge – Rechtsgutachten, S. 23; *Duden*, Digitale Sachherrschaft, S. 294 (Fn. 92).

1528 Vgl. *Wurmnest*, in: MüKo, BGB, § 308, Rn. 1.

1529 Dazu auch *Magnus*, Fernkontrolle im Internet der Dinge, S. 233.

1530 Vgl. BR-Drs. 60/21, S. 85 bzgl. § 327r BGB.

1531 So LG Frankfurt a.M., MMR 2013, 645 (646).

1532 i.E. auch *Wendehorst*, Besitz- und Eigentumsverhältnisse beim Internet der Dinge – Rechtsgutachten, S. 123; *Magnus*, Fernkontrolle im Internet der Dinge, S. 233; wohl auch *Schreiber/Esner*, RD 2022, 317 (321).

Nr.1 BGB unwirksam sein. Denn Anhang I Teil 2 Abs.2 CRA sieht im Hinblick auf Cyberbedrohungen vor, dass neue Sicherheitsaktualisierungen getrennt von Funktionsaktualisierungen bereitgestellt werden müssen, soweit dies technisch machbar ist.

γ) Abweichung vom gesetzlichen Leitbild bei fehlerbehebenden Updates

Beschränkt sich eine Klausel dagegen auf fehlerbeseitigende Updates, ist nicht ohne weiteres von ihrer Unwirksamkeit auszugehen.¹⁵³³ Gleichwohl könnte sich die unangemessene Benachteiligung des Verbrauchers auch hier zumindest künftig unter dem Gesichtspunkt der Abweichung vom gesetzlichen Leitbild nach § 307 Abs.2 Nr.1 BGB ergeben. Insoweit sieht Anhang I Teil 1 Abs.2 lit.c CRA zwar vor, dass im Hinblick auf Cyberbedrohungen sicherzustellen ist, dass Schwachstellen durch Sicherheitsaktualisierungen behoben werden können und dies gegebenenfalls auch durch automatische Sicherheitsaktualisierungen erfolgen kann, die als Standardeinstellung innerhalb eines angemessenen Zeitrahmens installiert werden.¹⁵³⁴ Allerdings muss diese Standardkonfiguration der automatischen Updates über einen klaren und einfach zu bedienenden Opt-out-Mechanismus verfügen, bei dem die Nutzer über verfügbare Aktualisierungen informiert werden und sie vorübergehend verschieben können. Auch unter der Berücksichtigung von Cybersicherheitsaspekten und damit im Hinblick auf Sicherheitsgefahren geht das gesetzliche Leitbild folglich von einer Letztentscheidungskompetenz des Nutzers über die Durchführung von sicherheitsrelevanten Updates aus.¹⁵³⁵ Diese Letztentscheidungskompetenz des Nutzers wird indes mit einer antizipierten Einwilligung beschränkt. Ob dem Nutzer in der Praxis bei dem konkret durchzuführenden Sicherheitsupdate die Möglichkeit eingeräumt wird, dieses auch abzulehnen, ist bei der hier vorzunehmenden abstrakten AGB-Kontrolle ohne Bedeutung.¹⁵³⁶

1533 Schreiber/Esner, RDt 2022, 317 (321); für eine entsprechende Zulässigkeit (allerdings noch ohne Berücksichtigung des CRA), Wiesemann/Mattheis/Wende, MMR 2020, 139 (142).

1534 Das Verhandlungsmandat des Rates (Nr. 11726/23) sah dagegen automatische Updates noch als Standardkonfiguration lediglich für den Fall vor, dass ein Update nicht innerhalb eines bestimmten Zeitraums installiert wird.

1535 Bereits nach Erwägungsgrund (30) der Warenkaufrichtlinie soll es den Verbrauchern freistehen, die bereitgestellten Aktualisierungen zu installieren, zur Bedeutung im hiesigen Kontext Wiesemann/Mattheis/Wende, MMR 2020, 139 (142).

1536 LG Frankfurt a.M., MMR 2013, 645 (646).

Damit ist auch eine Klausel, die eine antizipierte Einwilligung lediglich in Sicherheitsupdates vorsieht, jedenfalls künftig ebenfalls unwirksam.

dd) Rechtmäßigkeit aufgrund Einwilligung

Der mit einem Update verbundene Rechtseingriff kann jedoch durch die Einwilligung des Eigentümers gerechtfertigt sein.

(1) Voreingestellter Opt-out-Mechanismus

Zunächst sei auf die bereits erwähnte und vom CRA vorgezeichnete Möglichkeit eingegangen, automatische Updates als Standardeinstellung vorzugeben, die aber vom Nutzer jederzeit deaktiviert werden kann (Opt-out). Auch wenn der Nutzer hier keine ausdrückliche Erklärung abgibt, könnte in der unterlassenen Deaktivierung automatischer Updates eine konkludente Einwilligung gesehen werden. Da die Möglichkeit des Opt-out auch dauerhaft zur Verfügung steht, sodass auch ein neuer Eigentümer die automatischen Updates jederzeit deaktivieren kann, schadet ein nachgelagerter Erwerb nicht. Auch für die konkludente Einwilligung ist jedoch zu verlangen, dass diese eindeutig als solche erkennbar und auch die Art der Verwendung bzw. der Verwendungszweck bekannt ist.¹⁵³⁷ Dementsprechend setzt die Einwilligung die Erkenntnis des Eingriffs in das Rechtsgut sowie das Erkennen der Sachlage voraus.¹⁵³⁸ Der Einwilligende muss sich der potentiellen Rechtsgutsverletzung bewusst sein.¹⁵³⁹

α) Konkludente Einwilligung in Datenveränderung

Zwar wird sich der Nutzer regelmäßig keine Gedanken hinsichtlich der mit dem Update einhergehenden Datenveränderung machen, indes entspricht es gerade der gegenwärtigen Nutzererwartung, dass ein smartes Produkt bei Inverkehrgabe nicht in jeder Hinsicht fehlerfrei ist, aber jedenfalls

1537 Voigt, in: BeckOGK, BGB, § 823, Rn. 87.

1538 BGH, NJW 1964, 1177 (1177); Förster, in: BeckOK, BGB, § 823, Rn. 34.

1539 Voigt, in: BeckOGK, BGB, § 823, Rn. 83.; Förster, in: BeckOK, BGB, § 823, Rn. 34.

Sicherheitslücken durch spätere Updates geschlossen werden.¹⁵⁴⁰ Die entsprechende Nutzererwartung und die Alltäglichkeit, mit der Updates vorgestellt im Hintergrund durchgeführt werden, bedingen sich dabei gegenseitig. Normativ findet sich dieses Verständnis künftig in Anhang I Teil 1 Abs. 2 lit. c CRA. Gerade bei reinen Sicherheitsaktualisierungen wird man die Schwelle für die konkludente Zustimmung des Eigentümers daher nicht zu hoch ansetzen dürfen, liegen diese doch auch in seinem Interesse.¹⁵⁴¹ Da die Datenveränderung zur Erreichung dieses Fernziels ein notwendiges Durchgangsstadium darstellt und insgesamt als lediglich werterhöhender Eingriff zu werten ist, wird man sie als von der Einwilligung umfasst ansehen müssen, auch wenn sich der Eigentümer diesbezüglich keine konkreten Gedanken macht.

β) Keine konkludente Einwilligung in Nutzungsbeeinträchtigung

Fraglich ist dagegen, ob mit der Einwilligung in die Datenveränderung gleichzeitig eine Einwilligung in eine mögliche Nutzungsbeeinträchtigung und damit in eine Deaktivierung einzelner Funktionen oder die vollständige Stilllegung einhergeht. Auch wenn die Beeinträchtigungen regelmäßig unmittelbar zeitlich zusammenfallen, stellen sie doch unterschiedliche und jeweils eigenständig relevante Beeinträchtigungen dar, sodass auch deren Rechtmäßigkeit eigenständig zu beurteilen ist.¹⁵⁴² Dies ergibt sich schon daraus, dass sich die Einwilligung und das Bewusstsein der Rechtsgutsverletzung immer auf das konkret geschützte Rechtsgut beziehen müssen. Insofern bedarf es auch des Bewusstseins hinsichtlich der inhaltlichen Veränderung der Software. Eine Nutzungsbeeinträchtigung ist damit nicht von der Einwilligung in die Substanzverletzung gedeckt.¹⁵⁴³ Bei der Einwilligung in ein Sicherheitsupdate wird den Nutzern aber regelmäßig nicht bewusst sein, dass damit auch die Möglichkeit der Deaktivierung einzelner Funktio-

1540 Dazu *Riehm*, in: Schmidt-Kessel/Kramme (Hg.), Geschäftsmodelle in der digitalen Welt, S. 201 (204 f.).

1541 Im Vertragsrechtlichen Kontext *Metzger*, in: MüKo, BGB, § 327f, Rn. 16; *Schreiber/Esser*, RD 2022, 317 (320); *Hey*, Die außervertragliche Haftung des Herstellers autonomer Fahrzeuge, S. 94 f. sieht eine Zustimmung des Nutzers gar als entbehrlich an.

1542 *Duden*, Digitale Sachherrschaft, S. 275.

1543 Vgl. auch LG München I, DAR 2021, 633 (634), wonach innerhalb einer Vertragsbeziehung die Einwilligung in ein Update zur Mangelbeseitigung nicht auch eine mit dem Update verbundene Nutzungsbeeinträchtigung erlaubt.

nen oder gar die vollständige Stilllegung des Geräts einhergeht.¹⁵⁴⁴ Damit aber besteht eine Informationsasymmetrie zwischen dem Hersteller und dem Eigentümer des Geräts. Bei einem typischerweise überlegenen Wissen ist anerkannt, dass dem Eingreifenden Aufklärungspflichten obliegen.¹⁵⁴⁵ Insoweit hat auch das LG München I im Rahmen einer vertragsrechtlichen Konstellation eine Aufklärungspflicht des Vertragspartners angenommen, sollte ein Update nicht lediglich einen Mangel beseitigen, sondern gleichzeitig mit der Deaktivierung einzelner Funktionen einhergehen.¹⁵⁴⁶ Erst durch eine umfassende und transparente Information über die Auswirkungen eines Updates kann der Eigentümer die Bedeutung und Tragweite seiner Einwilligung erkennen und ist ihm der Verwendungszweck seiner Einwilligung bekannt.¹⁵⁴⁷ Der bloßen Nichtdeaktivierung automatischer Updates kommt damit mangels vorheriger Aufklärung jedenfalls hinsichtlich der Deaktivierung einzelner Funktionen bzw. der vollständigen Stilllegung des Geräts keine rechtfertigende Wirkung als Einwilligung zu.

y) Konkludente Einwilligung in Funktionsänderungen

Anders könnte die Situation bei Updates sein, die neben der Fehlerbehebung auch funktionale Änderungen mit sich bringen. Die Vornahme von Funktionsänderungen geht dabei auf das Interesse des Herstellers zurück, die Software an aktuelle Marktentwicklungen anzupassen. Dieses Interesse an der Weiterentwicklung der Software wird regelmäßig von einem beträchtlichen Nutzerkreis geteilt, während eine konservative Nutzererwartung dahin geht, dass zwar Fehler und Sicherheitsrisiken beseitigt werden, die Benutzeroberfläche und damit die Bedienungsweise aber unverändert bleiben soll.¹⁵⁴⁸ Gleichzeitig besteht das Interesse des Herstellers, nur eine Version eines digitalen Produkts für alle Nutzer anbieten zu müssen. Da-

1544 *Duden*, Digitale Sachherrschaft, S. 164; auch LG München I, DAR 2021, 633 (634): Greift ein Update in bestehende Funktionen ein und setzt diese weitgehend außer Kraft ist dies „überraschend“ und „nicht mit einem routinemäßigen Update [...] zu vergleichen“; Metzger, in: MüKo, BGB, § 327f, Rn. 16 lehnt im vertragsrechtlichen Kontext daher eine konkludente Einwilligung ab.

1545 *Sprau*, in: Grüneberg, BGB, § 823, Rn. 39.

1546 LG München I, DAR 2021, 633 (634).

1547 i.E. auch *Wendehorst*, Besitz- und Eigentumsverhältnisse beim Internet der Dinge – Rechtsgutachten, S. 124.

1548 Dazu *Riehm*, in: Schmidt-Kessel/Kramme (Hg.), Geschäftsmodelle in der digitalen Welt, S. 201 (205, 221).

bei spiegelt ein solches Vorgehen auch die tatsächliche Praxis bei der Durchführung von Updates wider. Aufgrund dieser tatsächlichen Praxis herrscht bei den Eigentümern der Geräte aber auch ein Bewusstsein dafür, dass Updates mit einer Veränderung der Produkteigenschaften einhergehen können.¹⁵⁴⁹ Dies gilt jedenfalls solange diese Änderungen nicht die Schwelle zur Deaktivierung einzelner Funktionen überschreiten, etwa weil eine Funktion als solche nicht mehr erkennbar ist. Da die Eigentümer diese Sachlage im Hinblick auf automatisch durchgeführte Updates kennen, sind sie sich auch der Bedeutung und Tragweite einer unterlassenen Deaktivierung automatischer Updates bewusst. Aufgrund einer fehlenden Informationsasymmetrie ist daher auch keine entsprechende Aufklärung des Herstellers erforderlich. Insoweit stellt die Nichtdeaktivierung automatischer Updates auch eine konkludente Einwilligung in funktionsändernde Updates dar.¹⁵⁵⁰ Voraussetzung für die Wirksamkeit der Einwilligung ist allerdings, dass diese freiwillig und ohne Zwang abgegeben wurde.¹⁵⁵¹ Im hiesigen Kontext bedeutet dies, dass sich aus der Deaktivierung der automatischen Updates keine Nachteile für den Eigentümer ergeben dürfen.¹⁵⁵² Insbesondere darf dies nicht dazu führen, dass er von zukünftigen Sicherheitsupdates abgeschnitten wird, die ihm aufgrund seiner nicht aktuellen Version gar nicht mehr zur Verfügung gestellt werden.¹⁵⁵³

Gleichwohl dürfte sich dieses Verständnis künftig drehen. Denn Anhang I Teil 2 Abs. 2 CRA sieht künftig im Hinblick auf Cyberbedrohungen vor, dass neue Sicherheitsaktualisierungen getrennt von Funktionsaktualisierungen bereitgestellt werden müssen, zumindest soweit dies technisch machbar ist. Damit aber wird sich bei den Nutzern auch eine entsprechende Updateerwartung einstellen. Sie werden bei automatischen Updates lediglich die Durchführung von Sicherheitsupdates erwarten. Ein Bewusstsein auch für funktionsändernde Updates besteht dann gerade nicht mehr, sodass diese auch nicht mehr von einer entsprechenden Einwilligung gedeckt sein werden.

1549 Vgl. dazu *Vaniea/Rader/Wash*, CHI 2014, 2671 (2671 ff.).

1550 So auch *Riehm*, in: Schmidt-Kessel/Kramme (Hg.), *Geschäftsmodelle in der digitalen Welt*, S. 201 (221); tendenziell zurückhaltender *Wendehorst*, *Besitz- und Eigentumsverhältnisse beim Internet der Dinge – Rechtsgutachten*, S. 124.

1551 Allg. Meinung, vgl. nur BGH, NJW 1964, 1177 (1178); *Sprau*, in: Grüneberg, BGB, § 823, Rn. 39.

1552 Vgl. *Wendehorst*, *Besitz- und Eigentumsverhältnisse beim Internet der Dinge – Rechtsgutachten*, S. 124.

1553 Vgl. auch *Duden*, *Digitale Sachherrschaft*, S. 165.

(2) Aufrechterhaltung der Schnittstellenkonnektivität

Ferner wird man in der bloßen Aufrechterhaltung der für das Update erforderlichen Schnittstellenkonnektivität – etwa der Internet- oder Bluetooth-Verbindung – des Geräts keine konkludente Einwilligung sehen können. Hier kann von einem abstrakt bei dem Eigentümer vorhandenen Wissen, dass die Konnektivität Voraussetzung für die Durchführung des Updates ist, nicht auch auf ein Bewusstsein hinsichtlich des konkreten Eingriffs geschlossen werden. Denn die Beibehaltung der Konnektivität erfolgt regelmäßig, um das Produkt funktionsgemäß nutzen zu können. In diesem Bewusstsein wird der Eigentümer die Konnektivität herstellen oder beibehalten. Es fehlt damit schon an der eindeutigen Erkennbarkeit einer entsprechenden Einwilligung. Um nicht Gefahr zu laufen, dass in seinem Verhalten eine konkludente Einwilligung gesehen wird, müsste ein Eigentümer andernfalls die Konnektivität aktiv unterbinden und folglich regelmäßig auf Funktionen seines smarten Produkts verzichten. Diese Überlegung zeigt, dass neben der fehlenden Erkennbarkeit der Einwilligung eine solche auch mit unzulässigem Zwang verbunden wäre, da die Folge einer fehlenden Einwilligung Funktionseinbußen am Produkt wären. Dies gilt auch nach vorheriger Aufklärung über die mit dem Update verbundenen Rechtseingriffe. Zwar kann durch einen entsprechenden Hinweis dem Eigentümer bewusst gemacht werden, dass bei weiterer Aufrechterhaltung der Konnektivität ein Update erfolgt und in seine Rechtspositionen eingegriffen wird. Sofern mit der Abschaltung der Konnektivität jedoch funktionale Beeinträchtigungen einhergehen, ist eine erteilte (konkludente) Einwilligung nicht mehr freiwillig.

(3) Ausdrückliche Einwilligung

Die eben dargestellten Erwägungen lassen sich auch auf eine ausdrücklich erteilte Einwilligung übertragen. Der Hersteller kann den Nutzer auch vor jedem Update gesondert und individuell um eine Einwilligungserklärung bitten. Auch dann gilt es zu beachten, dass eine entsprechende Einwilligung nicht durch unzulässigen Zwang eingeholt werden darf. Weiter ist vor Updates, die Funktionen beeinträchtigen oder gar zur Stilllegung des Geräts führen, entsprechend darüber aufzuklären. Dies zeigt, warum der ausdrücklichen Einwilligung kaum praktische Relevanz zukommt.

ee) Zwischenfazit

Neben den tatsächlichen Schwierigkeiten bei der Begründung eines Vertragsschlusses zwischen Hersteller und Eigentümer wird eine Klausel, die dem Hersteller das Recht einräumt, die mit einem Update verbundenen Rechtseingriffen vornehmen zu dürfen, regelmäßig im Rahmen der AGB-Kontrolle unwirksam sein. Eine Einwilligung in die konkrete Rechtsgutsverletzung rechtfertigt dagegen den Eingriff. Eine solche liegt konkludent in der unterlassenen Deaktivierung automatischer Updates. Dies allerdings nur in Bezug auf die Datenveränderung der Software. Damit kann der Hersteller fehlerbehebende Updates durchführen. Die Frage, ob die Einwilligung auch Funktionsänderungen umfasst, die die Schwelle zur Einschränkung von Funktionen nicht überschreiten, unterliegt angesichts der Regelungen im CRA einem Wandel. Jedenfalls künftig wird man hiervon nicht mehr ausgehen können. Hinsichtlich der Deaktivierung einzelner Funktionen oder gar der vollständigen Stilllegung des Geräts fehlt es schon am erforderlichen Bewusstsein der Rechtsgutsverletzung. Daher wäre eine vorherige Aufklärung über den Rechtseingriff erforderlich. In der bloßen Aufrechterhaltung der Schnittstellenkonnektivität kann keine konkludente Einwilligung gesehen werden. Ohne entsprechende Aufklärung erkennt der Eigentümer die Einwilligung schon nicht als solche und nach entsprechendem Hinweis fehlt es an der Freiwilligkeit der Einwilligung, führt die Unterbrechung der Konnektivität doch zu Funktionseinbußen am Gerät.

ff) Weitere gesetzliche Rechtfertigungsgründe

Aufgrund der unter E.III.2.b)bb) dargestellten Interessenlage kann der Hersteller gleichwohl ein Interesse daran haben, ein Update auch ohne Einwilligung des Nutzers durchzuführen. Möglicherweise stehen ihm in diesem Fall des Zwangsupdates gesetzliche Rechtfertigungsgründe zur Seite.

(1) Nothilfe, gem. § 227 BGB

Zunächst kommt eine Rechtfertigung unter dem Gesichtspunkt der Nothilfe nach § 227 Abs. 1 BGB zur Abwehr eines gegenwärtigen, rechtswidrigen Angriffs (§ 227 Abs. 2 BGB) in Betracht. Dabei ist danach zu differenzieren, ob der Hersteller das Update unvermittelt durchführt oder erst nachdem eine Warnung vom Nutzer ignoriert oder die Einwilligung in ein bereitge-

stelltes Update nicht erteilt wurde bzw. dieses nicht eigenverantwortlich durchgeführt wurde.

Im ersten Fall erfolgt das Zwangsupdate sowohl zu Gunsten des Produkt-nutzers als auch zu Gunsten der innocent bystander. Allerdings ist bereits bei der Prüfung der Notwehrlage das Vorliegen eines Angriffs problematisch. Denn dieser setzt ein menschliches Verhalten voraus und kann nicht von einer Sache ausgehen.¹⁵⁵⁴ Ein menschliches Verhalten kann freilich beim Ausnutzen einer Sicherheitslücke durch einen Hacker angenommen werden. Allerdings entfaltet die Notwehr oder Nothilfe keine Drittwirkung, sodass eine Nothilfehandlung allein gegen die Rechtsgüter des Angreifers gerechtfertigt ist, nicht aber gegen die Rechtsgüter Dritter, auch wenn eine solche Einwirkung mit der gegen den Angreifer erforderlichen Verteidigungshandlung einhergehen sollte.¹⁵⁵⁵ Damit aber wäre in dieser Konstellation allein eine Einwirkung gegen den Hacker als Angreifer, nicht aber gegen den Nutzer als Dritten gerechtfertigt. Geht die Gefahr dagegen – ohne dass ein weiteres menschliches Einschreiten erforderlich wäre – von der Fehlerhaftigkeit des Produkts aus, fehlt es schon an einem menschlichen Verhalten, das als Angriff qualifiziert werden könnte und liegt eine bloße Sachgefahr vor.

Anders könnte die Situation zu beurteilen sein, wenn das Zwangsupdate durch den Hersteller erst nach erfolgloser Warnung des Nutzers oder nach Bereitstellung des Updates zur eigenverantwortlichen Durchführung erfolgt und der Nutzer das Produkt gleichwohl unter Gefährdung weiterverwendet. In diesen Fällen ist der Nutzer mitverantwortlich für die Gefährdung und das Unterlassen der entsprechenden Gefahrenabwehrmaßnahme könnte als notstandsfähiger Angriff angesehen werden. Das Zwangsupdate erfolgte dann allein zu Gunsten der innocent bystander.¹⁵⁵⁶

Unabhängig von der Frage, ob für einen Angriff bei § 227 Abs.1 BGB auch ein pflichtwidriges Unterlassen ausreichend ist,¹⁵⁵⁷ fehlt es aber jedenfalls an der Gegenwärtigkeit eines solchen Angriffs im Sinne einer unmittelbar bevorstehenden oder gerade andauernden Verletzung rechtlich

1554 Allg. Meinung, vgl. nur *Grothe*, in: MüKo, BGB, § 227, Rn. 4; *Ellenberger*, in: *Grüneberg*, BGB, § 227, Rn. 2.

1555 Vgl. *Rövekamp*, in: BeckOGK, BGB, § 227, Rn. 44.

1556 Zugunsten unbestimmter Dritter kann ebenfalls Nothilfe geübt werden, vgl. *Grothe*, in: MüKo, BGB, § 227, Rn. 15.

1557 Str., ablehnend *Ellenberger*, in: *Grüneberg*, BGB, § 227, Rn. 2 und *Grothe*, in: MüKo, BGB, § 227, Rn. 5 m.w.N.; bejahend dagegen *Rövekamp*, in: BeckOGK, BGB, § 227, Rn. 17.

geschützter Güter.¹⁵⁵⁸ Eine ausnutzbare Sicherheitslücke hat nämlich noch keine direkten negativen Auswirkungen auf die Nutzer anderer Geräte. Selbst die Infektion des Geräts des Nutzers dient lediglich der Vorbereitung entsprechender Handlungen.¹⁵⁵⁹ Die Rechtsgutsverletzung Dritter durch das Unterlassen des Nutzers steht damit aber nicht unmittelbar bevor. Auch bei einem sonstigen Produktfehler steht eine Beeinträchtigung nicht unmittelbar bevor. Denn in diesem Fall lässt sich der voraussichtliche Zeitpunkt der Realisierung der Gefahr nicht vorhersagen. Es ist eine permanente Gefahr gegeben, die jederzeit in einen Schaden umschlagen kann. Eine solche Dauergefahr ist aber im Gegensatz zur Augenblicksgefahr nicht von der Notwehrregelung des § 227 Abs. 1 BGB erfasst.¹⁵⁶⁰

(2) Defensivnotstand, gem. § 228 S. 1 BGB

α) Notstandslage

Im Rahmen des Defensivnotstands ist die Beschädigung oder Zerstörung einer gefahrdrohenden Sache nach § 228 S. 1 BGB nicht widerrechtlich. Dabei braucht die von der Sache ausgehende Gefahr nicht gegenwärtig zu sein, sondern es reicht aus, wenn nach den tatsächlichen Umständen der Eintritt eines schädigenden Ereignisses wahrscheinlich ist.¹⁵⁶¹ So liegt aber der Fall, wenn die Fehlerhaftigkeit eines Produkts eine konkrete Gefahr begründet.¹⁵⁶²

Weiter müsste die Sache selbst aber auch als unmittelbare Gefahrenquelle anzusehen sein.¹⁵⁶³ Dies scheint aber gerade in der Konstellation der ausnutzbaren Sicherheitslücke fraglich, da hier die Gefahr erst durch die

1558 Vgl. *Ellenberger*, in: *Grüneberg*, BGB, § 227, Rn. 4; *Rövekamp*, in: *BeckOGK*, BGB, § 227, Rn. 29.

1559 *Regenfus*, JZ 2018, 79 (85); *Grünvogel/Dörrenbächer*, ZVertriebsR 2019, 87 (90); allgemein keine Nothilfe gegen Angriffsvorbereitungshandlungen, vgl. nur *Grothe*, in: *MüKo*, BGB, § 227, Rn. 9.

1560 So zur parallelen Bewertung im Strafrecht, *Neumann*, in: *NK-StGB*, § 34, Rn. 56.

1561 *Ellenberger*, in: *Grüneberg*, BGB, § 228, Rn. 4; *Rövekamp*, in: *BeckOGK*, BGB, § 228, Rn. 13; *Grothe*, in: *MüKo*, BGB, § 228, Rn. 7.

1562 Ausführlich noch unter E.III.5.c)bb)(1)α).

1563 Andernfalls wäre eine Rechtfertigung über den Angriffsnotstand nach § 904 S. 1 BGB zu prüfen, in dem auch die Beeinträchtigung unbeteiligter Sachen gerechtfertigt ist, der Handelnde aber im Gegensatz zu § 228 S. 2 nach § 904 S. 2 BGB verschuldensunabhängig für Schäden einzustehen hat, vgl. *Rövekamp*, in: *BeckOGK*, BGB, § 228, Rn. 17.

deliktische Handlung des Hackers begründet wird. Ob § 228 S. 1 BGB auch bei einer lediglich mittelbar von der beschädigten Sache ausgehenden Kausalität Anwendung findet, ist streitig.¹⁵⁶⁴ Es wird beispielhaft angeführt, dass der in einem Haus lagernde Tabak, der Plünderer anlockt, nicht selbst eine Gefahr begründe, sondern allein die Plünderer gefährlich seien.¹⁵⁶⁵ Jedenfalls für Fälle, in denen die Sache als Angriffsmittel von einem Dritten benutzt wird, ist ein Defensivnotstand aber ausgeschlossen.¹⁵⁶⁶ Indes liegt bei einem mit einer Sicherheitslücke behafteten Produkt eine besondere Konstellation vor. Denn weist ein Produkt eine ausnutzbare Sicherheitslücke auf, handelt es sich bei einem Hackerangriff gerade um eine spezifische Gefahr, die in der Sache angelegt ist.¹⁵⁶⁷ Damit aber kann keine Rede davon sein, dass die Sache die Gefahr nur mittelt und weiterleitet,¹⁵⁶⁸ vielmehr droht die Gefahr von der Sache selbst.¹⁵⁶⁹ Die Sache ist aus sich heraus gefährlich, auch wenn es zur Aktivierung der Gefahr einer hinzutretenden Handlung bedarf.

Zu differenzieren ist dann allerdings danach, ob die Gefahr allein dem Produktnutzer oder zumindest auch Dritten droht. Droht die Gefahr allein dem Nutzer und führt der Hersteller das Zwangsupdate nicht unvermittelt durch, sondern erst nachdem eine Warnung vom Nutzer ignoriert oder ein bereitgestelltes Update nicht installiert wurde, entfällt die Nothilfebefugnis. Denn die Abwehr einer drohenden Gefahr setzt den Abwehrwillen des Gefahrbedrohten voraus.¹⁵⁷⁰ Setzt der Nutzer aber trotz erfolgter Warnung oder bereitgestelltem Update in Kenntnis der ihm drohenden Gefahr den Gebrauch des Produkts fort, willigt er konkludent jedenfalls in seine Rechtsgutsgefährdung ein.¹⁵⁷¹ Eine gegen den erklärten Willen des Gefahrbedrohten aufgedrängte Hilfe kann aber grundsätzlich nicht geleistet wer-

1564 Vgl. die Nachweise bei *Rövekamp*, in: BeckOGK, BGB, § 228, Rn. 18.

1565 Vgl. zu diesem Beispiel *Grothe*, in: MüKo, BGB, § 227, Rn. 8; *Ellenberger*, in: Grüneberg, BGB, § 228, Rn. 6.

1566 Vgl. *Grothe*, in: MüKo, BGB, § 227, Rn. 8; *Ellenberger*, in: Grüneberg, BGB, § 228, Rn. 6; *Rövekamp*, in: BeckOGK, BGB, § 228, Rn. 15; AG Riesa, MMR 2019, 548 (579).

1567 Dazu allgemein *Rövekamp*, in: BeckOGK, BGB, § 228, Rn. 18.

1568 Zum Ausschluss von § 228 BGB, wenn die Sache nur ein „Medium“ bildet, *Grothe*, in: MüKo, BGB, § 228, Rn. 8.

1569 Hierzu *Dennhardt*, in: BeckOK, BGB, § 228, Rn. 5.

1570 *Rövekamp*, in: BeckOGK, BGB, § 228, Rn. 29; *Dennhardt*, in: BeckOK, BGB, § 228, Rn. 11.

1571 So auch *Regenfus*, JZ 2018, 79 (84).

den.¹⁵⁷² Wurde der Nutzer verständlich, deutlich und zuverlässig gewarnt, stellte sich eine dennoch durch den Hersteller erfolgtes Zwangsupdate als „Schutz des Nutzers vor sich selbst“ dar und widerspräche dem Prinzip der Eigenverantwortung.¹⁵⁷³ Etwas anderes kann nur dort gelten, wo es eine hinreichend deutliche und detaillierte Warnung dem Produktnutzer nicht ausreichend ermöglicht, die Gefahr einzuschätzen und sein Verhalten darauf einzurichten. Ein entgegenstehender Wille des Gefahrbedrohten ist nämlich dann unbeachtlich, wenn er mangels hinreichender Kenntnis gar nicht in der Lage ist, über das jeweilige Rechtsgut zu disponieren.¹⁵⁷⁴

β) Erforderlichkeit der Maßnahme

Die Notstandshandlung muss dann zur Abwendung der Gefahr erforderlich sein. Das ist der Fall, wenn die Maßnahme geeignet ist, die Gefährdung des Rechtsguts abzuwenden und kein weniger schädliches Mittel zur Verfügung steht. Nach dem Grundsatz des geringsten Eingriffs darf nur das mildeste der zur Verfügung stehenden geeigneten Mittel eingesetzt werden.¹⁵⁷⁵

Jedenfalls in den Fällen, in denen der Hersteller nach den oben dargestellten Grundsätzen keine Updatepflicht trifft, kommt eine Warnung als milderer Mittel gegenüber der Zwangsaktualisierung in Betracht. Gerade bei einem unvermittelten Zwangsupdate allein zum Schutz des Nutzers wird eine deutliche und unmissverständliche Warnung stets ein gleich geeignetes und erheblich milderer Mittel zur Abwehr des drohenden Schadens für seine Rechtsgüter darstellen.¹⁵⁷⁶ Ferner ist auch bei einer Drittgefährdung der Vorrang der Warnung, ggf. in Verbindung mit einer Stilllegungsaufforderung an den Nutzer, in Betracht zu ziehen.¹⁵⁷⁷ Allerdings ist bei Gefahren auch für Dritte nicht zu verkennen, dass eine Warnung des Geräteinhabers kein gleich wirksames Mittel darstellen könnte, da der

1572 Rövekamp, in: BeckOGK, BGB, § 228, Rn. 29.

1573 Regenfus, JZ 2018, 79 (84 f.); Wittig, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 234.

1574 Rövekamp, in: BeckOGK, BGB, § 228, Rn. 29.

1575 Vgl. nur Grothe, in: MüKo, BGB, § 228, Rn. 9; Dennhardt, in: BeckOK, BGB, § 228, Rn. 8; Rövekamp, in: BeckOGK, BGB, § 228, Rn. 20.

1576 Grünvogel/Dörrenbächer, ZVertriebsR 2019, 87 (90 f.); Wittig, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 234.

1577 So auch Piovano/Schucht/Wiebe, Produktbeobachtung in der Digitalisierung, S. 103.

Schutz des Dritten dem Wohlwollen des Nutzers unterstellt würde.¹⁵⁷⁸ Dies muss jedenfalls im Zusammenhang mit Software oder smarten Produkten gelten, bei denen regelmäßig damit zu rechnen ist, dass ein herstellerseitiger Warnhinweis ignoriert wird.¹⁵⁷⁹

Auch das bloße herstellerseitige Bereitstellen von Updates beseitigt die Gefahr ebenso wenig wie die reine Warnung. In beiden Fällen ist die Mitwirkung des Nutzers erforderlich. So liegt es gerade am Nutzer, die bereitgestellten Updates auch herunterzuladen und zu installieren, um so die Sicherheitsgefahr zu beseitigen. Die Gründe, warum dies in der Praxis nicht immer geschieht, sind vielfältig. Ausgemacht werden können dabei die Zufriedenheit mit der aktuellen Softwareversion, negative Erfahrungen mit früheren (nicht sicherheitsrelevanten) Updates, welche bspw. die Benutzeroberfläche verändert haben, die fehlende fachliche Expertise, um die Sinnhaftigkeit eines Updates beurteilen zu können sowie die Tatsache, dass mit der Sicherheitslücke keine Funktionsbeeinträchtigung einhergeht.¹⁵⁸⁰ Vor diesem Hintergrund sind viele Hackerangriffe gerade auf Sicherheitslücken zurückzuführen, für die zwar Updates zur Verfügung stehen, die aber von den Nutzern nicht installiert wurden.¹⁵⁸¹ Aus den gleichen Gründen kann auch die Einwilligung in Updates unterbleiben.

Damit bleiben aber sowohl die Warnung als auch das Bereitstellen eines Sicherheitsupdates bzw. die Einholung der entsprechenden Einwilligung aufgrund der erforderlichen Mitwirkung des Nutzers hinsichtlich der Geeignetheit der Gefahrenabwehr hinter der zwangsweisen Aktualisierung und Deaktivierung zurück. Allerdings muss der Verteidiger im Rahmen des Defensivnotstands zunächst auch weniger eingriffsintensive Abwehrmittel versuchen, auch wenn deren Wirkung nicht völlig sicher ist.¹⁵⁸² Dies muss jedenfalls dann gelten, wenn das Risiko eines Fehlschlags dem Angegriffen noch zugemutet werden kann.¹⁵⁸³ Sofern im Falle einer Sicherheitslücke oder eines sonstigen sicherheitsrelevanten Produktfehlers der Eintritt eines

1578 So Grünvogel/Dörrenbächer, ZVertriebsR 2019, 87 (91); i.E. auch Regenfus, JZ 2018, 79 (85 f.).

1579 Siehe oben E.III.1.b)cc).

1580 Ausführlich Vaniea/Rader/Wash, CHI 2014, 2671 (2671 ff.).

1581 Vgl. Vaniea/Rader/Wash, Betrayed By Updates, CHI 2014, 2671 (2671); 2019 wurden bei 60 Prozent der IT-Angriffe Schwachstellen ausgenutzt, für die ein Patch verfügbar gewesen wäre, vgl. <https://www.retarus.com/blog/de/alarmierende-zahlen-aktuelle-cybersecurity-statistiken/> (zuletzt abgerufen am 23.09.2024); Ritter, in: Raue (Hg.), Digitale Resilienz, S. 79 (87 f.).

1582 Rövekamp, in: BeckOGK, BGB, § 228, Rn. 21; Grothe, in: MüKo, BGB, § 228, Rn. 9.

1583 In diese Richtung BGH, NStZ-RR 2013, 105 (106).

Schadens nicht unmittelbar bevorsteht, etwa weil die Sicherheitslücke noch nicht öffentlich bekannt ist oder der Produktfehler sich erst im Laufe der Zeit auswirkt, sind weitergehende Maßnahmen als die bloße Bereitstellung des Sicherheitsupdates je nach Schwere und Ausmaß der bestehenden Gefahr erst dann erforderlich, wenn der Nutzer das bereitgestellte Update nicht innerhalb eines bestimmten Zeitraums durchgeführt hat.¹⁵⁸⁴

γ) Verhältnismäßigkeit der Maßnahme

Im Rahmen des Defensivnotstands nach § 228 S.1 BGB muss neben der Erforderlichkeit auch die Verhältnismäßigkeit der jeweiligen Maßnahme gewahrt sein. Der eintretende Schaden darf nicht außer Verhältnis zur abgewendeten Gefahr stehen.¹⁵⁸⁵ Dabei hat die Integrität der Schutzgüter Leib und Leben Vorrang vor dem Erhalt von Sachgütern.¹⁵⁸⁶ Bei einer entsprechenden Gefährlichkeit des Produkts, kann selbst eine Deaktivierung, durch die das Gerät wertlos wird, gerechtfertigt sein.¹⁵⁸⁷ Umgekehrt bedeutet dies aber auch, dass die vollständige Deaktivierung nur bei erheblichen Gefahren für bedeutende Rechtsgüter zulässig ist.¹⁵⁸⁸ Die vorübergehenden Deaktivierung hat dagegen keine gravierenden Auswirkungen – gerade im Verhältnis zu der von § 228 S.1 BGB selbst angesprochenen Beschädigung oder Zerstörung – und ist daher eher gerechtfertigt.¹⁵⁸⁹

1584 Vgl. *Fida*, Updates, Patches & Co, S.167; *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S.103; ähnlich *Wiebe*, InTer 2020, 66 (69); vgl. auch *Schmid*, IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme, S.242.

1585 *Ellenberger*, in: Grüneberg, BGB, § 228, Rn.8; *Grothe*, in: MüKo, BGB, § 228, Rn.10.

1586 *Ellenberger*, in: Grüneberg, BGB, § 228, Rn.8; *Grothe*, in: MüKo, BGB, § 228, Rn.10.

1587 *Regenfus*, JZ 2018, 79 (86).

1588 *Grünvogel/Dörrenbächer*, ZVertriebsR 2019, 87 (91); *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S.103; ähnlich auch *Sommer*, Haftung für autonome Systeme, S.284 f.; *Wiebe*, BB 2022, 899 (904); in anderem Kontext *Wiesemann/Mattheis/Wende*, MMR 2020, 139 (144) und *Meents/Obradovic*, ZfPC 2022, 13 (18); vgl. auch *Schmid*, IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme, S.242 f.

1589 *Regenfus*, JZ 2018, 79 (85).

δ) Drohender Schadensersatzanspruch nach § 228 S. 2 BGB

Der per Fernzugriff eingreifende Hersteller hat dann noch zu beachten, dass seine Einwirkungsbefugnis aus § 228 S. 1 BGB zu einer Schadensersatzpflicht nach § 228 S. 2 BGB führen kann, soweit er die Gefahr schuldhaft verursacht hat. Für die Beurteilung der Schadensersatzpflicht kommt es daher darauf an, ob der Auslöser für die Produktgefahr und seine daraus folgende Gefahrenabwehrmaßnahme ursprünglich in einem Konstruktions- oder Fabrikationsfehler lag.¹⁵⁹⁰ Nur in diesen Fällen liegt ein schuldhaftes Verhalten des Herstellers vor und es trifft ihn dadurch – anders als etwa bei einem Entwicklungsfehler – die Verantwortlichkeit für die Produktgefahr.

Zu beachten ist in diesem Zusammenhang allerdings, dass zugunsten des Handelnden ein etwaiges Mitverschulden des durch die Notstandshandlung Geschädigten nach § 254 BGB Berücksichtigung findet.¹⁵⁹¹ Gerade für den Fall, dass der Produktnutzer einer Updateaufforderung durch den Hersteller nicht nachkam, während der Hersteller seine Produktbeobachtungspflicht durch das Bereitstellen des Updates erfüllte, ist eine Anspruchskürzung bis auf Null denkbar. Daneben ist fraglich, inwieweit dem Nutzer durch eine Deaktivierung seines Produkts überhaupt ein Schaden entsteht, da er das Gerät wegen der Sicherheitsrisiken ohnehin nicht gefahrlos hätte benutzen können und ihn die Stilllegung nur zu dem Verhalten zwingt, das er sowohl aus Gründen der Eigenvernunft als auch zum Schutze Dritter ohnehin schuldet.¹⁵⁹² Hier wird im Einzelfall zu beurteilen sein, welchen Wert das gefährliche Produkt trotzdem noch hat. Auch wenn ein Schadensersatzanspruch daher im Einzelfall entfallen kann oder aufgrund Mitverschuldens des Nutzers sogar regelmäßig bis auf Null gekürzt sein wird, hängt dieser doch wie ein Damoklesschwert über dem Hersteller und seiner aufgedrängten Gefahrenabwehrmaßnahme. Dies und die Tatsache, dass auch aufgezwungene Maßnahmen zu negativer Presse und Vertrauensverlust führen können, dürfte dazu führen, dass sie trotz ihrer Einfachheit und Effektivität nur mit Bedacht vom Hersteller eingesetzt werden.

1590 So auch *Regenfus*, JZ 2018, 79 (86).

1591 *Grothe*, in: MüKo, BGB, § 228, Rn. 13; *Dennhardt*, in: BeckOK, BGB, § 228, Rn. 12; *Rövekamp*, in: BeckOGK, BGB, § 228, Rn. 34.

1592 *Regenfus*, JZ 2018, 79 (86).

d) Bedeutung für die Effektivität der Gefahrenabwehr und Ausgestaltung der Updatepflicht

Letztendlich ergibt sich aus dem Prinzip des geringsten Eingriffs ein „Stufenbau der Reaktionspflichten“.¹⁵⁹³ Hat der Eigentümer nicht bereits wirksam in einen entsprechenden Rechtseingriff eingewilligt, stellt die Grundmaßnahme nach hiesigem Verständnis regelmäßig das Bereitstellen eines Updates zur Behebung des Sicherheitsmangels dar. Nur wenn der Nutzer einer Updateaufforderung nicht nachkommt, diese von vorneherein keinen Erfolg verspricht oder die zeitnahe Verwirklichung der Gefahr ein Zuwarten nicht zulässt, ist eine fehlerbehebendes Zwangsupdate in Betracht zu ziehen. Darüber hinaus ist dem Nutzer das Zwangsupdate grundsätzlich zunächst anzudrohen, damit er selbst über den Zeitpunkt des Updates – und damit über die vorübergehende Nichtnutzbarkeit seines Produkts während der Durchführung des Updates – entscheiden kann.¹⁵⁹⁴ Ob dabei Maßnahmen, die faktischen Zwang auf den Nutzer ausüben, um ihn zur Installation des bereitgestellten Updates zu bewegen,¹⁵⁹⁵ wie z.B. die Herbeiführung von Systeminstabilitäten oder die Deaktivierung einzelner Funktionen bis hin zu betriebsnotwendigen Funktionen oder gleich die Installation des Zwangsupdates, weniger eingriffsintensiv sind, kann nur im Einzelfall beantwortet werden. In diesem Zusammenhang sind auch Funktionseinschränkungen oder Veränderungen der Bedienung gerechtfertigt, sofern das Sicherheitsupdate unter technischen Gesichtspunkten nicht anders entwickelt werden kann. Denn der Nutzer wird durch ein auch erzwungenes Update des Herstellers weit weniger beeinträchtigt als bei einer kompletten Stilllegung des Produkts.¹⁵⁹⁶

Ist dagegen das vom Produkt ausgehende Schadensrisiko nicht oder nur mit unzumutbarem Aufwand durch ein Softwareupdate zu beheben,

1593 Sommer, Haftung für autonome Systeme, S. 284.

1594 Dazu Wendehorst, in: Stabentheiner/Wendehorst/Zöchling-Jud (Hg.), Das neue europäische Gewährleistungsrecht, S. III (125).

1595 Dazu Wendehorst, in: Stabentheiner/Wendehorst/Zöchling-Jud (Hg.), Das neue europäische Gewährleistungsrecht, S. III (125); vgl. auch Wittig, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 234; Fida, Updates, Patches & Co, S. 167; Piovano/Schucht/Wiebe, Produktbeobachtung in der Digitalisierung, S. 103.

1596 Fida, Updates, Patches & Co, S. 167; Wittig, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 233 f.; Wiebe, BB 2022, 899 (904).

kommt die Deaktivierung des Produkts als ultima ratio in Betracht.¹⁵⁹⁷ Allerdings gilt es hier zu beachten, dass die Rechtfertigung einer vollständigen Deaktivierung dort ausscheidet, wo als mildere Maßnahme die bloße Deaktivierung einzelner Funktionen in Betracht kommt.¹⁵⁹⁸ Ferner muss das Gerät umgehend wieder freigegeben werden, nachdem die Gefahr beseitigt wurde.¹⁵⁹⁹ Eine ferngesteuerte Deaktivierung des Produktes kann somit insbesondere erfolgen, um eine Gefährdung bis zur Durchführung von Sicherheitsupdates oder Reparaturmaßnahmen auszuschließen.¹⁶⁰⁰

e) Zumutbarkeitsgesichtspunkte

Neben der Effektivität der Gefahrenabwehr stellt die Zumutbarkeit aber eine weitere zu beachtende Kenngröße bei der Beurteilung der Reaktionspflichten des Herstellers dar. So kann eine aus Gründen der Effektivität der Gefahrenabwehr erforderliche Maßnahme durch Erwägungen der Zumutbarkeit begrenzt sein.¹⁶⁰¹ Möglicherweise sind daher die faktischen Voraussetzungen für eine Verpflichtung zu Sicherheitsupdates für die Hersteller nicht realisierbar.¹⁶⁰²

Zunächst ist zu bedenken, dass Sicherheitsupdates ihrerseits zu keinen Gefahren führen dürfen.¹⁶⁰³ Es liegt auf der Hand, dass hinzugefügter Code selbst wieder neue Fehler aufweisen kann.¹⁶⁰⁴ Daneben ist zu berücksichtigen, dass es im Zuge steigender Komplexität und Vernetzung zunehmend

1597 So im Wesentlichen auch *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 102 f. und *Wagner*, in: MüKo, BGB, § 823, Rn. 1133 allerdings ohne Thematisierung der Zwangsaktualisierung.

1598 *Grünvogel/Dörrenbächer*, ZVertriebsR 2019, 87 (91); dies wird gerade dort relevant, wo sich die Sicherheitsgefährdung auf eine bloße Zusatzfunktion beschränkt, vgl. *Regenfus*, JZ 2018, 79 (85).

1599 *Grünvogel/Dörrenbächer*, ZVertriebsR 2019, 87 (91); *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 103.

1600 *Grünvogel/Dörrenbächer*, ZVertriebsR 2019, 87 (91); *Schmid*, IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme, S. 242; *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 103; *Gomille*, JZ 2016, 76 (81); *Lüftenegger*, RDt 2021, 293 (300).

1601 BGH, NJW 2009, 1080 (1082, Rn. 18).

1602 Schon beim herkömmlichen Rückruf äußert *Klindt*, BB 2009, 792 (795) diese Bedenken.

1603 *Wiebe*, InTer 2020, 66 (69); vgl. auch *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 100.

1604 *Reusch*, BB 2019, 904 (905).

zu einem Zusammenspiel verschiedener Komponenten und unterschiedlicher Programme kommt. Daher müssen auch nachteilige Auswirkungen des bereitgestellten Updates auf andere Anwendungen mitgedacht werden.¹⁶⁰⁵ Zudem befindet sich das Produkt gerade während der Updatephase in einem sicherheitskritischen Zustand, da je nach Art des Updates während der Installation sicherheitsrelevante Funktionen nicht verfügbar sein können.¹⁶⁰⁶ Daneben können für bestimmte Produktgattungen zulassungsrechtliche Fragestellung zu beachten sein.¹⁶⁰⁷ Bei diesen Herausforderungen handelt es sich jedoch weniger um Fragen der generellen Zumutbarkeit von Updatepflichten. Vielmehr geht es um Fragen der sorgfältigen Konstruktion der Updates selbst, der konkreten Ausgestaltung der Durchführung von Softwareupdates sowie der Folgen eines durchgeführten Updates. Nur en passant sei erwähnt, dass diesbezüglich speziell für den Automotive-Sektor durch die UN-Regelung Nr. 156 hinsichtlich der Softwareaktualisierung und des Softwareaktualisierungsmanagementsystems bereits Vorgaben entwickelt wurden (vgl. insbesondere Ziff. 7.2 und Ziff. 8).

Ferner ist für das Aufspielen der Updates eine entsprechende Netzabdeckung und Datenübertragungsrate erforderlich.¹⁶⁰⁸ Es überzeugt aber nicht, die Zumutbarkeit bereits aufgrund einer in Deutschland vorherrschenden lückenhaften Netzabdeckung in Zweifel zu ziehen.¹⁶⁰⁹ Bei IoT-Geräten besteht zumindest die Möglichkeit der Verbindung mit dem heimischen WLAN-Netzwerk – die ohnehin regelmäßig Voraussetzung ist, um über den vollen Funktionsumfang des jeweiligen Geräts zu verfügen.¹⁶¹⁰ Bei Produkten, die außerhalb der Reichweite des heimischen Netzwerks genutzt werden, kann die Bereitstellung des Updates mit dem Hinweis erfolgen, sich in einen Bereich ausreichender Netzabdeckung zu begeben.¹⁶¹¹ Ähnliches gilt für smarte Produkte, die nicht mit dem Internet verbunden wer-

1605 *Orthwein/Obst*, CR 2009, 1 (4) lehnen daher jedenfalls im „Nicht-PC-Bereich“ eine Updatepflicht ab; ähnlich, wenn auch zurückhaltender *Chibanguza*, in: Buck-Heeb/Oppermann (Hg.), *Automatisierte Systeme*, S. 407 (418).

1606 *May/Gaden*, InTer 2018, 110 (115); *Reusch*, BB 2019, 904 (905).

1607 Vgl. *Chibanguza*, in: Buck-Heeb/Oppermann (Hg.), *Automatisierte Systeme*, S. 407 (418); speziell für Kfz *Hartmann*, PHi 2017, 42 (47 ff.); *Geber*, NZV 2021, 14 (17 f.); *Schrader*, DAR 2018, 314 (317); *Xylander*, Die Verantwortlichkeit des Herstellers automatisierter PKW, S. 174 f.

1608 *Hartmann*, PHi 2017, 42 (45).

1609 So aber *May/Gaden*, InTer 2018, 110 (113).

1610 *Grünvogel/Dörrenbächer*, ZVertriebsR 2019, 87 (90).

1611 I.E. auch *Fida*, Updates, Patches & Co, S. 167.

den können, aber über eine andere Schnittstelle wie z.B. USB verfügen.¹⁶¹² Ein Update kann dann auf diesem Wege eingespielt werden.

Betrachtet man dann den anfallenden finanziellen Aufwand im Falle einer Kostentragungspflicht des Herstellers, lässt sich auch aus diesem regelmäßig nicht die Unzumutbarkeit der Updateverpflichtung folgern. Zum einen lässt sich der Aufwand über den Produktpreis auf die Nutzer abwälzen.¹⁶¹³ Da Softwarefehler eine gewisse Regelmäßigkeit aufweisen, dürften die über die Zeit anfallenden Updatekosten auch leichter zu kalkulieren sein als herkömmliche Reparaturkosten, die immer ein außerplanmäßiges Ereignis darstellen. Ferner ist zu berücksichtigen, dass ein Update nur einmal entwickelt werden muss, aber allen betroffenen Produkten und Nutzern zugutekommt. Die Entwicklungskosten des Updates verteilen sich daher auf alle betroffenen Installationen, für die Updates geschuldet sind. Erst anhand der so ermittelten Kosten ist zu beurteilen, ob diese im Hinblick auf den damit insgesamt erzielten Sicherheitsgewinn aller Nutzer für den Hersteller unzumutbar sind.¹⁶¹⁴ Zum anderen muss der Hersteller für den Zeitraum der weiteren Vermarktung des Produkts ohnehin Ressourcen bereithalten, um Updates zu entwickeln, sodass eine Updateverpflichtung eher zumutbar ist.¹⁶¹⁵ Die Frage der Zumutbarkeit stellt sich damit erst, wenn der Hersteller nicht mehr ohnehin aufgrund anderer Pflichten entsprechende Updates entwickeln muss.¹⁶¹⁶ Sie kann dann nur im jeweiligen Einzelfall beantwortet werden. Die Zumutbarkeitsgrenze könnte aber bei zugekaufter und verbauter Fremdsoftware, die nicht-standardisiert ist, erreicht sein,

1612 Eine angemessene Komplexität des Updatemechanismus stellt bereits eine anfängliche Produktanforderung dar, vgl. ausführlich *Brenner et al.*, RDt 2024, 252 (254 ff.).

1613 *Thöne*, Autonome Systeme, S. 216 f.; krit. aber Arbeitsgruppe „Digitaler Neustart“, Bericht vom 15. April 2019, S. 198, welche gerade aufgrund dieser Überwälzung der Kosten und der damit verbundenen entgegenstehenden wirtschaftlichen Interessen der Beteiligten einer kostenlosen Updatepflicht skeptisch gegenübersteht.

1614 So zum Einwand der Unverhältnismäßigkeit im Vertragsrecht *Riehm/Leithäuser/Brenner*, in: *Raue* (Hg.), *Digitale Resilienz*, S. 5 (26).

1615 Vgl. erneut *Lüftenegger*, RDt 2021, 293 (298 f.); *Wagner*, AcP 217 (2017), 707 (756); *Grünvogel/Dörrenbächer*, ZVertriebsR 2019, 87 (89); *Hinze*, Haftungsrisiken des automatisierten und autonomen Fahrens, S. 162 f.; *Eichelberger*, in: *Ebers et al.* (Hg.), *Künstliche Intelligenz und Robotik*, S. 189; *Wittig*, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 238.

1616 Schon herkömmlich zum Problem bei der Auslistung von Produkten *Klindt*, BB 2009, 792 (795); *Wittig*, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 238; *Wagner*, AcP 217 (2017), 707 (757); *Grünvogel/Dörrenbächer*, ZVertriebsR 2019, 87 (89).

sofern der Hersteller über keine eigene Softwareabteilung verfügt und die Programmierung eines Updates für ihn daher einen erheblichen Aufwand bedeutet.¹⁶¹⁷ Trifft den Hersteller indes im Rahmen des „Unbundlings“ die Verantwortung für die Produktbeobachtung,¹⁶¹⁸ hat er sicherzustellen, dass er seinen sich daraus ergebenden Pflichten auch nachkommen kann. Er kann sich aufgrund fehlender eigener Fachkompetenzen oder Ressourcen daher nicht pauschal auf die Unzumutbarkeit berufen, sondern hat über vertragliche Abreden sicherzustellen, dass sein Zulieferer die entsprechenden Updates bereitstellt.¹⁶¹⁹

Nicht vernachlässigt werden darf indes, dass Softwareupdates zunächst entwickelt und getestet werden müssen.¹⁶²⁰ Die Herausforderung besteht gerade darin, dass sich Fehlfunktionen regelmäßig erst bei der Anwendung durch den Nutzer zeigen und Updates daher nicht auf „Vorrat“ entwickelt werden können.¹⁶²¹ Indes muss auch bei einer klassischen Reparatur zunächst ein konstruktiver Lösungsweg gefunden werden und Ersatzteile ggf. erst entwickelt und getestet werden.¹⁶²² Ist dem Hersteller eine umgehende Bereitstellung des Updates nicht möglich, obliegt es ihm als Minus, den Nutzer zu warnen und ihm einen Zeitplan für die Entwicklung und Bereitstellung des Updates zu präsentieren.¹⁶²³ Hinzu kommt, dass sich hier gerade die Stärke smarter Reaktionsmöglichkeiten zeigt. Denn vernetzte Maßnahmen ermöglichen angesichts zahlreicher Ausgestaltungsmöglichkeiten sowohl ein differenziertes Vorgehen als auch die Verschmelzung von Maßnahmen. So kann ein Produkt auch, um jegliche Gefährdung auszuschließen, ferngesteuert so lange deaktiviert werden, bis ein Update zur Verfügung steht.¹⁶²⁴

1617 So Piovano/Schucht/Wiebe, Produktbeobachtung in der Digitalisierung, S. 99.

1618 Vgl. oben C.III.3.

1619 Vgl. Piovano/Schucht/Wiebe, Produktbeobachtung in der Digitalisierung, S. 100; Dötsch, Außervertragliche Haftung für KI, S. 263; allgemein Huber, Rechtsfragen des Produktrückrufs, S. 275 f.

1620 Hey, Die außervertragliche Haftung des Herstellers autonomer Fahrzeuge, S. 95; Gomille, JZ 2016, 76 (81).

1621 Hartmann, PHi 2017, 42 (45 f.); vgl. auch Thöne, Autonome Systeme, S. 215.

1622 So schon Klindt, BB 2009, 792 (795) und Handorn, MPR 2009, 37 (41).

1623 Grapentin, Vertragsschluss und vertragliches Verschulden beim Einsatz von KI, S. 180.

1624 Lüftenegger, RDi 2021, 293 (300); Grünvogel/Dörrenbächer, ZVertriebsR 2019, 87 (91); Dötsch, Außervertragliche Haftung für KI, S. 263; Piovano/Schucht/Wiebe, Produktbeobachtung in der Digitalisierung, S. 103; Wittig, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 234.

Im Rahmen der Zumutbarkeit bestehen damit keine grundsätzlichen Bedenken gegen eine Verpflichtung des Herstellers Sicherheitsupdates bereitzustellen. Freilich ist diese Frage stets im Einzelfall zu klären und die dargestellten Gesichtspunkte können im Einzelfall auch zu einem anderen Ergebnis führen. So ist es gerade bei autonomen Systemen, die auf neuronalen Netzen beruhen und nach dem Inverkehrbringen unerwünschte Lernergebnissen entwickeln, schwierig, diese wieder zu beseitigen. Denn das Verhalten neuronaler Netze kann nicht einfach durch Änderung oder Ergänzung des Programmcodes geändert werden, sondern bedarf des Umlernens. Sollte ein solches Umlernen nicht möglich sein, bleibt möglicherweise nur das Löschen oder Neuaufsetzen des gesamten Lernvorgangs.¹⁶²⁵

f) Fazit

Bei der Ausgestaltung der Updatepflicht hat der Hersteller den Stufenbau der Reaktionspflichten zu beachten. Fehlt es an einer entsprechenden Einwilligung, stellt das Bereitstellen eines Updates zur Behebung des Sicherheitsmangels die Grundmaßnahme und das Mittel der Wahl dar, um den Anforderungen des Produkthaftungsrechts zu genügen. Dies bedeutet jedoch keine systemwidrige deliktsrechtliche Ausweitung des Äquivalenzzinteresses, sondern ist Folge der auf den Integritätsschutz ausgerichteten effektiven Gefahrenabwehr. Die Folge dieser regelmäßigen Verpflichtung des Herstellers zur Bereitstellung von Sicherheitsupdates ist eine gewisse Dynamisierung des Zeitpunkts des Inverkehrbringens.¹⁶²⁶ Diese rechtfertigt sich aber durch die gesteigerten Zugriffs- und Einflussmöglichkeiten des Herstellers und der damit einhergehenden Kontrolle über das Produkt auch nach dem Zeitpunkt des Inverkehrbringens bei gleichzeitig abnehmenden Gefahrensteuerungsmöglichkeiten des Nutzers nach diesem Zeitpunkt.¹⁶²⁷

3. Kostentragungspflicht bei Sicherheitsupdates

Fraglich ist sodann, wer im Falle einer Updatepflicht die für die Sicherheitsupdates anfallenden Kosten zu tragen hat. Zwar mag das Aufspielen der

1625 Zum Ganzen Zech, DJT 2020 Gutachten, A S. 72 f.

1626 Wiesemann/Mattheis/Wende, MMR 2020, 139 (140) lehnen eine Updatepflicht des Herstellers daher ab.

1627 I.E. auch Thöne, Autonome Systeme, S. 218.

Software anders als eine klassische Reparatur kaum Kosten verursachen. Dies darf aber nicht darüber hinwegtäuschen, dass die Entwicklung des Updates auch mit Kosten einhergehen kann.¹⁶²⁸ Insbesondere muss der Hersteller dauerhaft Unternehmensressourcen für die kurzfristige Programmierung von Updates bereithalten.¹⁶²⁹ Die Frage der Kostentragungspflicht stellt sich daher nicht weniger dringlich als bei klassischen Produktrückrufen.

Anknüpfend an die Effektivität der Gefahrenabwehr ist zu unterscheiden, ob der Produktnutzer sich über eine Warnung hinwegsetzen wird, weil er die Produktgefahr erkennt oder ihm die Gefahrensteuerung in Form der Nutzungsaufgabe unzumutbar ist. Bei einer falschen Gefahreneinschätzung, insbesondere bei Sicherheitslücken ohne physische Gefahren für den Nutzer, wird die bloße Bereitstellung eines Updates mit der Aufforderung der Kostenübernahme die Nutzer kaum dazu bewegen, ihre Gefahreneinschätzung zu überdenken und die Sicherheitslücke mittels kostenpflichtiger Updates zu schließen. Der Anreiz ist hier deutlich höher, wenn das Update kostenfrei zur Verfügung gestellt wird. Eine im Ausgangspunkt davon unabhängige Frage ist, wie es sich auswirkt, dass Nutzer auch kostenfrei bereitgestellte Sicherheitsupdates häufig nicht installieren.¹⁶³⁰ Hier könnte der Hersteller zu weitergehenden Sicherungspflichten gehalten sein.¹⁶³¹ Wird dagegen die Eintrittswahrscheinlichkeit einer möglichen Rechtsgutsverletzung ausgeblendet, weil der Nutzer auf die Verwendung des Produkts angewiesen ist, gleichzeitig aber die Gefahrenbeseitigung nicht ohne Hilfe des Herstellers leisten kann, stellt die bloße Bereitstellung eines fehlerbehebenden Updates auch ohne Kostenübernahme durch den Hersteller einen erheblichen Mehrwert für den Nutzer dar. Denn dadurch muss er sich bei der Nutzung nicht weiter der vom Produkt ausgehenden Gefahr aussetzen, sondern kann das Sicherheitsdefizit beseitigen, ohne ein Ersatzprodukt anschaffen zu müssen.

Die Bereitstellung von sicherheitsrelevanten Softwareupdates hat folglich nicht zwingend kostenlos zu erfolgen.¹⁶³² Bei CPS wird sich eine Up-

1628 Arbeitsgruppe „Digitaler Neustart“, Bericht vom 15. April 2019, S. 198; Dötsch, Außervertragliche Haftung für KI, S. 262.

1629 Raue, NJW 2017, 1841 (1844).

1630 Vgl. zu den Gründen erneut Vaniea/Rader/Wash, CHI 2014, 2671 (2671 ff.).

1631 Vgl. Wiesemann/Mattheis/Wende, MMR 2020, 139 (141).

1632 So auch Kipker/Walkusz, DuD 2019, 513 (517); Wittig, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 242.

datepflicht sogar regelmäßig auf die Bereitstellung eines kostenpflichtigen Updates beschränken.¹⁶³³

4. Weitere gesetzliche Updatepflichten und deren Bedeutung

Updatepflichten der Hersteller könnten sich auch außerhalb der deliktsrechtlichen Produktbeobachtungspflicht aus weiteren Regelungen ergeben. Zu diesem Zweck sollen im Folgenden das öffentlich-rechtliche Produktsicherheits- und Marktüberwachungsrecht sowie die neue Produkthaftungsrichtlinie untersucht werden und sich daraus ergebende Updatepflichten in Bezug zur Produktbeobachtungspflicht aus § 823 Abs. 1 BGB gesetzt werden.

a) Bedeutung des ProdSG

Eine Pflicht zum Bereitstellen von Updates könnte sich aus § 6 Abs. 2 ProdSG ergeben. Hiernach hat der Hersteller Vorkehrungen für geeignete Maßnahmen zur Vermeidung von Risiken zu treffen, die mit dem Verbraucherprodukt, das sie auf dem Markt bereitgestellt haben, verbunden sein können. Dabei können die Maßnahmen bis zur Rücknahme, zu angemessenen und wirksamen Warnungen und zum Rückruf reichen.

Aufgrund der beispielhaften Nennung von Rücknahme, Rückruf und Warnung als konkret möglichen Gefahrenvermeidungsmaßnahmen könnte sich aus der Norm auch eine eigenständige Pflicht zur Ergreifung der jeweiligen Korrekturmaßnahmen – und in konsequenter Weiterentwicklung auch eine Updatepflicht – ergeben.¹⁶³⁴ Insoweit wird angeführt, dass angesichts des bezweckten Verbraucherschutzes eine reine Vorbereitungsspflicht ohne eine korrespondierende Pflicht zur Durchführung der Maßnahmen leerliefe.¹⁶³⁵ Dem wird allerdings entgegengehalten, dass die Pflicht den

1633 So auch *Lüftenegger*, RDt 2021, 293 (298).

1634 Die ganz herrschende Meinung lehnt ein solches Verständnis und damit eine Pflicht zur Durchführung von Risikovermeidungsmaßnahmen ab, vgl. nur *Schütte*, in: NK-ProdR, § 6 ProdSG, Rn. 41 m.w.N. auch zur gegenteiligen Auffassung.

1635 *Wiebe*, Unternehmerfreiheit versus Verbraucherschutz?!, S. 335 und *Wiebe*, NJW 2019, 625 (628), i.E. aber auch eine Ergreifungspflicht ablehnend. Einen Erstrecht-Schluss lehnt *Schütte*, in: NK-ProdR, § 6 ProdSG, Rn. 41, Fn. 88 mit der Begründung ab, dass ein *argumentum a minore ad maius* bei einem Verpflichtungstatbestand nicht verfängt.

Hersteller im Sinne des Vorsorgegrundsatzes immerhin dazu anhält, sich im Vorfeld schon mit potenziellen Gefahren und Abhilfemaßnahmen auseinanderzusetzen, um dann im Falle der tatsächlichen Ergreifung einer Maßnahme – sei es freiwillig, aufgrund behördlicher Anordnung oder aufgrund sonstiger Pflicht – vorbereitet zu sein. Dies entspricht auch dem Ziel, eine proaktive und präventive Verbraucherschutzpolitik in der Unternehmenskultur zu verankern.¹⁶³⁶ Eine darüberhinausgehende Pflicht, diese Maßnahmen auch aktiv zu ergreifen, besteht trotz der beispielhaften Auflistung einzelner Maßnahmen nicht. Vielmehr ist die Nennung als Merkposten für freiwillige Eigenmaßnahmen zu verstehen und soll die Ausgestaltung des Risikomanagementsystems verdeutlichen.¹⁶³⁷ Für dieses Ergebnis spricht auch der eindeutige Wortlaut, welcher gerade nur von „Vorkehrungen für geeignete Maßnahmen“ spricht.¹⁶³⁸ Zuletzt sieht Art. 5 Abs. 1 UAbs. 3 lit. b, UAbs. 5 der RL 2001/95/EG ausdrücklich vor, dass ein aktives Tätigwerden zur Gefahrenvermeidung allein freiwillig oder behördlich angeordnet erfolgt.¹⁶³⁹ Folglich handelt es sich lediglich um eine Organisationspflicht, zur Vorbereitung einer angemessenen Gefahrenabwehr,¹⁶⁴⁰ aus der keine Updatepflicht abgeleitet werden kann.

Auch aus § 6 Abs. 3 ProdSG lässt sich keine Updatepflicht folgern. Denn es werden lediglich Maßnahmen aufgelistet, die der Produktbeobachtungspflicht i.e.S. zugeordnet sind und der Gefahrerkennung dienen. Reaktionsmaßnahmen zur Gefahrenabwehr aufgrund von Erkenntnissen aus dieser Beobachtung sucht man dagegen vergeblich. Aufgrund der ratio legis dieser Norm lassen sich auch keine nachgeschalteten Maßnahmen zur Abwehr

1636 Hierzu *Klindt*, NJW 2004, 465 (468); *Kapoor*, in: *Klindt*, ProdSG, § 6, Rn. 50, 52.

1637 So *Wiebe*, NJW 2019, 625 (628), der zumindest einen „rechtliche[n] Appell zur Ergreifung unternehmereigener Schritte“ sieht.

1638 *Schütte*, in: NK-ProdR, § 6 ProdSG, Rn. 41; *Kapoor*, in: *Klindt*, ProdSG, § 6, Rn. 48; *Klindt*, NJW 2004, 465 (468).

1639 Art. 5 Abs. 1 UAbs. 5 der RL 2001/95/EG nimmt auf Maßnahmen (die Terminologie wurde hier dem § 6 Abs. 2 ProdSG angepasst, da insoweit eine Divergenz zu Art. 5 Abs. 1 UAbs. 3 besteht) wie den Rückruf in UAbs. 3 lit. b Bezug, vgl. auch *Wiebe*, NJW 2019, 625 (630).

1640 *Wilrich*, ProdSG, Rn. 439 ff.; *Becker/Ottinger*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 62, Rn. 67; ähnlich auch *Wagner*, in: Eifert (Hg.), Produktbeobachtung durch Private, S. 115 (144): „[D]azu verpflichtet, sich für einen möglicherweise notwendig werdenden Produktrückruf bereitzuhalten und sich entsprechend vorzubereiten, insbesondere durch Aufbau eines Rückrufmanagementsystems“ und *Wagner*, VersR 2014, 905 (915).

einer konkreten Produktgefahr hineinlesen.¹⁶⁴¹ Denn die öffentlich-rechtliche Produktbeobachtungspflicht setzt vor der Entstehung der Gefahr an und dient der Risikoerkennung im Feld. Dieses Verständnis entspricht auch dem im ProdSG allgemein verwendeten Konzept eines „appellativen Verbraucherschutts in jedweder kategorischen Ausprägung.“¹⁶⁴²

Die Kombination der Pflicht zur Produktbeobachtung i.e.S. nach § 6 Abs. 3 ProdSG mit der Pflicht zur Einrichtung eines Risikomanagementsystems nach § 6 Abs. 2 ProdSG soll also lediglich ermöglichen, Gefahren zu erkennen und in einer Produktkrise angemessen zu reagieren. Weder das „Ob“ der Reaktion noch das „Wie“ der Reaktion sind jedoch gesetzlich vorgeschrieben.

b) Künftige Bedeutung der GPSR

Die GPSR sieht dagegen eine gesetzliche Verpflichtung zum Ergreifen von Gefahrabwendungsmaßnahmen vor. Nach Art. 9 Abs. 8 UAbs. 1 lit. a GPSR sind die Hersteller verpflichtet, unverzüglich die erforderlichen Korrekturmaßnahmen zur Herstellung der Produktkonformität – wozu ggf. auch ein Rückruf gehören kann – zu ergreifen, wenn sie der Auffassung sind oder Grund zur Annahme besteht, dass ein von ihnen in Verkehr gebrachtes Produkt gefährlich ist.¹⁶⁴³ Außerdem ist in Art. 37 Abs. 1 GPSR geregelt, dass der Hersteller bei einem Rückruf dem Verbraucher eine wirksame, kostenfreie und zeitnahe Abhilfemaßnahme anbieten muss. Als mögliche Abhilfemaßnahme sieht Abs. 2 eine Reparatur, eine Ersatzlieferung des zurückgerufenen Produkts durch ein sicheres Produkt desselben Typs mit mindestens demselben Wert und derselben Qualität oder die Rückerstattung des Wertes vor. Dabei soll der Verbraucher grundsätzlich die Wahl zwischen mindestens zwei der Maßnahmen haben. Hinsichtlich Software wird nach Abs. 3 die zur Verfügungstellung von Softwareaktualisierungen im Rahmen der Reparatur als ausreichend erachtet.

1641 Vgl. zum Ganzen *Wiebe*, NJW 2019, 625 (627); auch *Kapoor*, in: *Klindt*, ProdSG, § 6, Rn. 57.

1642 *Klindt*, in: *Eifert* (Hg.), *Produktbeobachtung durch Private*, S. 55 (57); vgl. auch *Becker/Ottinger*, in: *Foerste/Graf v. Westphalen* (Hg.), *Produkthaftungsbandbuch*, § 62, Rn. 69.

1643 Dies entspricht bereits jetzt der – für smarte Produkte regelmäßig einschlägigen – Regelung nach § 9 Abs. 5 S. 1, 2 Funkanlagengesetz.

aa) Das neue Recht auf Abhilfe nach Art. 37 GPSR

Näherer Betrachtung bedarf nun die Frage, welchen Einfluss das neue Recht auf Abhilfe auf die Maßnahmen zur Gefahrenabwehr des Herstellers haben wird. Das Recht auf Abhilfe besteht schon dem Wortlaut nach nur „im Falle eines Produktsicherheitsrückrufs“. Die Zulässigkeit und Ausgestaltung milderer Gefahrenabwehrmaßnahmen, wie z.B. der Warnung, bleiben hiervon folglich unberührt.¹⁶⁴⁴ Dies wird auch systematisch dadurch bestätigt, dass Art. 9 Abs. 8 UAbs. 1 lit. a GPSR vom Hersteller lediglich verlangt, die „erforderlichen“ Korrekturmaßnahmen zu ergreifen, zu denen „gegebenenfalls“ auch ein Rückruf gehören kann (und man mag hineinlesen „aber nicht gehören muss“). Auf die Bestimmung der Erforderlichkeit der jeweiligen Gefahrenabwehrmaßnahme hat das Recht auf Abhilfe damit keine Auswirkung.¹⁶⁴⁵ Einfluss hat das Recht auf Abhilfe dagegen auf die konkrete Ausgestaltung des Rückrufs. Denn nach der Maxime der Effektivität der Gefahrenabwehr reicht es zur Erfüllung der zivilrechtlichen Produktbeobachtungspflicht aus, dass die Rückrufmaßnahme die Produktgefahr ergebnisorientiert beseitigt. Mit dem Grundsatz der Effektivität der Gefahrenabwehr kann indes nicht mehr begründet werden, dass dem Verbraucher stets (!) und einzelfallunabhängig (!) das ursprünglich erworbene Produkt kostenfrei (!) erneuert oder ersetzt werden muss.¹⁶⁴⁶ Es ist daher nicht verwunderlich, dass die Abhilfemaßnahmen gemäß Erwägungsgrund (88) GPSR nicht nur dazu dienen sollen, den Verbraucher zu veranlassen, auf Rückrufe zu reagieren, sondern – eigentlich systemwidrig im primär auf Gefahrenabwehr angelegten öffentlich-rechtlichen Produktsicherheitsrecht¹⁶⁴⁷ – auch dazu, ihm eine angemessene Wiedergutmachung zu gewähren.

Art. 37 GPSR sieht damit zwar keine explizite Pflicht des Herstellers zu Sicherheitsupdates vor, sondern regelt die Bereitstellung von Updates nur als eine mögliche Option der Abhilfe. Die Interessenlage sowohl des Herstellers als auch des Verbrauchers dürfte jedoch in der Praxis im Vergleich zu den anderen Möglichkeiten der Abhilfe, nämlich des Austausches des Produkts und des Wertersatzes, regelmäßig diese Maßnahme nahelegen.

1644 So auch *Ackermann/Golling*, ZfPC 2022, 67 (71); *Thöne*, ZfPC 2024, 49 (52), wonach keine Verhaltenspflicht aufgestellt wird, sondern die Rechtsfolgende adressiert wird.

1645 Dies verkennt *Reusch*, RDt 2023, 152 (156), der eine diametrale Abkehr von den Grundsätzen der Pflegebetten-Entscheidung ausmachen will.

1646 So auch *Ackermann/Golling*, ZfPC 2022, 67 (71).

1647 Sehr krit. daher *Hartmann/Klindt*, ZfPC 2022, 73 (76); *Niermeier*, NJW 2024, 1463 (1466).

bb) Bedeutung für die zivilrechtliche Produktbeobachtungspflicht

Da sich nach hiesigem Verständnis die Bereitstellung von Sicherheitsupdates ohnehin regelmäßig als deliktsrechtlich geschuldete Gefahrenabwehrmaßnahme darstellt, führt das Recht auf Abhilfe insoweit nicht zu Erweiterung der Herstellerpflichten. Ist der Hersteller im Einzelfall aus Gründen der Effektivität der Gefahrenabwehr verpflichtet und berechtigt eine Fernstilllegung des Produkts vorzunehmen, hat er künftig nach der GPSR den Nutzer zu entschädigen. Auch hinsichtlich Sicherheitsupdates ist zu beachten, dass diese nach der GPSR zwingend für den Verbraucher kostenfrei zu erfolgen haben. Zwar mag ein Hersteller im Rahmen seiner zivilrechtlichen Produktbeobachtungspflicht nicht verpflichtet sein, seine Rückrufmaßnahme entsprechend Art. 37 GPSR auszugestalten, sondern hat sie nur an der Effektivität der Gefahrenabwehr zu orientieren. Allerdings wird er dies mit Blick auf das Sanktionsrisiko (vgl. Art. 44 GPSR)¹⁶⁴⁸ zur Erfüllung seiner öffentlich-rechtlichen Pflicht gleichwohl tun.¹⁶⁴⁹

Hinzu kommt, dass einer Verletzung des Rechts auf Abhilfe unter dem Gesichtspunkt der Schutzgesetzverletzung auch einen Schadensersatzanspruch nach § 823 Abs. 2 BGB bedeuten könnte. Dann müsste es sich bei Art. 37 GPSR um ein Schutzgesetz handeln. Entscheidend ist dabei, dass die verletzte Einzelnorm – nicht das Gesetzeswerk, dessen Teil sie ist –¹⁶⁵⁰ zumindest auch dazu dienen soll, den Einzelnen gegen die Verletzung eines bestimmten Rechtsguts zu schützen. Dabei genügt es, dass die Norm auch das Interesse des Einzelnen schützen soll, mag sie auch in erster Linie dasjenige der Allgemeinheit im Auge haben. Nicht ausreichend ist aber, dass der Individualschutz durch Befolgung der Norm nur als ihr Reflex objektiv erreicht wird; er muss vielmehr im Aufgabenbereich der Norm liegen. Ein gesetzliches Gebot oder Verbot ist als Schutzgesetz nur geeignet, soweit das geschützte Interesse, die Art seiner Verletzung und der Kreis der geschützten Personen hinreichend klargestellt und bestimmt sind. Außerdem muss die Schaffung eines individuellen Schadensersatzanspruchs sinnvoll und im Lichte des haftungsrechtlichen Gesamtsystems tragbar erscheinen, wobei in umfassender Würdigung des gesamten Regelungszusammenhangs, in den

1648 Die konkrete Einführung von Sanktionsbestimmungen fällt in die Zuständigkeit der Mitgliedstaaten. Die genaue Ausgestaltung der Sanktionsbestimmungen durch die jeweiligen Mitgliedstaaten bleibt daher abzuwarten.

1649 Ein immer stärkeres Durchschlagen des öffentlich-rechtlichen Produktsicherheitsrechts prophezeit auch Lenz, in: Lenz, Produkthaftung, § 3, Rn. 231.

1650 Vgl. nur Wagner, VersR 2014, 905 (909).

die Norm gestellt ist, zu prüfen ist, ob es in der Tendenz des Gesetzgebers liegen konnte, an die Verletzung des geschützten Interesses die deliktische Einstandspflicht des dagegen Verstößenden mit allen damit zugunsten des Geschädigten gegebenen Haftungs- und Beweiserleichterungen zu knüpfen. Ein Schadensersatzanspruch aus § 823 Abs. 2 BGB setzt schließlich weiter voraus, dass sich im konkreten Schaden die Gefahr verwirklicht hat, vor der die betreffende Norm schützen sollte und der konkret Geschädigte vom persönlichen Schutzbereich der verletzten Norm erfasst ist.¹⁶⁵¹

Entstammt die Norm – wie im Falle des Art. 37 GPSR – dem Europarecht, ist neben dieser zweistufigen Prüfung nach dem Individualschutzzweck und der Tragbarkeit im haftungsrechtlichen Gesamtsystem aber auch insbesondere das Effektivitätsprinzip (*effet utile*) zu beachten. Danach muss für die Verletzung einer gemeinschaftsrechtlichen Rechtsnorm hinreichend abschreckende haftungsrechtliche Bewehrung vorgesehen sein, wenn nur auf diese Weise die praktische Wirksamkeit der Norm sichergestellt werden kann.¹⁶⁵²

In einer ersten Rechtsprechungsphase des EuGH¹⁶⁵³ konnte davon ausgegangen werden, dass nach dem Effektivitätsprinzip Verstöße gegen Unionsrecht stets Ersatzansprüche derjenigen auslösen müssen, die infolge eines solchen Verstößes einen Schaden erlitten haben.¹⁶⁵⁴ Dagegen ließ die zweite Rechtsprechungsphase¹⁶⁵⁵ Zurückhaltung bei der haftungsrechtlichen Bewehrung des Unionsrechts erkennen und mahnte an, dass selbst der Individualschutzzweck einer verletzten Verhaltensnorm nicht ohne Weiteres ausreicht, um eine Haftung auszulösen.¹⁶⁵⁶ Vielmehr schien es darauf anzukommen, ob in dem jeweiligen europäischen Rechtsakt selbst ein Schadensersatzanspruch anlegt ist oder ob es bei einer verwaltungsrechtlichen Durchsetzung und Sanktionierung sein Bewenden haben kann.¹⁶⁵⁷ Nunmehr stellt der EuGH¹⁶⁵⁸ dagegen Schutzweckerwägungen gerade in den Vordergrund, ohne dass vorhandene behördliche Durchsetzungsregime

1651 Insgesamt stehende Formulierung und ständige Rspr., vgl. nur BGH, NJW 2019, 3003 (3005).

1652 Dazu *Wagner*, in: MüKo, BGB, § 823, Rn. 627; *Riehm*, in: Langenbucher (Hg.), Europäisches Privat- und Wirtschaftsrecht § 3, Rn. 44.

1653 Vgl. EuGH, NJW 1984, 2021 (2022); EuGH, EuZW 2001, 715 (716); EuGH, BeckRS 2004, 75459.

1654 So *Wagner*, AcP 206 (2006), 352 (413 ff.).

1655 EuGH, EuZW 2013, 557; EuGH, NJW 2017, 1161 (1163).

1656 Dazu *Wagner*, in: MüKo, BGB, § 823, Rn. 630.

1657 Dazu *Wagner*, NJW 2023, 1761 (1763).

1658 EuGH, NJW 2023, 1111 (1114).

hieran etwas ändern könnten.¹⁶⁵⁹ Kohärente Kriterien für die Annahme subjektiver Rechte Privater auf Schadensersatz bei Verstößen gegen Unionsrecht konnten sich damit nicht ausbilden, sodass die entsprechenden Voraussetzungen weiterhin unklar bleiben.

Betrachtet man nur Art. 37 GPSR, so regelt dieser zwar nicht, unter welchen Voraussetzungen ein Produkt zurückzurufen ist, sondern die sich an einen Rückruf anschließenden Maßnahmen. Damit regelt die Norm zwar die Rechtsfolgen des Rückrufs, es wäre aber zu kurz gegriffen, hieraus bereits auf das Fehlen einer Verhaltenspflicht zu schließen und damit mangels entsprechenden Ge- oder Verbotscharakter der Norm eine Schutzgesetzeigenschaft zu verneinen.¹⁶⁶⁰ Eine entsprechende Verhaltenspflicht begründet nämlich auch die Rechtsfolge des Rückrufs, nämlich das Angebot von Abhilfemaßnahmen. Das Recht des Verbrauchers, Abhilfemaßnahmen zu verlangen, korrespondiert mit der Pflicht des Herstellers, solche Maßnahmen anzubieten. Daneben dienen Abhilfemaßnahmen im Falle eines Rückrufs ausweislich des Erwägungsgrunds (88) GPSR dazu, gefährliche Produkte vom Markt zu nehmen. Nach Art. 3 Nr. 3 i.V.m. Nr. 2 GPSR liegt ein gefährliches Produkt vor, wenn die von ihm ausgehenden Risiken nicht mit einem hohen Schutzniveau für die Gesundheit und Sicherheit der Verbraucher vereinbar sind. Insofern sind Abhilfemaßnahmen mit ihrer Anreizwirkung im Rahmen eines durchzuführenden Rückrufs unmittelbar auf den Schutz der Rechtsgüter Leib und Leben des durch das gefährliche Produkt bedrohten Verbrauchers gerichtet. Da die Abhilfemaßnahmen aber auch der Wiedergutmachung dienen, hat die Vorschrift auch einen Schutzzweck im Hinblick auf die Vermögensinteressen des Verbrauchers. Der dem Verbraucher zugute kommende Individualschutz ist damit von der Norm intendiert und geht über einen bloßen Reflex hinaus. Ein individueller Schadensersatzanspruch erscheint außerdem im Lichte des haftungsrechtlichen Gesamtsystems tragbar. Kommt im Falle eines Rückrufs der Hersteller einem Abhilfeverlangen des Verbrauchers nicht nach, unterminiert dies die mit den Abhilfemaßnahmen verbundene Anreizwirkung, sich an einem Rückruf zu beteiligen und verwehrt dem Verbraucher seine nach der Vorschrift zustehende Wiedergutmachung. Führt ein vom Hersteller ohne Abhilfemaßnahmen durchgeführter Rückruf – man denke an eine Zwangsdeaktivierung – zu einem Schaden bei dem Verbraucher oder beteiligt sich der Verbraucher mangels Anreizes durch entsprechende Abhilfemaßnahmen nicht an einem

1659 Dazu *Wagner*, NJW 2023, 1761 (1766).

1660 So aber *Thöne*, ZfPC 2024, 49 (52).

Rückruf und verletzt das Produkt seine Rechtsgüter, ist dem Einzelnen die Befugnis einzuräumen, den Geltungsanspruch der Norm im Zivilrechtsweg über einen Schadenersatzanspruch selbst durchzusetzen.¹⁶⁶¹ Ob dagegen die nach Art 44 GPSR vorgesehen Sanktionen hinreichend effektiv sind, um auf private Schadenersatzansprüche verzichten zu können, muss deren nationale Ausgestaltung zeigen.

Damit ist Art. 37 GPSR schon nach nationaler Auslegung als Schutzgesetz zu qualifizieren mit der Folge, dass ein nicht entsprechend Art. 37 GPSR ausgestalteter Rückruf im Falle des Eintritts eines Schadens ein erhebliches Haftungsrisiko für den Hersteller begründet. Ob eine entsprechende Einordnung darüber hinaus auch europarechtlich vor dem Hintergrund des Effektivitätsprinzips geboten ist, erscheint fraglich. Denn nach Erwägungsgrund (88) GPSR soll jegliche Abhilfe das Recht des Verbrauchers auf Schadenersatz nach nationalem Recht unberührt lassen. Insoweit normiert auch Art. 43 GPSR, dass die Entscheidung über einen Rückruf nicht die Bewertung über die Haftung nach nationalem Recht berührt.¹⁶⁶²

c) Bedeutung des Marktüberwachungsrechts

Kapitel V der MÜ-VO legt Befugnisse und Maßnahmen der Marktüberwachungsbehörden fest. Dabei regelt Art. 16 Abs. 1 MÜ-VO (i.V.m. § 8 Abs. 2 MüG) den Grundsatz des Tätigwerdens der Marktüberwachungsbehörden, wonach diese insbesondere dann geeignete Maßnahmen zu ergreifen haben, wenn ein Produkt die Gesundheit oder Sicherheit der Nutzer gefährden kann (lit. a). Es stellt sich daher die Frage, ob die Marktüberwachungsbehörde in diesem Fall ein Software-Sicherheitsupdate anordnen darf.

aa) Grundlagen der Marktüberwachung

Eine wirksame Marktüberwachung mit der Möglichkeit erforderliche Marktkorrekturen vorzunehmen, stellt einen Ausgleich für die liberalen und von wenig Regulierung geprägten Marktzugangsregelungen dar.¹⁶⁶³ Im öffentlichen Produktsicherheitsrecht entscheidet der Hersteller nämlich

1661 Zu dieser Formulierung BGH, NJW 1987, 1818 (1819).

1662 Vgl. auch Thöne, ZfPC 2024, 49 (52).

1663 Schucht, BB 2015, 654 (655).

grundsätzlich¹⁶⁶⁴ selbständig darüber, ob er seine Produkte als konform und damit als sicher betrachten kann und diese dann auf dem Markt bereitstellt. Um zu gewährleisten, dass sein Produkt im Anwendungsbereich einer speziellen Harmonisierungsvorschrift den dortigen Anforderungen entspricht, hat der Hersteller dies in einem Konformitätsbewertungsverfahren eigenverantwortlich zu überprüfen und nachzuweisen. Hierbei muss in Abhängigkeit des vom Produkt ausgehenden Risikos eine benannte Stelle hinzugezogen werden. Die Konformität des Produkts wird anschließend durch eine eigens ausgestellte Konformitätserklärung und das Anbringen der CE-Kennzeichnung als Eigenerklärung bestätigt.¹⁶⁶⁵ Auf ein staatliches Produktzulassungsverfahren wird dagegen verzichtet. Der Staat gibt folglich eigene Steuerungsmöglichkeiten hinsichtlich einer konkreten Gefahrenquelle auf und nimmt im Gegenzug einen privaten Wirtschaftsakteur in die Verantwortung.¹⁶⁶⁶

Die nachmarktliche öffentlich-rechtliche Produktbeobachtung ist dann gekennzeichnet durch ein Zusammenwirken der Produktverantwortlichen und der Verwaltung.¹⁶⁶⁷ Wurde die Produktbeobachtung aus Gründen der Effektivität insbesondere dem Hersteller aufgegeben, ruft die behördliche Notifikation (§ 6 Abs. 4 S. 1 ProdSG) im Falle eines möglichen Produkt-risikos im Feld die Marktüberwachungsbehörden wieder auf den Plan. Dieses präventive behördliche Vorgehen zur Gefahrenabwehr kann als Überwindung der Systemgrenze des Zivilrechtes angesehen werden.¹⁶⁶⁸ Denn auch wenn durch das Haftungsrecht präventive Anreize zur Gefahrenvermeidung geschaffen werden, ist als Rechtsfolge für den Verstoß gegen die Produktbeobachtungspflicht (genauer: die Reaktionspflicht) eine Schadensersatzpflicht vorgesehen. Klassischerweise setzt das Haftungsrecht damit kompensatorisch erst nach Eintritt eines Schadens an. Damit bleibt es dem Hersteller überlassen, zur Minimierung seines Schadensrisikos Maßnahmen zu ergreifen.¹⁶⁶⁹ Hinzu kommt, dass die zivilrechtlichen Ansprüche lediglich inter partes bestehen und damit nicht dazu führen können,

1664 Ausnahmen bilden hier bspw. die Erlaubnispflichtigkeit der Herstellung und des Inverkehrbringens von Arzneimitteln (§§ 13 ff., 21 AMG) oder die Genehmigungspflichtigkeit bei Kraftfahrzeugen (§§ 19 ff. StVZO).

1665 Vgl. hierzu *Krey/Kapoor*, Praxisleitfaden Produktsicherheitsrecht, S. 185 f.

1666 Vgl. *Klindt/Piovano*, NVwZ 2021, 1016 (1019).

1667 So auch *Schmidt am Busch*, in: Eifert (Hg.), Produktbeobachtung durch Private, S. 149 (150).

1668 *Oechsler*, in: Staudinger, BGB, § 3 ProdHaftG, Rn. 8.

1669 Vgl. *Appel*, in: Eifert (Hg.), Produktbeobachtung durch Private, S. 27 (30).

dass die Produktsicherheit auf dem Markt im Hinblick auf die übrigen gleichermaßen unsicheren Produkte insgesamt wiederhergestellt wird.¹⁶⁷⁰ Für den Fall also, dass der Hersteller trotz der drohenden deliktischen Haftung seinen Reaktionspflichten nicht nachkommt, entspricht es der staatlichen Letztverantwortungs- und Gewährleistungsfunktion, in Wahrnehmung der grundrechtlichen Schutzpflichten nach Art. 2 Abs. 2 S. 1 GG einzugreifen und Schäden präventiv zu verhindern.¹⁶⁷¹ Gerade an der Notifikationspflicht als Bindeglied zwischen gebotener privater Produktbeobachtung und staatlichen Marktüberwachungsmaßnahmen zeigt sich der im Produktsicherheitsrecht besonders ausgeprägte Kooperationsgrundsatz.¹⁶⁷² Durch diesen soll nicht nur eine wirksame Marktüberwachung sichergestellt werden, sondern auch ein angemessener Ausgleich zwischen der staatlichen Schutzpflicht und den Unternehmensinteressen hergestellt werden.¹⁶⁷³

bb) Anordnungsbefugnis bzgl. Updates

Eine ausdrückliche Anordnungsbefugnis für Updates hat in den Kanon der Korrekturmaßnahmen nach Art. 16 Abs. 3 MÜ-VO keinen Eingang gefunden. Allerdings kann die Behörde nach Art. 16 Abs. 3 lit. a MÜ-VO den Hersteller auffordern, die Konformität des Produkts herzustellen, damit von ihm kein Risiko mehr ausgeht.¹⁶⁷⁴ Konkrete Vorgaben zur Erreichung

1670 Oechler, in: Staudinger, BGB, § 3 ProdHaftG, Rn. 8.

1671 Klindt/Piovano, NVwZ 2021, 1016 (1019); allgemein zum Spannungsfeld aus der Übertragung der Produktbeobachtung an Private zwischen Effektivität und Wahrung der Gemeinwohlbelange Appel, in: Eifert (Hg.), Produktbeobachtung durch Private, S. 27 (passim).

1672 Vgl. Erwägungsgrund (21) der RL 2001/95/EG: „Sowohl die Hersteller als auch die Händler sollten mit den zuständigen Behörden im Rahmen von Maßnahmen zur Abwendung von Gefahren zusammenwirken und diese unterrichten, wenn sie zu dem Schluss kommen, dass bestimmte gelieferte Produkte gefährlich sind.“ Ebenso Erwägungsgrund (18) MÜ-VO: „Eine gute Zusammenarbeit zwischen den Herstellern und den Marktüberwachungsbehörden ist ein wichtiger Faktor, der ein unverzügliches Eingreifen und Korrekturmaßnahmen im Zusammenhang mit dem Produkt ermöglicht“; ausführlich hierzu Schucht, BB 2015, 654.

1673 Schmidt am Busch, in: Eifert (Hg.), Produktbeobachtung durch Private, S. 149 (150 f.).

1674 Es erschließt sich nicht, warum die Korrekturmaßnahme für Fälle, in denen von dem Produkt eine Gefahr für die Gesundheit und Sicherheit ausgeht, nicht greifen soll, so aber Giesberts/Gayger, in: NK-ProdR, Art. 16 MÜ-VO, Rn. 33. Denn Nichtkonformität, also eine Nichteinhaltung der Anforderungen gemäß den

dieses Ziels sieht der Wortlaut der Norm allerdings nicht vor. Die Standardmaßnahme ist daher als Merkposten für die Behörde zu verstehen, aus Gründen der Verhältnismäßigkeit in geeigneten Fällen dem Wirtschaftsakteur die Wahl der konkreten Maßnahme zu überlassen. Dem Hersteller bleibt demnach ein denkbar weiter Spielraum bei der Umsetzung der Aufforderung.¹⁶⁷⁵ Gerade das Bereitstellen eines Sicherheitsupdates stellt damit lediglich eine Möglichkeit dar, die der Hersteller eigenverantwortlich in Betracht ziehen und ergreifen kann.

Allerdings hat die Behörde nach Art. 16 Abs. 3 lit. c MÜ-VO die Befugnis, einen Rückruf des Produkts anzuordnen. Ausgehend von der Legaldefinition aus Art. 3 Nr. 22 MÜ-VO ist ein Rückruf jede Maßnahme, die auf die Erwirkung der Rückgabe eines dem Endnutzer bereits bereitgestellten Produkts abzielt. Der originäre Zweck des Rückrufs liegt damit in der Rückführung des Produkts an den Hersteller, um so die von ihm ausgehende Gefahr zu beseitigen.¹⁶⁷⁶ Das Ziel der Maßnahme ist demnach darauf gerichtet, das Produkt aus dem Verkehr zu ziehen.¹⁶⁷⁷ Da der Rückruf damit keinem Selbstzweck, sondern gerade der Gefahrenabwehr dient, kann die Behörde in Parallele der Rückführung des Produkts an den Hersteller auch die Fernstilllegung des Produkts anordnen, auch wenn dadurch das Produkt nicht physisch zurück zum Hersteller gelangt.

Möglicherweise lässt sich aber aus der Anordnungsbefugnis zum Rückruf auch eine Befugnis zur Anordnung von Sicherheitsupdates ableiten. Dem Wortlaut nach kann im Ausgangspunkt „jede Maßnahme“ angeordnet werden kann, die der Rückgabe des Produkts dient.¹⁶⁷⁸ Auch beim Austausch oder der Nachrüstung gelangt das gefährliche Produkt zurück

Harmonisierungsvorschriften (vgl. Art. 3 Nr. 7 MÜ-VO), kann ohne Weiteres auch Gefahren für Gesundheit und Sicherheit bedeuten; vgl. hierzu Bekanntmachung der EU-Kommission, Leitfaden für die Umsetzung der Produktvorschriften der EU 2022 (im Folgenden „Blue Guide“), ABl. 2022/C 247/01 (113): „Die Nichteinhaltung wesentlicher Anforderungen ist im Allgemeinen als erhebliche Nichtkonformität anzusehen, weil dies ein potenzielles oder tatsächliches Risiko für die Gesundheit und Sicherheit von Personen oder anderer schützenswerter Aspekte des öffentlichen Interesses durch das Produkt bedeuten kann“. Daneben hebt der Wortlaut der Vorschrift auch auf das vom Produkt ausgehende Risiko ab; zudem nimmt die Definition *des Produkts*, mit dem ein Risiko verbunden ist, die Gesundheit und Sicherheit ausdrücklich in Bezug (vgl. Art. 3 Nr. 19 MÜ-VO).

1675 So auch Giesberts/Gayger, in: NK-ProdR, Art. 16 MÜ-VO, Rn. 33.

1676 Vgl. Wiebe, NJW 2019, 625 (628).

1677 Giesberts/Gayger, in: NK-ProdR, Art. 16 MÜ-VO, Rn. 47.

1678 Dies konstatiert auch Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthafungshandbuch, § 24, Rn. 365.

zum Hersteller und wird aus dem Verkehr gezogen. Nachgerüstet oder ersetzt entspricht das Produkt dann wieder den gesetzlichen Sicherheitsstandards und kann wieder in den Verkehr gelangen.¹⁶⁷⁹ Allerdings ist schon allein mit Erwirkung der Rückgabe die Gefahr beseitigt. Darüberhinausgehende Maßnahmen wie die Nachrüstung oder der Austausch des Produkts, die zusätzlich auf die erneute Inverkehrgabe des Produkts gerichtet sind, könnten daher überschießend und ihre Anordnung daher in diesem Teil rechtswidrig sein.¹⁶⁸⁰ Jedenfalls darf die Behörde keine dieser Maßnahmen mit dem Ziel anordnen, dem Nutzer ein wieder in jeder Hinsicht gebrauchstaugliches Produkt zu verschaffen. Die Rückführung des Produkts soll nämlich nicht zum Zwecke der Kostenerstattung, des Umtauschs oder der Instandsetzung stattfinden,¹⁶⁸¹ sondern zum Zwecke der Gefahrenabwehr. Besteht aber der Hauptzweck der Maßnahme in der Gefahrenabwehr, verbleibt der Behörde ein gewisser Spielraum bei der konkreten Ausgestaltung der Rückrufanordnung.¹⁶⁸² Dies ergibt sich zum einen daraus, dass Art. 16 Abs. 3 MÜ-VO ohnehin keine abschließende Liste an Maßnahmen, sondern vielmehr Regelbeispiele enthält und die Behörde gerade nicht daran gehindert ist, andere Korrekturmaßnahmen zu ergreifen.¹⁶⁸³ Zum anderen daraus, dass der Behörde zwar ein Auswahlermessen zukommt, die gewählte Korrekturmaßnahme aber schon dem Wortlaut des Art. 16 Abs. 2 MÜ-VO nach angemessen und verhältnismäßig sein muss.¹⁶⁸⁴ Bereits aufgrund dieses Verhältnismäßigkeitsgebots muss eine behördliche Auseinandersetzung mit den Möglichkeiten, dem Umfang

1679 In diese Richtung zur Vorgängernorm *Wiebe*, NJW 2019, 625 (628) und dem folgend *Giesberts/Gayger*, in: NK-ProdR, Art. 16 MÜ-VO, Rn. 47.

1680 So *Klindt/Schucht*, in: Klindt, ProdSG, § 2, Rn. 180; *Foerste*, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungsbandbuch, § 24, Rn. 365.

1681 So noch ein Vorschlag im Rahmen des Gesetzgebungsverfahrens zur Vorgängerregelung, vgl. den Nachweis bei *Klindt/Schucht*, in: Klindt, ProdSG, § 2, Rn. 178.

1682 Zur Vorgängernorm *Wiebe*, NJW 2019, 625 (628); dem folgend *Giesberts/Gayger*, in: NK-ProdR, Art. 16 MÜ-VO, Rn. 47; i.E. wohl auch *Reusch*, BB 2017, 2248 (2250).

1683 Vgl. *Giesberts/Gayger*, in: NK-ProdR, Art. 16 MÜ-VO, Rn. 28.

1684 Vgl. daneben Art. 19 Abs. 1 S. 1 MÜ-VO (i.V.m. § 8 Abs. 2 S. 3 MüG), wonach die Marktüberwachungsbehörden im Fall eines ersten Produktrisikos dafür Sorge zu tragen haben, dass das Produkt zurückgerufen wird, sofern es keine andere wirksame Möglichkeit zur Beseitigung des ersten Risikos gibt. Aus dieser Regelung lässt sich ablesen, dass Rücknahme und Rückruf vornehmlich im Fall erster Risiken in Betracht kommen sollen, sich in diesem Fall aber auch das Auswahlermessen verkürzt, vgl. *Schucht*, in: Klindt, ProdSG, § 26, Rn. 157 „Sonderrecht für erste Risiken“.

und Aufwand von Nachrüstungsmaßnahmen stattfinden.¹⁶⁸⁵ Denn eine Maßnahme ist immer nur dann erforderlich, wenn nicht andere geeignete Mittel zur Verfügung stehen, die den Betroffenen und die Allgemeinheit weniger beeinträchtigen.¹⁶⁸⁶ Gerade mit Blick auf den Hersteller mag die Anordnung des Rückrufs oder der Fernstilllegung aber nicht stets die am wenigsten belastende Maßnahme darstellen. Gerade aus Reputationsgründen kann ein solches Vorgehen für ihn desaströs sein und die Anordnung eines Sicherheitsupdates trotz der damit verbundenen Kosten weniger belastend sein. Sofern eine entsprechende Anordnung damit dem Verhältnismäßigkeitsgrundsatz folgt und die Gefahrenabwehr intendiert, kann ihr – auch vor dem Hintergrund der grundrechtlichen Schutzpflichten der öffentlichen Gewalt zum Schutz der Rechtsgüter Leben und Gesundheit (vgl. Art. 2 Abs. 2 GG) – nicht entgegengehalten werden, dass sie auch der Verwirklichung des Äquivalenzinteresses des Nutzers dient.¹⁶⁸⁷ Unter der Berücksichtigung der Eingriffsintensität und der Größe der drohenden Gefahr kann die Bereitstellung von Sicherheitsupdates im Einzelfall folglich behördlich angeordnet werden.

Hinsichtlich einer möglichen Vollstreckung im Rahmen des Art. 16 Abs. 5 MÜ-VO ist freilich zu berücksichtigen, dass allein der Hersteller in der Lage ist, das Sicherheitsupdate zu entwickeln und bereitzustellen und eine Durchführung als Ersatzvornahme durch die Behörde selbst von vornherein nicht in Betracht kommt.¹⁶⁸⁸

Mittelbar kann eine entsprechende behördliche Anordnung auch haftungsrechtliche Konsequenzen nach sich ziehen. Zwar stellen die Bestimmungen über den Produktrückruf keine Schutzgesetze i.S.d. § 823 Abs. 2 BGB dar, da sie nicht ipso iure gelten, sondern einer im Ermessen der Behörde stehenden hoheitlichen Anordnung bedürfen.¹⁶⁸⁹ Erlässt die Behörde aber einen entsprechenden Verwaltungsakt, kommt es zu einer

1685 So auch *Wiebe*, NJW 2019, 625 (628).

1686 *Schucht*, in: Klindt, ProdSG, § 26, Rn. 66.

1687 *Wiebe*, NJW 2019, 625 (629 f.).

1688 Dabei ist auch die dreistufige Ausgestaltung des Marktüberwachungsverfahrens in Art. 16 MÜ-VO zu berücksichtigen. Erst nach Feststellung des Verstoßes und der Aufforderung nach Abs. 2, 3, Korrekturmaßnahmen eigenständig zu ergreifen, können nach Abs. 5 – mit Befehl und Zwang – als ultima ratio Bekämpfungsmaßnahmen seitens der Behörde durchgeführt werden, vgl. *Giesberts/Gayger*, in: NK-ProdR, Art. 16 MÜ-VO, Rn. 3 und *Schucht*, EuZW 2020, 554 (559). Anders nur im Fall des ernststen Risikos nach Art. 19 MÜ-VO.

1689 *Wagner*, in: MüKo, BGB, § 823, Rn. 1157; *Wagner*, VersR 2014, 905 (914); *Wagner*, in: Eifert (Hg.), Produktbeobachtung durch Private, S. 115 (142).

Konkretisierung der Gesetzesnorm zu einem Schutzgesetz.¹⁶⁹⁰ Wird der Hersteller folglich von der Behörde zur Bereitstellung von Updates verpflichtet und kommt er der Inanspruchnahme nicht nach, macht er sich im Schadensfalle gem. § 823 Abs. 2 BGB i.V.m. Art. 19 Abs. 2, Abs. 3 lit. c MÜ-VO ersatzpflichtig.¹⁶⁹¹ Da die behördliche Anordnung aber dem Verhältnismäßigkeitsgrundsatz entsprechen muss, dürfte sich in diesen Fällen ohnehin eine entsprechende Updatepflicht im Hinblick auf die Effektivität der Gefahrenabwehr aus der Produktbeobachtungspflicht nach § 823 Abs. 1 BGB ergeben.

d) Künftige Bedeutung der KI-VO

Vergleichbar zur GPSR trifft Anbieter nach Art. 20 Abs. 1 KI-VO eine gesetzliche Pflicht, bei einem begründeten Verdacht, dass ein im Verkehr befindliches Hochrisiko-KI-System nicht konform ist, auf Ebene der Risikoabwehr unverzüglich erforderliche Korrekturmaßnahmen zu ergreifen oder es gegebenenfalls zurückzurufen oder explizit auch zu deaktivieren. Den Anbietern kommt auch hier ein Ermessen bei der Auswahl der konkreten Korrekturmaßnahme zu.¹⁶⁹² Die Pflichten gehen damit nicht über die deliktsrechtlichen Gefahrenabwendungspflichten des § 823 Abs. 1 BGB hinaus.¹⁶⁹³ Nach Art. 74 Abs. 1 KI-VO gilt die MÜ-VO auch für KI-Systeme.

e) Künftige Bedeutung des CRA

Durch den CRA sollen nicht nur grundlegende Anforderungen an die Konzeption, Entwicklung und Herstellung von Produkten mit digitalen Elementen hinsichtlich der Cybersicherheit festgelegt werden, sondern auch grundlegende Anforderungen an die von den Herstellern festgelegten Verfahren zur Behandlung von Schwachstellen, um so die Cybersicherheit während der erwarteten Nutzungsdauer der Produkte zu gewährleisten, vgl. Art. 1 lit. b, lit. c CRA.¹⁶⁹⁴ Um dieses Ziel zu erreichen, verfolgt der CRA einen mehrstufigen Ansatz, bei dem Sicherheitsaktualisierungen im Mittelpunkt stehen.

1690 Wagner, VersR 2014, 905 (914).

1691 Vgl. Wagner, in: MüKo, BGB, § 823, Rn. 1157; Wagner, VersR 2014, 905 (914).

1692 Vgl. Wiebe, BB 2022, 899 (904).

1693 Anders aber Grützmacher, CR 2021, 433 (440).

1694 Vgl. auch Erwägungsgrund (2) CRA.

aa) Schwachstellenmanagement und Sicherheitsaktualisierungen

Zunächst muss das Produkt gem. Art. 13 Abs. 1 i.V.m. Anhang I Teil 1 Abs. 2 lit. c CRA bereits zum Zeitpunkt des Inverkehrbringens so konstruiert sein, dass sichergestellt ist, dass auftretende Schwachstellen durch Sicherheitsaktualisierungen behoben werden können („Updatability“)¹⁶⁹⁵. Dabei soll unter einer Schwachstelle nach Art. 3 Nr. 40 CRA eine Schwäche, Anfälligkeit oder Fehlfunktion eines Produkts mit digitalen Elementen verstanden werden, die bei einer Cyberbedrohung ausgenutzt werden kann. Weiter haben die Hersteller gem. Art. 13 Abs. 8 UAbs. 1 CRA sicherzustellen, dass solche potenziellen Schwachstellen wirksam behandelt werden können. Dafür haben sie nach Anhang I Teil II CRA Mechanismen für die sichere Verteilung von Aktualisierungen vorzusehen (Abs. 7) und dafür zu sorgen, dass Sicherheitsaktualisierungen unverzügliche und kostenlose verbreitet werden können (Abs. 8).¹⁶⁹⁶

Neben diese organisatorisch geprägte Pflicht tritt eine die Hersteller betreffende Gefahrenabwendungspflicht aus Art. 13 Abs. 6 CRA. Danach muss der Hersteller, sobald er eine Schwachstelle feststellt, diese Schwachstelle gemäß den in Anhang I Teil II CRA festgelegten Anforderungen behandeln und beheben. Dies hat gem. Anhang I Teil II Abs. 2 CRA unverzüglich unter anderem durch die Bereitstellung von Sicherheitsaktualisierungen zu erfolgen. Das regelhafte Anführen von Updates ist dabei nur logisch, da Schwachstellen oft gar nicht anders behoben werden können.¹⁶⁹⁷ Die Abwehr der Cybersicherheitsgefahr soll folglich durch die Behebung der Schwachstelle erfolgen. Insoweit ist Art. 13 Abs. 6 CRA im Hinblick auf Schwachstellen als *lex specialis* zu Art. 13 Abs. 21 CRA zu sehen, wonach der Hersteller, wenn er Grund zu der Annahme hat, dass sein Produkt die grundlegenden Anforderungen an die Cybersicherheit nach Anhang I CRA nicht erfüllt, unverzüglich die erforderlichen Korrekturmaßnahmen bis hin zum Rückruf zu ergreifen hat. Bei der Behebung von Schwachstellen gibt der CRA indes die Behebung der Schwachstelle als Mittel der Gefahrenabwehr vor. In Konsequenz stellt die bloße Warnung des Nutzers vor der Schwachstelle von vorneherein keine geeignete Maßnahme dar. Durch den CRA wird demnach de facto eine öffentlich-rechtliche Updatepflicht der

1695 Vgl. erneut *Reusch*, BB 2019, 904 (906); *Hartmann*, PHi 2017, 42 (46); *Wiesner*, in: *Leupold/Wiebe/Glossner* (Hg.), IT-Recht, Teil 10.6, Rn. 41; *Wagner*, in: *MüKo*, BGB, § 823, Rn. 1130; ausführlich *Brenner et al.*, RD 2024, 252 (254 ff.).

1696 Erwägungsgrund (38) CRA spricht insoweit von Schwachstellenmanagement.

1697 *Wiebe/Daelen*, EuZW 2023, 257 (262).

Hersteller zur Behebung von Schwachstellen eingeführt. Softwarefehler, die lediglich zu internen sicherheitskritischen Fehlfunktionen führen können, fallen hingegen nicht darunter, da eine Schwachstelle definitionsgemäß gerade an ihre Ausnutzbarkeit im Falle einer Cyberbedrohung geknüpft ist, vgl. auch Erwägungsgrund (50) CRA.

Nach Art. 52 Abs. 1 KI-VO gilt die MÜ-VO auch für Produkte, die in den Anwendungsbereich des CRA fallen.

bb) Bedeutung für die zivilrechtliche Produktbeobachtungspflicht

Zwar mag der Hersteller in den Fällen, in denen ihn die Updatepflicht nach dem CRA trifft, nicht zwangsläufig auch nach seiner allein auf die Effektivität der Gefahrenabwehr ausgerichteten deliktsrechtlichen Produktbeobachtungspflicht zur Bereitstellung eines Sicherheitsupdates verpflichtet sein. Denn auch nach hiesigem Verständnis kann das Bereitstellen von Sicherheitsupdates im (seltenen) Einzelfall nicht erforderlich oder zumutbar sein. Zudem hat die Verbreitung von Sicherheitsaktualisierungen nach Anhang I Teil 2 Abs. 8 CRA zwingend für den Nutzer kostenlos zu erfolgen.

Wiederum könnte den Hersteller dann jedoch eine Haftung für die Verletzung der ihm nach dem CRA obliegenden Updatepflicht unter dem Gesichtspunkt der Schutzgesetzverletzung nach § 823 Abs. 2 BGB treffen. Dann müsste es sich bei Art. 13 Abs. 6 i.V.m. Anhang I Teil 2 Abs. 2 CRA um ein Schutzgesetz im bereits dargelegten Sinne handeln. Die Pflicht des Herstellers zur Behandlung von Schwachstellen soll ausweislich Art. 1 lit. c CRA die Cybersicherheit von Produkten während ihres gesamten Lebenszyklus gewährleisten. Der CRA selbst verweist zur Definition des Begriffs der Cybersicherheit in Art. 3 Nr. 3 CRA auf Art. 2 Nr. 1 CSA. Danach zielt Cybersicherheit aber nicht nur allgemein auf den Schutz der Netz- und Informationssysteme ab, sondern auch auf den Schutz der Nutzer und anderer von Cyberbedrohungen betroffener Personen. Damit umfasst diese Definition aber nicht nur die Vertraulichkeit, Integrität und Verfügbarkeit als übergeordnete Schutzziele, sondern betont auch, dass nicht nur IT-Systeme, sondern primär Personen vor Cyberbedrohungen geschützt werden sollen.¹⁶⁹⁸ Auch nach Erwägungsgrund (1) CRA sollen die hohen Kosten sowohl für die Gesellschaft als auch für den Nutzer angegangen werden, die durch ein geringes Maß an Cybersicherheit, insbesondere aufgrund

¹⁶⁹⁸ Nolte/Schreitmüller, MPR 2024, 20 (23).

unzureichender und inkohärenter Bereitstellung von Updates, verursacht werden. Neben den Gefahren für die Wirtschaft und die Demokratie wird explizit auch auf die Sicherheit und Gesundheit der Verbraucher Bezug genommen. Damit aber versteht der CRA Cybersicherheit nicht nur gesamtgesellschaftlich, sondern auch in Bezug auf den einzelnen Nutzer. Folglich ist die Updatepflicht des CRA von ihrem Anwendungsbereich auch auf den Individualschutz der einzelnen Nutzer gerichtet. Da fehlende Sicherheitsupdates gerade dazu geeignet sind, privatrechtliche Schäden auszulösen, ist dem Einzelnen die Befugnis einzuräumen, den Geltungsanspruch der Norm im Zivilrechtsweg über einen Schadensersatzanspruch selbst durchzusetzen. Vor diesem Hintergrund ist erneut bereits bei nationaler Auslegung vom Schutzgesetzcharakter der Norm auszugehen. Den Hersteller trifft damit im Falle einer Nichtbereitstellung von Updates zur Behebung einer Schwachstelle nicht nur ein erhebliches Sanktionsrisiko (nach Art. 53 Abs. 3 CRA können Bußgelder bis zu 15 Mio. € oder bis zu 2,5 % des Jahresumsatzes fällig werden), sondern auch ein Haftungsrisiko.

f) Künftige Bedeutung der neuen Produkthaftungsrichtlinie

Auch die neue Produkthaftungsrichtlinie will künftig die Verantwortung des Herstellers für die Sicherheiten von Produkten über den gesamten Lebenszyklus stärker berücksichtigen, vgl. Erwägungsgrund (51) ProdHaftRL.

aa) Zeitliche Dynamisierung des Fehlerbegriffs

Anknüpfungspunkt für die Bestimmung der berechtigten Sicherheitserwartung und damit für die Beurteilung der Fehlerhaftigkeit eines Produkts bleibt zunächst das Inverkehrbringen. Da im digitalen Zeitalter viele Produkte aber auch nach dem Inverkehrbringen der Kontrolle des Herstellers unterliegen,¹⁶⁹⁹ tritt daneben („oder“) ein weiterer Anknüpfungspunkt, nämlich der Zeitpunkt, ab dem das Produkt nicht mehr der Kontrolle des Herstellers unterliegt, Art. 7 Abs. 2 lit. e ProdHaftRL. Eine solche Kontrolle des Herstellers nach dem Inverkehrbringen liegt nach Art. 4 Nr. 5 lit. b ProdHaftRL vor, wenn der Hersteller eines Produkts in der Lage ist, Software-Updates oder -Upgrades selbst bereitzustellen oder deren Bereit-

¹⁶⁹⁹ Vgl. Erwägungsgrund (32) ProdHaftRL.

stellung durch Dritte zu veranlassen.¹⁷⁰⁰ Demnach ist die grundsätzliche Updatefähigkeit eines Produkts ausreichend,¹⁷⁰¹ um die Kontrolle des Herstellers zu begründen. Allein die eigenmächtige Entscheidung des Herstellers, den Update-Support einzustellen, kann dagegen nicht beeinflussen, ob das Produkt weiterhin seiner Kontrolle unterliegt.¹⁷⁰² Dies steht auch in Einklang mit dem bereits angesprochenen gesetzgeberischen Ziel, dass die Verantwortung des Herstellers für die Sicherheit des Produkts über den gesamten Lebenszyklus gewährleistet werden soll. Entscheidend für die berechnete Verkehrserwartung ist damit der gesamte Zeitraum, in dem das Produkt unter der Kontrolle des Herstellers steht.¹⁷⁰³ Die entsprechende haftungsrechtliche Relevanz lässt sich dabei erst im Zusammenspiel mit den durch die ProdHaftRL verengten Entlastungsgründen ermitteln.

bb) Verengte Entlastungsgründe und produkthaftungsrechtliche Updatepflicht

Da das Inverkehrbringen des Produkts nicht mehr den allein maßgeblichen Zeitpunkt für die Beurteilung des Produktfehlers darstellt, wird auch der grundsätzlich nach Art. 11 Abs. 1 lit. c ProdHaftRL weiterhin bestehende Haftungsausschluss bei Fehlerfreiheit des Produkts im Zeitpunkt des Inverkehrbringens aufgeweicht. So greift der Haftungsausschluss gem. Art. 11 Abs. 2 ProdHaftRL dann nicht ein, wenn die Fehlerhaftigkeit des Produkts auf Software, einschließlich Software-Updates oder Upgrades (lit. b) oder das Fehlen eines solchen Updates oder -Upgrades, die zur Aufrechterhaltung der Sicherheit erforderlich sind (lit. c), zurückgeht.

Demnach haftet der Hersteller für Fehler, die durch ein aufgespieltes Update erst verursacht werden, aber auch für Fehler, die durch das Unterlassen eines entsprechenden Updates entstehen.¹⁷⁰⁴ Etwas versteckt ergibt sich damit eine produkthaftungsrechtliche Pflicht zur Durchführung von Updates, um die Produktsicherheit – nicht aber darüber hinausgehende

1700 Vgl. auch Erwägungsgrund (19) ProdHaftRL.

1701 Diese ist ohnehin normative Produkthanforderung, vgl. Brenner et al., RD 2024, 252 (254 ff.).

1702 Anders noch Spindler CR 2022, 689 (694) zum insoweit definitorisch noch unklaren Kommissionsentwurf, COM(2022) 495 final.

1703 So auch *Haftenberger*, Die Produkthaftung für künstlich intelligente Medizinprodukte, S. 338.

1704 Vgl. Erwägungsgrund (51) ProdHaftRL.

Funktionalitäten – aufrechtzuerhalten.¹⁷⁰⁵ Im Zusammenspiel mit der zeitraumbezogenen Anknüpfung des Fehlerbegriffs wird der Hersteller verpflichtet, seine Produkte mittels Updates an nach dem Inverkehrbringen gestiegene Sicherheitserwartungen anzupassen. Dies ist insbesondere bei Entwicklungslücken von Bedeutung, wenn sich die Fehlerhaftigkeit eines Produkts erst nach dem Inverkehrbringen durch die Weiterentwicklung von Wissenschaft und Technik und den sich daraus ergebenden Möglichkeiten der Gefahrenabwehr zeigt.

Dem Wortlaut nach könnten daneben auch Fälle der bloßen Produktalterung erfasst sein. Denn Art. 7 Abs. 2 lit. e ProdHaftRL knüpft für die Verantwortlichkeit des Herstellers über den Zeitpunkt der Inverkehrgabe hinaus allein an eine weiter bestehende Kontrolle des Herstellers an. Damit kommt dem Kriterium der Gefahrenbeherrschung anders als bei der Produktbeobachtungspflicht nach § 823 Abs. 1 BGB maßgebliche Bedeutung zu. Dass eine entsprechende kontinuierlichen Teilhabe des Nutzers am technischen Fortschritt allein durch die Beibehaltung der Kontrolle des Herstellers intendiert ist, zeigt Erwägungsgrund (57) ProdHaftRL. Danach soll die Haftung des Herstellers nämlich lediglich zeitlich begrenzt werden, da es angesichts der Tatsache, dass Produkte im Laufe der Zeit altern und im Zuge des Fortschritts von Wissenschaft und Technik höhere Sicherheitsstandards entwickelt werden, nicht angemessen wäre, den Hersteller für einen unbegrenzten Zeitraum für die Fehlerhaftigkeit seiner Produkte haftbar zu machen. Demnach begründet eine Änderung der Sicherheitserwartungen erst nach dem Inverkehrbringen des betreffenden Produkts auch dessen Fehlerhaftigkeit.¹⁷⁰⁶ Um eine Haftung zu vermeiden, hat der Hersteller als Reaktion auf sich wandelnde Sicherheitserwartungen auftretende Fehler zu beheben.¹⁷⁰⁷

In diesem Sinne bleibt dem Hersteller nach Art. 11 Abs. 1 lit. e ProdHaftRL auch der Einwand des Entwicklungsfehlers verwehrt, solange sich das

1705 So auch *Wagner*, JZ 2023, 1 (7); *Spindler*, CR 2022, 689 (694); Erwägungsgrund (51) ProdHaftRL weist dagegen darauf hin, dass die Richtlinie keine Verpflichtung zur Bereitstellung von Updates oder Upgrades für ein Produkt vorsieht. Um einem Schadensersatzverlangen zu entgehen, bleibt dem Hersteller aber gar nichts anderes übrig, als Updates bereitzustellen, sodass sich eine Pflicht de facto ergibt.

1706 Vgl. Erwägungsgrund (51) ProdHaftRL; *Spindler*, CR 2022, 689 (693) spricht davon, dass „der Hersteller kontinuierlich für die Verkehrssicherheit der IT-Produkte bzw. des KI-Systems zu sorgen hat“.

1707 Einschränkung dagegen *Wagner*, JZ 2023, 1 (6): „Das sollte richtigerweise aber nur insoweit gelten, als es um die Sicherheitseigenschaften des letzten Updates oder Upgrades geht, nicht aber für das Produkt insgesamt“.

Produkt unter seiner Kontrolle befindet. Demnach ist die fehlende Erkennbarkeit des Produktfehlers zum Zeitpunkt des Inverkehrbringens des Produkts unbeachtlich, wenn der Fehler durch ein Sicherheitsupdate hätte behoben werden können.¹⁷⁰⁸

Zur Aufrechterhaltung der Produktsicherheit ergibt sich daraus im Ergebnis eine produkthaftungsrechtliche Pflicht zur Durchführung von Updates. Ausgeschlossen ist die Haftung des Herstellers aber, wenn ein bereitgestelltes Update vom Nutzer nicht installiert wird.¹⁷⁰⁹ Dies unterliegt eben nicht mehr der Kontrolle des Herstellers. Aufgrund des explizit auf das Fehlen von Softwareupdates abstellenden Wortlauts der Norm, kann sich der Hersteller in diesen Fällen auch nicht auf eine Warnung zur Gefahrenabwehr zurückziehen.¹⁷¹⁰ Nach Erwägungsgrund (51) ProdHaftRL soll der Hersteller gerade auch für Schäden haftbar gemacht werden können, die durch die Nichtbereitstellung von Updates für die Softwaresicherheit entstehen. Bereits der CRA fordert öffentlich-rechtlich nicht nur eine einfache Gefahrenabwehr, sondern das Beheben der Schwachstelle. Hiermit in Einklang¹⁷¹¹ knüpft die ProdHaftRL zivilrechtlich an eine nicht durch Updates behobene Schwachstelle eine Schadensersatzpflicht gegenüber einem dadurch geschädigten Nutzer. Über die Reichweite des CRA hinaus gilt dies aber nicht nur bei Schwachstellen, sondern bei allen durch Updates behebbaren Sicherheitsgefahren. Dadurch dass der Hersteller sich einzelfallunabhängig weder auf eine Produktwarnung zurückziehen kann noch eine Fernstilllegung des Produkts in Betracht kommt, sieht die neue Produkthaftungsrichtlinie strengere Rechtsfolgen für auftretende Produktgefahren vor als dies im Rahmen der Produktbeobachtungspflicht nach § 823 Abs. 1 BGB der Fall ist. Zudem sind auch Gefahren, die sich allein aus der Produktalterung ergeben durch Sicherheitsupdates zu beheben.

g) Fazit

Während sich nach geltendem Recht außerhalb vertraglicher Beziehungen über die Produktbeobachtungspflicht nach § 823 Abs. 1 BGB hinaus keine

1708 Kapoor/Klindt, BB 2023, 67 (70); Kapoor/Sedlmaier, RAW 2023, 8 (12).

1709 Explizit Erwägungsgrund (51) ProdHaftRL.

1710 So i.E. auch Dötsch, Außervertragliche Haftung für KI, S. 406.

1711 Erwägungsgrund (46) ProdHaftRL betont allgemein, dass der enge Zusammenhang zwischen den Produktsicherheitsvorschriften und den Haftungsvorschriften gestärkt werden soll.

weitergehenden Anforderungen des Herstellers an die Gefahrenabwehr aus anderen Vorschriften ergeben, wird sich dies künftig ändern. Schon mit Geltungsbeginn der neuen GPSR am 13.12.2024 werden die Hersteller, falls ein Rückruf im Einzelfall erforderlich sein sollte, bei dessen Ausgestaltung das Recht des Verbrauchers auf Abhilfe zu berücksichtigen haben. In Bezug auf die Bereitstellung von Updates bedeutet dies insbesondere, dass diese kostenlos zur Verfügung gestellt werden müssen. Weitergehend sieht ein Entwurf eines CRA im Falle von Cyberbedrohungen sogar eine Pflicht vor, Schwachstellen (durch Sicherheitsupdates) zu beheben. Gleichzeitig sieht der Entwurf einer neuen Produkthaftungsrichtlinie vor, dass der Hersteller zur Vermeidung einer Haftung die Sicherheit des Produkts zwingend durch Sicherheitsupdates aufrechterhalten muss.

5. Updateansprüche

Unklar ist schließlich, ob und ggf. unter welchen Voraussetzungen im Einzelnen eine derartige Updatepflicht, die im Kern eine rein präventiv wirkende deliktische Verkehrspflicht ist, durch einen vorbeugenden Anspruch auf Sicherheitsupdates durchgesetzt werden kann.¹⁷¹² Im Regelfall werden deliktische Verkehrspflichten erst ex post relevant, wenn ein Schaden bereits eingetreten ist und sich die Frage stellt, ob dieser auf einer verkehrspflichtwidrigen Handlung eines Schädigers beruht.

Einen entsprechenden Anspruch allein mit Hinweis auf ein Zitat der Pflegebetten-Entscheidung zu verneinen, wonach eine deliktsrechtliche Verkehrspflicht „inhaltlich nicht auf die Nachrüstung“ gerichtet sein könne,¹⁷¹³ greift aber zu kurz.¹⁷¹⁴ Weder inhaltlich noch vom Kontext ist die Aussage auf Ansprüche des Nutzers bezogen. Es wird im Rahmen der Pflichtenbestimmung des Herstellers lediglich verdeutlicht, dass deliktsrechtlich nur das Integritätsinteresse geschützt ist und das Äquivalenzinteresse allein (!) keine Nachrüstung rechtfertigen kann.¹⁷¹⁵ Eine

1712 Grundlegend und allgemein dazu v. Bar, Karlsruher Forum 1983, S. 80 (80 ff.); ein solcher Automatismus wird ohne Weiteres von Michalski, BB 1998, 961 (964) und Hager, in: Staudinger, BGB, § 823, Rn. F 25 angenommen; dagegen Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 39, Rn. 1 „eine andere Frage“ und Sedlmaier, in: Kühne/Nack (Hg.), Connected Cars, S. 43.

1713 BGH, NJW 2009, 1080 (1082, Rn. 17).

1714 So aber Chibanguza/Schubmann, GmbHR 2019, 313 (317); Schrader/Engstler, MMR 2018, 356 (360); im Ansatz auch Raue, NJW 2017, 1841 (1845).

1715 In diese Richtung auch Lüftenegger, Die Rückrufpflicht des Herstellers, S. 211 f.

deliktsrechtliche Nachrüstungspflicht kann es nicht geben, wohl aber kann sich eine deliktsrechtliche Gefahrabwendungspflicht im Ergebnis mit ihr überschneiden. Bei der Ablehnung von korrespondierenden Gefahrabwendungsansprüchen schwingt regelmäßig mit, dass hiermit eine noch weitergehende Verwässerung der Abgrenzung zu den vertraglichen Gewährleistungsrechten einherginge.¹⁷¹⁶ Vor diesem Hintergrund soll nachfolgend untersucht werden, ob Gefahrenabwehransprüche des Nutzers gegenüber einem Hersteller bestehen können.

a) Praxisrelevanz

Die Praxisrelevanz dieser Frage lässt sich dabei schwer ermessen. Herkömmliche Rückrufansprüche haben die Gerichte bisher wenig beschäftigt.¹⁷¹⁷ Ob dies tatsächlich am Prozesskostenrisiko (§ 91 ZPO) oder an den Schwierigkeiten liegt, einen Antrag überhaupt hinreichend konkret (§ 253 Abs. 2 Nr. 2 ZPO) zu formulieren, darf bezweifelt werden,¹⁷¹⁸ stellen sich diese Fragen doch regelmäßig bei einer klageweisen Geltendmachung von Ansprüchen.¹⁷¹⁹ Zu berücksichtigen ist aber, dass ein Gefahrenabwehranspruch des Nutzers nur dort in Betracht kommt, wo er auch Kenntnis von der Gefährlichkeit seines Produkts hat.¹⁷²⁰ Diese Kenntnis wird aber häufig erst mit Verwirklichung der Gefahr und damit bei Eintritt der Rechtsgutsverletzung einsetzen. Ein Anspruch auf Abwehr der Gefahr geht dann fehl. Relevant können folglich nur Fälle sein, in denen der Produktnutzer von

1716 *Chibanguza/Schubmann*, GmbHR 2019, 313 (317); *Gless/Janal*, JR 2016, 561 (570); *Wittig*, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 245; *Sedlmaier*, in: Kühne/Nack (Hg.), *Connected Cars*, S. 43; *Oster*, in: Foerste/Graf v. Westphalen (Hg.), *Produkthaftungshandbuch*, § 57, Rn. 29.

1717 Vgl. *Lenz*, in: *Lenz*, *Produkthaftung*, § 4, Rn. 73; skeptisch auch *Schmidt*, *Produktrückruf und Regress*, S. 121.

1718 So aber die Vermutung von *Lenz*, in: *Lenz*, *Produkthaftung*, § 4, Rn. 73.

1719 *Voß*, in: Raue (Hg.), *Digitale Resilienz*, S. 97 (98) spricht dagegen von der rationalen Apathie des Verbrauchers, weil Zeit- und Kostenaufwand eines Gerichtsprozesses außer Verhältnis zum Nutzen des Updates stünden. Ferner verschärften normative Unschärfen und damit einhergehende Rechtsunsicherheiten das Durchsetzungsdefizit (S. 101); vgl. auch *Riehm/Leithäuser/Brenner*, in: Raue (Hg.), *Digitale Resilienz*, S. 5 (26).

1720 Speziell im Kontext von möglichen Updateansprüchen *Voß*, in: Raue (Hg.), *Digitale Resilienz*, S. 97 (100).

der Gefährdung erfährt.¹⁷²¹ Dies wird häufig durch eine Herstellerwarnung geschehen, so dass Abwehransprüche gerade dann von Bedeutung sind. Da die Warnung den Produktnutzer aber lediglich vor die Wahl stellt, ein gefährliches Produkt weiter zu benutzen oder dieses vor Erreichen seiner erwarteten Lebensdauer auszusortieren, dürfte die Geltendmachung eines Gefahrabwendungsanspruchs vordergründig vom Interesse des Nutzers getragen sein, das Äquivalenzinteresse über die Hintertür des Deliktsrechts zu verwirklichen.¹⁷²² Während der Gewährleistungsfrist wird sich der Käufer zwar an den Verkäufer wenden und seine vertraglichen Rechte geltend machen. Hier mag es sein, dass dem Updateanspruch aufgrund der bestehenden Sekundärrechte nur untergeordnete Bedeutung zukommt.¹⁷²³ Nach Ablauf der Gewährleistungsfrist¹⁷²⁴ wäre ein deliktsrechtlicher Updateanspruch aber die einzige Möglichkeit, „selbst aktiv“ zu werden und die unattraktive Lösung des Nutzungsverzichts zu verhindern.¹⁷²⁵ Aufgrund des Bedeutungsgewinns der Produktbeobachtungspflicht und der regelmäßig anknüpfenden Updatepflicht könnten auch korrespondierende Updateansprüche an Bedeutung gewinnen.¹⁷²⁶ Nur kurz sei in diesem Zusammenhang darauf hingewiesen, dass durch das neue Verbraucherrecht durchsetzungsgesetz¹⁷²⁷ qualifizierte Verbände mit der Abhilfeklage die Möglichkeit erhalten sollen, individuelle Ansprüche von Verbrauchern und kleinen Unternehmen gebündelt geltend zu machen.¹⁷²⁸

Die eng mit dem Bestehen eines subjektiven Anspruchs verknüpfte Frage nach einem Aufwendungsersatzanspruch gegen den Hersteller bei erfolgter Selbstvornahme soll hier mangels besonderer Relevanz im Update-Kontext – der Nutzer wird hierzu kaum jemals in der Lage sein (s.o. unter

1721 Voß, in: Raue (Hg.), *Digitale Resilienz*, S. 97 (100) führt an, dass bei allgemein bekannten Sicherheitslücken der Hersteller ohnehin proaktiv ein Update bereitstellen wird oder ihn der Marktdruck hierzu regelmäßig motivieren wird.

1722 Gless/Janal, JR 2016, 561 (569 f.).

1723 In diese Richtung auch Voß, in: Raue (Hg.), *Digitale Resilienz*, S. 97 (99).

1724 Hierbei ist freilich zu beachten, dass § 327f Abs. 1 S. 3 Nr. 2 BGB eine Aktualisierungspflicht für den Zeitraum vorsieht, „den der Verbraucher aufgrund der Art und des Zwecks des digitalen Produkts und unter Berücksichtigung der Umstände und der Art des Vertrags erwarten kann“.

1725 Huber, *Rechtsfragen des Produktrückrufs*, S. 70.

1726 Freilich ist zu berücksichtigen, dass die Hersteller schon aus Imagegründen vielfach Updates bereitstellen werden.

1727 Regierungsentwurf, BT-Drs. 20/6520 in Umsetzung der Verbandsklagenrichtlinie (EU) 2020/1828.

1728 Ausführlich zur Bedeutung für Updateansprüche Voß, in: Raue (Hg.), *Digitale Resilienz*, S. 97 (104 ff.).

E.III.1.b)cc)(2α)) – ausgeklammert werden.¹⁷²⁹ Ebenso wird die Frage nach einem Anspruch auf die Vornahme einer Warnung kaum einmal relevant werden. Zwar mag die Feststellung, dass derjenige, der die Gefahr kennt, nicht gewarnt werden muss und derjenige, der die Gefahr nicht kennt, schon denklogisch keinen Anspruch geltend machen wird, in ihrer Apodiktik nicht immer zutreffen.¹⁷³⁰ Denn es kann Fälle geben, in denen die betroffene Person zwar über ein diffuses Gefahrenwissen verfügt, dieses aber nicht ausreicht, um die Gefahr konkret und realistisch einzuschätzen. Gleichzeitig ist das Wissen um eine Gefahr nicht immer mit dem Wissen um die Gefahrenvermeidung gleichzusetzen. Daher kann ein Auskunftsanspruch über den tatsächlichen Charakter der Gefahr und den Umgang mit dieser durchaus sinnvoll sein.¹⁷³¹ Allerdings geht ein solches Szenario davon aus, dass der Hersteller wesentliche Gefahreninformationen vorenthält und eine Rechtsgutsverletzung bei den Betroffenen sehenden Auges in Kauf nimmt.¹⁷³² Dies wird auch unter Berücksichtigung eines möglichen Imageschadens durch die Warnung kaum einmal der Fall sein, da der Imageschaden bei eingetretener Rechtsgutsverletzung gravierender zu bewerten sein wird.

b) Rückrufanspruch aufgrund des deliktsrechtlichen
Beseitigungsanspruchs nach §§ 823 Abs. 1, 249 S. 1 BGB

Nach dem Grundsatz der Naturalrestitution ist im Rahmen eines Schadensersatzanspruchs der gleiche wirtschaftliche Zustand herzustellen, der ohne das schädigende Ereignis bestünde.¹⁷³³ Der deliktsrechtliche Beseitigungsanspruch stellt insoweit eine besondere Ausprägung dieses Grundsatzes dar, indem die Folgen eines schuldhaften und rechtswidrigen Eingriffs beseitigt werden sollen.¹⁷³⁴ Problematisch ist allerdings, dass ein Rückruf- oder Updateanspruch auf die Beseitigung eines Gefahrenherds gerichtet wären, ohne dass eine Rechtsgutsverletzung oder ein Schaden bereits einge-

1729 Vgl. hierzu allgemein *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 330; sehr wohl relevant dagegen ist der Regress innerhalb der Lieferkette.

1730 So indes *Schwenzer*, JZ 1987, 1059 (1063).

1731 Dazu *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 352.

1732 Feststellung bei *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 354.

1733 Vgl. statt aller *Flume*, in: BeckOK, BGB, § 249, Rn. 37.

1734 *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 339; *Beck*, Die präventive Durchsetzung der Rückrufflicht, S. 135.

treten sind.¹⁷³⁵ In dieser Konstellation kann man § 823 Abs. 1 BGB für den deliktsrechtliche Beseitigungsanspruch nur fruchtbar machen, indem eine unmittelbare Rechtsgutsgefährdung der Rechtsgutsverletzung gleichgestellt wird.¹⁷³⁶

Hierfür wird angeführt, dass die Schadensverhütung der Schadensregulierung vorgehe.¹⁷³⁷ Weiter wird auf die Rechtsprechung zur Ersatzfähigkeit von Vorsorgeaufwendungen als Schadensabwehrkosten verwiesen,¹⁷³⁸ wonach Aufwendungen, die vor einem Schadensfall für Maßnahmen zur Abwendung einer unmittelbar bevorstehenden Verletzung eines der in § 823 Abs. 1 BGB genannten Rechtsgüter gemacht werden, als Schaden im Sinne dieser Vorschrift zu qualifizieren und zu ersetzen sein können.¹⁷³⁹ Konsequenterweise sei daher jedenfalls bei einer drohenden und auf andere Weise nicht zu verhindernden Verletzung von Rechtsgütern der deliktsrechtliche Beseitigungsanspruch gegeben.¹⁷⁴⁰ Der BGH hat in seiner Pflegebetten-Entscheidung ausdrücklich offen gelassen, ob er sich einer solchen Sichtweise anschließt.¹⁷⁴¹ Indes ist das Deliktsrecht auf den Schadensausgleich bei eingetretener Rechtsgutsverletzung und Schaden ausgelegt und entfaltet präventiven Rechtsschutz lediglich mittelbar über die Androhung eines Schadensersatzanspruchs.¹⁷⁴² Eine Ausdehnung des Anwendungsbereichs des Deliktsrechts auch auf Rechtsgutsgefährdungen wäre insoweit systemwidrig, da der vorbeugende Rechtsschutz außerdeliktischen Normen wie bspw. §§ 862, 1004 BGB zugeordnet ist und bereits dadurch gewährleistet

1735 Dies räumt auch *Hager*, VersR 1984, 799 (802) ein; pauschal aber OLG Stuttgart, NJW 1967, 572 (573), vgl. auch *Lenz*, in: *Lenz*, Produkthaftung, § 4, Rn. 75.

1736 So *Schwenzer*, JZ 1987, 1059 (1060); *Hager*, VersR 1984, 799 (802).

1737 *Hager*, VersR 1984, 799 (800).

1738 In diese Richtung OLG Karlsruhe, VersR 1986, 1125; grundsätzlich auch *Tamme*, Rückrufkosten, S. 302 f.

1739 Allgemein zur Ersatzfähigkeit solcher Vorsorgeaufwendungen BGH, NJW 1960, 1339 (1339); *Grüneberg*, in: *Grüneberg*, BGB, § 249, Rn. 62; vgl. auch BGH, NJW 2009, 1080 (1081, Rn. 24).

1740 *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), Produkthaftungshandbuch, § 39, Rn. 3 ff.; *Tamme*, Rückrufkosten, S. 303; *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 342.

1741 BGH, NJW 2009, 1080 (1081, Rn. 23 f.); insoweit wird die Entscheidung von *Mäsch*, JuS 2015, 556 (558) und übertragen auf den Kontext von Updateansprüchen von *Schrader/Engstler*, MMR 2018, 356 (360) zu apodiktisch verstanden, wie hier dagegen *Schmidt*, Produktrückruf und Regress, S. 139 und *Lüftenegger*, Die Rückrufflicht des Herstellers, S. 209.

1742 So *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 341; *Huber*, Rechtsfragen des Produktrückrufs, S. 77; v. *Bar*, Karlsruher Forum 1983, S. 80 (80); vgl. auch *Pieper*, BB 1991, 985 (989) und *Lenz*, in: *Lenz*, Produkthaftung, § 4, Rn. 75.

ist, dass der Betroffene auch bei einer Rechtsgutsgefährdung nicht schutzlos gestellt ist.¹⁷⁴³

Während die Rückrufpflicht als Verkehrssicherungspflicht bei vorhandener Rechtsgutsgefährdung einen Schaden verhindern soll, knüpft der deliktsrechtliche Beseitigungsanspruch als Ausprägung eines Schadensersatzanspruchs an eine eingetretene Rechtsgutsverletzung und vorliegenden Schaden. Daher ist ein auf § 823 Abs.1 BGB gestützter Anspruch der Produktnutzer bei bloßer Rechtsgutsgefährdung zu verneinen. Insoweit handelt es sich bei der Produktbeobachtungspflicht um eine Handlungsanweisung,¹⁷⁴⁴ die bereits bei Gefährdung von Rechtsgütern durch die Androhung eines Schadensersatzanspruchs zu den erforderlichen Gefahrenabwehrmaßnahmen anhalten soll, während es in der Natur der Sache von Schadensersatzansprüchen liegt, dass ein Schaden bereits eingetreten sein muss.¹⁷⁴⁵

c) Rückrufanspruch nach 1004 Abs. 1 BGB (analog)

Während der Anspruch nach § 823 Abs.1 BGB eine Rechtsgutsverletzung voraussetzt, handelt es sich bei § 1004 Abs.1 BGB um eine Norm des vorbeugenden Rechtsschutzes. Dabei ist anerkannt, dass über den Wortlaut hinaus nicht nur das Eigentum, sondern in analoger Anwendung auch alle deliktsrechtlich geschützten Rechtsgüter erfasst sind.¹⁷⁴⁶ Voraussetzung des Beseitigungsanspruchs nach § 1004 Abs.1 S.1 BGB ist das Vorliegen einer gegenwärtigen Beeinträchtigung, während für den Unterlassungsanspruch nach § 1004 Abs.1 S.2 BGB eine (auch erstmals)¹⁷⁴⁷ drohende Beeinträchtigung ausreichend ist.¹⁷⁴⁸ Für ein in Verkehr gebrachtes gefährliches Produkt

1743 *Wagner*, in: MüKo, BGB, Vor § 823, Rn. 40; *Huber*, Rechtsfragen des Produktrückrufs, S. 77; *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 342; *Schmidt*, Produktrückruf und Regress, S. 140; *Beck*, Die präventive Durchsetzung der Rückrufpflicht, S. 138 f.

1744 *So Lenz*, in: *Lenz*, Produkthaftung, § 3, Rn. 232.

1745 *Huber*, Rechtsfragen des Produktrückrufs, S. 78f.

1746 Vgl. nur *Wellenhofer*, Sachenrecht, § 24, Rn. 45; *Herrler*, in: *Grüneberg*, BGB, § 1004, Rn. 4; *Wagner*, in: MüKo, BGB, Vor § 823, Rn. 41.

1747 Einhellige Ansicht – entgegen dem Wortlaut „weitere Beeinträchtigungen“ – vgl. nur *Wellenhofer*, Sachenrecht, § 24, Rn. 34; *Herrler*, in: *Grüneberg*, BGB, § 1004, Rn. 32 m.w.N zur Rspr.

1748 Vgl. zu dieser Abgrenzung *Thole*, in: *Staudinger*, BGB, § 1004, Rn. 344; *Fritzsche*, in: *BeckOK*, BGB, § 1004, Rn. 56.

stellt sich daher zunächst die Frage, welcher der beiden Ansprüche in Betracht kommt.¹⁷⁴⁹

Die Differenzierung der beiden Ansprüche zeigt aber schon, dass das bloße Vorhandensein eines Produktfehlers als bereits bei Inverkehrbringen latent vorhandene Produktgefahr noch keine gegenwärtige Beeinträchtigung i.S.d § 1004 Abs. 1 S. 1 BGB darstellen kann, sondern es hierfür entscheidend erst auf die Verwirklichung der dem Produktfehler innewohnenden Gefahr und die konkrete Rechtsgutsverletzung ankommen muss.¹⁷⁵⁰ Zwar setzt eine Beeinträchtigung nicht zwingend einen bereits eingetretenen Schaden voraus,¹⁷⁵¹ doch besteht im Hinblick auf den Unterlassungsanspruch nach § 1004 Abs. 1 S. 2 BGB weder Raum noch Notwendigkeit, den Zeitpunkt der Beeinträchtigung auf den der drohenden Gefahr vorzuverlegen.¹⁷⁵² Auch kann nicht auf die eingeschränkte Nutzbarkeit des Produkts infolge seiner Gefährlichkeit als Beeinträchtigung des Eigentums abgestellt werden, da insoweit nie fehlerfreies Eigentum erlangt wurde.¹⁷⁵³ Folglich kommt ein Rückruf- oder Updateanspruch unter dem Gesichtspunkt eines Unterlassungsanspruchs nach § 1004 Abs. 1 S. 2 BGB in Betracht.

aa) Anwendbarkeit des Unterlassungsanspruchs

Bevor auf die einzelnen Tatbestandsmerkmale eingegangen werden soll, muss zunächst die grundsätzliche Anwendbarkeit des Unterlassungsanspruchs auf diese Konstellation geklärt werden. Fraglich ist nämlich, ob präventiver Rechtsschutz auch gegen die sich abzeichnende Verletzung einer Verkehrspflicht möglich ist und damit, ob eine Rückruf- bzw. Updatepflicht in ihrer Eigenschaft als Verkehrspflicht überhaupt einklagbar

1749 Zur Relevanz der Abgrenzung *Tamme*, Rückrufkosten, S. 243 ff.; *Pieper*, BB 1991, 985 (989 f.) und *Foerste*, in: *Foerste/Graf v. Westphalen* (Hg.), *Produkthaftungs-handbuch*, § 39, Rn. 13 ff. lassen die Unterscheidung dagegen offen.

1750 *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 344; *Beck*, Die präventive Durchsetzung der Rückrufpflicht, S. 81; a.A. *Hager*, VersR 1984, 799 (806 f.) und *Schwenzer*, JZ 1987, 1059 (1060); für eine Beeinträchtigung bei hinreichender Konkretisierung der Gefahr *Tamme*, Rückrufkosten, S. 256 ff. und *Huber*, Rechtsfragen des Produktrückrufs, S. 85; anders womöglich für den bei Produktgefahren kaum denkbaren Fall, dass die Gefahr zwangsläufig bald eine Beeinträchtigung herbeiführen muss, vgl. *Fritzsche*, in: *BeckOK*, BGB, § 1004, Rn. 56.

1751 *Hager*, VersR 1984, 799 (802).

1752 *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 345; *Beck*, Die präventive Durchsetzung der Rückrufpflicht, S. 81; *Schmidt*, Produktrückruf und Regress, S. 125.

1753 *Huber*, Rechtsfragen des Produktrückrufs, S. 84; *Tamme*, Rückrufkosten, S. 276.

ist. Denn bei Verkehrspflichten handelt es sich im Ausgangspunkt um unselbständige Pflichten, die zwar zur Haftungsbegründung herangezogen werden, für die aber gesetzlich (abgesehen von §§ 907, 908 BGB) kein vorbeugender Rechtsschutz vorgesehen ist. Allerdings scheint über den Unterlassungsanspruch des § 1004 Abs. 1 S. 2 BGB gerade eine Aufwertung der Verkehrspflichten hin zu selbständig einklagbaren Pflichten denkbar.¹⁷⁵⁴

Problematisch ist dabei aber schon, dass ein Unterlassungsanspruch seinem Wortlaut nach eben auf ein Unterlassen des Pflichtigen gerichtet ist, während eine Nachrüstung oder die Bereitstellung von Updates ein aktives Handeln des Herstellers erfordern.¹⁷⁵⁵ Allerdings ist der Unterlassungsanspruch nicht lediglich auf die Vermeidung eines bestimmten Tuns gerichtet, sondern zielt auch auf die Vermeidung eines bestimmten Erfolgs ab.¹⁷⁵⁶ Daher ist anerkannt, dass der zur Unterlassung Verpflichtete auch das erforderliche positive Tun schuldet, sollte sich die drohende Beeinträchtigung nur durch aktives Eingreifen verhindern lassen.¹⁷⁵⁷ Da durch die präventiv wirkenden Abwehransprüche sämtliche deliktsrechtlich geschützten Rechtspositionen vor drohenden Eingriffen abgesichert werden sollen,¹⁷⁵⁸ wird mit dieser Erfolgsbezogenheit des Unterlassungsanspruchs die Entwicklung im Deliktsrecht konsequent nachgezeichnet.¹⁷⁵⁹ Es wird abgebildet, dass eine Gefahr nicht nur durch aktives Tun entstehen kann, das durch einen Unterlassungsanspruch im wörtlichen Sinne abgewendet werden kann, sondern auch durch ein Unterlassen, für das ein „Verhinderungsanspruch“¹⁷⁶⁰ zur Prävention künftiger Störungen erforderlich ist.¹⁷⁶¹

Daneben ist problematisch, dass bei einer Beeinträchtigung durch ein aktives Tun sowohl die zu unterlassende Handlung als auch – aufgrund der erkennbaren Stoßrichtung – das gefährdete Rechtsgut und deren In-

1754 Grundlegend v. Bar, *Karlsruher Forum* 1983, S. 80 (80); vgl. auch Beck, Die präventive Durchsetzung der Rückruffpflicht, S. 94.

1755 Ausführlich zu dieser Ausgangslage Beck, Die präventive Durchsetzung der Rückruffpflicht, S. 86.

1756 Vgl. Bodewig, Der Rückruf fehlerhafter Produkte, S. 347 f.

1757 Vgl. BGH, NJW 2004, 1035 (1037); BGH, NJW-RR 2019, 1035 (1035); Herrler, in: Grüneberg, BGB, § 1004, Rn. 33; Thole, in: Staudinger, BGB, § 1004, Rn. 467; v. Bar, *Karlsruher Forum* 1983, S. 80 (82) „Anspruch auf Unterlassung einer Unterlassung, also auf ein positives Tun“.

1758 Vgl. hierzu Wagner, in: MüKo, BGB, Vor § 823, Rn. 41.

1759 Ausführlich Beck, Die präventive Durchsetzung der Rückruffpflicht, S. 89 ff.; v. Bar, *Karlsruher Forum* 1983, S. 80 (84).

1760 Dazu Larenz/Canaris, *Lehrbuch des Schuldrechts II/2*, S. 706.

1761 Bodewig, Der Rückruf fehlerhafter Produkte, S. 347 (Fn. 847).

haber ausreichend konkretisiert werden, während Verkehrspflichten Verhaltensgebote aufstellen, die gegenüber der Allgemeinheit gelten. Indes sieht § 908 BGB einen vorbeugenden Abwehranspruch für den Eigentümer eines Grundstücks gegen den nach § 836 Abs. 1 BGB zur Verkehrssicherung des gefährlichen Nachbargrundstücks Verpflichteten vor. Zwar zeigt die Tatsache, dass Verkehrspflichten als selbständig einklagbare Pflichten lediglich in den §§ 907, 908 BGB geregelt sind, dass die Gesetzessystematik grundsätzlich einen Schwerpunkt auf den repressiven Ausgleich von Schäden legt. Allerdings ergibt sich aus dem Zusammenspiel zwischen dem gesetzlich normierten Fall einer Haftung für eine Verkehrspflichtverletzung in § 836 Abs. 1 BGB und einem korrespondierenden gesetzlichen vorbeugenden Abwehranspruch auch die Intention des Gesetzgebers, dass Verkehrspflichten unter bestimmten Voraussetzungen präventiv einklagbar sein sollen.¹⁷⁶² Betrachtet man die Voraussetzungen des vorbeugenden Abwehranspruchs aus § 908 BGB, so steht ein Individualanspruch nicht jedem zu, der mit einiger Wahrscheinlichkeit Opfer einer nach § 836 BGB Schadensersatzpflichtigen unerlaubten Handlung werden könnte, sondern nur dem Nachbarn. Während die dem Haftungstatbestand des § 836 BGB zugrundeliegende Verkehrspflicht jedermann schützt, kann nicht jedermann die Einhaltung der Verkehrspflicht verlangen und einklagen.¹⁷⁶³ Insoweit lassen sich die hinreichende Konkretisierung der Gefahr und die Unausweichlichkeit der Gefahr, als Voraussetzungen für die Individualisierung des Anspruchs ausmachen.¹⁷⁶⁴ Ein Individualanspruch auf Einhaltung einer Verkehrspflicht erfordert folglich, dass sich die Bedrohung durch eine unterlassene Sicherungsmaßnahme so sehr konkretisiert, dass sie qualitativ mit einer drohenden Beeinträchtigung durch ein aktives Handeln vergleichbar ist.¹⁷⁶⁵ Dann aber kann grundsätzlich jede Verkehrspflicht in eine selbständig einklagbare Pflicht umschlagen.¹⁷⁶⁶

1762 v. Bar, *Karlsruher Forum* 1983, S. 80 (84); Beck, Die präventive Durchsetzung der Rückrufpflicht, S. 100 f.

1763 Grundlegend v. Bar, *Karlsruher Forum* 1983, S. 80 (85).

1764 Grundlegend v. Bar, *Karlsruher Forum* 1983, S. 80 (84 f.); dem folgend Wagner, in: MüKo, BGB, Vor § 823, Rn. 44; Hager, in: Staudinger, BGB, Vor § 823, Rn. 64; Beck, Die präventive Durchsetzung der Rückrufpflicht, S. 101 ff.; Schmidt, Produktrückruf und Regress, S. 129 ff.; Bodewig, Der Rückruf fehlerhafter Produkte, S. 349.

1765 Dazu Bodewig, Der Rückruf fehlerhafter Produkte, S. 348 f.; Beck, Die präventive Durchsetzung der Rückrufpflicht, S. 94, 101.

1766 So schon v. Bar, *Karlsruher Forum* 1983, S. 80 (84); mittlerweile einhellige Meinung, vgl. Wagner, in: MüKo, BGB, Vor § 823, Rn. 44; Hager, in: Staudinger, BGB, Vor § 823, Rn. 64; Beck, Die präventive Durchsetzung der Rückrufpflicht, S. 101.

bb) Tatbestandsmäßigkeit des Unterlassungsanspruchs

Vorangestellt sei, dass ein individuell einklagbarer Anspruch nur dort in Betracht kommt, wo auch eine entsprechende Pflicht besteht. Denn ein Unterlassungsanspruch nach § 1004 Abs. 2 BGB ist nur gegeben, wenn der Betroffene nicht zur Duldung der Störung verpflichtet ist. Nicht zur Duldung verpflichtet ist der Betroffene, wenn die drohende Beeinträchtigung rechtswidrig ist. Rechtswidrig kann eine durch Untätigkeit drohende Beeinträchtigung aber nur sein, wenn eine entsprechende Handlungspflicht besteht.¹⁷⁶⁷

(1) Konkrete Gefahr

Droht erstmalig eine Beeinträchtigung, verlangt der vorbeugende Unterlassungsanspruch eine konkrete, unmittelbar bevorstehende und ernstliche Gefahr.¹⁷⁶⁸ Eine solche Konkretisierung einer Gefahr ist jedoch in Bezug auf gefährliche Produkte zwar nicht inhaltlich, wohl aber personell problematisch.¹⁷⁶⁹

α) Inhaltliche Konkretisierung

Ein Konstruktionsfehler haftet jedem Produkt einer Serie an, sodass auch jedes Produkt als gefährlich einzustufen ist.¹⁷⁷⁰ Dass sich die Gefahr auch erst nach langer Benutzungsdauer verwirklichen mag, lässt die Konkretheit der Gefahr nicht entfallen, da es jederzeit zu einer Beeinträchtigung kommen kann.¹⁷⁷¹ Ein Fabrikationsfehler betrifft dagegen nur einzelnen Exemplaren einer Serie, weshalb es nicht immer möglich sein wird, ein konkretes Produkt als fehlerhaft und gefährlich zu identifizieren, sodass

1767 Zum Ganzen *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 349; *Beck*, Die präventive Durchsetzung der Rückruffpflicht, S. 120 f.

1768 Vgl. nur *Wellenhofer*, Sachenrecht, § 24, Rn. 34; *Fritzsche*, in: BeckOK, BGB, § 1004, Rn. 95 f. m.w.N.

1769 *Schmidt*, Produktrückruf und Regress, S. 130; *Tamme*, Rückrufkosten, S. 257; in der Sache findet sich diese Differenzierung auch bei *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 358 ff.

1770 *Schmidt*, Produktrückruf und Regress, S. 131.

1771 *Schmidt*, Produktrückruf und Regress, S. 129; zurückhaltender *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 361.

häufig nur ein Gefahrenverdacht gegeben sein wird.¹⁷⁷² Damit kann inhaltlich bei einem Fabrikationsfehler mit Blick auf die Eintrittswahrscheinlichkeit das Vorliegen einer konkreten Gefahr in Zweifel gezogen werden.¹⁷⁷³ Da Fabrikationsfehler bei Software und damit für die Zugänglichkeit von Sicherheitsupdates kaum eine Rolle spielen, soll hier aber nicht näher darauf eingegangen werden.

β) Personelle Konkretisierung

Um von einer konkreten Gefahr sprechen zu können muss die Gefahr folglich ihrer Eigenart nach einer von vornherein feststehenden Person drohen und der Bezugspunkt der Gefahr damit in personeller Hinsicht individualisiert sein.¹⁷⁷⁴ In Abgrenzung zur bloß abstrakten Gefährdung und in Anlehnung an das Nachbarschaftsbeispiel des § 908 BGB muss eine gewisse Nähe¹⁷⁷⁵ zwischen der Person und dem gefährdenden Produkt bestehen, sodass gerade bei dieser Person eine erhöhte Wahrscheinlichkeit¹⁷⁷⁶ einer Beeinträchtigung durch das gefährdende Produkt besteht und die Verwirklichung der Gefahr bei ihr nicht vom Zufall¹⁷⁷⁷ abhängt. Anders als beim Produktnutzer, dessen Rechtsgüter regelmäßig mit dem gefährlichen Produkt in Berührung kommen, wird diese individualisierte Gefahr bei allen anderen Personen, die auf irgendeine Weise zu irgendeinem Zeitpunkt an irgendeinem Ort zufällig mit dem Produkt in Kontakt kommen in der Regel nicht gegeben sein.¹⁷⁷⁸ Die Einräumung eines Beseitigungsanspruchs auch gegenüber den innocent bystandern würde damit nicht der Abwehr einer konkreten Gefahr, sondern entgegen dem Sinn und Zweck eines Individualanspruchs der allgemeinen Sicherheit im Sinne einer Popularklage

1772 Huber, Rechtsfragen des Produktrückrufs, S. 85; Schmidt, Produktrückruf und Regress, S. 131.

1773 Ablehnend daher Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungs-handbuch, § 39, Rn. 18; tendenziell auch Bodewig, Der Rückruf fehlerhafter Produkte, S. 362.

1774 v. Bar, Karlsruher Forum 1983, S. 80 (85).

1775 Schmidt, Produktrückruf und Regress, S. 130.

1776 Beck, Die präventive Durchsetzung der Rückrufpflicht, S. 118.

1777 Bodewig, Der Rückruf fehlerhafter Produkte, S. 359.

1778 So auch Schmidt, Produktrückruf und Regress, S. 130; Beck, Die präventive Durchsetzung der Rückrufpflicht, S. 118 f.; Bodewig, Der Rückruf fehlerhafter Produkte, S. 359.

dienen.¹⁷⁷⁹ Anderes kann nur dann gelten, wenn sich die Gefahr auch gegenüber einem unbeteiligten Dritten hinreichend konkretisiert, er also regelmäßig mit dem Produkt in Kontakt kommt und einem Produktnutzer vergleichbar ist.¹⁷⁸⁰

(2) Hersteller als Störer

Ferner ist die Störereigenschaft des Herstellers problematisch. Denn die eigentliche Gefährdung geht erst durch die (fortgesetzte) Verwendung des Produkts und daher vom Produktnutzer aus, der die Beeinträchtigung durch die Aufgabe der weiteren Nutzung beenden könnte.¹⁷⁸¹ Der Hersteller dagegen hat die Beeinträchtigung nur indirekt durch das Unterlassen des Rückrufs des Produktes verursacht.¹⁷⁸²

α) Allgemeine Erwägungen

Abhängig davon, ob der Schwerpunkt des unterlassenen Rückrufs darin gesehen wird, dass der Hersteller das Produkt entgegen einer entsprechenden Handlungspflicht in einem gefährlichen Zustand belassen hat, oder ob in dieser Verkehrspflichtverletzung die Veranlassung des Produktnutzers zur weiteren Verwendung des Produkts gesehen wird, kommt die Zustandsstörereigenschaft oder die mittelbare Handlungsstörereigenschaft in Betracht.¹⁷⁸³

1779 Bodewig, Der Rückruf fehlerhafter Produkte, S. 359; Pieper, BB 1991, 985 (990); Beck, Die präventive Durchsetzung der Rückruffpflicht, S. 119; v. Bar, Karlsruher Forum 1983, S. 80 (80) wirft die Frage auf, ob sich ein Verbraucher „zum Produktsicherheitspolizisten aufspielen“ kann.

1780 Bodewig, Der Rückruf fehlerhafter Produkte, S. 359 und Beck, Die präventive Durchsetzung der Rückruffpflicht, S. 119 jeweils mit Beispielen.

1781 Vgl. Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 39, Rn. 14; Huber, Rechtsfragen des Produktrückrufs, S. 88; Beck, Die präventive Durchsetzung der Rückruffpflicht, S. 122.

1782 Prägnant Beck, Die präventive Durchsetzung der Rückruffpflicht, S. 123.

1783 Allgemein Herrler, in: Grüneberg, BGB, § 1004, Rn. 18 f. und Fritzsche, in: BeckOK, BGB, § 1004, Rn. 19; Beck, Die präventive Durchsetzung der Rückruffpflicht, S. 123 geht vom mittelbaren Handlungsstörer aus; Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 39, Rn. 14 spricht vom „Untätigkeitsstörer“.

In beiden Fällen ist eine besondere Zurechnung dergestalt erforderlich, dass die Beeinträchtigung adäquat kausal verursacht wurde und hätte verhindert werden können.¹⁷⁸⁴ Hiervon ist aber gerade bei der Verletzung einer bestehenden Verkehrspflicht – hier zur Durchführung des Rückrufs – auszugehen. Insbesondere verliert der Hersteller mit dem Inverkehrbringen nicht die Einwirkungsmöglichkeit auf das Produkt, sondern behält diese gerade durch die Möglichkeit des Rückrufs – andernfalls bestünde schon gar keine entsprechende Verkehrspflicht.¹⁷⁸⁵

Dem § 908 BGB lässt sich der Gedanke entnehmen, dass ein individueller Abwehranspruch gerade deswegen besteht, weil für den Grundstücksnachbarn trotz Gefahrenkenntnis kraft seiner besonderen Nähe zum Gefahrenherd gerade keine Möglichkeit des Ausweichens besteht und er daher zur eigenverantwortlichen Schadensvorsorge mit zumutbaren Mitteln nicht in der Lage ist.¹⁷⁸⁶ Fehlt dem Betroffenen eine Ausweichmöglichkeit, kann er der Gefahr nur entgehen, wenn ihm vorbeugender Rechtsschutz gewährt wird, so dass für diesen Fall die Umwandlung einer unselbstständigen Pflicht in einen individuell einklagbaren Anspruch gerechtfertigt ist.¹⁷⁸⁷

β) Bedeutung für die individuellen Gefahrenabwehransprüche

Hinsichtlich der Bedeutung für die Frage nach individuellen Rückruf- bzw. Updateansprüchen ist nun die richtige Perspektive einzunehmen.

Kommt es zu einer Gefährdung auch unbeteiligter Dritter, kann der Produktnutzer keine eigenen Ansprüche geltend machen. Ihm gegenüber ist die Gefahr zwar hinreichend konkret, allerdings fehlt ihm zur Geltendmachung eines individuellen Anspruchs ein eigenes Schutzbedürfnis. Denn soweit Rückruffpflichten unter Berücksichtigung des Hinwegsetzens des Produktnutzers über eine Warnung angenommen werden, geschieht dies ausschließlich zu Gunsten der unbeteiligten Dritten wegen deren geringeren Möglichkeiten der Gefahrenkenntnis und -vermeidung. Auf dieses Schutzbedürfnis Dritter kann sich der Produktnutzer bei der Durchsetzung

1784 Vgl. nur Herrler, in: Grüneberg, BGB, § 1004, Rn. 18 f.

1785 Huber, Rechtsfragen des Produktrückrufs, S. 90; Beck, Die präventive Durchsetzung der Rückruffpflicht, S. 123 f.; anders wohl Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 39, Rn. 16.

1786 Grundlegend v. Bar, Karlsruher Forum 1983, S. 80 (85).

1787 v. Bar, Karlsruher Forum 1983, S. 80 (85); Beck, Die präventive Durchsetzung der Rückruffpflicht, S. 103.

entsprechender Rückruffpflichten aber nicht stützen.¹⁷⁸⁸ Die Gefährdung eigener Rechtsgüter kann er aber ohne Weiteres dadurch vermeiden, dass er den weiteren Gebrauch des Produkts einstellt.¹⁷⁸⁹ Mit anderen Worten ist der Nutzer sich selbst gegenüber in der Lage, die Gefahr durch Selbstschutzmaßnahmen auszuschließen.¹⁷⁹⁰ Insoweit kann niemand „von einem Hersteller die Reparatur oder den Austausch eines fehlerhaften Produkts mit dem Argument fordern, man werde sich andernfalls über die Warnung hinwegsetzen und trotz erkannter Gefahr den Gebrauch des Produkts fortsetzen“.¹⁷⁹¹ Dies gilt auch, wenn das Hinwegsetzen über die Warnung wegen der Unzumutbarkeit der Nichtbenutzung als naheliegend anzusehen ist. Auf den ersten Blick mag dabei zwar die Zumutbarkeit der Gefahrensteuerung bei der Frage nach der Gefahrabwendungspflicht anders beurteilt werden als bei der Frage nach einem entsprechenden individuellen Anspruch.¹⁷⁹² Die Unzumutbarkeit der Gefahrenbeherrschung führt bei der Bestimmung der Pflichten des Herstellers jedoch nicht dazu, dass der gebotene Selbstschutz des Nutzers zurücktritt, sondern dazu, dass der Hersteller gegenüber Dritten verpflichtet bleibt. Andernfalls wäre konsequenterweise auch eine Gefahrabwendungspflicht des Herstellers zu Gunsten des Produktnutzers anzunehmen. Mit der Ablehnung einer entsprechenden Pflicht zu Gunsten des Nutzers wird inzident aber auch die Zumutbarkeit des Selbstschutzes bejaht. Lediglich in Bezug auf unbeteiligte Dritte wird das Kriterium der Unzumutbarkeit der Gefahrensteuerung herangezogen, um ein Hinwegsetzen über eine Warnung nachvollziehbar zu machen, nicht aber, um den eigenen Selbstschutz als unzumutbar anzusehen. Insoweit sind also unterschiedliche Perspektiven einzunehmen.¹⁷⁹³

Ein individuell einklagbarer Anspruch des Produktnutzers kommt nur dort in Betracht, wo eine Rückruffpflicht ihm selbst gegenüber besteht.¹⁷⁹⁴

1788 Zum Ganzen überzeugend *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 362.

1789 Ein hieraus resultierender Schaden wäre allein auf die Mangelhaftigkeit des Produkts bei Erwerb zurückzuführen und betrifft daher allein die enttäuschte Vertragserwartung, vgl. BGH, NJW 2009, 1080 (1083, Rn. 25).

1790 So speziell im Kontext von Updateansprüchen *Eichelberger*, in: Ebers et al. (Hg.), Künstliche Intelligenz und Robotik, S. 190.

1791 Prägnant *Wagner*, in: MüKo, BGB, § 823, Rn. 1128.

1792 Zum Gleichlauf *Beck*, Die präventive Durchsetzung der Rückruffpflicht, S. 120; *Schmidt*, Produktrückruf und Regress, S. 133; *Huber*, Rechtsfragen des Produktrückrufs, S. 90; im Grundsatz auch *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 350.

1793 So i.E. auch *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 362 ff.

1794 *Bodewig*, Der Rückruf fehlerhafter Produkte, S. 362 f.

Dies ist jedoch nur dann der Fall, wenn eine Warnung nicht ausreichend ist, um die Gefahr einzuschätzen und sich entsprechend zu verhalten. Dort aber, wo der Nutzer in der Lage ist, einen Gefahrenabwehranspruch ausreichend konkret zu formulieren und zu begründen (§ 253 Abs. 2 Nr. 2 ZPO), wird die Gefahrenkenntnis regelmäßig auch ausreichen, um Selbstschutzmaßnahmen zu ergreifen.¹⁷⁹⁵ Folglich entfallen spätestens mit der Geltendmachung des Anspruchs die Anspruchsvoraussetzungen.¹⁷⁹⁶

Eigene Ansprüche unbeteiligter Dritter scheiden dagegen in der Regel schon mangels hinreichender (personeller) Konkretisierung der Gefahr aus. Wenn sich eine Gefahr hinsichtlich eines unbeteiligten Dritten ausnahmsweise hinreichend konkretisiert, wird mit dieser stärkeren Konkretisierung der Gefahr in der Regel auch eine verbesserte Möglichkeit bestehen, der Gefahr auszuweichen.¹⁷⁹⁷ Daher wird man vergleichbar zum gefährdeten Produktnutzer argumentieren müssen. Lediglich in Fällen der konkreten Drittgefährdung, bei der keine zumutbare Ausweichmöglichkeit in Betracht kommt, wird ein individueller Anspruch des Dritten anzuerkennen sein.¹⁷⁹⁸

d) Fazit

Auch wenn der Hersteller in der Regel verpflichtet ist, dem Nutzer im Rahmen der Produktbeobachtung Updates zur Verfügung zu stellen, hat der Nutzer keinen subjektiven Anspruch auf den Erhalt von Updates.¹⁷⁹⁹ Die in Bezug auf Software ausgemachten Besonderheiten haben lediglich Einfluss auf die Pflichtenbestimmung beim Hersteller, nicht aber auf den Anspruch des Nutzers.¹⁸⁰⁰ Nur ganz ausnahmsweise können individuelle Ansprüche von hinreichend konkret Gefährdeten Dritten geltenden gemacht werden, die über keine zumutbare Ausweichmöglichkeit vor dem gefährlichen Produkt verfügen. Bleiben deliktsrechtlich geschuldete Sicherheitsupdates

1795 Bodewig, Der Rückruf fehlerhafter Produkte, S. 364.

1796 Speziell im Kontext von Updateansprüchen Raue, NJW 2017, 1841 (1845).

1797 So Bodewig, Der Rückruf fehlerhafter Produkte, S. 359 f.

1798 Beck, Die präventive Durchsetzung der Rückrufflicht, S. 119; Bodewig, Der Rückruf fehlerhafter Produkte, S. 360 hält solche Fallkonstellationen zumindest für denkbar; im Kontext von Updateansprüchen Eichelberger, in: Ebers et al. (Hg.), Künstliche Intelligenz und Robotik, S. 190.

1799 Ohne nähere Begründung auch Thöne, Autonome Systeme, S. 218.

1800 So auch Wittig, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, S. 245.

gleichwohl aus, schwebt stets das Damoklesschwert der Produkthaftung über dem Hersteller. Daneben dürfte es sich ein Hersteller aus Gründen des Wettbewerbs und der Reputation kaum leisten können, entsprechende Updates nicht bereitzustellen.

e) Bedeutung des Rechts auf Reparatur

Updateansprüche der Nutzer könnten sich aber künftig aus der am 30.07.2024 in Kraft getretenen und ab dem 31.07.2026 anzuwendenden Richtlinie zur Förderung der Reparatur von Waren (im Folgenden „Reparaturrichtlinie“; „Recht auf Reparatur“)¹⁸⁰¹ ergeben.

Das Recht auf Reparatur sieht in Art. 5 Abs. 1 vor, dass die Mitgliedsstaaten sicherstellen, dass der Hersteller außerhalb des Gewährleistungsrechts auf Verlangen des Verbrauchers Produkte repariert, die in Anhang II gelistet sind und für die ohnehin gesetzlichen Reparaturanforderungen (insbesondere aus dem Ökodesignrecht) bestehen und zwar in dem Umfang, in dem sie dort festgelegt sind. Während die Anforderungen an die Reparierbarkeit gewährleisten, dass die Produkte überhaupt reparierbar sind, soll das Recht auf Reparatur die Hersteller verpflichten, die Produkte auch zu reparieren (vgl. Erwägungsgrund (16) Reparaturrichtlinie). Durch diese Beschränkung wird sichergestellt, dass nur Waren, die aufgrund ihrer Konstruktion reparierbar sind (und sein müssen), Gegenstand der Reparaturverpflichtung sind und die Hersteller damit nicht übermäßig belastet werden (vgl. Erwägungsgrund (16) Reparaturrichtlinie).

So legt die Durchführungsverordnung (EU) 2023/1670 der Kommission zur Festlegung von Ökodesign-Anforderungen an Smartphones, Mobiltelefone, schnurlose Telefone und Slate-Tablets fest, dass Sicherheitsaktualisierungen spätestens vier Monate und Funktionsaktualisierungen spätestens sechs Monate nach der Veröffentlichung des Quellcodes durch den Betriebssystemhersteller oder nach dessen Freigabe kostenlos für alle Einheiten eines Produktmodells mit demselben Betriebssystem zugänglich gemacht werden müssen. Dies gilt für einen Mindestzeitraum von fünf Jahren ab dem Datum der Beendigung des Inverkehrbringens (Art. 3 i.V.m. Anh. II A, Nr. 1.1, Abs. 6, lit. a¹⁸⁰²). Damit trifft den Hersteller des Produkts aber keine originäre Updatepflicht. Er hat vielmehr ein freiwillig oder aufgrund

1801 Richtlinie (EU) 2024/1799.

1802 Der Anhang A gilt für Mobiltelefone, die keine Smartphones sind. Entsprechende Regelungen finden sich für Smartphones und Tablets.

gesetzlicher Verpflichtung (insoweit klarstellend Anh. II A, Nr. 1.1, Abs. 6, lit. a) zur Verfügung gestelltes Update für alle dafür infrage kommenden Produktmodelle zugänglich zu machen. Ein Gerätehersteller kann sich damit im Zeitraum von fünf Jahren nicht darauf zurückziehen, dass der Update-Support für ein bestimmtes Produktmodell eingestellt wird, wenn für dieses Updates technisch noch verfügbar sind. Die Frage unter welchen Voraussetzungen solche Updates aber originär zu entwickeln und bereitzustellen sind, wird nicht geregelt. Lediglich in diesem Umfang wird dem Nutzer dann über die Reparaturrichtlinie auch ein Anspruch gegen den Hersteller eingeräumt. Damit schafft das Recht auf Reparatur für diese Produktgruppen keinen originären Updateanspruch, sondern entsprechend den Ökodesignanforderungen nur einen Anspruch auf Teilhabe an bereits zur Verfügung gestellten und auch für das eigene Produktmodell geeigneter Updates.

Anders verhält es sich bei anderen durch Durchführungsverordnungen der Kommission geregelten Produktgruppen wie bei Kühlgeräten. Hier sieht die Durchführungsverordnung (EU) 2019/2024 der Kommission über Art. 3 in Anhang II Abs. 2 lit. a (1) vor, dass Software und Firmware, einschließlich Reset-Software zur Verfügung gestellt werden müssen.¹⁸⁰³ Dies hat nach Abs. 4 für einen Zeitraum von mindestens 10 Jahren zu geschehen. In diesem Umfang besteht folglich auch ein Recht auf Reparatur und ein entsprechender Updateanspruch.

Für die Frage, ob über das Recht auf Reparatur ein Updateanspruch für den Nutzer besteht, müssen folglich produktspezifisch die entsprechenden Ökodesignanforderungen betrachtet werden. Aktuell besten solche Ökodesignanforderungen aber nur für vereinzelte Produktgruppen, sodass künftig auch der Erlass weiterer Durchführungsverordnung durch die Kommission zu berücksichtigen sein wird.

IV. Fazit zu den smarten Reaktionspflichten des Herstellers

Bei Software und smarten Produkten wird die vorzunehmende Einzelfallbetrachtung regelmäßig zu einer Updateverpflichtung des Herstellers führen, da vielfach ein Hinwegsetzen über eine Warnung erwartet werden muss. Bei reiner Software folgt dies aus dem Verkennen des Gefahrenpotentials von Sicherheitslücken, bei smarten Produkten aus der unzumut-

¹⁸⁰³ Gleiches gilt bspw. nach der Durchführungsverordnung (EU) 2019/2023 der Kommission auch für Haushaltswaschmaschinen.

baren Gefahrensteuerung aufgrund der Abnahme der Gefahrensteuerungsmöglichkeiten des Nutzers bei gleichzeitig gesteigerten Einflussmöglichkeiten des Herstellers.

Bei der Ausgestaltung der Updatepflicht hat der Hersteller den Stufenbau der Reaktionspflichten zu beachten. Fehlt es an einer entsprechenden Einwilligung, stellt die das Bereitstellen eines Updates zur Behebung des Sicherheitsmangels die Grundmaßnahme und das Mittel der Wahl dar, um den Anforderungen des Produkthaftungsrechts zu genügen. Eine Zwangsaktualisierung kann nur unter bestimmten Umständen in Betracht gezogen werden, während die Deaktivierung des Produkts als letztes Mittel möglich ist.

Ab dem Geltungsbeginn der neuen GPSR am 13.12.2024 müssen Hersteller im Falle eines erforderlichen Rückrufs die Rechte des Verbrauchers auf Abhilfe berücksichtigen. Updates müssen kostenlos bereitgestellt werden. Daneben wird sich eine Pflicht zur kostenlosen Behebung von Schwachstellen durch Updates aus dem CRA ergeben. Außerdem sieht der Entwurf einer neuen Produkthaftungsrichtlinie vor, dass der Hersteller zur Vermeidung einer Haftung die Sicherheit des Produkts durch Updates aufrechterhalten muss.

Einen subjektiven Anspruch auf den Erhalt von Updates hat der Nutzer dagegen nicht. Individuelle Ansprüche können nur in Ausnahmefällen von hinreichend konkret gefährdeten Dritten geltend gemacht werden.

F. Dauer der Produktbeobachtungspflicht

Nachdem die Pflichten des Herstellers im Rahmen der Produktbeobachtungspflicht untersucht wurden, stellt sich abschließend noch die Frage, wie lange der Hersteller diesen Pflichten nachkommen muss. Mit anderen Worten geht es um die Dauer der Produktbeobachtungspflicht.

I. Fehlen eines zeitlich starren Rahmens

Dabei gibt es im Ausgangspunkt keinen zeitlichen Rahmen, nach dem die Produktbeobachtungspflicht jedenfalls endet.¹⁸⁰⁴ Bei der Produktbeobachtungspflicht handelt es sich schon um keinen der Verjährung unterliegenden Anspruch (§ 194 Abs. 1 BGB), sondern um eine der Gefahrenabwehr dienende Verkehrspflicht.¹⁸⁰⁵ An dem Ziel der Gefahrenabwehr muss sich die Produktbeobachtungspflicht auch in zeitlicher Hinsicht messen lassen. Die der Verjährung zugrundeliegenden Gedanken des Schuldnerschutzes, insbesondere nicht unbegrenzt Rückstellungen für Risiken aus Gefahren mit dem Inverkehrbringen von Produkten bilden zu müssen, sowie des Rechtsfriedens, können auf die Situation der Gefahrenabwehr nicht übertragen werden.¹⁸⁰⁶ Hier ist der Hersteller aufgrund seiner Sachnähe auch im Zeitablauf am ehesten in der Lage, mögliche vom Produkt ausgehende Gefahren zu erkennen und wirksam zu reagieren. Ferner ändert sich nichts an der Tatsache, dass der Hersteller mit der Inverkehrgabe eine potenzielle Gefahrenquelle geschaffen hat, für die ihn auch nach dem Inverkehrbringen die Verantwortung trifft.¹⁸⁰⁷

1804 Veltins, in: Moosmayer/Lösler (Hg.), Corporate Compliance, § 35, Rn. 18.

1805 Lediglich der sich aus der Verletzung der Produktbeobachtungspflicht ergebende Anspruch auf Schadensersatz oder Schmerzensgeld nach § 823 Abs. 1 BGB kann verjähren (§§ 195, 199 Abs. 1, 2 BGB), nicht aber die Produktbeobachtungspflicht selbst, vgl. Wagner, in: MüKo, BGB, § 823, Rn. 1109; Lenz, in: Lenz, Produkthaftung, § 3, Rn. 240.

1806 Tendenziell weniger restriktiv aber Lenz, in: Lenz, Produkthaftung, § 3, Rn. 240.

1807 Vgl. zu diesen Argumenten Lenz, in: Lenz, Produkthaftung, § 3, Rn. 238 f.

1. Abschwächung der Produktbeobachtungspflicht

Indes ist nicht zu verkennen, dass auch die Produktbeobachtungspflicht nur im Rahmen des Erforderlichen und Zumutbaren besteht. Nimmt daher die im Zusammenhang mit dem Produkt stehende Gefährdungslage mit der Zeit ab, etwa weil es sich in der Praxis als sicher bewährt hat, kann es zu einer Abschwächung der Produktbeobachtungspflicht kommen. Angesichts der wohl bei fast jedem Produkt denkbaren Langzeitschäden wird man jedoch kaum einmal ein völliges Ende der Produktbeobachtungspflicht annehmen können.¹⁸⁰⁸

2. Besonderheiten bei smarten Produkten

Im Hinblick auf Softwareprodukte ist aber zu beachten, dass die Wahrscheinlichkeit des Auftretens bisher unerkannter Sicherheitsmängel gerade nicht mit der Dauer des Einsatzes abnehmen wird. Die sicherheitskritischen Eigenschaften von Software werden vielmehr dazu führen, dass sicherheitsrelevante Produktgefahren mit der Zeit wieder zunehmen.¹⁸⁰⁹ Gerade Sicherheitslücken werden regelmäßig erst im Laufe der Zeit bekannt und Hackern gelingt es erst nach und nach, durch innovative Angriffstechniken Zugang zum System zu erlangen.¹⁸¹⁰ Daneben nehmen die Anzahl der mit dem Produkt vernetzten Geräte und die damit verbundenen potenziellen Wechselwirkungen während der Lebensdauer des Produkts ständig zu.¹⁸¹¹ Beim Einsatz von KI ist zudem zu berücksichtigen, dass es in jeder Phase der Nutzung zu Unberechenbarkeiten in Form von neuen, unerwarteten Reaktionen kommen kann.¹⁸¹² Ein fortlaufender Lernprozess verliert außerdem auch nach längerer Zeit nichts an seiner Gefährlichkeit und eine

1808 v. Bar, in: Lieb (Hg.), Produktverantwortung und Risikoakzeptanz, S. 29 (40); Voigt, in: BeckOGK, BGB, § 823, Rn. 677; Hager, in: Staudinger, BGB, § 823, Rn. F 21; Foerste, in: Foerste/Graf v. Westphalen (Hg.), Produkthaftungshandbuch, § 24, Rn. 386; Chibanguza, in: Buck-Heeb/Oppermann (Hg.), Automatisierte Systeme, S. 407 (413 f.); vgl. auch Art. 82 Abs. 2 MDR; a.A. LG Frankfurt a.M., NJW 1977, 1108, wonach sich die Produktbeobachtungspflicht auch bei Arzneimitteln bereits nach ein bis zwei Jahren auf Null reduzieren könne.

1809 Piovano/Schucht/Wiebe, Produktbeobachtung in der Digitalisierung, S. 74; und Sedlmaier, in: Kühne/Nack (Hg.), Connected Cars, S. 41.

1810 Vgl. A.II.2.

1811 Vgl. C.III.3.a).

1812 Haagen, Verantwortung für Künstliche Intelligenz, S. 258.

KI kann jederzeit fehlerhaft erlerntes Verhalten zeigen.¹⁸¹³ Eine Abschwächung der Produktbeobachtungspflicht bei Softwareprodukten scheint ausgehend von deren zeitloser Gefährlichkeit daher nicht angezeigt.

II. Differenzierung zwischen Beobachtung und Reaktion

Dies muss jedenfalls für die Produktbeobachtungspflicht i.e.S. gelten. Denn die Beobachtung des Produkts dient der vorgelagerten Gefahrenerkennung und ist Voraussetzung der Gefahrenabwehr. Bei einer über die Lebensdauer eines Softwareprodukts gleichbleibenden oder sich sogar erhöhenden Gefährlichkeit können die Maßnahmen zur Informationsgewinnung aber keine Abschwächung erfahren. Die Anforderungen an die Informationssammlung sind ohnehin bereits nach der individuellen Gefährlichkeit eines Produkts abgestuft, dort aber auch erforderlich, um den von Softwareprodukten ausgehenden latenten Unsicherheiten nach Inverkehrgabe gerecht zu werden. Den Hersteller nach einer gewissen Zeit aus seinen bei Softwareprodukten intensiveren Beobachtungspflichten zu entlassen, würde folglich mit einer erheblichen Gefahrerhöhung für den Nutzer einhergehen und diesen mit einer „tickenden Zeitbombe“ allein lassen.

1. Abschwächung der Rückrufpflicht zur Warnpflicht

Etwas anderes könnte allerdings für die Reaktionspflichten gelten.¹⁸¹⁴ Hier könnte sich die Rückrufpflicht im Laufe der Zeit zu einer bloßen Warnpflicht abschwächen.¹⁸¹⁵ Durch eine solche Abschwächung findet eine Verantwortungsüberlagerung auf den Nutzer statt, unter der zwar die Effektivität der Gefahrenabwehr leidet, diese aber nicht gänzlich in Frage stellt. Denn immerhin erfährt der Nutzer von der sicherheitskritischen Eigenschaft des Produkts und kann sein Handeln grundsätzlich darauf einstellen. Die Abschwächung zur bloßen Warnpflicht kann aber nicht daraus hergeleitet werden, dass der Hersteller andernfalls zu einer zeitlich nicht endenden sicherheitstechnischen Gewährleistung verpflichtet wäre

1813 Eichelberger, in: Ebers et al., (Hg.), Künstliche Intelligenz und Robotik, S. 187.

1814 Bereits herkömmlich plädiert Lenz, in: Lenz, Produkthaftung, § 3, Rn. 242 für eine Differenzierung.

1815 Vgl. Lenz, in: Lenz, Produkthaftung, § 3, Rn. 242; ferner Mayrhofer, Außervertragliche Haftung für fremde Autonomie, S. 318.

und der Nutzer hiervon systemwidrig profitieren würde.¹⁸¹⁶ Steht nämlich aus Erwägungen der effektiven Gefahrenabwehr fest, dass ein Rückruf erforderlich ist, ist es hinzunehmen, dass der Nutzer auch nach Ablauf der vertraglichen Gewährleistungsfristen in den Genuss eines (weiterhin) sicheren Produkts kommt.¹⁸¹⁷ Vielmehr darf nicht verkannt werden, dass sich die Zumutbarkeit einer Maßnahme neben der Gefährlichkeit auch nach dem vom Hersteller zu leistenden Sicherheitsaufwand bemisst. Es gilt daher zu untersuchen, ob es einen Punkt gibt, ab dem die Reaktionspflichten trotz der über die Lebensdauer eines Softwareprodukts gleichbleibenden oder sich sogar erhöhenden Gefährlichkeit hierzu nicht mehr im Verhältnis stehen.

2. Maßgeblicher Zeitpunkt der Abschwächung der Rückruffpflicht

a) Einstellung der Weiterentwicklung und des Vertriebs des Produkts

Zunächst könnte auf die Einstellung der Weiterentwicklung und des Vertriebs des Produkts mit dieser Software abgestellt werden. Denn muss ein Hersteller die Software mit Blick auf die Inverkehrgabe neuer Produkte nicht mehr ohnehin auf dem aktuellen Stand von Wissenschaft und Technik halten, könnte ihm die Entwicklung von Updates allein mit Blick auf die bereits im Verkehr befindlichen Produkte nicht mehr zumutbar sein.¹⁸¹⁸ Angesichts der Tatsache, dass Produkte zwangsläufig auch noch kurz vor Ende des Vertriebs dieser Produktlinie erworben werden und sich weiterhin eine weit verbreitete Nutzung dieser Produkte ergeben kann, wird dies allerdings dem berechtigten Sicherheitsbedürfnis der Allgemeinheit nicht gerecht.¹⁸¹⁹ Denn Dritte, zu deren Gunsten eine Updatepflicht des Herstellers besteht, müssten sich hinsichtlich dieser Produkte sofort darauf verlassen, dass der Nutzer eigenverantwortlich auf eine Warnung reagiert. Dass dies aber nicht erwartet werden kann, zeigt die Existenz der herstel-

1816 So aber *Dötsch*, Außervertragliche Haftung für KI, S. 264 und *Lenz*, in: *Lenz*, Produkthaftung, § 3, Rn. 240.

1817 So auch *Wagner*, in: *MüKo*, BGB, § 823, Rn. 1109.

1818 So *Wagner*, AcP 217 (2017), 707 (757); *Thöne*, Autonome Systeme, S. 218 f.; *Leupold/Wiesner*, in: *Leupold/Wiebe/Glossner* (Hg.), IT-Recht, Teil 9.6.4, Rn. 75; grundsätzlich auch *Grünvogel/Dörrenbächer*, ZVertriebsR 2019, 87 (89).

1819 Vgl. auch *Dötsch*, Außervertragliche Haftung für KI, S. 264; ohne nähere Begründung i.E. auch *Kipker/Walkusz*, DuD 2019, 513 (517).

lerseitigen Updateverpflichtung. Mit einer solchen Betrachtungsweise ginge ein erheblicher gesamtgesellschaftlicher Sicherheitsverlust einher. Auch wenn damit die Einstellung des Produktvertriebs nicht als Stichtag für die Reduktion der Reaktionspflicht herangezogen werden kann, lässt sich nicht leugnen, dass dadurch die Zumutbarkeit beeinflusst wird und der weitere Entwicklung von Updates dem Hersteller umso weniger zuzumuten ist, je länger er die Weiterentwicklung der Produktlinie eingestellt hat.¹⁸²⁰ Eine ewige Updatepflicht für jedes noch auf dem Markt befindliche Produkt wird es daher nicht geben können.¹⁸²¹ Dies muss umso mehr für isolierte Software gelten, die in der Cloud läuft und für die es daher keine physische Begrenzung der Lebensdauer gibt.¹⁸²²

b) Erwartete maximale Lebensdauer eines Produkts

Gerade vor dem Hintergrund der Rechtssicherheit wäre eine starre Frist zwar wünschenswert,¹⁸²³ diese würde allerdings unter Berücksichtigung der unterschiedlichen Lebensdauern von Produkten den Sicherheitsbedürfnissen nicht gerecht.¹⁸²⁴ Selbst im Vertragsrecht bestimmt sich die Aktualisierungspflicht gem. § 327f Abs. 1 S. 3 BGB unabhängig von der Verjährung der Gewährleistungsansprüche und losgelöst von starren Fristen nach der jeweiligen Verbrauchererwartung (Nr. 2) und kann insbesondere hinsichtlich Sicherheitsaktualisierungen über den Gewährleistungszeitraum hinaus gehen.¹⁸²⁵

Das Sicherheitsbedürfnis Dritter hängt maßgeblich davon ab, ob das Produkt noch in relevantem Ausmaß genutzt wird und sie daher mit dem gefährlichen Produkt in Kontakt kommen werden.¹⁸²⁶ Eine weiterhin weit

1820 Piovano/Schucht/Wiebe, Produktbeobachtung in der Digitalisierung, S. 74; Raue, NJW 2017, 1841 (1844).

1821 So i.E. allgemein zum Rückruf auch Lenz, in: Lenz, Produkthaftung, § 3, Rn. 242 ff.

1822 Vgl. dazu Eichelberger, in: Ebers et al., (Hg.), Künstliche Intelligenz und Robotik, S. 187; Sedlmaier, in: Kühne/Nack (Hg.), Connected Cars, S. 41.

1823 Lenz, in: Lenz, Produkthaftung, § 3, Rn. 240 ff. plädiert vor dem Hintergrund des Rechtsgedanken des § 13 ProdHaftG für eine Frist von 10 Jahren und will damit insbesondere Rechtssicherheit schaffen.

1824 Stöhr, PHi 2015, 206 (210).

1825 Vgl. Erwägungsgrund (47) S. 2 Digitale-Inhalte-RL; zurückhaltend indes Oechsler, NJW 2022, 2713 (2715).

1826 Hieran anknüpfend daher Wittbrodt, InTer 2020, 74 (79); als wichtigen Faktor sehen dies auch Raue, NJW 2017, 1841 (1844) und Piovano/Schucht/Wiebe, Produktbeobachtung in der Digitalisierung, S. 74.

verbreite Nutzung wird indes nach Ablauf der erwarteten maximalen Lebensdauer eines in Verkehr gegebenen Produkts nicht mehr gegeben sein. In Abwägung der Gefährlichkeit für Dritte und des Aufwands für den Hersteller scheint es daher sachgerecht, eine Reduktion der Updatepflicht auf eine bloße Warnpflicht nach Erreichen der erwarteten maximalen Lebensdauer eines Produkts anzunehmen.¹⁸²⁷ Gehen „Ausreißer“¹⁸²⁸ über diese erwartete maximale Lebensdauer hinaus, ist die geringere Effektivität einer Warnung bei der Gefahrenabwehr hinzunehmen, zumal ein Nutzer am Ende der Produktlebensdauer eher geneigt sein dürfte, das gefährliche Produkt eigenverantwortlich nicht mehr zu benutzen. Zur Bestimmung dieser erwarteten maximalen Lebensdauer wird man nicht umhinkommen, entsprechende Angaben bereits bei Inverkehrgabe des Produkts von den Herstellern zu fordern.¹⁸²⁹ Dadurch könnte ein Hersteller dann das Ende seiner Verantwortlichkeit aber willkürlich selbst bestimmen.¹⁸³⁰ Zwar darf es in der Tat nicht sein, dass der Hersteller sich einseitig von seinen produkthaftungsrechtlichen Pflichten befreien kann.¹⁸³¹ Allerdings geht es zum einen nicht um eine vollständige Freizeichnung von der Produktverantwortung nach dem Inverkehrbringen, sondern nur um eine Abschwächung im Rahmen der Zumutbarkeit von der Aktualisierungs- zur Warnpflicht.¹⁸³² Zum anderen wird sich die herstellerseitige Bestimmung der erwarteten maximalen Lebensdauer an den entsprechenden Erwartungen der Nutzer messen lassen müssen. Hier ist auch auf die regulierende Wirkung des Marktes zu vertrauen. Denn die angegebene maximale Lebensdauer der Produkte wird erheblichen Einfluss auf die Kaufentscheidung nehmen.¹⁸³³

1827 Schon bei herkömmlichen Produkten hinsichtlich des gänzlichen Endes der Produktbeobachtungspflicht auf den Lebenszyklus abstellend *Ackermann*, in: NK-ProdR, § 823 BGB, Rn. 120; für Software *Schmon*, IWRZ 2018, 254 (256); *Kipker/Walkusz*, DuD 2019, 513 (517); *Piovano/Schucht/Wiebe*, Produktbeobachtung in der Digitalisierung, S. 74; für die übliche durchschnittliche Produktnutzungsdauer *Schraeder*, DAR 2016, 242 (244) und *Dötsch*, Außervertragliche Haftung für KI, S. 264.

1828 In diesem Kontext *Lenz*, in: *Lenz*, Produkthaftung, § 3, Rn. 243.

1829 Bereits jetzt sieht Art. 55 Abs. 1 lit. b CSA vor, dass ein Hersteller, der (freiwillig) ein zertifiziertes IKT-Produkt anbieten will, Angaben über den Zeitraum machen muss, in dem cybersicherheitsbezogene Aktualisierungen angeboten werden.

1830 Krit. dazu allgemein *Dötsch*, Außervertragliche Haftung für KI, S. 265.

1831 *Spindler*, in: *Hornung/Schallbruch* (Hg.), IT-Sicherheitsrecht, § 11, Rn. 34.

1832 So wohl auch *Spindler*, in: *Hornung/Schallbruch* (Hg.), IT-Sicherheitsrecht, § 11, Rn. 34.

1833 So sieht auch Erwägungsgrund (33) der Richtlinie zur Stärkung der Verbraucher für den ökologischen Wandel (Richtlinie (EU) 2024/825) vor, dass Verbraucher

c) Fristen nach anderen Vorschriften

Diese Überlegungen dürften auch den Regelungen im CRA zu Grunde liegen. Insoweit sah der Kommissionsentwurf in Art. 10 Abs. 12 CRA noch eine Updatepflicht während der erwarteten Produktlebensdauer oder während eines Zeitraums von fünf Jahren ab dem Inverkehrbringen eines Produkts mit digitalen Elementen vor, je nachdem, welcher Zeitraum kürzer ist.¹⁸³⁴ Das Verhandlungsmandat des Rates (Nr. 11726/23) stellte dagegen ausschließlich auf die erwartete Lebensdauer des Produkts ab. Diese sollte von den Herstellern unter Berücksichtigung der vom Nutzer aufgrund der Funktionalität und des Verwendungszwecks erwarteten Nutzungsdauer und der darauf basierenden Erwartung von Sicherheitsupdates festgelegt werden.

Nach Abschluss der Trilog-Verhandlungen wird nun der sog. Unterstützungszeitraum maßgeblich sein. Dieser kombiniert einen starren Zeitrahmen mit eigenverantwortlichen Festlegungen der Hersteller. Nach Art. 13 Abs. 8 UAbs. 2 CRA haben die Hersteller den Unterstützungszeitraum jedenfalls im Ausgangspunkt ausgerichtet an der voraussichtlichen Nutzungsdauer des Produkts festzulegen. Nach Art. 13 Abs. 8 UAbs. 3 CRA muss der Unterstützungszeitraum aber mindestens fünf Jahre betragen. Eine Abweichung hiervon ist nur zulässig, wenn die voraussichtliche Nutzungsdauer des Produktes weniger als fünf Jahre beträgt. Diese kürzere Erwartung muss aber durch die Art des Produkts gerechtfertigt sein, vgl. Erwägungsgrund (61) CRA. So könnte bspw. die Lebensdauer einer App zur Ermittlung von Kontaktpersonen, die für den Einsatz während einer Pandemie vorgesehen ist, auf die Dauer der Pandemie begrenzt werden. Geht die voraussichtliche Nutzungsdauer über die fünf Jahre hinaus, hat der Hersteller seine Unterstützung entsprechend länger sicherzustellen, vgl. Erwägungsgrund (61) CRA. Bei der Ermittlung der voraussichtlichen Nutzungsdauer gibt der CRA den Herstellern eine Reihe von Kriterien an die Hand, die in einer verhältnismäßigen Weise zu berücksichtigen sind. Hierzu gehören insbesondere die Erwartungen vernünftiger Nutzer, die Art des Produkts, einschließlich seiner Zweckbestimmung, sowie die einschlä-

über den Mindestzeitraum zu informieren sind, für den der Hersteller sich verpflichtet, Softwareaktualisierungen zur Verfügung zu stellen, damit Verbraucher besser informierte Entscheidungen treffen können und um den Wettbewerb zwischen den Herstellern hinsichtlich der Haltbarkeit zu fördern. Die Regelungen der Richtlinie finden gem. Art. 4 Abs. 1 UAbs. 2 ab dem 27.09.2026 Anwendung.

1834 Krit. hierzu Kipker, MMR-Aktuell 2022, 452009.

gigen Rechtsvorschriften der Union zur Festlegung der Lebensdauer von Produkten mit digitalen Elementen zu berücksichtigen. Ferner können vergleichbare Produkte anderer Hersteller, die Verfügbarkeit der Betriebsumgebung sowie der Unterstützungszeitraum von Dritten bezogener integrierter Komponente berücksichtigt werden. Diesen Unterstützungszeitraum haben die Hersteller nach Art. 13 Abs. 19 UAbs. 1 CRA zum Zeitpunkt des Kaufs klar und verständlich anzugeben sowie nach Art. 13 Abs. 19 UAbs. 2 CRA – soweit möglich – dem Nutzer bei Erreichen des Endes des Unterstützungszeitraums eine entsprechende Meldung anzuzeigen. Um einem entsprechenden Marktversagen bei der Festlegung der Unterstützungszeiträume entgegenzuwirken, behält sich die Kommission in Art. 13 Abs. 8 UAbs. 4 CRA vor, im Wege von delegierten Rechtsakten Mindestunterstützungszeiträume für bestimmte Produktkategorien festzulegen.

Art. 17 Abs. 1 lit. a ProdHaftRL unterwirft Ansprüche grundsätzlich einer absoluten Ausschlussfrist von zehn Jahren ab dem Datum des Inverkehrbringens. Da der Hersteller nach diesem Zeitpunkt, ungeachtet einer eventuell noch bestehenden Kontrolle, nicht mehr haftbar gemacht werden kann, ist er auch nicht gehalten, Updates zur Verfügung zu stellen, um eine Haftung zu vermeiden. Führt ein Update zu einer wesentlichen Änderung¹⁸³⁵ des Produkts (und nur dann)¹⁸³⁶, beginnt die Frist nach Art. 17 Abs. 1 lit. b ProdHaftRL erst mit der entsprechenden Bereitstellung.

Die neue GPSR sieht für den Fall, dass ein Produkt zurückgerufen wird ausweislich des Erwägungsgrund (88) GPSR vor, dass es keine zeitliche Beschränkung für Abhilfemaßnahmen geben soll. Hat sich nach der hier vertretenen Auffassung aber die Rückrufflicht schon zur Warnpflicht abgeschwächt, stellt sich die Frage nach der Ausgestaltung des Rückrufs und damit nach den Abhilfemaßnahmen gar nicht mehr.

III. Fazit

Eine starre zeitliche Grenze kennt die an der Gefahrenabwehr orientierte Produktbeobachtungspflicht nicht. Da die sicherheitskritischen Eigenschaften von Software dazu führen, dass sicherheitsrelevante Produktgefahren mit der Zeit wieder zunehmen, ist auch bei der Annahme einer Abschwächung der Produktbeobachtungspflicht Zurückhaltung geboten. Indes ist der vom Hersteller zu leistende Sicherheitsaufwand durch die Zumutbar-

1835 Zum Begriff Art. 4 Nr. 18 ProdHaftRL.

1836 Vgl. Erwägungsgrund (58) ProdHaftRL.

keit der Maßnahme begrenzt. Daher erscheint es in Abwägung der Gefährlichkeit für Dritte und des Aufwands für den Hersteller sachgerecht, eine Reduktion der Updatepflicht auf eine bloße Warnpflicht nach Erreichen der erwarteten maximalen Lebensdauer eines Produkts anzunehmen.

G. Zusammenfassung

1. Die deliktische Produzentenhaftung und damit auch die Produktbeobachtungspflicht des Herstellers nach § 823 Abs. 1 BGB sind technikneutral ausgestaltet und finden daher auf Software und embedded Software Anwendung. Denn die Verantwortlichkeit des Herstellers knüpft – anders als das ProdHaftG – nicht an eine wie auch immer geartete Produktqualität, sondern allgemein an Verkehrssicherungspflichten und die geschaffene Gefahrenlage an.
2. Die Produktbeobachtungspflicht perpetuiert die Herstellerverantwortung für das Produkt über den Zeitpunkt des Inverkehrbringens hinaus. Über die Produktbeobachtungspflicht hat der Hersteller die Produktsicherheit seiner Produkte auch nach dem Inverkehrbringen kontinuierlich zu überwachen und gegebenenfalls Gefahrensteuerungsmaßnahmen zu ergreifen. Die Verantwortlichkeit des Herstellers über den Zeitpunkt der Inverkehrgabe hinaus lässt sich dabei nicht mit dem Inverkehrbringen des Produkts allein begründen. Vielmehr muss berücksichtigt werden, ob die vom Hersteller abverlangte Gefahrensteuerung noch in einem angemessenen Verhältnis zu dem von ihm gesetzten Risiko bei Inverkehrgabe steht.
 - a) Dies ist jedenfalls dann der Fall, wenn das Produkt bereits bei seinem Inverkehrbringen fehlerhaft war oder ein Entwicklungsfehler vorliegt. Denn ohne dass es auf eine Pflichtverletzung des Herstellers ankäme, entsprach das Produkt bereits bei Inverkehrgabe nicht den berechtigten Sicherheitserwartungen. Aufgrund der objektiven Fehlerhaftigkeit des Produkts, geht von ihm eine Gefahr aus, die auf den Herstellungsprozess zurückzuführen ist. Als Inhaber der Bestimmungsgewalt während des Produktionsvorgangs fällt die Fehlerhaftigkeit in den Verantwortungsbereich des Herstellers. Die Verantwortlichkeit des Herstellers rührt aus der von ihm geschaffenen andauernden Gefahrenquelle, auch wenn das Sicherheitsdefizit erst in der Nutzungsphase erkennbar wird.
 - b) Bei einer Entwicklungslücke haben die Produkte indes bei Inverkehrgabe den historischen Sicherheitserwartungen entsprochen. Gewährleistet ein Produkt die Basissicherheit, darf es trotz nicht (zumutbar) vermeidbarer Restgefahren in den Verkehr gebracht werden. Wird das Produkt nun aber aufgrund der Weiterentwicklung von Wis-

senschaft und Technik den gehobeneren Sicherheitsstandards nicht mehr gerecht, ist gleichwohl die Verantwortung des Herstellers nach der Inverkehrgabe angesprochen. Auch den Hersteller, der eine Gefahr zunächst nicht abwenden konnte, das Produkt aber trotz Kenntnis der unvermeidbaren Gefährlichkeit in den Verkehr gebracht hat, müssen nach dem Inverkehrbringen latente Pflichten treffen. Insoweit haftet dem Produkt eine inhärente Gefahr an, die auf den Herstellungsprozess zurückzuführen ist und die damit aus der Sphäre des Herstellers stammt. Die Fortschreibung der Verantwortung für das Produkt knüpft als Kehrseite an das Inverkehrbringen einer unbeherrschbaren Gefahrenquelle an.

- c) Soll dagegen keine bereits bei der Inverkehrgabe vorliegende Sicherheitslücke geschlossen werden, sondern kommt es infolge der Weiterentwicklung des Standes von Wissenschaft und Technik zu Produktverbesserungen (Produktalterung), fehlt es mangels entsprechendem Gefahrenlevels bei Inverkehrgabe an einem Zurechnungsgrund zur Begründung einer Verkehrspflicht des Herstellers für die Phase nach der Inverkehrgabe.
3. Gerade diese Phase nach dem Inverkehrbringen gewinnt bei Software und smarten Produkten an Bedeutung, da moderne Software hochkomplex und deshalb fehleranfällig ist. So führt die Vernetzung mit anderen Systemen zu nicht vollumfänglich abschätzbaren Kombinationsrisiken und Fehlfunktionen ergeben sich aus dem Zusammenspiel der einzelnen Systeme. Zudem werden Sicherheitslücken der Software oft erst im Laufe der Zeit bekannt und Bedrohungslagen ändern sich fortlaufend. Hinzu kommt, dass die Entscheidungen autonomer Systeme ex ante nicht exakt vorhersehbar sind. Daher ist eine abschließend sichere Entwicklung am Reißbrett kaum möglich. Im Einzelnen:
- a) Bei der Tatsache, dass Software nie gänzlich fehlerfrei ist, handelt es sich zunächst um eine technische Kategorie. Die Erwartung des Nutzers geht indes dahin, dass der Hersteller diejenigen Qualitätssicherungsmaßnahmen ergreift, die dem Stand von Wissenschaft und Technik entsprechen. Sofern die Basissicherheit erreicht wird, schuldet der Hersteller aber nur solche Sicherheitsvorkehrungen, die ihm auch zumutbar sind. Aufgrund der technisch erhöhten Fehleranfälligkeit bei der Softwareentwicklung befindet sich gleichwohl eine hohe Dunkelziffer an produkthaftungsrechtlich fehlerhaften Produkten im Verkehr, die wegen Programmierfehlern die Basissicherheit nicht gewährleisten. Andere Produkte sind mit Entwicklungslücken

behaftet. Sie gewährleisten zwar die Basissicherheit und sind im produkthaftungsrechtlichen Sinne nicht fehlerhaft, weisen jedoch Programmierfehler auf, deren Behebung aufgrund der kostenintensiven Testläufe zum Aufsuchen von Fehlern bei der Inverkehrgabe nicht zumutbar war. Daneben sind haftungsausschließende Entwicklungsfehler denkbar, bei denen der Programmierfehler auch objektiv erst nach der Inverkehrgabe erkennbar wird.

Über die Produktbeobachtungspflicht wird der Hersteller hierfür aber über den Zeitpunkt der Inverkehrgabe hinaus in Verantwortung genommen.

- b) Auch Anforderungen an die IT-Sicherheit sind vom produkthaftungsrechtlichen Fehlerbegriff umfasst, sodass der Hersteller die digitale Resilienz seiner Softwareprodukte gewährleisten muss. Traditionell bezieht sich die Produktsicherheit zwar auf den Schutz vor produktbezogenen Gefahren (safety), während IT-Sicherheit den Schutz vor unbefugten Eingriffen auf das Produkt bedeutet (security). Spätestens mit der Implementierung von Software in physische Produkte beschränken sich Gefährdungen durch das Ausnutzen von Sicherheitslücken nicht mehr auf die Schutzgüter der security. Vielmehr kann ein Zugriff von außen Integritätsschäden und damit wiederum safety-relevante Gefahren nach sich ziehen, die klassischerweise dem Rechtsgüterschutz des Produkthaftungsrechts unterfallen. Dass es sich bei einem Hackerangriff um eine bewusste und vorsätzliche Schädigung eines Dritten handelt, schließt die Verantwortlichkeit des Herstellers dabei nicht aus. Entsprechend den allgemeinen Erwägungen der Kausalitätslehre und des Deliktsrechts besteht bei einer bei Inverkehrgabe vorhandenen Sicherheitslücke, die ein mögliches Einfallstor für Hacker darstellt, eine latente und vom Hersteller zu verantwortende besondere Gefahrenlage, die eine schädigende Handlung Dritter erst ermöglicht oder zumindest wesentlich erleichtert. Damit schließt das vorsätzliche Dazwischentreten Dritter die Zurechnung nicht aus. Gleichwohl besteht keine absolute Haftung für Schäden, die durch Angriffe von Hackern verursacht werden. Geschuldet ist nach allgemeinen Grundsätzen die Sorgfalt im Rahmen des Möglichen und Zumutbaren.

Da Sicherheitslücken nichts anderes als ausnutzbare Softwarefehler sind, gelten hinsichtlich der Produktbeobachtungspflicht die dort aufgestellten Grundsätze. Werden indes neue Angriffsmethoden entwickelt, die bei Inverkehrgabe noch nicht absehbar waren – z.B.

durch neue kryptographische Methoden, die eine zunächst sichere Verschlüsselung angreifbar machen - entspricht dies der Produktalterung, welche keine nachträgliche Verantwortung des Herstellers auslöst.

- c) Hinsichtlich der Gefahren, die sich aus der Vernetzung einzelner Systeme ergeben, trägt der Hersteller bei der Verfolgung eines geschlossenen Ansatzes die volle Verantwortung hinsichtlich des Auftretens von Kombinationsrisiken. Bezieht der Hersteller eines IoT-Geräts Komponenten (insbesondere Software) von einem Zulieferer, ist er dafür verantwortlich, dass sich auch aus der Kombination der für sich genommen fehlerfreien Komponenten keine Gefahren ergeben. Denn die Systemkonzeption und die Sicherheitsarchitektur lässt sich insgesamt auf den Hersteller zurückführen. Die Abstimmung und die Zuverlässigkeit der einzelnen Komponenten, insbesondere auch deren Wechselwirkungen unterliegen allein seiner Herrschaftssphäre. Ähnlich verhält es sich beim Vorhalten eines eigenen App-Stores, über den Drittanbieter ihre Apps bereitstellen. Hier kann der Hersteller selbst bestimmen, welche Drittanbieter ihre Apps bereitstellen dürfen. Damit behält er die Kontrolle über die verfügbaren Apps und ist in der Lage, Sicherheitsstandards durchzusetzen. Darauf vertraut auch der Nutzer. Bei einem offenen System hält der Hersteller dagegen lediglich die Schnittstelle oder den Zugang zu einem App-Store eines großen Anbieters vor und öffnet somit das System und lässt Produktergänzungen durch den Nutzer oder Dritte zu. 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. Hier trifft den Hersteller nur die Produktbeobachtungspflicht entsprechend der Grundsätze der Honda-Entscheidung für allgemeingebräuchliches Zubehör.

Falsche Daten, die das IoT-Gerät bezieht und auf die es angewiesen ist, fallen dagegen im Ausgangspunkt auch bei geschlossenen Systemen und bestehender Geschäftsbeziehung zwischen dem Hersteller und dem Daten-Zulieferer in den alleinigen Verantwortungsbereich des Zulieferers. Da das IoT-Produkt fortlaufend mit Daten beliefert wird und diese selbständig und in Echtzeit vom Gerät verarbeitet und umgesetzt werden, ist dem Hersteller eine auch stichprobenartige Überprüfung der Daten – anders als bei herkömmlichen Zuliefererteilen – vor der Verarbeitung nicht möglich. Dieses Defizit an Kon-

trollmöglichkeit der Daten im Vorfeld muss durch eine sorgfältige Auswahl des Informationsanbieters im Rahmen der herstellerseitigen Organisations- und Kontrollpflichten ausgeglichen werden. Weiter wird die Stichprobenkontrolle nachgelagert stattfinden müssen und kann Reaktionspflichten nach sich ziehen. Bei offenen Systemen dagegen schuldet der Hersteller keine Produktbeobachtung hinsichtlich dieser fehlervermittelnden Gefahren. Die Honda-Entscheidung betrifft lediglich Kombinationsrisiken und ist auf Fehler im alleinigen Verantwortungsbereich des Zubehörherstellers bzw. des Informationsanbieters nicht übertragbar.

- d) Entwickelt ein autonomes System trotz einer Programmierung und eines Trainings, das dem Stand von Wissenschaft und Technik entsprach, eine schädigende Verhaltensweise nach der Inverkehrgabe, handelt es sich beim so verstandenen Autonomierisiko um eine Entwicklungslücke. Der Hersteller wird dann aber über die Produktbeobachtungspflicht auch für das Autonomierisiko in Verantwortung genommen.
4. Bei der Erfüllung der Produktbeobachtungspflicht hat der Hersteller die Möglichkeiten, die sich durch die Digitalisierung bieten, auch zu nutzen. Denn die Produktbeobachtungspflicht als Verkehrspflicht muss sich auch am Stand der Wissenschaft und Technik ausrichten.
5. Im Rahmen der Produktbeobachtung i.e.S. führt die zunehmende Datenverfügbarkeit und Datenkenntnis auch zu einer Ausdehnung der Verantwortung des Herstellers.
 - a) Der Hersteller hat seine Produktbeobachtung auch auf zugängliche Informationen über sicherheitskritische Eigenschaften seines Produkts im Internet zu erstrecken. Dies muss zunächst dort gelten, wo den Hersteller die Information auf einer unternehmenseigenen Internetseite oder auf externen Seiten auf einem vom Hersteller eingerichteten Unternehmensprofil erreicht. Unabhängig vom Kommunikationsweg muss der Hersteller alle Informationen, die ihn erreichen, auch auswerten. Daneben hat der Hersteller grundsätzlich auch sicherzustellen, dass er Meldungen über Produktgefahren auf sonstigen Social-Media-Kanälen wahrnimmt. Hier führen automatisierte Prozesse und KI-gestützte Big Data-Auswertungen sowie die Möglichkeit der Auslagerungen an externe Dienstleister zu einer Verschiebung der Kriterien der Erforderlichkeit und Zumutbarkeit zu Lasten des Herstellers. In einer Zeit, in der Unternehmen aus Marketinggründen unermüdlich Daten über den Nutzer und sein Nutzungsverhalten

sammeln, ist ihnen auch ein Social-Media-Monitoring hinsichtlich sich abzeichnender Produktgefahren zumutbar. Allerdings ist im Rahmen eines Produkthaftungsprozess auf die Trennung zwischen dem Bestehen der Produktbeobachtungspflicht und deren schuldhafter Verletzung zu achten. So können auch beim Social-Media-Monitoring trotz des Ergreifens aller zumutbaren Sicherheitsvorkehrungen einzelne Produktinformationen unerfasst bleiben, ohne dass damit gleich ein Sorgfaltsverstoß einherginge.

- b) Außerdem hat der Hersteller die sensorisch von seinem Produkt erhobenen und an ihn übermittelten Daten auszuwerten. Insoweit kann an die Grundsätze der passiven Produktbeobachtung angeknüpft werden. Wiederum kann der Kommunikationsweg keinen Unterschied machen und der Kenntnisstand des Herstellers ist als produktbeobachtungsrechtliche Quelle der auszuwertenden Informationen anzusehen.

Weiter muss der Hersteller die vom Produkt generierten Daten auch erheben und sich übermitteln lassen. Für den Hersteller bedeutet dies ein aktives Erschließen neuer, bisher nicht vorhandener Erkenntnisquellen und geht über die Informationsbeschaffung aus öffentlich zugänglichen Quellen hinaus. Allerdings sieht § 6 Abs. 3 S. 1 Nr. 1 ProdSG bereits jetzt eine Pflicht zur Durchführung von Stichproben vor. Außerdem hat die Rechtsprechung über die Durchführung von Stichproben hinaus gerade bei Neuentwicklungen eine Verpflichtung des Herstellers angenommen, auch nach der Inverkehrgabe mögliche Gefahren und neue wissenschaftliche Erkenntnisse über das Produkt zu erforschen. Betrachtet man die bei smarten Produkten gemachten Unsicherheiten nach der Inverkehrgabe, lässt sich durchaus eine Parallele zum diffusen Gefahrenverdacht bei Neuentwicklungen ziehen. Daneben rechtfertigt das große Potential der Sensor-Datenerhebung, insbesondere die Möglichkeit für den Nutzer versteckte, weil noch nicht zu Tage getretene Produktfehler zu identifizieren und dadurch Produktfehler noch vor der ersten Schadensverursachung zu erkennen, eine Weiterentwicklung hin zu einer „aktivistischen“ Produktbeobachtungspflicht. Ausgehend von der großen Flut an dadurch generierten Daten kann die Reichweite und konkrete Ausgestaltung dieser Pflicht aber nur im Einzelfall unter der Berücksichtigung von Zumutbarkeitsgesichtspunkten bestimmt werden. Insbesondere der selbständigen Systemfehleranalyse wird hier entscheidende Bedeutung zukommen. Auch vom konkreten Einzelfall abhän-

gig ist die Frage, ob der Hersteller darüber hinaus verpflichtet ist, sich die generierten Daten nicht nur übermitteln zu lassen, sondern ihn eine Pflicht trifft, die entsprechende Sensorik und Schnittstellen erst zu verbauen.

- c) Weder das Datenschutzrecht noch der Schutz der Integrität von End-einrichtungen gegen den Zugriff Dritter nach dem TTDSG stellen insoweit Hemmnisse dar. Die Erfüllung der Produktbeobachtungspflicht zur Abwehr von Gefahren vom Nutzer und der Allgemeinheit stellt eine Rechtfertigung dar.
6. Hinsichtlich der Reaktionspflichten des Herstellers auf eine nach Inverkehrgabe erkannte Produktgefahr ermöglichen smarte Produkte eine direkte und effektive Kommunikations- und Interaktionsebene zwischen Hersteller und Nutzer.
7. In Anknüpfung an die Pflegebetten-Entscheidung kommen Updatepflichten – ungeachtet ihrer konkreten Ausgestaltung – als weitergehende Sicherungsmaßnahmen erst in Betracht, wenn eine Warnung zur Gefahrenabwehr nicht hinreichend effektiv ist. Dies ist insbesondere dann der Fall, wenn Grund zur Annahme besteht, dass sich der Nutzer über die Warnung hinwegsetzt und dadurch Dritte gefährdet. Aufgrund der tatsächlichen Gegebenheiten bei smarten Produkten wird aber vielfach ein Hinwegsetzen über eine Warnung erwartet werden müssen.
- a) Bei reiner Software folgt dies daraus, dass Nutzer häufig eine falsche Gefahrenereinschätzung vornehmen und sich deshalb über eine Warnung hinwegsetzen. Denn bisher gingen von Sicherheitslücken kaum physische Gefahren aus. Zudem resultieren aus Cyberattacken regelmäßig keine unmittelbaren Beeinträchtigungen für den Nutzer, sondern es wird dessen kompromittiertes System lediglich für einen Angriff gegen Dritte verwendet. Die Einstellung, dass man selbst nicht Opfer eines solchen Angriffs wird bzw. dass die Auswirkungen vor allem Dritte treffen, kann in Verbindung mit den Rechtsgutverletzungen, die man hinzunehmen bereit ist, zu einer Fehleinschätzung der Gefährdung führen. Aufgrund fehlender Gefahrensensibilität können Nutzer daher in ihrer Abwägung zu dem Ergebnis kommen, dass die Kosten der Nutzungsaufgabe im Verhältnis zu den Risiken überwiegen.
 - b) Bei smarten Produkten ist ein Hinwegsetzen über eine Warnung gerade deswegen denkbar, weil es den Nutzern nicht zumutbar ist, die Gefahr selbst zu steuern. Diese Unzumutbarkeit kann sich daraus ergeben, dass der Nutzer selbst nicht in der Lage ist, Sicherheitslücken

cken zu beseitigen, während der Hersteller auch nach dem Zeitpunkt der Inverkehrgabe noch gesteigerte Einflussmöglichkeiten besitzt. Da allein der Hersteller den Aufbau und die Konzeption der Software in Gänze versteht, ist er regelmäßig der einzige Akteur, der Fehler beheben und die Software sicherer machen kann. Bei der Gefahrenbeseitigung durch eine Behebung des ursprünglichen Fehlers ist der Nutzer damit auf den Hersteller und von ihm bereitgestellte Sicherheitsupdates angewiesen. Wegen der fehlenden Möglichkeit des Nutzers, die Sicherheitsmängel selbst oder unter Zuhilfenahme Dritter als Fachleute zu beheben, ist die Warnung in diesen Fällen ein wenig wirksames Mittel der Gefahrenabwehr. Denn in solchen Konstellationen verbleibt dem Nutzer keine andere Möglichkeit, als im Rahmen der Gefahrensteuerung auf die Nutzung des Produkts zu verzichten. Bei Produkten, die für die Lebensführung von zentraler Bedeutung sind, ist ein Nutzungsverzicht aber kaum zu erwarten. Angesichts der allgegenwärtigen Fehleranfälligkeit von Software gilt dies dort umso mehr. Hinzu kommt, dass die Abhängigkeit des Nutzers bei der Fehlerbehebung vom Hersteller mit erhöhten Einflussmöglichkeiten des Herstellers auf das Produkt auch nach dem Inverkehrbringen korrespondiert. Da Softwareprodukte über das Internet verbunden sind, können die Hersteller jederzeit aus der Ferne auf ihre Produkte zugreifen und auf die sicherheitsrelevanten Eigenschaften per Aktualisierung Einfluss nehmen, sodass diese weiterhin ihrer Kontrolle unterliegen. Im Vergleich zur Nachrüstung körperlicher Gegenstände ist die Bereitstellung von Softwareaktualisierungen zudem mit geringem Aufwand und geringen Kosten für den Hersteller möglich.

- c) Die konkrete Ausgestaltung der Updatepflicht betrifft den Kern der Abgrenzung des Integritäts- vom Äquivalenzinteresse. Zwar kommen Sicherheitsupdates zur Fehlerbehebung als weitergehende Sicherungsmaßnahmen erst dann in Betracht, wenn es aus Gründen der Effektivität der Gefahrenabwehr nicht ausreichend ist, das Produkt aus dem Verkehr zu ziehen. Entscheidend ist damit, wann sich eine vom Hersteller aus der Ferne vorgenommene aufgedrängte Sicherheitsbereicherung, die eine weitere (gefährliche) Nutzung gerade ausschließt, bei der Gefahrenabwehr als nicht hinreichend effektiv darstellt. Dabei ist zu beachten, dass jeder derartige nachträgliche Eingriff des Herstellers in das Produkt potenziell in Konflikt mit dem Eigentumsrecht des Nutzers steht. Diese Konfliktlage hat nun

Rückwirkungen auf die Präventionspflichten des Herstellers: Eine Maßnahme zur Vermeidung von Rechtsgutsverletzungen genügt nur dann den Anforderungen an die Produktbeobachtungspflicht, wenn sie auch praktisch wirksam ist. Fehlt es an der Einwilligung zu einer entsprechenden Maßnahme und besteht auch kein anderer Rechtfertigungsgrund, ist diese Maßnahme nicht geeignet, um Rechtsgutsverletzungen durch das Produkt effektiv zu verhindern.

- d) Eine Klausel, die dem Hersteller das Recht einräumt, die mit einem Update verbundenen Rechtseingriffen vornehmen zu dürfen, wird regelmäßig im Rahmen der AGB-Kontrolle unwirksam sein, sofern überhaupt ein Vertragsschluss zwischen Hersteller und Eigentümer vorliegt. Eine Einwilligung in die konkrete Rechtsgutsverletzung rechtfertigt dagegen den Eingriff. Eine solche liegt konkludent in der unterlassenen Deaktivierung automatischer Updates. Dies allerdings nur in Bezug auf die Datenveränderung der Software. Damit kann der Hersteller fehlerbehebende Updates durchführen. Die Frage, ob die Einwilligung auch Funktionsänderungen umfasst, die die Schwelle zur Einschränkung von Funktionen nicht überschreiten, unterliegt angesichts der Regelungen im CRA einem Wandel. Jedenfalls künftig wird man hiervon nicht mehr ausgehen können. Hinsichtlich der Deaktivierung einzelner Funktionen oder gar der vollständigen Stilllegung des Geräts fehlt es schon am erforderlichen Bewusstsein der Rechtsgutsverletzung. Daher wäre eine vorherige Aufklärung über den Rechtseingriff erforderlich.
- e) Verweigert der Nutzer seine Einwilligung in eine solche Maßnahme, kommt zwar eine Rechtfertigung des Herstellers unter dem Gesichtspunkt des Defensivnotstands nach § 228 S. 1 BGB in Betracht. Allerdings gilt es hier zu berücksichtigen, dass nach dem Grundsatz des geringsten Eingriffs nur das mildeste der zur Verfügung stehenden geeigneten Mittel eingesetzt werden darf. Weniger eingriffsintensiv als die Deaktivierung des Gerätes ist zunächst die zwangsweise, d.h. die ohne Zustimmung des Nutzers durchgeführte Aktualisierung durch den Hersteller. Gleiches gilt für die bloße Bereitstellung einer Aktualisierung, auf die der Nutzer hingewiesen wird und die er eigenverantwortlich herunterladen sowie installieren kann. Nachdem im Rahmen des Defensivnotstands zunächst grundsätzlich auch weniger eingriffsintensive Abwehrmittel versucht werden müssen, selbst wenn deren Wirkung nicht völlig sicher ist, stellt sich die bloße Bereitstellung einer Aktualisierung somit als „Grundmaßnahme“ dar.

Nur wenn der Nutzer einer Aktualisierungsaufforderung nicht nachkommt, diese von vorneherein keinen Erfolg verspricht oder die zeitnahe Verwirklichung der Gefahr ein Zuwarten nicht zulässt, ist eine Zwangsaktualisierung oder -deaktivierung in Betracht zu ziehen. Insoweit ist ein „Stufenbau der Reaktionspflichten“ zu beachten, so dass die Bereitstellung von Updates zunächst das Mittel der Wahl darstellt, um den Anforderungen der Produktbeobachtungspflicht zu genügen.

8. Updatepflichten der Hersteller könnten sich auch außerhalb der deliktsrechtlichen Produktbeobachtungspflicht aus weiteren Regelungen ergeben
 - a) Mit Geltungsbeginn der GPSR müssen Hersteller im Falle eines erforderlichen Rückrufs die Rechte des Verbrauchers auf Abhilfe berücksichtigen. Dies bedeutet, dass im Falle einer Updatepflicht, diese auch kostenlos bereitgestellt werden müssen.
 - b) Indem die neue Produkthaftungsrichtlinie für die Bestimmung der berechtigten Sicherheitserwartungen und damit für die Fehlerhaftigkeit eines Produkts nicht mehr allein auf den Zeitpunkt der Inverkehrgabe, sondern auf den gesamten Zeitraum abstellt, in dem der Hersteller die Kontrolle über das Produkt behält, wird der Hersteller verpflichtet, nach dem Inverkehrbringen gestiegene Sicherheitserwartungen zu berücksichtigen. Ohne eine Updatepflicht explizit zu normieren, wird es dadurch implizit zu einer produkthaftungsrechtlichen Updatepflicht des Herstellers zur Aufrechterhaltung der Produktsicherheit kommen. Insoweit wird sich ein Hersteller im Falle eines erst nachträglich auftretenden Fehlers nicht entlasten können, sollte die Fehlerhaftigkeit des Produkts auf das Fehlen von Softwareupdates zurückzuführen sein. Auch ein Entwicklungshelfer wird künftig nicht zu einem Haftungsausschluss führen, wenn der Fehler später durch ein Update hätte behoben werden können.
 - c) Daneben wird sich eine Pflicht zur Behebung von Schwachstellen durch Updates aus dem CRA ergeben.
9. Derartige Updatepflichten können nicht durch einen vorbeugenden Anspruch auf Updates durchgesetzt werden. Zwar ist der Anspruch nach § 1004 Abs. 1 S. BGB auf die Beseitigung einer konkreten Gefahr gerichtet. In den Fällen aber, in denen der Nutzer in der Lage ist, einen Gefahrenabwehranspruch hinreichend konkret zu formulieren und zu begründen (§ 253 Abs. 2 Nr. 2 ZPO), wird die Kenntnis der Gefahr regelmäßig auch für die Ergreifung von Selbstschutzmaßnahmen ausreichen.

Insoweit kann niemand von einem Hersteller mit der Begründung ein Update verlangen, dass andernfalls die Warnung ignoriert und das Produkt trotz der erkannten Gefahr weiter verwendet werde. Dieser einfache und zumutbare Selbstschutz wird Dritten, die zufällig mit dem gefährlichen Produkt in Kontakt kommen, zwar nicht möglich sein. Allerdings fehlt es in diesen Fällen regelmäßig an der hinreichenden Konkretisierung der Gefahr, sodass auch Ansprüche Dritter auf Vornahme von Sicherheitsaktualisierungen ausscheiden.

H. Literaturverzeichnis

- Ackermann, Tobias/Golling, Manuel*: Entwurf einer neuen Produktsicherheits-Verordnung – Worauf sich Hersteller zukünftig einstellen müssen, in: *ZfPC* 2022, S. 67 ff.
- Altschwager, Martin*: Haftung von Pharmaunternehmen auf Social Media, in: *PharmR* 2021, S. 461 ff.
- Appel, Ivo*: Grundrechtliche Fragen privater Produktbeobachtungspflichten, in: Eifert, Martin (Hg.): *Produktbeobachtung durch Private*, Berlin 2015, S. 27 ff.
- Arndt, Christine/Wende, Susanne*: Die Abgrenzung von vorhersehbarem Fehlgebrauch und Produktmissbrauch – ein Pulverfass?, in: *ZfPC* 2023, S. 110 ff.
- Arzt, Clemens/Kleemann, Steven/Plappert, Christian/Rieke, Roland/Zelle, Daniel*: Datenverarbeitung und Cybersicherheit in der Fahrzeugautomatisierung, in: *MMR* 2022, S. 593 ff.
- Bachmeier, Werner*: *Rechtshandbuch Autokauf. Neu- und Gebrauchtwagen. Kauf und Leasing. Kauf im Internet*, 2. Auflage, München 2013.
- Bartsch, Michael*: Die „Vertraulichkeit und Integrität informationstechnischer Systeme“ als sonstiges Recht nach § 823 Abs. 1 BGB. (§ 823 Abs. 1 BGB), in: *CR* 2008, S. 613 ff.
- Beck, Thomas Alexander*: *Die präventive Durchsetzung der Rückrufpflicht. Möglichkeiten zur Erzwingung eines Produktrückrufs*, Tübingen 2002.
- Beck'scher Online-Kommentar BGB, hrsg. von *Hau, Wolfgang/Poseck, Roman*, 71. Edition, München 2024 (zitiert als Bearbeiter, in: BeckOK, BGB).
- beck-online.Grosskommentar zum Zivilrecht, hrsg. von *Gsell, Beate/Krüger, Wolfgang/Lorenz, Stephan/Reymann, Christoph*, Kommentierung zu § 823 BGB, Stand von 01.07.2024, Kommentierung zu § 227 BGB, Stand von 01.06.2024, Kommentierung zu § 249 BGB, Stand von 01.03.2022, München 2024 (zitiert als Bearbeiter, in: BeckOGK, BGB).
- Beierle, Benedikt*: Die Bedeutung des Inverkehrbringens für IoT-Produkte bei der Produkthaftung, in: *ZfPC* 2022, S. 22 ff.
- Beierle, Benedikt*: *Die Produkthaftung im Zeitalter des Internet of Things. Analyse des ProdHaftG vor dem Hintergrund vernetzter und intelligenter Produkte*, Baden-Baden 2021.
- Benenson, Zinaida/ Kroll-Peters, Olaf/ Krupp, Matthias*: Attitudes to IT Security when Using a Smartphone, in: *FedCSIS* 2012, S. 1179 ff.
- Böck, Nicole/Reinsberg, Johannes*: Einbeziehung cybersicherheitsrechtlicher Produktanforderungen in die Funkanlagenrichtlinie, in: *ZfPC* 2022, S. 126 ff.
- Böck, Nicole/Theurer, Jakob*: Herstellerpflichten und Haftungsrisiken bei IT-Sicherheitslücken vernetzter Produkte, in: *BB* 2021, S. 520 ff.
- Bodewig, Theo*: *Der Rückruf fehlerhafter Produkte. Eine Untersuchung der Rückrufpflichten und Rückrufansprüche nach dem Recht Deutschlands, der Europäischen Union und der USA*, Tübingen 1999.

- Bomhard, David/Merkle, Marieke: Der Entwurf eines EU Data Acts, in: RDİ 2022, S. 168 ff.
- Bomhard, David/Merkle, Marieke: Europäische KI-Verordnung, in: RDİ 2021, S. 276 ff.
- Borges, Georg: Rechtliche Rahmenbedingungen für autonome Systeme, in: NJW 2018, S. 977 ff.
- Bräutigam, Peter/Klindt, Thomas (Hg.), Digitalisierte Wirtschaft / Industrie 4.0.
- Bräutigam, Peter/Klindt, Thomas: Industrie 4.0, das Internet der Dinge und das Recht, in: NJW 2015, S. 1137 ff.
- Bräutigam, Peter/Kraul, Thorsten (Hg.): Internet of Things. Rechtshandbuch, München 2021.
- Brenner, Raphael/Leithäuser, Malte/Jänich, Sebastian/Pöhls, Henrich C.: Updatefähigkeit als Konstruktionsanforderung. Eine rechtliche Begriffsbildung, in: RDİ 2024, S. 252 ff.
- Brenner, Raphael: Software im Fokus der neuen Produkthaftungsrichtlinie, in: RDİ 2024, S. 345 ff.
- Brügge, Gert: Schadensersatz für implantierte fehlerhafte Medizinprodukte – Zwei Vorlagebeschlüsse des Bundesgerichtshofs, in: MedR 2014, S. 537 ff.
- Buchner, Benedikt: Datenschutz im vernetzten Automobil, in: DuD 2015, S. 372 ff.
- Buck-Heeb, Petra/Oppermann, Bernd H. (Hg.): Automatisierte Systeme, München 2022.
- Burchardi, Sophie: Risikotragung für KI-Systeme. Zur Zweckmäßigkeit einer europäischen Betreiberhaftung, in: EuZW 2022, S. 685 ff.
- Burckhardt, Markus: BGH, Urteil v. 16.12.2008, VI ZR 170/07 (Anmerkung), in: BB 2009, S. 630 ff.
- Burckhardt, Markus: Das Ende kostenloser Nachrüstung beim Rückruf von Produkten? – Die Pflicht zur Mängelbehebung und zur Kostentragung beim Produktrückruf im Lichte der neuesten Rechtsprechung -, in: VersR 2007, S. 1601 ff.
- Chibanguza, Kuuya J./Kuß, Christian/Steege, Hans (Hg.): Künstliche Intelligenz. Recht und Praxis automatisierter und autonomer Systeme, Baden-Baden, 2022.
- Chibanguza, Kuuya J./Schubmann Daniel: Die Produktbeobachtungspflicht im Wandel der Digitalisierung und die Haftung der handelnden Personen, in: GmbHR 2019, S. 313 ff.
- Cornelius, Kai: Autonome Softwareagenten im Verbandssanktionenrecht, in: ZRP 2019, S. 8 ff.
- Daute, Ingvar/Sütthoff, Alicia: Vereinbarkeit von Produktbeobachtungspflicht und Datenschutz beim autonomen Kraftfahrzeug, in: EuZW 2023, S. 500 ff.
- Deusch, Florian/Eggendorfer, Tobias: Softwaremängel 4.0 – Zu Risiken und Nebenwirkungen fragen Sie Ihren Softwarehersteller oder Sachverständigen, in: Taeger, Jürgen (Hg.): Tagungsband DSRI Herbstakademie 2015. Internet der Dinge: Digitalisierung von Wirtschaft und Gesellschaft, Edewecht 2015, S. 833 ff. (zitiert als Deusch/Eggendorfer, DSRI 2015, 833).
- Dietborn, Christof/Müller, Alexander: Beschränkung der deliktischen Herstellerpflichten: Kein Produktrückruf und kostenloser Austausch, in: BB 2007, S. 2358 ff.

- Dötsch, Tina*: Außervertragliche Haftung für Künstliche Intelligenz am Beispiel von autonomen Systemen, Wiesbaden 2023.
- Droste, Johannes*: Produktbeobachtungspflichten der Automobilhersteller bei Software in Zeiten vernetzten Fahrens, in: CCZ 2015, S. 105 ff.
- Droste, Wiebke*: Intelligente Medizinprodukte: Verantwortlichkeiten des Herstellers und ärztliche Sorgfaltspflichten, in: MPR 2018, S. 109 ff.
- Duden, Konrad*: Digitale Sachherrschaft, Tübingen 2023.
- Ebers, Martin/Heinze, Christian/Krügel, Tina/Steinrötter, Björn* (Hg.): Künstliche Intelligenz und Robotik. Rechtshandbuch, München 2020 (zitiert als: Ebers et al., (Hg.), Künstliche Intelligenz und Robotik).
- Ebers, Martin/Steinrötter, Björn* (Hg.): Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, Baden-Baden 2021.
- Ebert, Andreas/Busch, Philip/Spiecker gen. Döhmman, Indra/Wendt, Janine*: Roboter im Supermarkt. Eine Betrachtung haftungs- und datenschutzrechtlicher Probleme beim Einsatz von Robotern im Einzelhandel, in: ZfPC 2023, S. 16 ff.
- Eckhardt, Dennis/Feist, Nelli/ Herrmann, Dominik*: Selbstbestimmt (un)sicher?. Herausforderungen an Datensicherheit und Datenschutz im digitalen Alltag, in: Jahrbuch Konsum & Verbraucherwissenschaften 2023 (im Erscheinen).
- Edenfeld, Stefan*: Grenzen der Verkehrssicherungspflicht, in: VersR 2002, S. 272 ff.
- Eifert, Martin/Hoffmann-Riem, Wolfgang* (Hg.): Innovationsverantwortung, Berlin 2009.
- Eifert, Martin*: Einführung, in: Eifert, Martin (Hg.): Produktbeobachtung durch Private, Berlin 2015, S. 9 ff.
- Engel, Friedrich-Wilhelm*: Produzentenhaftung für Software, in: CR 1986, S. 702 ff.
- Ensthaler, Jürgen/Gollrad, Markus*: Rechtsgrundlagen des automatisierten Fahrens. Standardessentielle Patente und Fahrzeugvernetzung, Zulässigkeit und Zulassung, Haftungsrecht, Datenschutz, Datensicherheit und Datenhoheit, Frankfurt am Main 2019.
- Erman BGB Kommentar*, hrsg. von *Westermann, Harm Peter/Grunewald, Barbara/Maier-Reimer, Georg*, Band 2, 17. Auflage, Köln 2023 (zitiert als Bearbeiter, in: Erman, BGB).
- Essers, David*: Haftungsfragen automatisierter Systeme, Berlin 2024.
- Etzkorn, Philipp*: (Vertragliche) Datenzugangsansprüche nach dem Data Act, in: RD 2024, S. 116 ff.
- Etzkorn, Philipp*: Bedeutung der „Entwicklungslücke“ bei selbstlernenden Systemen. Rechtliche Fragen zur fortwährenden Softwareentwicklung durch maschinelles Lernen im Praxiseinsatz, in: MMR 2020, S. 360 ff.
- Faust, Florian*: Gefahrabwendungspflicht des Herstellers von Produkten mit Sicherheitsmängeln, in: JuS 2009, S. 377 ff.
- Faustmann, Jörg*: Der deliktische Datenschutz, in: VuR 2006, S. 260 ff.
- Fida, Sophia*: Updates, Patches & Co. Zivilrechtliche Fragen zur Softwareaktualisierung, Wien 2022.

- Foerste, Ulrich/Graf v. Westphalen, Friedrich (Hg.): Produkthaftungshandbuch, 4. Auflage, München 2024.
- Foerste, Ulrich: BGH, 9. 5. 1995 – VI ZR 158/94 (Anmerkung), in: JZ 1995, S. 1063 f.
- Foerste, Ulrich: Die Produkthaftung für Druckwerke, in: NJW 1991, S. 1433 ff.
- Fox, Dirk: Wie finden wir Fehler?, in: DuD 2016, S. 701.
- Fries, Martin/Paal, Boris P. (Hg.): Smart Contracts, Tübingen 2019.
- Gansmeier, Johannes/Kochendörfer, Luca: Konkurrenzen im Kontext der §§ 327 d ff. BGB, in: JuS 2022, S. 704 ff.
- Gauger, Dörte/Hartmannsberger, Roland: Rechtliche Anforderungen an Verbraucherprodukte – Pflichten, Risiken, Praxisprobleme, in: NJW 2014, S. 1137 ff.
- Geber, Frederic: Rechtliche Anforderungen an Software-Updates von vernetzten und automatisierten Pkw, in: NZV 2021, S. 14 ff.
- Geistfeld, Mark A.: A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation, in: California Law Review 105 (2017), S. 1611 ff.
- Gilga, Carolin: EDSB: Überwachung sozialer Medien – Social Media Monitoring, in: ZD-Aktuell 2020, 07022.
- Gless, Sabine/Janal, Ruth: Hochautomatisiertes und autonomes Autofahren – Risiko und rechtliche Verantwortung, in: JR 2016, S. 561 ff.
- Gomille, Christian: Herstellerhaftung für automatisierte Fahrzeuge, in: JZ 2016, S. 76 ff.
- Gondlach, Kai Arne/Regneri Michaela: Das Gespenst der German Angst: Sind wir zu skeptisch für KI-Entwicklung?, in: Gondlach, Kai/Knappertsbusch, Inka (Hg.): Arbeitswelt und KI 2030. Herausforderungen und Strategien für die Arbeit von morgen, Wiesbaden 2021, S. 3 ff.
- Graf v. Westphalen, Friedrich: Das Milupa-Urteil – eine beträchtliche Verschärfung der Produkthaftung, in: ZIP 1992, S. 18 ff.
- Graf v. Westphalen, Friedrich: Haftungsfragen beim Einsatz Künstlicher Intelligenz in Ergänzung der Produkthaftungs-RL 85/374/EWG. (-RL 85/374/EWG), in: ZIP 2019, S. 889 ff.
- Grages, Jan-Michael: Rechtfertigung und Zweckänderung im Spannungsverhältnis von DSGVO und TTDSG. Reichweite der TTDSG-Wertungen bei typischen Verarbeitungsabläufen, in: CR 2021, S. 834 ff.
- Grapentin, Justin: Konstruktionspflichten des Herstellers und Mitverschulden des Anwenders beim Einsatz von Künstlicher Intelligenz, in: JR 2019, S. 175 ff.
- Grapentin, Justin: Vertragsschluss und vertragliches Verschulden beim Einsatz von Künstlicher Intelligenz und Softwareagenten, Baden-Baden 2018.
- Grüneberg, Christian: Bürgerliches Gesetzbuch, 83. Auflage, München 2024 (zitiert als: Bearbeiter, in: Grüneberg, BGB).
- Grünvogel, Thomas/Dörrenbächer, Felix: Smartere Anforderungen an smarte Hausgeräte? – Der Maßstab für die Produktbeobachtungspflicht bei vernetzten Hausgeräten im Wandel, in: ZVertriebsR 2019, S. 87 ff.

- Grützmacher, Malte/Heckmann, Jörn*: Autonome Systeme und KI – vom vollautomatisierten zum autonomen Vertragsschluss?. Die Grenzen der Willenserklärung, in: CR 2019, S. 553 ff.
- Grützmacher, Malte*: Die deliktische Haftung für autonome Systeme – Industrie 4.0 als Herausforderung für das bestehende Recht?. Ein Plädoyer für die Nutzung von Beweislastregeln und wider den vorschnellen Ruf nach der Einführung einer Gefährdungshaftung, in: CR 2016, S. 695 ff.
- Grützmacher, Malte*: Die zivilrechtliche Haftung für KI nach dem Entwurf der geplanten KI-VO. Potentielle zivilrechtliche Auswirkungen des geplanten KI-Sicherheitsrechts: ein neues Schutzgesetz i.S.v. § 823 Abs. 2 BGB am Horizont, in: CR 2021, S. 433 ff.
- Günther, Jan-Philipp*: Roboter und rechtliche Verantwortung. Eine Untersuchung der Benutzer- und Herstellerhaftung, München 2016.
- Haagen, Christian*: Haftungsbeschränkung bei technisch nicht vermeidbaren Risiken, in: Beck, Susanne/Kusche, Carsten/Valerius, Brian (Hg.): Digitalisierung, Automatisierung, KI und Recht. Festgabe zum 10-jährigen Bestehen der Forschungsstelle RobotRecht, Baden-Baden 2020, S. 215 ff.
- Hacker, Philipp*: Europäische und nationale Regulierung von Künstlicher Intelligenz, in: NJW 2020, S. 2142 ff.
- Haftenberger, Anna*: Die Produkthaftung für künstlich intelligente Medizinprodukte. Eine Analyse der Anwendbarkeit und Eignung der europäischen Produkthaftungsrichtlinie 85/374/EWG. Baden-Baden 2023.
- Hager, Johannes*: Die Kostentragung bei Rückruf fehlerhafter Produkte, in: VersR 1984, S. 799 ff.
- Hamm, Christoph* (Hg.): Beck'sches Rechtsanwaltslexikon, 12. Auflage, München 2022.
- Hammel, Tobias*: Haftung und Versicherung bei Personenkraftwagen mit Fahrerassistenzsystemen, Karlsruhe 2016.
- Handorn, Boris/Juknat, Ulrich*: KI und Haftung bei Medizinprodukten, in: MPR 2022, S. 77 ff.
- Handorn, Boris*: Die „Pflegebetten“-Entscheidung des Bundesgerichtshofs – neue Leitlinien zur Kostentragung bei Produktrückrufen, in: MPR 2009, S. 37 ff.
- Handorn, Boris*: Medizinproduktehaftung für Implantate: Erhöhtes Ausfallrisiko innerhalb einer Produktserie als Produktfehler, in: MPR 2015, S. 91 ff.
- Hanloser, Stefan*: Schutz der Geräteintegrität durch § 25 TTDSG, in: ZD 2021, S. 399 ff.
- Hans, Armin*: Automotive Software 2.0: Risiken und Haftungsfragen, in: GWR 2016, S. 393 ff.
- Hartmann, Christoph/Klindt, Thomas*: Kritisches zum Kommissions-Entwurf für eine Produktsicherheits-VO, in: ZfPC 2022, S. 73 ff.
- Hartmann, Volker*: Big Data und Produkthaftung. Produkthaftungsrechtliche Chancen und Risiken des Einsatzes von Big Data-Technologien im Automobil, in: DAR 2015, S. 122 ff.

- Hartmann, Volker*: Der Kfz-Hersteller im Spannungsfeld zwischen Produkthaftungsrecht und UWG, in: BB 2012, S. 267 ff.
- Hartmann, Volker*: Der Warenhersteller im Spannungsfeld zwischen Produkthaftungs- und Wettbewerbsrecht. Produkthaftungsrechtliche Warnpflichten hinsichtlich Fremdzubehör und deren Vereinbarkeit mit dem UWG am Beispiel des Kfz-Herstellers, 2014.
- Hartmann, Volker*: Digitale Produktbeobachtungspflichten für Smart Products, in: Gondlach, Kai/Knappertsbusch, Inka (Hg.): Arbeitswelt und KI 2030. Herausforderungen und Strategien für die Arbeit von morgen, Wiesbaden 2021, S. 63 ff.
- Hartmann, Volker*: Here come the robots — Produkthaftung und Robotik am Beispiel des automatisierten und autonomen Fahrens (Teil 2: Anforderungen an die Produktbeobachtung), in: PHi 2017, S. 42 ff.
- Hauke, Christian/Kremer, Gerhard*: Arzneimittelfälschungen: Reaktionspflichten und Haftung des Originalherstellers, in: PharmR 2013, S. 213 ff.
- Hauschka, Christoph E./Klindt, Thomas*: Eine Rechtspflicht zur Compliance im Reklamationsmanagement?, in: NJW 2007, S. 2726 ff.
- Heckmann, Dirk/Schmid, Alexander*: Rechtliche Aspekte automatisierter Systeme. Rechtskonforme Gestaltung unserer Zukunft, in: Informatik Spektrum 2017, S. 430 ff.
- Helte, Christian*: Anforderungen an die Produktsicherheit bei späterem Fortschritt von Wissenschaft und Technik, Göttingen 2020.
- Herley, Cormac*: So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users, in: NSPW 2009, S. 133 ff.
- Hessel, Stefan/Callewaert, Christoph*: Das aktuelle und zukünftige Cybersicherheitsrecht der EU – Die wesentlichen Pflichten für Unternehmen und deren praktische Umsetzung, in: DB 2022, S. 2589 ff.
- Heuer-James, Jens-Uwe/Chibanguza, Kuuya/Stücker, Benedikt*: Industrie 4.0 – vertrags- und haftungsrechtliche Fragestellungen, in: BB 2018, S. 2818 ff.
- Heussen, Benno*: Unvermeidbare Softwarefehler. Neue Entlastungsmöglichkeiten für Hersteller, in: CR 2004, S. 1 ff.
- Hey, Tim*: Die außervertragliche Haftung des Herstellers autonomer Fahrzeuge bei Unfällen im Straßenverkehr, Wiesbaden 2019.
- Hinrichs, Ole/Becker, Moritz*: Connected Car vs. Privacy – Teil 1. Datenschutzrechtliche Grundlagen und Anforderungen an vernetzte Automobile, in: ITRB 2015, S. 164 ff.
- Hinze, Jonathan*: Haftungsrisiken des automatisierten und autonomen Fahrens, Frankfurt am Main 2021.
- Hoeren, Thomas/Pinelli, Stefan* (Hg.): Künstliche Intelligenz – Ethik und Recht, München 2022.
- Hoffmann, Dirk W.*: Software-Qualität, 2. Auflage, Berlin, Heidelberg 2013.
- Hofmann, Christian*: Öffentlich-rechtlich statuierte Produktbeobachtungspflichten als Mittel der Sicherheitsgewährleistung im Produkt-, Stoff- und Technikrecht, Baden-Baden 2014.
- Hofmann, Franz*: Der Einfluss von Digitalisierung und künstlicher Intelligenz auf das Haftungsrecht. Der Umgang mit technischen Risiken, in: CR 2020, S. 282 ff.

- Horner, Susanne/Kaulartz, Markus*: Haftung 4.0. Verschiebung des Sorgfaltsmaßstabs bei Herstellung und Nutzung autonomer Systeme, in: CR 2016, S. 7 ff.
- Hornung, Gerrit/Fuchs, Katharina*: Einstandspflicht des Fälschungsofers? – Die Haftung von Originalherstellern für Schäden durch Arzneimittelfälschungen, in: PharmR 2012, S. 501 ff.
- Hornung, Gerrit/Hofmann, Kai*: Industrie 4.0 und das Recht: Drei zentrale Herausforderungen, in: Hornung, Gerrit (Hg.): Rechtsfragen der Industrie 4.0. Datenhoheit – Verantwortlichkeit – rechtliche Grenzen der Vernetzung, Baden-Baden 2018, S. 9 ff.
- Hornung, Gerrit/Schallbruch, Martin* (Hg.): IT-Sicherheitsrecht. Praxishandbuch, Baden-Baden 2021.
- Hossenfelder, Martin*: Pflichten von Internetnutzern zur Abwehr von Malware und Phishing in Sonderverbindungen, Baden-Baden 2013.
- Huber, Carolin*: Rechtsfragen des Produktrückrufs aus versicherungsrechtlicher Perspektive, Karlsruhe 2022.
- J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, begr. von v. Staudinger, Julius, Buch 1. Allgemeiner Teil, Einleitung zum BGB §§ 1–14; VerschG, Neubearbeitung, Berlin 2024, Buch 2. Recht der Schuldverhältnisse, §§ 826–826; ProdHaftG, Neubearbeitung, Berlin 2021, Buch 3. Sachenrecht §§ 985–1011, Neubearbeitung, Berlin 2023 (zitiert als Bearbeiter, in: Staudinger, BGB).
- Jajodia, Sushil/Samarati, Pierangela/Yung, Moti* (Hg.): Encyclopedia of Cryptography, Security and Privacy, 3. Auflage, Berlin, Heidelberg 2021.
- Kaboth, Daniel*: Freies Dekompilieren zur Fehlerberichtigung: Ein Dammbbruch?, in: ZUM 2022, S. 126 ff.
- Käde, Lisa/von Maltzan, Stephanie*: Die Erklärbarkeit von Künstlicher Intelligenz (KI). Entmystifizierung der Black Box und Chancen für das Recht, in: CR 2020, S. 66 ff.
- Kahl, Thomas/Behrendt, Philipp*: Datenschutzrechtliche Herausforderungen der Cyber-Abwehr im Connected-Car-Umfeld, in: RAW 2020, S. 82 ff.
- Kahl, Thomas*: Datenschutz im Automotive-Aftersales. Ergebnisse der Prüfkationen der Aufsichtsbehörden – Herausforderungen und Lösungsansätze für die Praxis, in: RAW 2019, S. 70 ff.
- Kapoor, Arun/Klindt, Thomas*: Verschärfung der Produkthaftung in Europa: Der Vorschlag der neuen Produkthaftungsrichtlinie, in: BB 2023, S. 67 ff.
- Kapoor, Arun/Sedlmaier, Felix*: Verschärfung der Produkthaftung in Europa – Eine Zäsur für die Automobilindustrie?, in: RAW 2023, S. 8 ff.
- Kaulartz, Markus/Braegelman, Tom* (Hg.): Rechtshandbuch Artificial Intelligence und Machine Learning, München 2020.
- Kettler, Christian*: BGH, Urteil v. 16.12.2008, VI ZR 170/07 (Anmerkung), in: VersR 2009, S. 272 ff.
- Kian, Bardia/Tettenborn, Alexander*: Ist die Providerhaftung im Lichte vernetzter autonomer Systeme noch zeitgemäß?, in: Hilgendorf, Eric/Höltitzsch, Sven/Lutz, Lennart S. (Hg.): Rechtliche Aspekte automatisierter Fahrzeuge. Beiträge zur 2. Würzburger Tagung zum Technikrecht im Oktober 2014, Baden-Baden 2015, S. 101 ff.

- Kipker, Dennis-Kenji (Hg.): *Cybersecurity*, 2. Auflage, München 2023.
- Kipker, Dennis-Kenji/Walkusz, Michael: Hersteller- und Verkäuferpflichten bei softwarebezogenen IT-Sicherheitsupdates. Rechtsgrundlagen und Umfang, in: *DuD* 2019, S. 513 ff.
- Kipker, Dennis-Kenji: Der EU „Cyber Resilience Act“ kommt – und mit ihm die umfassendsten Compliance-Pflichten in der IT-Sicherheit, die es jemals gab, in: *MMR-Aktuell* 2022, 452009.
- Kipker, Dennis-Kenji: EU Cybersecurity Act und Certification Schemes: ein aktueller Fortschrittsbericht, in: *DuD* 2020, S. 263 ff.
- Kirn, Stefan/Müller-Hengstenberg, Claus D.: Intelligente (Software-)Agenten: Von der Automatisierung zur Autonomie? – Verselbstständigung technischer Systeme, in: *MMR* 2014, S. 225 ff.
- Klett, Detlef/Gehrmann, Mareike: Sicherheitsmängel in der Software, in: *MMR* 2022, S. 435 ff.
- Klindt, Thomas (Hg.): *Produktsicherheitsgesetz. ProdSG. Kommentar*, 3. Auflage, München 2021. (zitiert als Bearbeiter, in: Klindt, ProdSG).
- Klindt, Thomas/Handorn, Boris: Haftung eines Herstellers für Konstruktions- und Instruktionsfehler, in: *NJW* 2010, S. 1105 ff.
- Klindt, Thomas/Piovano, Christian: Fristfragen in der produktsicherheitsrechtlichen Notifikationspflicht, in: *NVwZ* 2021, S. 1016 ff.
- Klindt, Thomas/Wende, Susanne: Produktbeobachtungspflichten 2.0 – Social-Media-Monitoring und Web-Screening, in: *BB* 2016, S. 1419 ff.
- Klindt, Thomas/Wende, Susanne: *Rückrufmanagement. Ein Leitfaden für die professionelle Abwicklung von Krisenfällen*, 4. Auflage, Berlin, Wien, Zürich, 2021.
- Klindt, Thomas: BGH, Urt. v. 12.11.1991 – VI ZR 7/91 (Anmerkung), in: *NJW* 2017, S. 3087 ff.
- Klindt, Thomas: Das neue Geräte- und Produktsicherheitsgesetz, in: *NJW* 2004, S. 465 ff.
- Klindt, Thomas: Der Vollzug des europäischen Produktsicherheitsrechts in Deutschland – Eine erste Bilanz, in: *NVwZ* 2008, S. 1073 ff.
- Klindt, Thomas: Digitalisierung und Konnektivität bei Produktrückrufen, in: *DAR* 2023, S. 7 ff.
- Klindt, Thomas: Hilft das Produkthaftungsgesetz gegen IT-Vandalismus?, in: *Tagesspiegel Background*, 21.11.2018 (<https://background.tagesspiegel.de/hilft-das-produkthaftungsgesetz-gegen-it-vandalismus> [zuletzt abgerufen am 23.09.2024]).
- Klindt, Thomas: Produktbeobachtung zwischen Produktsicherheitsrecht und Social Media, in: Eifert, Martin (Hg.): *Produktbeobachtung durch Private*, Berlin 2015, S. 55 ff.
- Klindt, Thomas: Produktrückrufe und deren Kostenerstattung nach der Pflegebetten-Entscheidung des BGH, in: *BB* 2009, S. 792 ff.
- Klindt, Thomas: Robotik, Recht, Risiko. Heute: Die Produktsicherheits-Verordnung, in: *Robotik und Produktion* 2022, S. 38.

- Klinger, Max*: Die Produktbeobachtungspflicht bezüglich Fremdzubehörteilen, Tübingen 1998.
- Koch, Frank A*: Updating von Sicherheitssoftware – Haftung und Beweislast. Eine Problemskizze zur Verkehrssicherungspflicht zum Einsatz von Antivirenprogrammen, in: CR 2009, S. 485 ff.
- Koch, Robert*: Haftung für die Weiterverbreitung von Viren durch E-Mails, in: NJW 2004, S. 801 ff.
- Kort, Michael*: "Stand der Wissenschaft und Technik" im neuen deutschen und "state of the art" im amerikanischen Produkthaftungsrecht, in: VersR 1989, S. 1113 ff.
- Krause, Rüdiger*: Entwicklungsrisiken und Produkthaftung, in: Viehweg, Klaus (Hg.): Risiko – Recht – Verantwortung. Erlanger Symposium am 09./10. Juli 2004, Köln, Berlin, München 2006, S. 451 ff.
- Krauß, Christoph/Waidner, Michael*: IT-Sicherheit und Datenschutz im vernetzten Fahrzeug. Bedrohungen und Herausforderungen, in: DuD 2015, S. 383 ff.
- Krey, Volker/Kapoor, Arun*: Praxisleitfaden Produktsicherheitsrecht. CE-Kennzeichnung – Risikobeurteilung – Betriebsanleitung – Konformitätserklärung – Produkthaftung – Fallbeispiele, 4. Auflage, München 2023.
- Krüger, Daniel/Wagner, Susan*: Das Phänomen „Künstliche Intelligenz“ aus regulatorischer und haftungsrechtlicher Sicht, in: ZfPC 2023, S. 124 ff.
- Kühne, Armin/Nack, Ralph* (Hg.): Rechtshandbuch Connected Cars, München 2022.
- Kullmann, Hans Josef*: Das Risiko in der Produzentenhaftung, in: VersR 1988, S. 655 ff.
- Kunz, Jürgen*: Die Produktbeobachtungs- und die Befundunsicherungspflicht als Verkehrssicherungspflichten des Warenherstellers, in: BB 1994, S. 450 ff.
- Kuschel, Linda*: Digitale Eigenmacht. Digitale Eingriffe in vernetzte Sachen als Herausforderung für den possessorischen Besitzschutz, in: AcP 220 (2020), S. 98 ff.
- Lach, Sebastian/Polly, Sebastian*: Produkt-Compliance. Leitfaden zum Produktsicherheitsgesetz, 3. Auflage, Wiesbaden 2017.
- Lach, Sebastian/Schönberger, Simone*: Die Haftung des Vertriebshändlers von Medizinprodukten, in: MPR 2012, S. 73 ff.
- Langenbucher, Katja* (Hg.): Europäisches Privat- und Wirtschaftsrecht, 5. Auflage, Baden-Baden 2022.
- Larenz, Karl/Canaris, Claus-Wilhelm*, Lehrbuch des Schuldrechts. II. Band: Besonderer Teil. 2. Halbband, 13. Auflage, München 1994.
- Lehmann, Michael*: Produkt- und Produzentenhaftung für Software, in: NJW 1992, S. 1721 ff.
- Lejeune, Mathias*: Vorschlag für eine neue EU-Produkthaftungsrichtlinie: Erweiterung auf digitale Produkte und digitale Dienste, Zusammenspiel mit anderen Rechtsakten der EU – Teil 1. Anwendungsbereich und Abgrenzung zur KI-Haftungsrichtlinie, Begriffsbestimmungen, Schäden und Produktfehler, in: ITRB 2024, S. 102 ff.
- Lenhard, Thomas H.*: Datensicherheit. Technische und organisatorische Schutzmaßnahmen gegen Datenverlust und Computerkriminalität, 2. Auflage, Wiesbaden 2020.
- Lenz, Tobias*: Produkthaftung, 2. Auflage, München 2022.

- Leupold, Andreas/Wiebe, Andreas/Glossner, Silke* (Hg.): IT-Recht. Recht, Wirtschaft und Technik der digitalen Transformation, 4. Auflage, München 2021.
- Libertus, Michael*: Zivilrechtliche Haftung und strafrechtliche Verantwortlichkeit bei unbeabsichtigter Verbreitung von Computerviren, in: MMR 2005, S. 507 ff.
- Linaratos, Dimitrios*: Künstliche Intelligenz und Verantwortung, in: ZIP 2019, S. 504 ff.
- Lohmann, Melinda F.*: Roboter als Wundertüten – eine zivilrechtliche Haftungsanalyse, in: AJP/PJA 2017, S. 152 ff.
- Looschelders, Dirk*, Schuldrecht. Besonderer Teil, 19. Auflage, München 2024.
- Lüdemann, Volker*: Connected Cars – Das vernetzte Auto nimmt Fahrt auf, der Datenschutz bleibt zurück, in: ZD 2015, S. 247 ff.
- Lüftenegger, Klaus*: „Alexa, warum geht der Kühlschrank nicht mehr?“. Reaktionsmaßnahmen bei vernetzten Produkten, in: RDt 2021, S. 293 ff.
- Lüftenegger, Klaus*: Der Fall Volkswagen – (k)ein Rückruf wie jeder andere?, in: DAR 2016, S. 122 ff.
- Lüftenegger, Klaus*: Die deliktische Pflicht zum Rückruf von Fahrzeugen, in: NJW 2018, S. 2087 ff.
- Lüftenegger, Klaus*: Die Rückrufpflicht des Herstellers – unter Berücksichtigung der höchstrichterlichen „Pflegebetten“-Rechtsprechung, Berlin 2018.
- Magnus, Hanno*: Fernkontrolle im Internet der Dinge, Trier 2022.
- Marly, Jochen*: Praxishandbuch Softwarerecht. Rechtsschutz und Vertragsgestaltung, 7. Auflage, München 2018.
- Martin, Manuela/Uhl, Kathrin*: Cyberrisiken bei vernetzten Fahrzeugen – (Produkt-)Haftungsrechtliche Fragestellungen im Zusammenhang mit Hackerangriffen, in: RAW 2020, S. 7 ff.
- Martinek, Michael/Semler, Franz-Jörg/Flohr, Eckhard* (Hg.): Handbuch des Vertriebsrechts, 4. Auflage, München 2016.
- Mäsch, Gerald*: Schuldrecht BT: Ersatzpflicht wegen eines potenziell fehlerhaften Herzschrittmachers, in: JuS 2015, S. 556 ff.
- May, Elisa/Gaden, Justus*: Vernetzte Fahrzeuge. Rechtsfragen zu Over-the-Air-Updates, in: InTer 2018, S. 110 ff.
- Mayr, Stefan/Rauner, Timon/Schweiger, Matthias M.*: Die geplante Produkthaftungsreform und ihre Auswirkungen auf die Medizinproduktehaftung, in: ZfPC 2023, S. 2 ff.
- Mayrhofer, Ann-Kristin*: Außervertragliche Haftung für fremde Autonomie, Tübingen 2023.
- Meents, Jan Geert/Obradovic, Julia*: Pflicht zur Durchführung und Duldung von Over-the-Air-Updates, in: ZfPC 2022, S. 13 ff.
- Meents, Jan Geert*: Over-the-Air-Updates bei vernetzten Fahrzeugen – Pflicht zur Durchführung und Pflicht zur Duldung, in: Specht-Riemenschneider, Louisa/Buchner, Benedikt/Heinze, Christian/Thomsen, Oliver (Hg.): IT-Recht in Wissenschaft und Praxis. Festschrift für Jürgen Taeger, Frankfurt am Main 2020, S. 13 ff. (zitiert als: Meents, in: FS Taeger).

- Mehrbrey, Kim Lars/Schreibauer, Marcus*: Haftungsverhältnisse bei Cyber-Angriffen. Ansprüche und Haftungsrisiken von Unternehmen und Organen, in: MMR 2016, S. 75 ff.
- Meier, Klaus/Wehlau, Andreas*: Produzentenhaftung des Softwareherstellers. § 823 Abs. 1 BGB und das Produkthaftungsgesetz, in: CR 1990, S. 95 ff.
- Meyer, Matthias*: Nanomaterialien im Produkthaftungsrecht. – Die Haftung des Herstellers für neuartige, ungewisse Risiken –, in: VersR 2010, S. 869 ff.
- Meyer, Oliver/Harland, Hanno*: Haftung für softwarebezogene Fehlfunktionen technischer Geräte am Beispiel von Fahrerassistenzsystemen, in: CR 2007, S. 689 ff.
- Michalski, Lutz*: Produktbeobachtung und Rückrufflicht des Produzenten, in: BB 1998, S. 961 ff.
- Mielchen, Daniela*: Verrat durch den eigenen PKW – wie kann man sich schützen?, in: SVR 2014, S. 81 ff.
- Moelle, Henning/Dockhorn, Ilka*: EuGH, Urteil vom 5.3.2015 – C-503/13, C-504/13, in: NJW 2015, S. 1163 ff.
- Molitoris, Michael/Klindt, Thomas*: Die Entwicklung im Produkthaftungs- und Produktsicherheitsrecht, in: NJW 2012, S. 1489 ff.
- Molitoris, Michael/Klindt, Thomas*: Produkthaftung und Produktsicherheit – Ein aktueller Rechtsprechungsüberblick für 2008/2009, in: NJW 2010, S. 1569 ff.
- Molitoris, Michael*: „Kehrtwende“ des BGH bei Produktrückrufen? – Keine generelle Verpflichtung zur kostenfreien Nachrüstung/Reparatur von mit sicherheitsrelevanten Fehlern behafteten Produkten, in: NJW 2009, S. 1049 ff.
- Moos, Flemming/Rothkegel, Tobias*: EuGH, Urteil v. 19.10.2016 – C-582/14 – Breyer (Anmerkung), in: MMR 2016, S. 842 ff.
- Moosmayer, Klaus/Lösler, Thomas* (Hg.): Corporate Compliance. Handbuch der Haftungsvermeidung im Unternehmen, 4. Auflage, München 2024.
- Moseschus, Alexander Marcus*: Hände hoch!. Risiko Produkterpressung und Produktsabotage, in: Risknews 2005, S. 69 ff.
- Müller, Anne-Kathrin*: Software als „Gegenstand“ der Produkthaftung. Zugleich eine Betrachtung des Verhältnisses von § 823 Abs. 1 BGB zum Produkthaftungsgesetz, Baden-Baden 2019.
- Müller, Gerda*: Produkthaftung im Schatten der ZPO-Reform, in: VersR 2004, S. 1073 ff.
- Münchener Kommentar zum Bürgerlichen Gesetzbuch*, hrsg. von *Säcker, Franz Jürgen/Rixecker, Roland/Oetker, Hartmut/Limperf, Bettina*, Bd. 1. Allgemeiner Teil, §§ 1 – 240, Allgemeines Gleichbehandlungsgesetz, 9. Auflage München 2021, Bd. 2. Schuldrecht – Besonderer Teil I, §§ 241 – 310, 9. Auflage München 2022, Bd. 3. Schuldrecht, §§ 311 – 432, 9. Auflage München 2022, Bd. 7. Schuldrecht – Besonderer Teil IV, §§ 705–853, Partnerschaftsgesellschaftsgesetz, Produkthaftungsgesetz, 9. Auflage, München 2024 (zitiert als Bearbeiter, in: MüKo, BGB).
- Niermeier, Florian*: „Gewährleistung“ bei Rückrufen nach der neuen EU-Produktsicherheits-VO, in: NJW 2024, S. 1463 ff.
- Nolte, Henrik/Schreitmüller, Zeynep*: Cybersicherheit KI-basierter Medizinprodukte im Lichte der MDR und KI-VO, in: MPR 2024, S. 20 ff.

- Nomos Kommentar. Bundesdatenschutzgesetz, hrsg. von *Simitis, Spiros*, 8. Auflage, Baden-Baden 2014 (zitiert als Bearbeiter, in: NK-BDSG).
- Nomos Kommentar. Bürgerliches Gesetzbuch. Handkommentar, Schriftleitung *Schulze, Reiner*, Baden-Baden 2024 (zitiert als Bearbeiter, in: NK-BGB).
- Nomos Kommentar. Datenschutzrecht. DSGVO mit BDSG, hrsg. von *Simitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmman, Indra*, Baden-Baden 2022 (zitiert als Bearbeiter, in: NK-DatenschutzR).
- Nomos Kommentar. Produkthaftungs- und Produktsicherheitsrecht. BGB | ProdHaftG | ProdSG | MÜ-VO | MüG | ÜAnlG, hrsg. von *Ehring, Philipp/Taeger, Jürgen*, Baden-Baden 2022 (zitiert als Bearbeiter, in: NK-ProdR).
- Nomos Kommentar. StGB. Strafgesetzbuch, hrsg. von *Kindhäuser, Urs/Neumann, Ulfried/Paeffgen, Hans-Ullrich/Saliger, Frank*, 6. Auflage, Baden-Baden 2023 (zitiert als Bearbeiter, in: NK-StGB).
- Nugel, Michael*: Auslesen von Fahrzeugdaten auf Grundlage der DS-GVO, in: ZD 2019, S. 341 ff.
- Oeben, Marc*: Der potenzielle Produktfehler nach der EuGH-Rechtsprechung. Eine perspektivische Betrachtung für die Haftung der Medizinproduktehersteller in Deutschland, Baden-Baden 2016.
- Oechsler, Jürgen*: Die Haftungsverantwortung für selbstlernende KI-Systeme, in: NJW 2022, S. 2713 ff.
- Ohly, Ansgar*: Ohly: Zwölf Thesen zur Einwilligung im Internet, in: GRUR 2012, S. 983 ff.
- Oppermann, Bernd H./Stender-Vorwachs, Jutta* (Hg.): Autonomes Fahren. Rechtsfolgen, Rechtsprobleme, technische Grundlagen, 1. Auflage, München 2017.
- Oppermann, Bernd H./Stender-Vorwachs, Jutta* (Hg.): Autonomes Fahren. Rechtsfolgen, Rechtsprobleme, technische Grundlagen, 2. Auflage, München 2020.
- Orthwein, Matthias/Obst, Jean-Stephan*: Embedded Systems – Updatepflichten für Hersteller hardwarenaher Software, in: CR 2009, S. 1 ff.
- Ortner, Roderic/Daubenbüchel, Felix*: Medizinprodukte 4.0 – Haftung, Datenschutz, IT-Sicherheit, in: NJW 2016, S. 2918 ff.
- Pfeifer, Tilo/Schmitt, Robert* (Hg.): Masing Handbuch Qualitätsmanagement, 7. Auflage, München 2021.
- Pieper, Fritz-Ulli*: Vertrags- und haftungsrechtliche Fragen der Vernetzung autonomer Systeme, in: Taeger, Jürgen (Hg.): Tagungsband DSRI Herbstakademie 2016. Smart World – Smart Law? Weltweite Netze mit regionaler Regulierung, Edewecht 2016, S. 971 ff. (zitiert als Pieper, DSRI TB 2016, 971).
- Pieper, Helmut*: Verbraucherschutz durch Pflicht zum "Rückruf" fehlerhafter Produkte?, in: BB 1991, S. 985 ff.
- Piltz, Carlo/Reusch, Philipp*: Internet der Dinge: Datenschutzrechtliche Anforderungen bei der Produktbeobachtung, in: BB 2017, S. 841 ff.
- Piltz, Carlo*: Das neue TTDSG aus Sicht der Telemedien. Anwendungsbereich, Tracking und Aufsichtsbehörden, in: CR 2021, S. 555 ff.

- Piovano, Christian/Hess, Christian*: Das neue europäische Produkthaftungsrecht. EU-Produkthaftungsrichtlinie (ProdHaftRL), Baden-Baden 2024.
- Piovano, Christian/Schucht, Carsten/Wiebe, Gerhard*: Quick Guide: Produktbeobachtung in der Digitalisierung. Wie Sie Product Compliance bei der Beobachtung der digitalisierten Produktwelt gewährleisten, Wiesbaden 2023.
- Plagemann, Hermann/Tietzsch, Rainer*: „Stand der Wissenschaft“ und „Stand der Technik“ als unbestimmte Rechtsbegriffe, Tübingen 1980.
- Raith, Nina*: Das vernetzte Automobil. Im Konflikt zwischen Datenschutz und Beweisführung, Wiesbaden 2019.
- Raue, Benjamin*: Raue: Haftung für unsichere Software, in: NJW 2017, S. 1841 ff.
- Redeker, Helmut*: IT-Recht, 8. Auflage, München 2023.
- Reese, Jürgen*: Produkthaftung und Produzentenhaftung für Hard- und Software, in: DStR 1994, S. 1121 ff.
- Regenfus, Thomas*: Deaktivierte Geräte – Rechte des Nutzers bei Einschränkung der Funktionsfähigkeit „smarter“ Produkte durch den Hersteller, in: JZ 2018, S. 79 ff.
- Reich, Norbert*: Fehlerhaftigkeit von Medizinprodukten. Anmerkung zu den Schlussanträgen von Generalanwalt Bot in den verbundenen Rechtssachen C-503 und 504/13 – Boston Scientific Medizintechnik-GmbH, in: EuZW 2014, S. 898 ff.
- Reichwald, Julian/Pfisterer, Dennis*: Autonomie und Intelligenz im Internet der Dinge. Möglichkeiten und Grenzen autonomer Handlungen, in: CR 2016, S. 208 ff.
- Rempe, Christoph*: Smart Products in Haftung und Regress, in: InTer 2016, S. 17 ff.
- Reusch, Philipp*: KI und Software im Kontext von Produkthaftung und Produktsicherheit, in: RDt 2023, S. 152 ff.
- Reusch, Philipp*: Mobile Updates – Updatability, Update-Pflicht und produkthaftungsrechtlicher Rahmen, in: BB 2019, S. 904 ff.
- Reusch, Philipp*: Pflichtenkreis von Unternehmen im Umgang mit unsicheren Produkten – Thesen zum Produktrückruf, in: BB 2017, S. 2248 ff.
- Riehm, Thomas/Stanislaus Meier*: Product Liability in Germany, in: EuCML 2019, S. 161 ff.
- Riehm, Thomas/Leithäuser, Malte/Brenner, Raphael*: Vertragliche Ansprüche auf Sicherheitsaktualisierungen?, in: Raue, Benjamin (Hg.): Digitale Resilienz. Effektives Recht auf Sichere Software, Trier 2024, S. 5 ff.
- Riehm, Thomas/Meier, Stanislaus*: Künstliche Intelligenz im Zivilrecht, in: Fischer, Veronika/Hoppen, Peter J./Wimmers, Jörg (Hg.): DGRI Jahrbuch 2018, Köln 2019, S. 1 ff.
- Riehm, Thomas/Meier, Stanislaus*: OLG Köln, Urteil v. 30.10.2019 – 6 U 100/19 (Anmerkung), in: MMR 2020, S. 250 ff.
- Riehm, Thomas/Meier, Stanislaus*: Rechtliche Durchsetzung von Anforderungen an die IT-Sicherheit, in: MMR 2020, S. 571 ff.

- Riehm, Thomas*: Haftung und Verantwortung für Entscheidungen digitaler autonomer Systeme aus Sicht der Zivilrechtsdogmatik, in: Ständige Deputation des Deutschen Juristentages (Hg.): Verhandlungen des 73. Deutschen Juristentages. Band II/1. Sitzungsberichte – Referate und Beschlüsse. Bonn 2022, München 2023, S. K 47 ff. (zitiert als Riehm, DJT 2022 Referat).
- Riehm, Thomas*: Rechte an Daten – Die Perspektive des Haftungsrechts, in: VersR 2019, S. 714 ff.
- Riehm, Thomas*: Updates, Patches & Co. – Schutz nachwirkender Qualitätserwartungen, in: Schmidt-Kessel, Martin/Kramme, Malte (Hg.): Geschäftsmodelle in der digitalen Welt, S. 201 ff.
- Ritter, Steve*: Welche Befugnisse braucht das BSI, um IT-Sicherheitslücken bekämpfen zu können?, in: Raue, Benjamin (Hg.): Digitale Resilienz. Effektives Recht auf Sichere Software, Trier 2024, S. 79 ff.
- Rockstroh, Sebastian/Kunkel, Hanno*: IT-Sicherheit in Produktionsumgebungen, in: MMR 2017, S. 77 ff.
- Rockstroh, Sebastian/Peschel, Christopher*: Sicherheitslücken als Mangel, in: NJW 2020, S. 3345 ff.
- Rockstroh, Sebastian*: Die Verantwortlichkeit der Hersteller für Schwachstellen in Industriekomponenten, in: Taeger, Jürgen (Hg.): Tagungsband DSRI Herbstakademie 2016. Smart World – Smart Law? Weltweite Netze mit regionaler Regulierung, Ede- wecht 2016, S. 279 ff. (zitiert als Rockstroh, DSRI TB 2016, 279).
- Roos, Philipp/Schumacher, Philipp*: Botnetze als Herausforderung für Recht und Gesellschaft – Zombies außer Kontrolle?, in: MMR 2014, S. 377 ff.
- Rosenberger, Miriam*: Die außervertragliche Haftung für automatisierte Fahrzeuge. Auf Grundlage des Achten Gesetzes zur Änderung des StVG. Baden-Baden 2022.
- Roßnagel, Alexander/Hornung, Gerrit* (Hg.): Grundrechtsschutz im Smart Car. Kommunikation, Sicherheit und Datenschutz im vernetzten Fahrzeug, Wiesbaden 2019.
- Roßnagel, Alexander/Schnabel, Christoph*: Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, in: NJW 2008, S. 3534 ff.
- Roßnagel, Alexander*: Big Data – Small Privacy? – Konzeptionelle Herausforderungen für das Datenschutzrecht, in: ZD 2013, S. 562 ff.
- Rudkowski, Lena*: Aktuelle Herausforderungen für die Rückrufkostenhaftpflichtversicherung, in: VersR 2018, S. 65 ff.
- Ruttloff, Marc/Wagner, Eric/Schuster, Frederic*: Instruktive Produktvideos im Fokus des Produktrechts, in: BB 2022, S. 67 ff.
- Sassenberg, Thomas/Faber, Tobias* (Hg.): Rechtshandbuch Industrie 4.0 und Internet of Things. Praxisfragen und Perspektiven der digitalen Zukunft, München 2020.
- Schallbruch, Martin*: Das IT-Sicherheitsgesetz 2.0 – neue Regeln für Unternehmen und IT-Produkte. Neue Rechtslage im IT-Sicherheitsrecht (Teil I), in: CR 2021, S. 450 ff.
- Schallbruch, Martin*: IT-Sicherheitsrecht – Abwehr von IT-Angriffen, Haftung und Ausblick. Zur Entwicklung des IT-Sicherheitsrechts in der 18. Wahlperiode (Folge 3), in: CR 2018, S. 215 ff.

- Schaub, Renate*: Interaktion von Mensch und Maschine. Haftungs- und immaterialgüterrechtliche Fragen bei eigenständigen Weiterentwicklungen autonomer Systeme, in: JZ 2017, S. 342 ff.
- Schefzig, Jens*: Big Data = Personal Data? Der Personenbezug von Daten bei Big Data-Analysen, in: Taeger, Jürgen (Hg.): Tagungsband DSRI Herbstakademie 2014. Big Data & Co. Neue Herausforderungen für das Informationsrecht, Edewecht 2014, S. 103 ff. (zitiert als Schefzig, DSRI TB 2014, 103).
- Schlotthauer, Sergej/Schmitz, Peter*: IT-Sicherheit und Datenschutz. Security und Privacy by Design und Default, Security Insider, 11.02.2019 (<https://www.security-insider.de/security-und-privacy-by-design-und-default-a-797638/> [Zuletzt abgerufen am 23.09.2024]).
- Schmid, Alexander/Wessels, Ferdinand*: Event Data Recording für das hoch- und vollautomatisierte Kfz – eine kritische Betrachtung der neuen Regelungen im StVG, in: NZV 2017, S. 357 ff.
- Schmid, Alexander*: IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme. Event Data Recording und integrierte Produktbeobachtung als Maßnahmen der IT-Risikominimierung am Beispiel automatisierter und vernetzter Luft- und Straßenfahrzeuge, Berlin 2019.
- Schmid, Alexander*: Pflicht zur „integrierten Produktbeobachtung“ für automatisierte und vernetzte Systeme. Die Verkehrssicherungspflichten des Herstellers als dogmatische Grundlage einer zukunftsfähigeren Produktbeobachtung, in: CR 2019, S. 141 ff.
- Schmidt am Busch, Birgit*: Verhältnis privater Produktbeobachtung und öffentlicher Aufsicht, in: Eifert, Martin (Hg.): Produktbeobachtung durch Private, Berlin 2015, S. 149 ff.
- Schmidt, Mareike*: Produktrückruf und Regress, Tübingen 2013.
- Schmidt-Kessel, Martin*: Digitale Produktsicherheit im neuen Vertragsrecht, in: ZfPC 2022, S. 117 ff.
- Schmitz, Peter*: Datenverarbeitung und Erlaubnis nach EuGH-Rechtsprechung, TT-DSG und DSA, in: MMR 2022, S. 735 ff.
- Schmon, Christoph*: Product Liability of Emerging Digital Technologies, in: IWRZ 2018, S. 254 ff.
- Schonhofen, Sven*: Orientierungshilfe Telemedien 2022, in: ZD 2023, S. 326 ff.
- Schrader, Paul T. /Engstler, Jonathan*: Anspruch auf Bereitstellung von Software-Updates?, in: MMR 2018, S. 356 ff.
- Schrader, Paul T.*: Die neue vertragliche Haftung für „smarte Produkte“, in: JA 2022, S. 1 ff.
- Schrader, Paul T.*: Haftung für fehlerhaft zugelieferte Dienste in Fahrzeugen, in: NZV 2018, S. 489 ff.
- Schrader, Paul T.*: Haftungsfragen für Schäden beim Einsatz automatisierter Fahrzeuge im Straßenverkehr, in: DAR 2016, S. 242 ff.
- Schrader, Paul T.*: Herstellerhaftung nach dem StVG-ÄndG 2017, in: DAR 2018, S. 314 ff.
- Schreck, Giuliana*: Fahrzeugdaten. Möglichkeiten und Grenzen der Nutzung für die forensische Unfallrekonstruktion aus zivilrechtlicher Perspektive, Baden-Baden 2020.

- Schreiber, Kristina/Esser, Julia: Einheitliche Update-Zyklen im Spannungsfeld der §§ 327f, 327r BGB. Aktualisierung und Funktionsänderung, in: RD i 2022, S. 317 ff.
- Schucht, Carsten: Die Produktlebensdauer im Produktsicherheitsrecht, in: BB 2020, S. 1990 ff.
- Schucht, Carsten: Kooperation zwischen Wirtschaftsakteuren und Marktüberwachungsbehörden – auch ein Compliance-Instrument im Produktsicherheits- und Technikrecht, in: BB 2015, S. 654 ff.
- Schucht, Carsten: Produktbeobachtung als Gegenstand des Produktsicherheitsrechts (Teil 1), in: PH i 2023, S. 126 ff.
- Schucht, Carsten: Produktbeobachtung als Gegenstand des Produktsicherheitsrechts (Teil 2), in: PH i 2023, S. 148 ff.
- Schucht, Carsten: Rechtsfallen im Produktrecht, in: BB 2016, S. 456 ff.
- Schucht, Carsten: Safety & Security bei smarten Produkten. Weichenstellungen zur IT-Sicherheit durch den Ausschuss für Produktsicherheit, in: NVwZ 2021, S. 532 ff.
- Schucht, Carsten: Sollbruchstellen in der neuen EU-Marktüberwachungsverordnung, in: EuZW 2020, S. 554 ff.
- Schulte, Martin/Schröder, Rainer (Hg.): Handbuch des Technikrechts, 2. Auflage, Berlin Heidelberg, 2011, S. 337 ff.
- Schulz, Thomas: Sicherheit im Straßenverkehr und autonomes Fahren, in: NZV 2017, S. 548 ff.
- Schulz, Thomas: Verantwortlichkeit bei autonom agierenden Systemen. Fortentwicklung des Rechts und Gestaltung der Technik, Baden-Baden 2015.
- Schuster, Fabian/Grützmaker, Malte (Hg.): IT-Recht. Kommentar. EU-Recht. Nationales Recht. Besondere Vertragsbedingungen, Hamburg 2020 (zitiert als Bearbeiter, in: Schuster/Grützmaker (Hg.), IT-Recht).
- Schuster, Frank Peter: Providerhaftung und der Straßenverkehr der Zukunft, in: Hilgenhof, Eric (Hg.): Autonome Systeme und neue Mobilität. ausgewählte Beiträge zur 3. und 4. Würzburger Tagung zum Technikrecht, Baden-Baden 2017, S. 49 ff.
- Schwenzer, Ingeborg: Rückruf- und Warnpflichten des Warenherstellers, in: JZ 1987, S. 1059 ff.
- Seehafer, Astrid/Kohler, Joel: Künstliche Intelligenz: Updates für das Produkthaftungsrecht?, in: EuZW 2020, S. 213 ff.
- Sessa-Jahn, Claudia: Automatisiertes Fahren – Haftung und Regress, Wien 2022.
- Seufert, Julia: Cybersicherheitsrechtliche Anforderungen an die Automobilindustrie. Überblick und Umsetzungsempfehlung der UN-Regelung Nr. 155 für Cybersicherheit in Fahrzeugen, in: CR 2023, S. 73 ff.
- Siglmüller, Jonas: Cyber Resilience Act und Digital Operational Resilience Act – Lässt sich IT-Sicherheit rechtlich erzwingen?, in: ZfPC 2023, S. 221 ff.
- Söbbing, Thomas: Embedded Software. Rechtliche Grenzen der Veräußerung und Vermietung von Systemen mit eingebetteter Software, in: ITRB 2013, S. 162 ff.

- Söbbing, Thomas*: Security Vulnerability: Ist eine Sicherheitslücke in einer Software ein Mangel i.S.v. § 434 BGB? (§ 434 BGB). Erörterung unter Berücksichtigung der bisherigen Gesetzeslage, der einschlägigen Entscheidungen und der zukünftigen Neuerung durch entsprechenden EU-Richtlinien, in: ITRB 2020, S. 12 ff.
- Soergel, BGB Bürgerliches Gesetzbuch mit Einführungsgesetz und Nebengesetzen Kommentar*, begr. von *Soergel, Hans-Theodor*, Bd. 12 Schuldrecht, §§ 823 – 853, ProdHG, UmweltHG, 13. Auflage, Stuttgart 2005 (zitiert als Bearbeiter, in: Soergel, BGB).
- Solmecke, Christian/Vondrlík, Simon-Elias*: Rechtliche Probleme bei Produkten mit serverbasierten Zusatzdiensten – Was passiert, „wenn der Kühlschrank keine Einkaufsliste mehr schreibt ...“, in: MMR 2013, S. 755 ff.
- Solmecke, Christian/Wahlers, Jakob*: Rechtliche Situation von Social Media Monitoring-Diensten – Rechtskonforme Lösungen nach dem Datenschutz- und dem Urheberrecht, in: ZD 2012, S. 550 ff.
- Sommer, Martin*: Haftung für autonome Systeme. Verteilung der Risiken selbstlernender und vernetzter Algorithmen im Vertrags- und Deliktsrecht, Baden-Baden 2020.
- Sorge, Christoph*: Maschinelle Verantwortlichkeit: Technische Grundlagen und rechtliche Schlussfolgerungen, in: Hornung, Gerrit (Hg.): Rechtsfragen der Industrie 4.0, Baden-Baden 2018, S. 139 ff.
- Sosnitza, Olaf*: Das Internet der Dinge – Herausforderung oder gewohntes Terrain für das Zivilrecht?, in: CR 2016, S. 764 ff.
- Specht, Louisa/Herold, Sophie*: Roboter als Vertragspartner?. Gedanken zu Vertragsabschlüssen unter Einbeziehung automatisiert und autonom agierender Systeme, in: MMR 2018, S. 40 ff.
- Specht, Louisa/Mantz, Reto* (Hg.): Handbuch Europäisches und deutsches Datenschutzrecht. Bereichsspezifischer Datenschutz in Privatwirtschaft und öffentlichem Sektor, München 2019.
- Spiecker gen. Döhmman, Indra*: Zur Zukunft systemischer Digitalisierung – Erste Gedanken zur Haftungs- und Verantwortungszuschreibung bei informationstechnischen Systemen. Warum für die systemische Haftung ein neues Modell erforderlich ist, in: CR 2016, S. 698 ff.
- Spindler, Gerald/Schmitz, Peter/Liesching, Marc* (Hg.): Telemediengesetz mit Netzwerkdurchsetzungsgesetz. Kommentar, 2. Auflage, München 2018 (zitiert als: Bearbeiter, in: Spindler/Schmitz, TMG).
- Spindler, Gerald*: Die Vorschläge der EU-Kommission zu einer neuen Produkthaftung und zur Haftung von Herstellern und Betreibern Künstlicher Intelligenz Die haftungsrechtliche Einordnung von Software als Produkt nach Unionsrecht – endlich, in: CR 2022, S. 689 ff.
- Spindler, Gerald*: IT-Sicherheit – Rechtliche Defizite und rechtspolitische Alternativen, in: MMR 2008, S. 7 ff.
- Spindler, Gerald*: IT-Sicherheit und Produkthaftung – Sicherheitslücken, Pflichten der Hersteller und der Softwarenutzer, in: NJW 2004, S. 3145 ff.

- Spindler, Gerald*: IT-Sicherheitsgesetz und zivilrechtliche Haftung. Auswirkungen des IT-Sicherheitsgesetzes im Zusammenspiel mit der endgültigen EU-NIS-Richtlinie auf die zivilrechtliche Haftung, in: CR 2016, S. 297 ff.
- Spindler, Gerald*: Roboter, Automation, künstliche Intelligenz, selbst-steuernde Kfz – Braucht das Recht neue Haftungskategorien?. Eine kritische Analyse möglicher Haftungsgrundlagen für autonome Steuerungen, in: CR 2015, S. 766 ff.
- Spindler, Gerald*: User Liability and Strict Liability in the Internet of Things and for Robots, in: Lohsse, Sebastian/Schulze, Reiner/Staudenmayer, Dirk (Hg.): Liability for Artificial Intelligence and the Internet of Things. Münster Colloquia on EU Law and the Digital Economy IV, Baden-Baden 2019, S. 125 ff.
- Spindler, Gerald*: Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären. Studie im Auftrag des BSI, Bonn 2007.
- Spindler, Gerald*: Verschuldensabhängige Produkthaftung im Internet, in: MMR 1998, S. 23 ff.
- Spindler, Gerald*: Zivilrechtliche Fragen beim Einsatz von Robotern, in: Hilgendorf, Eric (Hg.): Robotik im Kontext von Recht und Moral, Baden-Baden 2014, S. 63 ff.
- Ständige Deputation des Deutschen Juristentages* (Hg.): Verhandlungen des 73. Deutschen Juristentages. Band II/2. Sitzungsberichte – Diskussion und Beschlussfassung: Hamburg 2020/Bonn 2022, München 2023, S. (zitiert als Redebeitrag, DJT 2022 Diskussion).
- Staudenmayer, Dirk*: Haftung für Künstliche Intelligenz, in: NJW 2023, S. 894 ff.
- Staudinger, Ansgar/Czaplinski, Paul*: Rückruf- und Kostentragungspflicht des Produzenten bei In- wie Auslandssachverhalten, in: JA 2008, S. 401 ff.
- Steege, Hans*: Auswirkungen von künstlicher Intelligenz auf die Produzentenhaftung in Verkehr und Mobilität. Zum Thema des Plenarvortrags auf dem 59. Deutschen Verkehrsgerichtstag, in: NZV 2021, S. 6 ff.
- Steege, Hans*: Haftung für Künstliche Intelligenz im Straßenverkehr, in: SVR 2023, S. 9 ff.
- Steffen, Erich*: Verkehrspflichten im Spannungsfeld von Bestandsschutz und Handlungsfreiheit, in: VersR 1980, S. 409 ff.
- Steinrötter, Björn*: Datenschutz als Gretchenfrage für autonome Mobilität, in: ZD 2021, S. 513 ff.
- Stiernerling, Oliver*: „Künstliche Intelligenz“ – Automatisierung geistiger Arbeit, Big Data und das Internet der Dinge. Eine technische Perspektive, in: CR 2015, S. 762 ff.
- Stöhr, Karlheinz*: Dauerhaftigkeit der Produkthaftung, in: PHi 2015, S. 206 ff.
- Stöhr, Karlheinz*: Haftung trotz eines perfekten Rückrufs?, in: Greiner, Hans-Peter/Gross, Norbert/Nehm, Kay/Spickhoff, Andreas (Hg.): Neminem laedere. Aspekte des Haftungsrechts. Festschrift für Gerda Müller zum 65. Geburtstag am 26. Juni 2009, Köln 2009, S. 173 ff. (zitiert als: Stöhr, in: FS Müller).
- Taeger, Jürgen/Gabel, Detlev* (Hg.): DSGVO – BDSG – TTDSG. Kommentar, 4. Auflage, Frankfurt am Main 2022.

- Taeger, Jürgen/Pohle, Jan*: Computerrechts-Handbuch. Informationstechnologie in der Rechts- und Wirtschaftspraxis, Stand: 39. EL April 2024 (Teil 18, Stand: 38. EL August 2023), München 2024.
- Taeger, Jürgen*: Produkt- und Produzentenhaftung bei Schäden durch fehlerhafte Computerprogramme, in: CR 1996, S. 257 ff.
- Tamme, Andreas*: Rückrufkosten. Haftung und Versicherung, Karlsruhe 1996.
- Taschner, Hans Claudius*: Die künftige Produzentenhaftung in Deutschland, in: NJW 1986, S. 611 ff.
- Taschner, Hans Claudius*: Produkthaftung – Noch einmal: Verschuldenshaftung oder vom Verschulden unabhängige Haftung?, in: ZEuP 2012, S. 560 ff.
- Teubner, Gunther*: Digitale Rechtssubjekte?, Zum privatrechtlichen Status autonomer Softwareagenten, in: AcP 218 (2018), S. 155 ff.
- Theurer, Jakob/Reinsberg, Johannes/Borst, Leopold/Bosch, Philipp*: Perspektiven der Produkthaftung und Produktsicherheit in der Industrie 4.0, in: ZdiW 2021, S. 83 ff.
- Thöne, Meik*: Autonome Systeme und deliktische Haftung. Verschulden als Instrument adäquater Haftungsallokation?, Tübingen 2020.
- Thöne, Meik*: Der produktsicherheitsrechtliche Rückruf – Anlass zur Neuordnung haftungsrechtlicher Determinanten?, in: ZfPC 2024, S. 49 ff.
- Thürmann, Dagmar*: Rückruf und Haftpflichtversicherung nach AHB oder ProdHB, in: NVersZ 1999, S. 145 ff.
- Ulmer, Peter*: Produktbeobachtungs-, Prüfungs- und Warnpflichten eines Warenherstellers in bezug auf Fremdprodukte?, – Delikts-, wettbewerbs- und kartellrechtliche Bemerkungen zum Honda-Urteil BGHZ 99, 167, in: ZHR 152 (1988), S. 564 ff.
- v. *Bar, Christian*: Die Grenzen der Haftung des Produzenten, in: Lieb, Manfred (Hg.): Produktverantwortung und Risikoakzeptanz: Kriterien der Risikoverteilung; wissenschaftliches Symposium der Bayer-Stiftung für Deutsches und Internationales Arbeits- und Wirtschaftsrecht am 28. und 29. November 1996 in Leverkusen, München 1998, S. 29 ff.
- v. *Bar, Christian*: Vorbeugender Rechtsschutz vor Verkehrspflichtverletzungen, in: 25 Jahre Karlsruher Forum: Beiträge zum Haftungs- und Versicherungsrecht, Jubiläumsausgabe 1983, Beilage VersR 1983, S. 80 ff. (zitiert als v. Bar, Karlsruher Forum 1983).
- v. *Bodungen, Benjamin/Hoffmann, Martin*: Autonomes Fahren – Haftungsverschiebung entlang der Supply Chain? (2. Teil), in: NZV 2016, S. 503 ff.
- Vaniea, Kami/Rader, Emilee/Wash, Rick*: Betrayed By Updates: How Negative Experiences Affect Future Security, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14), S. 2671 ff.
- Vofß, Wiebke*: Recht ohne Realisierungschance? – Zur (kollektiven) Durchsetzung privater Ansprüche auf Sicherheitsupdates, in: Raue, Benjamin (Hg.): Digitale Resilienz. Effektives Recht auf Sichere Software, Trier 2024, S. 97 ff.
- Wagner, Eric/Ruttloff, Marc/Miederhoff, Rebecca*: Product Compliance – Ein wesentlicher Baustein für Compliance-Organisationen, in: CCZ 2020, S. 1 ff.

- Wagner, Eric/Ruttloff, Marc/Römer, Sophie: Neuerungen und digitale Aspekte des Vorschlags der EU-Kommission für eine neue Produkthaftungsrichtlinie, in: CCZ 2023, S. 109 f.
- Wagner, Gerhard, Deliktsrecht, 14. Auflage, München 2021.
- Wagner, Gerhard: BGH, Urteil v. 16.12.2008, VI ZR 170/07 (Anmerkung), in: JZ 2009, S. 905 ff.
- Wagner, Gerhard: Der Fehlerverdacht als Produktfehler, in: JZ 2016, S. 292 ff.
- Wagner, Gerhard: Prävention und Verhaltenssteuerung durch Privatrecht – Anmaßung oder legitime Aufgabe?, in: AcP 206 (2006), S. 352 ff.
- Wagner, Gerhard: Privatrechtliche Haftung und öffentlich-rechtliche Produktbeobachtung, in: Eifert, Martin (Hg.): Produktbeobachtung durch Private, Berlin 2015, S. 115 ff.
- Wagner, Gerhard: Produkthaftung für autonome Fahrzeuge – die zweite Spur der Straßenverkehrshaftung, in: NJW 2023, S. 1313 ff.
- Wagner, Gerhard: Produkthaftung für autonome Systeme, in: AcP 217 (2017), S. 707 ff.
- Wagner, Gerhard: Produkthaftung für das digitale Zeitalter – ein Paukenschlag aus Brüssel, in: JZ 2023, S. 1 ff.
- Wagner, Gerhard: Produktvigilanz und Haftung, in: VersR 2014, S. 905 ff.
- Wagner, Gerhard: Robot Liability, in: Lohsse, Sebastian/Schulze, Reiner/Staudenmayer, Dirk (Hg.): Liability for Artificial Intelligence and the Internet of Things. Münster Colloquia on EU Law and the Digital Economy IV, Baden-Baden 2019, S. 27 ff.
- Wagner, Gerhard: Schadensersatz wegen Verletzung von Unionsrecht – Luxemburg locuta, causa aperta, in: NJW 2023, S. 1761 ff.
- Wagner, Gerhard: Verantwortlichkeit im Zeichen digitaler Techniken, in: VersR 2020, S. 717 ff.
- Wahlster, Wolfgang: Künstliche Intelligenz als Grundlage autonomer Systeme, in: Informatik Spektrum 2017, S. 409 ff.
- Weisser, Ralf/Färber, Claus: Rechtliche Rahmenbedingungen bei Connected Car – Überblick über die Rechtsprobleme der automobilen Zukunft, in: MMR 2015, S. 506 ff.
- Wellenhofer, Marina: Sachenrecht, 39. Auflage, München 2024.
- Wende, Susanne: Software in IoT-Plattformen, in: RDİ 2021, S. 341 ff.
- Wendehorst, Christiane: Aktualisierungen und andere digitale Dauerleistungen. Das neue Gewährleistungsrecht auf dem Prüfstand, in: Stabenheiner, Johannes/Wendehorst, Christiane/Zöchling-Jud, Brigitta (Hg.): Das neue europäische Gewährleistungsrecht. Zu den Richtlinien (EU) 2019/771 über den Warenkauf sowie (EU) 2019/770 über digitale Inhalte und digitale Dienstleistungen, Wien 2019, S. 111 ff.
- Wendehorst, Christiane: Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge. Teil 2: Wissenschaftliches Rechtsgutachten, Berlin 2016 (zitiert als: Wendehorst, Besitz- und Eigentumsverhältnisse beim Internet der Dinge – Rechtsgutachten).
- Wendt, Janine/Oberländer, Marcel: Produkt- und Produzentenhaftung bei selbstständig veränderlichen Systemen, in: InTeR 2016, S. 58 ff.

- Wiebe, Andreas: Der Data Act – Innovation oder Illusion?, in: GRUR 2023, S. 1569 ff.
- Wiebe, Gerhard/Daelen, Johannes: Der Cyber Resilience Act aus produktsicherheitsrechtlicher Perspektive, in: EuZW 2023, S. 257 ff.
- Wiebe, Gerhard: Cybersicherheitsrecht 2.0 – Vorschlag eines Cyber Resilience Act, in: ZRP 2023, S. 73 ff.
- Wiebe, Gerhard: IT-sicherheitsbezogene Pflichten von Herstellern smarter Produkte, in: InTer 2020, S. 66 ff.
- Wiebe, Gerhard: Produktsicherheitsrechtliche Betrachtung des Vorschlags für eine KI-Verordnung, in: BB 2022, S. 899 ff.
- Wiebe, Gerhard: Produktsicherheitsrechtliche Pflicht zur Bereitstellung sicherheitsrelevanter Software-Updates, in: NJW 2019, S. 625 ff.
- Wiebe, Gerhard: Unternehmerfreiheit versus Verbraucherschutz?!. Das Verhältnis zwischen Unternehmerfreiheit und Verbraucherschutz im Spiegel des öffentlichen Verbraucherschutzrechts, Baden-Baden 2017.
- Wiesemann, Hans Peter/Mattheis, Clemens/Wende, Susanne: Software-Updates bei vernetzten Geräten, in: MMR 2020, S. 139 ff.
- Wiesemann, Hans Peter: Die Update-Pflicht für Firmware. Praxisleitfaden zur Bestimmung des Bereitstellungszeitraums und zur Umsetzung der Aktualisierungspflicht bei Waren mit digitalen Elementen, in: MMR 2022, S. 343 ff.
- Wilrich, Thomas, Das neue Produktsicherheitsgesetz (ProdSG). Leitfaden für Hersteller, Importeure und Händler, Berlin, Wien, Zürich, 2012 (zitiert als Wilrich, ProdSG).
- Wittbrodt, Saskia: Industrie 4.0 und die Haftung für Maschinensoftware, in: InTer 2020, S. 74 ff.
- Wittig, Daniel: Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, Baden-Baden 2021.
- Wurm, Manuel: Automotive Cybersecurity. Security-Bausteine für Automotive Embedded Systeme, Berlin 2022.
- Xia, Haohan: Die Pflicht zum Produktrückruf gemäß § 823 Abs.1 BGB unter Berücksichtigung der neueren Rechtsprechung, Berlin 2019.
- Xylander, Benedikt Julian: Die Verantwortlichkeit des Herstellers automatisierter PKW nach Deliktsrecht sowie nach dem Produkthaftungsgesetz, Berlin 2021.
- Yamaguchi, Fabian/Rieck, Konrad: Die Codeanalyseplattform „Octopus“. Semi-automatisierte Schwachstellenidentifikation mit Big Data Technologien, in: DuD 2016, S. 713 ff.
- Zech, Herbert: Entscheidungen digitaler autonomer Systeme: Empfehlen sich Regelungen zu Verantwortung und Haftung?. Gutachten A zum 73. Deutschen Juristentag, in: Ständige Deputation des Deutschen Juristentages (Hg.): Verhandlungen des 73. Deutschen Juristentages. Band I. Gutachten. Hamburg 2020/Bonn 2022, München 2020, S. A 1 ff. (zitiert als Zech, DJT 2020 Gutachten).
- Zech, Herbert: Gefährdungshaftung und neue Technologien, in: JZ 2013, S. 21 ff.
- Zech, Herbert: Künstliche Intelligenz und Haftungsfragen, in: ZfPW 2019, S. 198 ff.

H. Literaturverzeichnis

Zech, Herbert: Zivilrechtliche Haftung für den Einsatz von Robotern – Zuweisung von Automatisierungs- und Autonomierisiken, in: Gless, Sabine/Seelmann, Kurt (Hg.): *Intelligente Agenten und das Recht*, Baden-Baden 2016, S. 163 ff.