G. Zusammenfassung

1. Die deliktische Produzentenhaftung und damit auch die Produktbeobachtungspflicht des Herstellers nach § 823 Abs. 1 BGB sind technikneutral ausgestaltet und finden daher auf Software und embedded Software Anwendung. Denn die Verantwortlichkeit des Herstellers knüpft – anders als das ProdHaftG – nicht an eine wie auch immer geartete Produktqualität, sondern allgemein an Verkehrssicherungspflichten und die geschaffene Gefahrenlage an.
2. Die Produktbeobachtungspflicht perpetuiert die Herstellerverantwortung für das Produkt über den Zeitpunkt des Inverkehrbringens hinaus. Über die Produktbeobachtungspflicht hat der Hersteller die Produktsicherheit seiner Produkte auch nach dem Inverkehrbringen kontinuierlich zu überwachen und gegebenenfalls Gefahrensteuerungsmaßnahmen zu ergreifen. Die Verantwortlichkeit des Herstellers über den Zeitpunkt der Inverkehrgabe hinaus lässt sich dabei nicht mit dem Inverkehrbringen des Produkts allein begründen. Vielmehr muss berücksichtigt werden, ob die vom Hersteller abverlangte Gefahrensteuerung noch in einem angemessenen Verhältnis zu dem von ihm gesetzten Risiko bei Inverkehrgabe steht.
   a) Dies ist jedenfalls dann der Fall, wenn das Produkt bereits bei seinem Inverkehrbringen fehlerhaft war oder ein Entwicklungsfehler vorliegt. Denn ohne dass es auf eine Pflichtverletzung des Herstellers ankäme, entsprach das Produkt bereits bei Inverkehrgabe nicht den berechtigten Sicherheitserwartungen. Aufgrund der objektiven Fehlerhaftigkeit des Produkts, geht von ihm eine Gefahr aus, die auf den Herstellungsprozess zurückzuführen ist. Als Inhaber der Bestimmungsgewalt während des Produktionsvorgangs fällt die Fehlerhaftigkeit in den Verantwortungsbereich des Herstellers. Die Verantwortlichkeit des Herstellers rührt aus der von ihm geschaffenen andauernden Gefahrenquelle, auch wenn das Sicherheitsdefizit erst in der Nutzungsphase erkennbar wird.
   b) Bei einer Entwicklungslücke haben die Produkte indes bei Inverkehrgabe den historischen Sicherheitserwartungen entsprochen. Gewährleistet ein Produkt die Basissicherheit, darf es trotz nicht (zumutbar) vermeidbarer Restgefahren in den Verkehr gebracht werden. Wird das Produkt nun aber aufgrund der Weiterentwicklung von Wis-

senschaft und Technik den gehobeneren Sicherheitsstandards nicht mehr gerecht, ist gleichwohl die Verantwortung des Herstellers nach der Inverkehrgabe angesprochen. Auch den Hersteller, der eine Gefahr zunächst nicht abwenden konnte, das Produkt aber trotz Kenntnis der unvermeidbaren Gefährlichkeit in den Verkehr gebracht hat, müssen nach dem Inverkehrbringen latente Pflichten treffen. Insoweit haftet dem Produkt eine inhärente Gefahr an, die auf den Herstellungsprozess zurückzuführen ist und die damit aus der Sphäre des Herstellers stammt. Die Fortschreibung der Verantwortung für das Produkt knüpft als Kehrseite an das Inverkehrbringen einer unbeherrschbaren Gefahrenquelle an.

c) Soll dagegen keine bereits bei der Inverkehrgabe vorliegende Sicherheitslücke geschlossen werden, sondern kommt es infolge der Weiterentwicklung des Standes von Wissenschaft und Technik zu Produktverbesserungen (Produktalterung), fehlt es mangels entsprechendem Gefahrenlevels bei Inverkehrgabe an einem Zurechnungsgrund zur Begründung einer Verkehrspflicht des Herstellers für die Phase nach der Inverkehrgabe.

3. Gerade diese Phase nach dem Inverkehrbringen gewinnt bei Software und smarten Produkten an Bedeutung, da moderne Software hochkomplex und deshalb fehleranfällig ist. So führt die Vernetzung mit anderen Systemen zu nicht vollumfänglich abschätzbaren Kombinationsrisiken und Fehlfunktionen ergeben sich aus dem Zusammenspiel der einzelnen Systeme. Zudem werden Sicherheitslücken der Software oft erst im Laufe der Zeit bekannt und Bedrohungslagen ändern sich fortlaufend. Hinzu kommt, dass die Entscheidungen autonomer Systeme ex ante nicht exakt vorhersehbar sind. Daher ist eine abschließend sichere Entwicklung am Reißbrett kaum möglich. Im Einzelnen:

a) Bei der Tatsache, dass Software nie gänzlich fehlerfrei ist, handelt es sich zunächst um eine technische Kategorie. Die Erwartung des Nutzers geht indes dahin, dass der Hersteller diejenigen Qualitätssicherungsmaßnahmen ergreift, die dem Stand von Wissenschaft und Technik entsprechen. Sofern die Basissicherheit erreicht wird, schuldet der Hersteller aber nur solche Sicherheitsvorkehrungen, die ihm auch zumutbar sind. Aufgrund der technisch erhöhten Fehleranfälligkeit bei der Softwareentwicklung befindet sich gleichwohl eine hohe Dunkelziffer an produkthaftungsrechtlich fehlerhaften Produkten im Verkehr, die wegen Programmierfehlern die Basissicherheit nicht gewährleisten. Andere Produkte sind mit Entwicklungslücken

behaftet. Sie gewährleisten zwar die Basissicherheit und sind im produkthaftungsrechtlichen Sinne nicht fehlerhaft, weisen jedoch Programmierfehler auf, deren Behebung aufgrund der kostenintensiven Testläufe zum Aufsuchen von Fehlern bei der Inverkehrgabe nicht zumutbar war. Daneben sind haftungsausschließende Entwicklungsfehler denkbar, bei denen der Programmierfehler auch objektiv erst nach der Inverkehrgabe erkennbar wird.

Über die Produktbeobachtungspflicht wird der Hersteller hierfür aber über den Zeitpunkt der Inverkehrgabe hinaus in Verantwortung genommen.

b) Auch Anforderungen an die IT-Sicherheit sind vom produkthaftungsrechtlichen Fehlerbegriff umfasst, sodass der Hersteller die digitale Resilienz seiner Softwareprodukte gewährleisten muss. Traditionell bezieht sich die Produktsicherheit zwar auf den Schutz vor produktbezogenen Gefahren (safety), während IT-Sicherheit den Schutz vor unbefugten Eingriffen auf das Produkt bedeutet (security). Spätestens mit der Implementierung von Software in physische Produkte beschränken sich Gefährdungen durch das Ausnutzen von Sicherheitslücken nicht mehr auf die Schutzgüter der security. Vielmehr kann ein Zugriff von außen Integritätsschäden und damit wiederum safety-relevante Gefahren nach sich ziehen, die klassischerweise dem Rechtsgüterschutz des Produkthaftungsrechts unterfallen. Dass es sich bei einem Hackerangriff um eine bewusste und vorsätzliche Schädigung eines Dritten handelt, schließt die Verantwortlichkeit des Herstellers dabei nicht aus. Entsprechend den allgemeinen Erwägungen der Kausalitätslehre und des Deliktsrechts besteht bei einer bei Inverkehrgabe vorhandenen Sicherheitslücke, die ein mögliches Einfallstor für Hacker darstellt, eine latente und vom Hersteller zu verantwortende besondere Gefahrenlage, die eine schädigende Handlung Dritter erst ermöglicht oder zumindest wesentlich erleichtert. Damit schließt das vorsätzliche Dazwischentreten Dritter die Zurechnung nicht aus. Gleichwohl besteht keine absolute Haftung für Schäden, die durch Angriffe von Hackern verursacht werden. Geschuldet ist nach allgemeinen Grundsätzen die Sorgfalt im Rahmen des Möglichen und Zumutbaren.

Da Sicherheitslücken nichts anderes als ausnutzbare Softwarefehler sind, gelten hinsichtlich der Produktbeobachtungspflicht die dort aufgestellten Grundsätze. Werden indes neue Angriffsmethoden entwickelt, die bei Inverkehrgabe noch nicht absehbar waren – z.B.

durch neue kryptographische Methoden, die eine zunächst sichere Verschlüsselung angreifbar machen - entspricht dies der Produktalterung, welche keine nachträgliche Verantwortung des Herstellers auslöst.

c) Hinsichtlich der Gefahren, die sich aus der Vernetzung einzelner Systeme ergeben, trägt der Hersteller bei der Verfolgung eines geschlossenen Ansatzes die volle Verantwortung hinsichtlich des Auftretens von Kombinationsrisiken. Bezieht der Hersteller eines IoT-Geräts Komponenten (insbesondere Software) von einem Zulieferer, ist er dafür verantwortlich, dass sich auch aus der Kombination der für sich genommen fehlerfreien Komponenten keine Gefahren ergeben. Denn die Systemkonzeption und die Sicherheitsarchitektur lässt sich insgesamt auf den Hersteller zurückführen. Die Abstimmung und die Zuverlässigkeit der einzelnen Komponenten, insbesondere auch deren Wechselwirkungen unterliegen allein seiner Herrschaftssphäre. Ähnlich verhält es sich beim Vorhalten eines eigenen App-Stores, über den Drittanbieter ihre Apps bereitstellen. Hier kann der Hersteller selbst bestimmen, welche Drittanbieter ihre Apps bereitstellen dürfen. Damit behält er die Kontrolle über die verfügbaren Apps und ist in der Lage, Sicherheitsstandards durchzusetzen. Darauf vertraut auch der Nutzer. Bei einem offenen System hält der Hersteller dagegen lediglich die Schnittstelle oder den Zugang zu einem App-Store eines großen Anbieters vor und öffnet somit das System und lässt Produktergänzungen durch den Nutzer oder Dritte zu. Dieses Weniger an Herstellerkontrolle in Bezug auf die Abstimmung und das Zusammenspiel der Produkte rechtfertigt es, den Nutzer, der die Geräte kombiniert, hinsichtlich der Systemkompatibilität verstärkt in die Pflicht zu nehmen. Hier trifft den Hersteller nur die Produktbeobachtungspflicht entsprechend der Grundsätze der Honda-Entscheidung für allgemeingebräuchliches Zubehör.

Falsche Daten, die das IoT-Gerät bezieht und auf die es angewiesen ist, fallen dagegen im Ausgangspunkt auch bei geschlossenen Systemen und bestehender Geschäftsbeziehung zwischen dem Hersteller und dem Daten-Zulieferer in den alleinigen Verantwortungsbereich des Zulieferers. Da das IoT-Produkt fortlaufend mit Daten beliefert wird und diese selbständig und in Echtzeit vom Gerät verarbeitet und umgesetzt werden, ist dem Hersteller eine auch stichprobenartige Überprüfung der Daten – anders als bei herkömmlichen Zulieferteilen – vor der Verarbeitung nicht möglich. Dieses Defizit an Kon-

trollmöglichkeit der Daten im Vorfeld muss durch eine sorgfältige Auswahl des Informationsanbieters im Rahmen der herstellerseitigen Organisations- und Kontrollpflichten ausgeglichen werden. Weiter wird die Stichprobenkontrolle nachgelagert stattfinden müssen und kann Reaktionspflichten nach sich ziehen. Bei offenen Systemen dagegen schuldet der Hersteller keine Produktbeobachtung hinsichtlich dieser fehlervermittelnden Gefahren. Die Honda-Entscheidung betrifft lediglich Kombinationsrisiken und ist auf Fehler im alleinigen Verantwortungsbereich des Zubehörherstellers bzw. des Informationsanbieters nicht übertragbar.

d) Entwickelt ein autonomes System trotz einer Programmierung und eines Trainings, das dem Stand von Wissenschaft und Technik entsprach, eine schädigende Verhaltensweise nach der Inverkehrgabe, handelt es sich beim so verstandenen Autonomierisiko um eine Entwicklungslücke. Der Hersteller wird dann aber über die Produktbeobachtungspflicht auch für das Autonomierisiko in Verantwortung genommen.

4. Bei der Erfüllung der Produktbeobachtungspflicht hat der Hersteller die Möglichkeiten, die sich durch die Digitalisierung bieten, auch zu nutzen. Denn die Produktbeobachtungspflicht als Verkehrspflicht muss sich auch am Stand der Wissenschaft und Technik ausrichten.
5. Im Rahmen der Produktbeobachtung i.e.S. führt die die zunehmende Datenverfügbarkeit und Datenkenntnis auch zu einer Ausdehnung der Verantwortung des Herstellers.
   a) Der Hersteller hat seine Produktbeobachtung auch auf zugängliche Informationen über sicherheitskritische Eigenschaften seines Produkts im Internet zu erstrecken. Dies muss zunächst dort gelten, wo den Hersteller die Information auf einer unternehmenseigenen Internetseite oder auf externen Seiten auf einem vom Hersteller eingerichteten Unternehmensprofil erreicht. Unabhängig vom Kommunikationsweg muss der Hersteller alle Informationen, die ihn erreichen, auch auswerten. Daneben hat der Hersteller grundsätzlich auch sicherzustellen, dass er Meldungen über Produktgefahren auf sonstigen Social-Media-Kanälen wahrnimmt. Hier führen automatisierte Prozesse und KI-gestützte Big Data-Auswertungen sowie die Möglichkeit der Auslagerungen an externe Dienstleister zu einer Verschiebung der Kriterien der Erforderlichkeit und Zumutbarkeit zu Lasten des Herstellers. In einer Zeit, in der Unternehmen aus Marketinggründen unermüdlich Daten über den Nutzer und sein Nutzungsverhalten

sammeln, ist ihnen auch ein Social-Media-Monitoring hinsichtlich sich abzeichnender Produktgefahren zumutbar. Allerdings ist im Rahmen eines Produkthaftungsprozess auf die Trennung zwischen dem Bestehen der Produktbeobachtungspflicht und deren schuldhafter Verletzung zu achten. So können auch beim Social-Media-Monitoring trotz des Ergreifens aller zumutbaren Sicherheitsvorkehrungen einzelne Produktinformationen unerfasst bleiben, ohne dass damit gleich ein Sorgfaltsverstoß einherginge.

b) Außerdem hat der Hersteller die sensorisch von seinem Produkt erhobenen und an ihn übermittelten Daten auszuwerten. Insoweit kann an die Grundsätze der passiven Produktbeobachtung angeknüpft werden. Wiederum kann der Kommunikationsweg keinen Unterschied machen und der Kenntnisstand des Herstellers ist als produktbeobachtungsrechtliche Quelle der auszuwertenden Informationen anzusehen.

Weiter muss der Hersteller die vom Produkt generierten Daten auch erheben und sich übermitteln lassen. Für den Hersteller bedeutet dies ein aktives Erschließen neuer, bisher nicht vorhandener Erkenntnisquellen und geht über die Informationsbeschaffung aus öffentlich zugänglichen Quellen hinaus. Allerdings sieht § 6 Abs. 3 S. 1 Nr. 1 ProdSG bereits jetzt eine Pflicht zur Durchführung von Stichproben vor. Außerdem hat die Rechtsprechung über die Durchführung von Stichproben hinaus gerade bei Neuentwicklungen eine Verpflichtung des Herstellers angenommen, auch nach der Inverkehrgabe mögliche Gefahren und neue wissenschaftliche Erkenntnisse über das Produkt zu erforschen. Betrachtet man die bei smarten Produkten ausgemachten Unsicherheiten nach der Inverkehrgabe, lässt sich durchaus eine Parallele zum diffusen Gefahrenverdacht bei Neuentwicklungen ziehen. Daneben rechtfertigt das große Potential der Sensor-Datenerhebung, insbesondere die Möglichkeit für den Nutzer versteckte, weil noch nicht zu Tage getretene Produktfehler zu identifizieren und dadurch Produktfehler noch vor der ersten Schadensverursachung zu erkennen, eine Weiterentwicklung hin zu einer „aktivistischen" Produktbeobachtungspflicht. Ausgehend von der großen Flut an dadurch generierten Daten kann die Reichweite und konkrete Ausgestaltung dieser Pflicht aber nur im Einzelfall unter der Berücksichtigung von Zumutbarkeitsgesichtspunkten bestimmt werden. Insbesondere der selbständigen Systemfehleranalyse wird hier entscheidende Bedeutung zukommen. Auch vom konkreten Einzelfall abhän-

gig ist die Frage, ob der Hersteller darüber hinaus verpflichtet ist, sich die generierten Daten nicht nur übermitteln zu lassen, sondern ihn eine Pflicht trifft, die entsprechende Sensorik und Schnittstellen erst zu verbauen.

c) Weder das Datenschutzrecht noch der Schutz der Integrität von Endeinrichtungen gegen den Zugriff Dritter nach dem TTDSG stellen insoweit Hemmnisse dar. Die Erfüllung der Produktbeobachtungspflicht zur Abwehr von Gefahren vom Nutzer und der Allgemeinheit stellt eine Rechtfertigung dar.

6. Hinsichtlich der Reaktionspflichten des Herstellers auf eine nach Inverkehrgabe erkannte Produktgefahr ermöglichen smarte Produkte eine direkte und effektive Kommunikations- und Interaktionsebene zwischen Hersteller und Nutzer.
7. In Anknüpfung an die Pflegebetten-Entscheidung kommen Updatepflichten – ungeachtet ihrer konkreten Ausgestaltung – als weitergehende Sicherungsmaßnahmen erst in Betracht, wenn eine Warnung zur Gefahrenabwehr nicht hinreichend effektiv ist. Dies ist insbesondere dann der Fall, wenn Grund zur Annahme besteht, dass sich der Nutzer über die Warnung hinwegsetzt und dadurch Dritte gefährdet. Aufgrund der tatsächlichen Gegebenheiten bei smarten Produkten wird aber vielfach ein Hinwegsetzen über eine Warnung erwartet werden müssen.
   a) Bei reiner Software folgt dies daraus, dass Nutzer häufig eine falsche Gefahreneinschätzung vornehmen und sich deshalb über eine Warnung hinwegsetzen. Denn bisher gingen von Sicherheitslücken kaum physische Gefahren aus. Zudem resultieren aus Cyberattacken regelmäßig keine unmittelbaren Beeinträchtigungen für den Nutzer, sondern es wird dessen kompromittiertes System lediglich für einen Angriff gegen Dritte verwendet. Die Einstellung, dass man selbst nicht Opfer eines solchen Angriffs wird bzw. dass die Auswirkungen vor allem Dritte treffen, kann in Verbindung mit den Rechtsgutverletzungen, die man hinzunehmen bereit ist, zu einer Fehleinschätzung der Gefährdung führen. Aufgrund fehlender Gefahrensensibilität können Nutzer daher in ihrer Abwägung zu dem Ergebnis kommen, dass die Kosten der Nutzungsaufgabe im Verhältnis zu den Risiken überwiegen.
   b) Bei smarten Produkten ist ein Hinwegsetzen über eine Warnung gerade deswegen denkbar, weil es den Nutzern nicht zumutbar ist, die Gefahr selbst zu steuern. Diese Unzumutbarkeit kann sich daraus ergeben, dass der Nutzer selbst nicht in der Lage ist, Sicherheitslü-

cken zu beseitigen, während der Hersteller auch nach dem Zeitpunkt der Inverkehrgabe noch gesteigerte Einflussmöglichkeiten besitzt. Da allein der Hersteller den Aufbau und die Konzeption der Software in Gänze versteht, ist er regelmäßig der einzige Akteur, der Fehler beheben und die Software sicherer machen kann. Bei der Gefahrenbeseitigung durch eine Behebung des ursprünglichen Fehlers ist der Nutzer damit auf den Hersteller und von ihm bereitgestellte Sicherheitsupdates angewiesen. Wegen der fehlenden Möglichkeit des Nutzers, die Sicherheitsmängel selbst oder unter Zuhilfenahme Dritter als Fachleute zu beheben, ist die Warnung in diesen Fällen ein wenig wirksames Mittel der Gefahrenabwehr. Denn in solchen Konstellationen verbleibt dem Nutzer keine andere Möglichkeit, als im Rahmen der Gefahrensteuerung auf die Nutzung des Produkts zu verzichten. Bei Produkten, die für die Lebensführung von zentraler Bedeutung sind, ist ein Nutzungsverzicht aber kaum zu erwarten. Angesichts der allgegenwärtigen Fehleranfälligkeit von Software gilt dies dort umso mehr. Hinzu kommt, dass die Abhängigkeit des Nutzers bei der Fehlerbehebung vom Hersteller mit erhöhten Einflussmöglichkeiten des Herstellers auf das Produkt auch nach dem Inverkehrbringen korrespondiert. Da Softwareprodukte über das Internet verbunden sind, können die Hersteller jederzeit aus der Ferne auf ihre Produkte zugreifen und auf die sicherheitsrelevanten Eigenschaften per Aktualisierung Einfluss nehmen, sodass diese weiterhin ihrer Kontrolle unterliegen. Im Vergleich zur Nachrüstung körperlicher Gegenstände ist die Bereitstellung von Softwareaktualisierungen zudem mit geringem Aufwand und geringen Kosten für den Hersteller möglich.

c) Die konkrete Ausgestaltung der Updatepflicht betrifft den Kern der Abgrenzung des Integritäts- vom Äquivalenzinteresse. Zwar kommen Sicherheitsupdates zur Fehlerbehebung als weitergehende Sicherungsmaßnahmen erst dann in Betracht, wenn es aus Gründen der Effektivität der Gefahrenabwehr nicht ausreichend ist, das Produkt aus dem Verkehr zu ziehen. Entscheidend ist damit, wann sich eine vom Hersteller aus der Ferne vorgenommene aufgedrängte Sicherheitsbereicherung, die eine weitere (gefährliche) Nutzung gerade ausschließt, bei der Gefahrenabwehr als nicht hinreichend effektiv darstellt. Dabei ist zu beachten, dass jeder derartige nachträgliche Eingriff des Herstellers in das Produkt potenziell in Konflikt mit dem Eigentumsrecht des Nutzers steht. Diese Konfliktlage hat nun

Rückwirkungen auf die Präventionspflichten des Herstellers: Eine Maßnahme zur Vermeidung von Rechtsgutsverletzungen genügt nur dann den Anforderungen an die Produktbeobachtungspflicht, wenn sie auch praktisch wirksam ist. Fehlt es an der Einwilligung zu einer entsprechenden Maßnahme und besteht auch kein anderer Rechtfertigungsgrund, ist diese Maßnahme nicht geeignet, um Rechtsgutsverletzungen durch das Produkt effektiv zu verhindern.

d) Eine Klausel, die dem Hersteller das Recht einräumt, die mit einem Update verbundenen Rechtseingriffen vornehmen zu dürfen, wird regelmäßig im Rahmen der AGB-Kontrolle unwirksam sein, sofern überhaupt ein Vertragsschluss zwischen Hersteller und Eigentümer vorliegt. Eine Einwilligung in die konkrete Rechtsgutsverletzung rechtfertigt dagegen den Eingriff. Eine solche liegt konkludent in der unterlassenen Deaktivierung automatischer Updates. Dies allerdings nur in Bezug auf die Datenveränderung der Software. Damit kann der Hersteller fehlerbehebende Updates durchführen. Die Frage, ob die Einwilligung auch Funktionsänderungen umfasst, die die Schwelle zur Einschränkung von Funktionen nicht überschreiten, unterliegt angesichts der Regelungen im CRA einem Wandel. Jedenfalls künftig wird man hiervon nicht mehr ausgehen können. Hinsichtlich der Deaktivierung einzelner Funktionen oder gar der vollständigen Stilllegung des Geräts fehlt es schon am erforderlichen Bewusstsein der Rechtsgutsverletzung. Daher wäre eine vorherige Aufklärung über den Rechtseingriff erforderlich.

e) Verweigert der Nutzer seine Einwilligung in eine solche Maßnahme, kommt zwar eine Rechtfertigung des Herstellers unter dem Gesichtspunkt des Defensivnotstands nach § 228 S. 1 BGB in Betracht. Allerdings gilt es hier zu berücksichtigen, dass nach dem Grundsatz des geringsten Eingriffs nur das mildeste der zur Verfügung stehenden geeigneten Mittel eingesetzt werden darf. Weniger eingriffsintensiv als die Deaktivierung des Gerätes ist zunächst die zwangsweise, d.h. die ohne Zustimmung des Nutzers durchgeführte Aktualisierung durch den Hersteller. Gleiches gilt für die bloße Bereitstellung einer Aktualisierung, auf die der Nutzer hingewiesen wird und die er eigenverantwortlich herunterladen sowie installieren kann. Nachdem im Rahmen des Defensivnotstands zunächst grundsätzlich auch weniger eingriffsintensive Abwehrmittel versucht werden müssen, selbst wenn deren Wirkung nicht völlig sicher ist, stellt sich die bloße Bereitstellung einer Aktualisierung somit als „Grundmaßnahme“ dar.

Nur wenn der Nutzer einer Aktualisierungsaufforderung nicht nachkommt, diese von vorneherein keinen Erfolg verspricht oder die zeitnahe Verwirklichung der Gefahr ein Zuwarten nicht zulässt, ist eine Zwangsaktualisierung oder -deaktivierung in Betracht zu ziehen. Insoweit ist ein „Stufenbau der Reaktionspflichten" zu beachten, sodass die Bereitstellung von Updates zunächst das Mittel der Wahl darstellt, um den Anforderungen der Produktbeobachtungspflicht zu genügen.

8. Updatepflichten der Hersteller könnten sich auch außerhalb der deliktsrechtlichen Produktbeobachtungspflicht aus weiteren Regelungen ergeben
   a) Mit Geltungsbeginn der GPSR müssen Hersteller im Falle eines erforderlichen Rückrufs die Rechte des Verbrauchers auf Abhilfe berücksichtigen. Dies bedeutet, dass im Falle einer Updatepflicht, diese auch kostenlos bereitgestellt werden müssen.
   b) Indem die neue Produkthaftungsrichtlinie für die Bestimmung der berechtigten Sicherheitserwartungen und damit für die Fehlerhaftigkeit eines Produkts nicht mehr allein auf den Zeitpunkt der Inverkehrgabe, sondern auf den gesamten Zeitraum abstellt, in dem der Hersteller die Kontrolle über das Produkt behält, wird der Hersteller verpflichtet, nach dem Inverkehrbringen gestiegene Sicherheitserwartungen zu berücksichtigen. Ohne eine Updatepflicht explizit zu normieren, wird es dadurch implizit zu einer produkthaftungsrechtlichen Updatepflicht des Herstellers zur Aufrechterhaltung der Produktsicherheit kommen. Insoweit wird sich ein Hersteller im Falle eines erst nachträglich auftretenden Fehlers nicht entlasten können, sollte die Fehlerhaftigkeit des Produkts auf das Fehlen von Softwareupdates zurückzuführen sein. Auch ein Entwicklungshelfer wird künftig nicht zu einem Haftungsausschluss führen, wenn der Fehler später durch ein Update hätte behoben werden können.
   c) Daneben wird sich eine Pflicht zur Behebung von Schwachstellen durch Updates aus dem CRA ergeben.
9. Derartige Updatepflichten können nicht durch einen vorbeugenden Anspruch auf Updates durchgesetzt werden. Zwar ist der Anspruch nach § 1004 Abs. 1 S. BGB auf die Beseitigung einer konkreten Gefahr gerichtet. In den Fällen aber, in denen der Nutzer in der Lage ist, einen Gefahrenabwehranspruch hinreichend konkret zu formulieren und zu begründen (§ 253 Abs. 2 Nr. 2 ZPO), wird die Kenntnis der Gefahr regelmäßig auch für die Ergreifung von Selbstschutzmaßnahmen ausreichen.

Insoweit kann niemand von einem Hersteller mit der Begründung ein Update verlangen, dass andernfalls die Warnung ignoriert und das Produkt trotz der erkannten Gefahr weiter verwendet werde. Dieser einfache und zumutbare Selbstschutz wird Dritten, die zufällig mit dem gefährlichen Produkt in Kontakt kommen, zwar nicht möglich sein. Allerdings fehlt es in diesen Fällen regelmäßig an der hinreichenden Konkretisierung der Gefahr, sodass auch Ansprüche Dritter auf Vornahme von Sicherheitsaktualisierungen ausscheiden.