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 ProdSG[820] 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 Hersteller[822] 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: 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 insoweit 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/Steege (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 Stichprobenentnahme[852] 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 Fachkongresse[855] 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 Werbeaussagen[862] – maßgeblich die berechtigte 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 beigefügte Bedienungsanleitung erfolgte. Denn eine solche wird durch den zeitlich nachfolgenden und für die Nutzer vermeintlich neueren 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 ich 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 öffentlichrechtlichen 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-Guideline[881] 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 steigere. 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 „Kinderschuhen" stecke.

898 Vgl. folgenden Pressebericht zum Anbieter Consline AG (https://consline.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 Consline 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/Braegelmann (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/assistenzsysteme/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 diente 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 Risiko[949] 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 festlegt[954] 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 Anforderrungen, 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/Steege (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 gewonnen 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 gewonnen 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] Vergegenwärtigt 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); *Grützmacher*, 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 *Piovano/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 Gefahrengeneigtheit des Produkts und die Schadenshöhe an. Sodann ist bei dieser Betrachtung einzustellen, dass schon die allgemein erhöhte Gefahrengeneigtheit smarter Produkte aufgrund der bestehenden Unsicherheiten nach dem Inverkehrbringen zu einer erhöhten Eintrittswahrscheinlichkeit von Schädigungen führt, die zu der individuellen und produktspezifischen Gefahrengeneigtheit 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 Gefahrengeneigtheit 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/Geminn*, 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 Act[1009] 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/Braegelmann (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.

I. 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. Düsseldorfer 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 erhobenen 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 vorlegende 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 Auskunftsrechte 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 Düsseldorfer 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 zuordnen 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" Gefahrenabwendungsmaßnahmen 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 Betroffenem 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, ein 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 Telemediendiensts 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] Anderseits wird angeführt, dass die Ausnahmevorschrift 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-VO[1109] 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.1.c).
1114 So *Bomhard/Merkle*, RDi 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.