www.jusletter-it.eu

Rolf H. Weber

Braucht die digitale Welt ein neues Haftungsrecht?

Technical developments (especially digitization) undermine the traditional liability regime basing on the connection to physical goods. Therefor, a reorganization is ubtruding; the assignment of responsibility and risk management have to be paramount. (ah)

Category: Articles
Region: Switzerland
Field of law: Data Protection

Citation: Rolf H. Weber, Braucht die digitale Welt ein neues Haftungsrecht?, in: Jusletter IT 21 September 2017

ISSN 1664-848X, https://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

Inhaltsübersicht

I. Einleitung

[Rz 1] Die Digitalisierung, ob disruptiv wirkend oder nicht, ermöglicht eine Vielzahl neuer Geschäftsmodelle und verändert auch die Ausgestaltung der Kommunikations- und Lieferwege mit Bezug auf Güter, Dienstleistungen und Daten. Die Europäische Kommission hat bereits im Mai 2015 mit einem Grundlagendokument die Rahmenbedingungen eines digitalen Binnenmarkts skizziert.[1] Neue Regeln für digitale Geschäftsmodelle sind danach in einer Weise auszugestalten, dass die Wettbewerbsfähigkeit und die Innovationsbereitschaft der Unternehmen sich intensivieren.[2]

[Rz 2] Die Digitalisierung führt aber auch zu neuen Haftungsfragen, die im weitesten Sinne meist einen Bezug zum Thema der Datensicherheit aufweisen, sich inhaltlich indessen ebenso auf neue Geschäftsmodelle auswirken. Dass die Prinzipien des Haftungsrechts, die zumindest in Kontinentaleuropa auf dem römischen Recht aufbauen, die neuen Herausforderungen nur schwer zu bewältigen vermögen, erscheint als offensichtlich. Weil digitale Geschäftsmodelle zudem global angeboten werden können, erweisen sich die unterschiedlichen Haftungskonzepte in den grossen Rechtskreisen (z.B. «civil law» und «common law») als nicht unproblematisch.

[Rz 3] Einen Handlungsbedarf hat auch die Europäische Kommission erkannt: Mit einem Grundlagendokument vom 10. Januar 2017 wird versucht, die Diskussion zu den Haftungsfragen in der digitalen Welt zu vertiefen und breitere Kreise in die Debatte einzubinden.[3] Mit ersten Ergebnissen und der Formulierung weiterer Vorgehensschritte ist in den nächsten Monaten zu rechnen.

---

1 European Commission, A Digital Single Market Strategy for Europe, Communication of 6 May 2015, COM (2015) 192 final.

2 Rolf H. Weber, Competitiveness and Innovation in the Digital Single Market, European Cybersecurity Journal 2006, 72 ff.

3 European Commission, Buidling a European Data Economy, Communication of 10 January 2017, COM (2017) 9 final.

[Rz 4] Früher oder später wird die Frage, ob die digitale Welt ein neues Haftungsrecht braucht, auch auf die Schweiz überschwappen. Aus diesem Grunde sollen die nachfolgenden (noch vorläufigen) Überlegungen nach einer Übersicht zu den technologischen Entwicklungen eine Auslegeordnung zum heute gegebenen Haftungsinstrumentarium bieten, gefolgt von Hinweisen zu möglichen Entwicklungen des Haftungsrechts.

II. Neue technologische Entwicklungen

[Rz 5] Die wesentlichsten technologischen Entwicklungen kristallisieren sich derzeit im Internet of Things (IoT) und den sog. autonomen Systemen (Robotik) heraus; zudem stellen die datenschutzrechtlichen Anforderungen neue Haftungsfragen.[4]

1. Internet of Things

[Rz 6] Das Internet of Things als relativ neue, auf dem Internet aufgebaute Netzwerkstruktur ist ursprünglich für den Geschäftsverkehr konzipiert worden, erfasst aber mehr und mehr auch private Belange. Von grosser praktischer Bedeutung ist insoweit der Gesundheitssektor, der besonders datenintensiv, aber auch datensensitiv ist. Neuere Fitness-Applikationen[5] haben bereits zu datenschutzrechtlichen Auseinandersetzungen geführt.[6]

[Rz 7] Eine im IoT auftretende Fehlfunktion (z.B. wegen eines Design- oder Konstruktionsfehlers oder einer Manipulation) kann angesichts der Abhängigkeit vieler Personen bzw. Unternehmen von der Qualität und zeitlichen Verfügbarkeit der Daten doppelte (negative) Konsequenzen haben:[7]

- Die Fehlfunktion führt ggf. zu Datenverlusten oder zur widerrechtlichen Offenlegung von Daten; rechtlich steht dabei die Einhaltung des Datenschutz- und des Datensicherheitsrechts zur Diskussion.
- Die Fehlfunktion vermag zu physischen Schäden zu führen, etwa zur Explosion angeschlossener Geräte oder zur Beeinträchtigung von Drittprodukten (z.B. Verderben von Lebensmitteln im ausser Betrieb gesetzten Kühlschrank).

[Rz 8] Die Vielzahl der (Markt-)Beteiligten in den IoT-Netzstrukturen (Anbieter von Hardware, Software, Wartung, Datenanalyse) erschwert angesichts der oft vorhandenen Abhängigkeiten das Auffinden des bzw. der Verantwortlichen. Beim explodierenden Kühlschrank kann es z.B. der Gerätehersteller, der Netzwerkbetreiber, der Entwickler des Softwareprogramms oder der sich falsch verhaltende Kunde sein. Die Haftungsordnung ist somit einem Mehrebenensystem ausgesetzt, wie sie dem traditionellen Verständnis noch kaum bekannt ist. Bipolare Rechtsverhältnisse

---

4 Rolf H. Weber, Liability in the Internet of Things, erscheint in Journal of European Consumer and Market Law 2017, Heft 5 (Oktober 2017); weitere Hinweise auf diesen Beitrag unterbleiben hernach.

5 Vgl. etwa fitbit, https://www.fitbit.com/de (alle Websites zuletzt besucht am 7. September 2017), or Google NEST, https://nest.com.

6 College Bescherming Persoonsgegevens, An Investigation Nike+ Running App, 2015, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/conclusions_dpa_investigation_nike_running_app.pdf; see also Nike+, http://www.nikeplus.com.br/.

7 Vgl. schon Rolf H. Weber/Romana Weber, Internet of Things, Zürich 2010, 64 f.

treten in den Hintergrund und Verbundelemente zwischen mehreren Marktteilnehmern gewinnen an Bedeutung.

2. Autonome Systeme

[Rz 9] Noch komplexer sind die Haftungsprobleme bei den sog. autonomen Systemen, z.B. beim Einsatz von Industrierobotern, Medizinrobotern, selbstfahrenden Autos[8] oder Drohnen. Die Charakteristik der autonomen Systeme besteht darin, dass sie in der Lage sind, die Umgebung zu «verstehen» und zu «interpretieren» sowie gestützt darauf grundsätzlich sachgerecht zu agieren oder zu reagieren.[9]

[Rz 10] Die traditionellen Haftungsregeln beruhen auf dem Prinzip, dass jemand eine «Kontrolle» auszuüben vermag, etwa mit Bezug auf das eigene Verhalten, auf produzierte und angebotene Produkte oder auf spezifische Tätigkeitsentfaltungen. Diese traditionelle «Kontrollfunktion» lässt sich bei autonomen Systemen personal oft nicht leicht zuordnen. Bei einem selbstfahrenden Auto kann dessen Produzent, der Bestandteilzulieferer oder der Entwickler eines der vielen eingesetzten Softwareprogramme für die Fehlfunktion verantwortlich sein.[10]

[Rz 11] Die meisten Rechtsordnungen kennen zwar die sog. Gefährdungshaftungen; wer einen «gefährlichen» Zustand schafft, unterliegt der Verantwortung, Vorsichtsmassnahmen zu ergreifen, um Schädigungen zu vermeiden. Ein Roboter bzw. ein autonomes System ist aber weder eine Person, die eine Haftungsanknüpfung ermöglicht, noch an sich ein gefährliches Werkzeug, weshalb sich die verschiedenen Formen der Gefährdungshaftungen nicht uneingeschränkt als passend erweisen. Dementsprechend sind die anwendbaren Haftungsregeln neu auszurichten.

3. Datensicherheitssensitive Märkte

[Rz 12] Die Datensicherheit spielt nicht nur beim Internet of Things und bei den autonomen Systemen eine grosse Rolle, sondern ganz allgemein, wenn Daten bearbeitet und übermittelt werden.[11] Die Komplexität der Datensicherheitsanforderungen ergibt sich daraus, dass Produkte und Dienstleistungen die verschiedensten Datenebenen betreffen, z.B. die Sammlung und Bearbeitung von Daten, die Softwareentwicklung (in Produkte integriert oder nicht), die Anwendungsebene (z.B. Vielzahl von Apps) sowie die Sensoren und Aktuatoren.[12] Bereits heute zeigen sich

---

8 Ausführlich Melinda Florina Lohmann/Markus Müller-Chen, Selbstlernende Fahrzeuge – eine Haftungsanalyse, SZW 2017, 48 ff.

9 Zu den technologischen Aspekten vgl. Arun K. Ramakrishnan/Davy Preuveneers/Yolanda Berbers, Enabling self-learning in dynamic and open IoT environments, Procedia Computer Science 32 (2014), 207 ff.; vgl. auch die verschiedenen Beiträge im Sonderheft «Roboterrecht», AJP 2017, 135 ff.

10 Vgl. auch Lohmann/Müller-Chen (Fn. 8), 50 ff.

11 Rolf H. Weber/Dominic N. Staiger, New Liabilty Patterns in the Digital Era, in: T. Synodinou/Ph. Jongleux/Chr. Marcou/Th. Prastitou-Merdi (eds.), EU Internet Law, Regulation and Enforcement, Berlin 2017, Kap. 9 (erscheint im September 2017); weitere Hinweise auf diesen Beitrag unterbleiben hernach.

12 Vgl. auch Andrea Bertolini, Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules, LIT 5/2 (2013), 217 ff.

die Herausforderungen der Haftungszuordnung z.B. im Kontext des Cloud Computing oder des Outsourcing.[13]

[Rz 13] Überdies ist zu berücksichtigen, dass die eigentlichen gesetzlichen Grundlagen zur Datensicherheit nicht sehr stark entwickelt sind (Art. 7 des Bundesgesetzes über den Datenschutz [DSG; SR 235.1]). Vielmehr beruhen die Anforderungen an die Datensicherheit zu weiten Teilen auf mannigfaltigen Selbstregulierungen der Branchenverbände; der Vorteil solcher Regulierungen besteht in der Technologieorientierung und der Flexibilität, doch ist deren Verbindlichkeit bzw. Durchsetzbarkeit nicht immer gewährleistet (Beispiele: ISO, BSI, usw.).[14]

III. Schwächen des heutigen Haftungsrechts

[Rz 14] Überblicksmässig betrachtet kennen die meisten Haftungsordnungen der europäischen Länder vier Grundtypen von Haftungsarten, nämlich (i) die Vertragshaftung, (ii) die Deliktshaftung, (iii) die Gefährdungshaftungen und (iv) die besonderen Spezialhaftungen.

1. Vertragshaftung

[Rz 15] Die Vertragshaftung ist Regelungsgegenstand des Vertragsrechts (Art. 97 des Bundesgesetzes betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches [Fünfter Teil: Obligationenrecht, OR; SR 220]). Die gesetzlichen Bestimmungen sind indessen auf physische Güter ausgerichtet. Der Qualitätsbegriff lässt sich nicht ohne weiteres auf Daten bzw. Informationen übertragen. Diese Tatsache ist umso problematischer, je mehr Verträge einen digitalen Inhalt aufweisen. Mit Blick auf die sich dabei stellenden Rechtsfragen hat die Europäische Kommission im Dezember 2015 einen Vorschlag zu den digitalen Vertragsinhalten präsentiert.[15] Der Entwurf enthält eine Umschreibung des Begriffs «digitaler Inhalt»: Erfasst sind danach alle Güter in digitaler Form (z.B. Video, Audio, Apps, digitale Spiele und andere Software); digitale Inhalte weisen dementsprechend einen breiten Anwendungsbereich auf.

[Rz 16] Zur Diskussion gestellt hat die Europäische Kommission auch neue Regelungen zur Vertragskonformität, weil der Begriff der Schlechterfüllung nicht gut zu digitalen Vertragsinhalten passt.[16] Zur Erreichung von Vertragskonformität ist eine genaue vertragliche Umschreibung des Vertragsinhalts bzw. des Zweckes, der mit dem Erwerb des digitalen Inhalts (Dateninformation) angestrebt wird, erforderlich. Der beabsichtigte Verwendungszweck ist hernach der Ausgangspunkt der Konformitätsbeurteilung. Nur im Falle einer ausreichenden Konkretisierung des Vertragsgegenstands lässt sich feststellen, ob der digitale Vertragsinhalt den Erwartungen des Abnehmers entspricht. Die Auslegung hat dabei subjektive und objektive Elemente in Betracht zu ziehen.

---

13 Vgl. Rolf H. Weber/Dominic N. Staiger, Cloud Computing: A cluster of complex liability issues, Web JCLI 20/1 (2014), 1 ff.

14 Ausführlich dazu Rolf H. Weber/Annette Willi, IT-Sicherheit und Recht, Zürich 2006, 68 ff.

15 Richtlinienentwurf zu den Contracts for the Supply of Digital Content, COM (2015) 635 final.

16 Vgl. Aurelia Colombi Ciacchi/Esther van Schagen, Conformity under the Draft Digital Content Directive: Regulatory Challenges and Gaps, in: R. Schulze/D. Staudenmayer/S. Lohsse (eds.), Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps, Baden-Baden 2017, 99 ff.

[Rz 17] Die Vertragskonformität ist auch mit Blick auf die Intensität des «Gebrauchs» digitaler Vertragsinhalte zu konkretisieren, weil der «Gebrauch» die digitalen Inhalte (im Gegensatz zum «Gebrauch» von Sachgütern) qualitativ und quantitativ grundsätzlich nicht beeinträchtigt. Weiter ist zu klären, ob der Abnehmer ein Recht hat, digitale Vertragsinhalte an Dritte weiterzugeben. Schwierige Abgrenzungsfragen ergeben sich insoweit mit Blick auf die Anwendung urheberrechtlicher Bestimmungen. Falls die digitalen Vertragsinhalte auch Personendaten von Dritten mitumfassen, spielt zudem das Datenschutzrecht eine Rolle.[17]

[Rz 18] Weiter erweisen sich spezifische Regelungen zu den Rechtsbehelfen als notwendig.[18] Ist der digitale Vertragsinhalt unbrauchbar und kommt es deshalb zu einer Vertragsaufhebung, ist eine Rückerstattung der Daten in einem standardisierten Format vorzunehmen. Weicht der digitale Vertragsinhalt nicht erheblich von der vertraglichen in Aussicht gestellten Qualität ab, kommt ggf. eine Kaufpreisminderung in Frage. Dennoch ist nicht zu übersehen, dass die quantitative Berechnung des Minderwerts eines digitalen Vertragsinhalts regelmässig Schwierigkeiten verursacht.

[Rz 19] Die auf der Blockchain abgewickelten Smart Contracts stellen mit Bezug auf die Ausgestaltung von Rechtsbehelfen regelmässig neue Herausforderungen. Weil Intermediäre auf der Blockchain fehlen, muss der (selbst-ausführende) Programmcode einen Konfliktmechanismus vorsehen, damit im Falle einer Abweichung vom Leistungsprogramm eine Vertragsanpassung stattfinden kann.[19] Über ein Orakel (Verbindung zur Offline-Welt) lässt sich z.B. die Mitwirkung einer Schlichtungs- oder Schiedsgerichtsstelle vorsehen. Die technischen Details für eine Bewältigung der Probleme, die im Falle einer fehlenden Vertragskonformität eintreten, sind erst in der Entwicklung begriffen. Wie Streitschlichtungsverfahren abzuwickeln sind, und welche Folgen sich für ein gescheitertes Vertragsverhältnis bzw. die Rechte und Pflichten der Vertragsparteien ergeben, bedarf noch der weiterführenden Klärung.

[Rz 20] Die steigende Bedeutung der Ausgestaltung der Vertragssprache im Programmcode führt überdies zu einer Verwischung von Vertrags- und Delikts- bzw. Produktehaftung. Zwar besteht zwischen dem Benutzer und dem Anbieter eines virtuellen Gutes eine Vertragsbeziehung, doch erstreckt diese sich nicht zwingend auf den Entwickler des Programmcode (je nach vertraglicher Ausgestaltung), womit dem Benutzer im Falle einer Fehlfunktion nur ausservertragliche Ansprüche verbleiben.

2. Deliktshaftung

[Rz 21] Die Deliktshaftung (Art. 41 OR) kommt im Falle der Verursachung eines voraussehbaren Schadens, gestützt auf ein absichtliches oder fahrlässiges Verhalten, zum Zuge. Regelmässig vorausgesetzt ist die Verletzung einer (standardisierten) Sorgfaltspflicht, doch besteht insoweit die Problematik, dass Anbieter verschiedener Elemente (Hardware, Software, usw.) unterschiedliche

17 Vgl. Rolf H. Weber, Data Protection in the Termination of Contract, in: Schulze/Staudenmayer/Lohsse (Fn. 16), 189 ff.

18 Vgl. Martine Behar-Touchais, Remedies in the Proposed Digital Content Directive: An Overview, in: Schulze/Staudenmayer/Lohsse (Fn. 16), 155 ff.

19 Vgl. Rolf H. Weber, Blockchain als rechtliche Herausforderung, in: Jusletter IT 18. Mai 2017, Rz. 30 ff.

Anforderungen zu erfüllen haben (z.B. mit Blick auf die Datenbearbeitung und -aufbewahrung, die anwendbaren Applikationen oder die eingesetzten Apps und Sensoren).[20]

[Rz 22] Im hochtechnologischen Kontext ist zudem die Besonderheit zu beachten, dass für den Anbieter eines Produkts oder einer Dienstleistung oft nur schwer abschätzbar ist, welche Dritte durch eine Fehlfunktion geschädigt werden könnten. Die Einschätzung des Risikobereichs gestützt auf die übliche Sorgfaltspflicht erweist sich somit als sehr komplex. Diese Beurteilung trifft für IoT-Produkte und autonome Systeme gleichermassen zu. Die Hauptschwierigkeit im Vergleich zu traditionellen Rechtsgeschäften liegt somit in der angesprochenen (Rz. 8) komplexen Mehrebenenstruktur, die sich situativ ändern kann und für die geschädigte Person oft auch nicht klar durchschaubar ist.[21]

[Rz 23] Umgekehrt vermag der Anbieter eines IoT-Produktes oder eines autonomen Systems oft auch nicht abzuschätzen, welchen Einfluss die Einzelbestandteile, die von Dritten bereitgestellt worden sind, auf die Lieferung haben. Vertraglich wird zudem die Haftung für von Dritten gelieferte Einzelbestandteile oft wegbedungen,[22] was zur Folge hat, dass der betroffene (geschädigte) Benutzer lediglich über einen ausservertraglichen Haftungsanspruch verfügt, der ihm die ganze Beweislast bei der Durchsetzung von Ersatzansprüchen auferlegt.

3. Gefährdungshaftungen

3.1. Produktehaftung

[Rz 24] Gestützt auf die Richtlinie 85/347 kennen die Länder der EU seit den späten 80er Jahren gesetzliche Vorgaben zur Produktehaftung.[23] Die Schweiz ist mit dem Produktehaftpflichtgesetz (PrHG; SR 221.112.944) von 1993 gefolgt. Bei der Produktehaftung handelt es sich um eine verschuldensunabhängige Kausalhaftung, die auf die üblichen Sicherheitserwartungen abstellt.[24]

[Rz 25] Die Problematik des Produktehaftungsrechts liegt in der Tatsache, dass grundsätzlich nur von physischen Gütern verursachte Schäden erfasst sind. Als Produkte gelten bewegliche Sachen und Elektrizität (Art. 3 PrHG). Virtuelle Güter (z.B. Daten) fallen somit grundsätzlich nicht in den Anwendungsbereich des Produktehaftungsrechts.[25] Jedenfalls im kommerziellen Bereich geht es bei den IoT-Geschäften zwar meist um (physische) Güterlieferungen, doch verursachen in der Regel nicht diese Güter einen Schaden, sondern die integrierte Software für die Lieferkette oder die Bearbeitung bzw. Auswertung der zugrundeliegenden Daten. Diese Elemente sind indessen meist nicht physisch und deshalb kein Produkt. Ähnliche Überlegungen gelten für autonome Systeme, wie etwa das Beispiel des selbstfahrenden Autos zeigt; ein Unfall dürfte eher auf einen

20 Zur Sorgfaltspflicht vgl. hinten IV.1.

21 Vgl. vorne II.1 und II.2.

22 Die Kontrolle von Allgemeinen Geschäftsbedingungen ist in der Schweiz grundsätzlich auf den Überprüfungsmassstab von Art. 8 UWG beschränkt, der ein hohes Mass an Benachteiligung des schwächeren Verbrauchers voraussetzt; diese Hürde dürfte regelmässig nicht zu überspringen sein, wenn der Anbieter einzelner Leistungsbestandteile seine Haftung für die Elemente eines anderen Leistungsanbieters wegbedingt.

23 ABl 1985 L 210/29.

24 Art. 55 OR sieht zusätzlich verschiedene Organisationspflichten des Geschäftsherrn vor, die im Einzelfall einer Produzentenhaftung annähern können.

25 European Commission, Staff Working Paper to the Communication «Building a European Data Economy», 10 January 2017, SWD (2017) 2 final, 44.

«Datenfehler» als auf einen Konstruktionsfehler beim Auto zurückzuführen sein.[26] Eine Anwendung des Produktehaftungsrechts wäre somit nur auf der Basis eines nicht unproblematischen weiten Analogieschlusses möglich.

[Rz 26] Bei virtuellen Gütern ist es überdies schwierig, den traditionellen Begriff des «Mangels» zu konkretisieren. Gemäss Art. 4 PrHG ist ein Produkt fehlerhaft, wenn es nicht die Sicherheit bietet, die man unter Berücksichtigung aller Umstände zu erwarten berechtigt ist.[27] Abgesehen davon, dass in der Realität oft nicht immer völlig klar ist, mit welchen Sicherheitsstandards ein Benutzer rechnet, mag auch der Nachweis der vorhandenen Kausalkette, die zum «Mangel» führt, nur schwierig zu erbringen sein.

[Rz 27] Die Problematik ist insoweit nicht ganz neu, als schon während der letzten 20 Jahre immer wieder das Anliegen vorgebracht worden ist, Software als ein «Produkt» anzuerkennen, und trotz der fehlenden Körperlichkeit die Regelungen des Produktehaftungsrechts zur Anwendung zu bringen. Bisher sind aber entsprechende Bemühungen in Europa (und auch in der Schweiz) nicht erfolgreich gewesen.[28]

[Rz 28] Dass die «traditionelle» Produktehaftung im Lichte der neuen technologischen Entwicklungen einer Anpassung bedarf, hat die EU nicht verkannt. Derzeit läuft eine von der Kommission initiierte breite Vernehmlassung zur Anpassung der gut 30-jährigen Richtlinie 85/347.[29] Ähnliche Überlegungen müsste sich auch der Schweizer Gesetzgeber machen.

3.2. Produktesicherheitshaftung

[Rz 29] Erst einige Jahre nach dem Erlass der Produktesicherheits-Richtlinie 2001/95 der EU[30] hat die Schweiz diese Thematik mit dem Bundesgesetz über die Produktesicherheit von 2009 angegangen. Gemäss dessen Art. 2 handelt es sich beim Produkt um seine verwendungsbereite bewegliche Sache, was bedeutet, dass virtuelle Güter entsprechend wie bei der Produktehaftung nur mit einem sehr weiten Analogieschluss zu erfassen wären.[31]

[Rz 30] Weil die Bestimmungen des Produktesicherheitsrechts insbesondere für autonome Systeme nicht mehr als vollumfänglich sachgerecht erscheinen, stellt sich die Frage, ob durch analoge Anwendung dieser Vorschriften im neuen technologischen Kontext sinnvolle Lösungen erreicht werden können oder ob eine Gesetzesanpassung in Betracht zu ziehen ist.

---

26 Vgl. auch Lohmann/Müller-Chen (Fn. 8), 53 ff.

27 Der Vollständigkeit halber lässt sich noch anfügen, dass autonome Systeme in der Europäischen Union wohl auch unter die weite Umschreibung des Begriffs «Maschine» in der Maschinen-Richtlinie 2006/42 fallen würden (ABl 2006 L 157/24), doch stellen sich die identischen Probleme wie unter der Produktehaftungs-Richtlinie, weil die von Maschinen erwartete Körperlichkeit bei autonomen Systemen kaum zu begründen ist.

28 Zur Diskussion vgl. W. Straub, Software als Produkt, in: Jusletter 18. März 2002.

29 Communication (Fn. 3), 14.

30 ABl 2001 L 11/4; einen Überblick über die Rechtsprechung gibt der umstrittene Delfi-Fall von 2015 (Delfi AS v. Estonia, ECHR no. 64569, 16. Juni 2015).

31 Das Produktesicherheitsgesetz folgt bewusst der Diktion des Produktehaftungsgesetzes; entsprechend ergeben sich parallele Probleme im Kontext des IoT und der autonomen Systeme.

4. Spezialhaftungen

4.1. Providerhaftung

[Rz 31] Die E-Commerce-Richtlinie 2000/31 der EU enthält besondere Haftungsregeln zuhanden der Internet Provider (Art. 12–15).[32] Die Haftungsregelung ist abgestuft nach dem Ausmass, in welchem der Internet Provider in die inhaltliche Ausgestaltung der durch ihn angebotenen Informationen involviert ist; je mehr sich der Internet Provider nur auf die technische Abwicklung der elektronischen Kommunikationen beschränkt, desto tiefer ist das Haftungsniveau.

[Rz 32] Die Schweiz kennt keine entsprechenden Regeln; ungeachtet jahrelanger Diskussionen im Bundesamt für Justiz ist angesichts der unterschiedlichen Betrachtungsweisen der Betroffenen kein Gesetzesprojekt herangereift.[33] Ein teilweiser Ersatz für das Fehlen gesetzlicher Normen wird durch Selbstregulierungen der Branche erreicht. Die Erfahrungen der letzten Jahre haben gezeigt, dass zwar das Fehlen gesetzlicher Regelungen zur Provider Haftung gewisse Rechtsunsicherheiten verursacht und dass auch nicht jeder Gerichtsentscheid immer leicht nachvollziehbar ist;[34] die Selbstregulierungen haben dennoch durch die vermittelten Handlungsanweisungen weitgehend sachlich vernünftige Problemlösungen ermöglicht.[35]

4.2. Datenschutzhaftung

[Rz 33] Mit der neuen Datenschutz-Grundverordnung 2016/679 der EU (DSGVO) und dem bevorstehenden DSG kommt es zu einer starken Ausweitung der Pflichten von Datenbearbeitern jeglicher Art. Die Pflichten weisen einen ganz unterschiedlichen Inhalt auf: Verschiedene Vorgaben betreffen die Erhöhung der Transparenz durch aktive Informationspflichten (Art. 12–14 DSGVO; Art. 17–19 E-DSG) und passive Auskunftspflichten (Art. 15 DSGVO; Art. 23–25 E-DSG), aber auch durch Pflichten zur Offenlegung eingetretener Datenpannen gegenüber Datenschutzbehörden und Betroffenen (Art. 33/34 DSGVO; Art. 22 E-DSG). Andere Anordnungen zielen mehr auf den Innenbereich von Unternehmen; verlangt werden die Implementierung von den Datenschutz stärkenden vorbeugenden Massnahmen bzw. datenschutzfreundlichen Voreinstellungen (Privacy by design: Art. 25 DSGVO; Art. 6 E-DSG), die Durchführung von Datenschutz-Folgeabschätzungen (Data Protection Impact Assessment: Art. 35 DSGVO; Art. 20 E-DSG) und die Einrichtung eines innerbetrieblichen Datenschutzbeauftragten (Art. 37 DSGVO; Art. 9 E-DSG als Kann-Vorschrift).[36]

[Rz 34] Die Einhaltung dieser Pflichten ist mit v.a. in der EU hohen, wenn zwar gestützt auf unterschiedliche Faktoren zu berechnenden, Bussen strafbewehrt (Art. 83 DSGVO; Art. 54/55 E-DSG). Die Bussen sollen einen wirksamen Beitrag dazu leisten, dass die Datenbearbeiter künftig die datenschutzrechtlichen Pflichten ernst nehmen; wie im Wettbewerbsrecht gehen die entsprechenden Geldleistungen aber an den Staat, nicht an die von einem Rechtsverstoss betroffenen Personen.

---

32 ABl 2000 L 178/1.

33 Rolf H. Weber, E-Commerce und Recht, 2. Aufl. Zürich 2010, 507 ff., 516 ff.

34 Urteil des Bundesgerichts 5A_792/2011 vom 14. Januar 2013 (Tribune de Genève).

35 Vgl. Bericht des Bundesrates, Die zivilrechtliche Verantwortlichkeit von Providern, 11. Dezember 2015.

36 Für einen Überblick vgl. Niko Härting, Datenschutz-Grundverordnung, Köln 2016.

[Rz 35] Überwiegend handelt es sich bei den vorerwähnten Pflichten zwar um aufsichtsrechtlich relevante Datenschutzpflichten. Im Falle einer Verletzung lassen sich die aufsichtsrechtlichen Pflichten aber auch im Rahmen der Durchsetzung zivilrechtlicher Ansprüche heranziehen, um die Rechtswidrigkeit zu begründen.

[Rz 36] Konkret beruht in diesem Fall die zivilrechtliche Haftung auf Vertrag oder Delikt. Der Vorteil des Aufsichtsrechts besteht indessen darin, dass der Aspekt der Widerrechtlichkeit in einem amtlichen Verfahren geprüft wird und hernach der Geltendmachung von Ansprüchen in einem Zivilverfahren zugrunde gelegt werden kann. Die Zahl solcher Verfahren dürfte künftig deshalb steigen. Ein spezifischer Regelungsbedarf abgesehen vom Erlass des DSG lässt sich indessen nicht diagnostizieren.

4.3. Netzwerkinfrastrukturhaftung

[Rz 37] Im Jahre 2016 hat die EU die «Network and Information Security»-Richtlinie 2016/1148 erlassen.[37] Diese bis 2018 umzusetzende Richtlinie sieht vor, dass eine ganze Reihe von Massnahmen zu treffen ist, welche die Sicherheit der Netzwerkinfrastrukturen verbessern, vor allem mit Blick auf Störungsanfälligkeiten als auch mit Blick auf Attacken verschiedenster Art durch Dritte (Cybersicherheit). Zwar sind die ursprünglich vorgeschlagenen Vorgaben der EU-Kommission in der Endfassung teilweise etwas abgeschwächt worden, doch ist nach Verankerung der Grundsätze im nationalen Recht doch mit einem verbesserten Cybersicherheitsniveau zu rechnen.[38]

[Rz 38] Die fernmelderechtlichen Rahmenbedingungen in der Schweiz gehen wesentlich weniger weit als die «Network and Information Security»-Richtlinie; aus diesem Grunde stellt sich für den Gesetzgeber die Frage, inwieweit die Grundsätze im schweizerischen Recht autonom nachzuvollziehen sind. Die im Moment in Überarbeitung sich befindende Cybersecurity-Strategie des Bundes wäre ein geeigneter Anlass, auch spezifische regulatorische Handlungsanforderungen mit Bezug auf eine Netzwerkinfrastrukturhaftung in Betracht zu ziehen.

IV. Neue Haftungskonzepte

[Rz 39] Mit der erwähnten Kommunikation und einem ausführlichen Staff Working Paper vom Januar 2017 schlägt die EU vor, neue Haftungskonzepte zu diskutieren und ggf. später zu implementieren.[39] Im Vordergrund stehen m.E. drei Themen, nämlich (i) die – von der Europäischen Kommission nicht detailliert diskutierten – Sorgfaltspflichten und die Verantwortlichkeitszuordnung, (ii) die möglichen Risikomanagement-Modelle sowie (iii) die freiwilligen oder zwingenden Versicherungslösungen.

---

37 ABl 2016 L 194/1.

38 Für eine detailliertere Darstellung vgl. R.H. Weber/E. Studer, Cybersecurity in the Internet of Things: Legal aspects, Computer Law & Security Review 32 (2016), 715 ff.

39 Communication (Fn. 3), 14/15, und Staff Working Paper (Fn. 25), 45. Vgl. jüngst auch Rolf H. Weber, IT-Governance: unverzichtbar für jedes Unternehmen, in: schulthess manager handbuch 2017, Zürich 2017, 37 ff.

1. Sorgfaltspflichten und Verantwortlichkeitszuordnung

[Rz 40] Schon heute besteht, insbesondere angesichts der durch die Delikts- und Gefährdungshaftungen bewirkten Herausforderungen, eine Pflicht, Strategien zu entwickeln und Massnahmen umzusetzen, welche die Datensicherheitsrisiken im Unternehmen sowie in den Geschäftsbeziehungen mit Dritten minimieren. Die entsprechenden Aufgaben werden von den Unternehmen auch in einem mehr oder weniger weitgehenden Umfang bereits wahrgenommen. Das Stichwort lautet «Enterprise Risk Management»; neben technischen Präventionsmassnahmen kommt der Schulung und Sensibilisierung der Mitarbeiter/innen eine immer grössere Bedeutung zu.[40]

[Rz 41] Zu den relevanten Faktoren der Risikominimierung gehören auch selbstregulatorische Vorgaben mit Bezug auf die Benutzung von elektronischen Hilfsmitteln (z.B. iPhone, iPad, usw.). Die getroffenen Massnahmen können einen Einfluss auf die Beurteilung der Risikoallokation bei Auftreten eines Schadensfalls haben; die Implementierung der präventiven Vorkehren wirkt sich somit letztlich risikomindernd für die Unternehmen aus.[41]

[Rz 42] Vermehrt hat zudem der Aspekt einer sachgerechten Verantwortlichkeitszuordnung in den Vordergrund zu rücken. Passend dafür ist der englische Begriff der «accountability». Wer Leistungen anbietet, hat dafür einzustehen, dass die berechtigten Erwartungen der Empfänger nicht enttäuscht werden.

2. Risikomanagement-Modelle

[Rz 43] Über die Sorgfaltspflichten und die Verantwortlichkeitszuordnung hinaus sind eigentliche Vorgaben zu Risikomanagement-Modellen einzuführen; je nach Grösse des verursachten Datensicherheitsrisikos ist von den Anbietern von Gütern und Dienstleistungen ein unterschiedliches Ausmass an Risikovermeidungs- und Risikominimierungsmassnahmen zu verwirklichen.[42]

[Rz 44] Bei der Allokation der entsprechenden Aufgaben denkt die EU daran, das von der Ökonomie schon vor Jahrzehnten entwickelte Konzept des «*cheapest cost avoider*» zu realisieren. Die Vornahme von Massnahmen zur Vermeidung von Datensicherheitsrisiken ist also demjenigen Marktteilnehmer aufzuerlegen, welcher die niedrigsten Kosten für deren Vornahme hat (Aspekt der Risikogenerierung); betroffen sein kann auch der Benutzer, falls es für ihn leicht ist, einen Beitrag zur Datensicherheit zu leisten.[43]

3. Freiwillige und zwingende Versicherungslösungen

[Rz 45] Eine weitere, wohl alternative Massnahme, die von der EU in Betracht gezogen wird, liegt in der Einführung einer Versicherungslösung, die freiwillig oder verpflichtend sein kann. Das Ziel einer solchen Lösung liegt darin, denjenigen Beteiligten (v.a. den Endabnehmern von Produkten) eine Entschädigung zukommen zu lassen, die einen (grösseren) Schaden erlitten haben, ohne dass eine Ersatzleistung durch den Haftpflichtigen erfolgt, entweder weil der Schädiger an-

40 Communication (Fn. 3), 14/15, und Staff Working Paper (Fn. 25), 45.

41 Vgl. Weber/Willi (Fn. 14), 188 ff.

42 Staff Working Paper (Fn. 25), 45.

43 Staff Working Paper (Fn. 25), 45.

gesichts der Komplexität der wirtschaftlichen Beziehungen kaum gefunden werden kann, oder weil der Geschädigte seinen Beweispflichten angesichts der gegebenen Umstände nicht nachzukommen vermag.[44]

[Rz 46] Ob eine solche Versicherungslösung in der nun laufenden Vernehmlassung in der EU eine ausreichende Anerkennung findet, lässt sich im Moment noch nicht abschätzen. Die Diskussion in der Schweiz steckt noch ganz in den Anfängen;[45] ähnlich wie im Kontext der Cybersecurity-Risiken könnte sich in dieser Hinsicht ein neuer Versicherungszweig etablieren.

V. Ausblick

[Rz 47] Die Digitalisierung und die neuen technologischen Infrastrukturen verändern nicht nur die Geschäftsmodelle und die Kommunikationsformen, sondern auch das haftungsrechtliche Umfeld. Im Kontext des Internet of Things und der autonomen Systeme bilden sich komplexe Mehrebenen-Zuständigkeiten heraus, welchen das traditionelle Haftungsrecht nur schwer gerecht zu werden vermag.

[Rz 48] Zudem beruhen alle bisherigen Haftungssysteme (Vertrags-, Delikts-, Gefährdungs-, Spezialhaftungen) auf einem Konnex zu einer physischen Sache. Die Schadensverursachung durch virtuelle Güter ist nicht im Blickfeld der geltenden Normen.

[Rz 49] Aus diesen Gründen ist das Haftungsrecht zu überdenken. Sorgfaltspflichten und Verantwortlichkeitszuordnung sind in der digitalen Welt neu auszutarieren. An Bedeutung gewinnen muss zudem ein umfassendes Risikomanagement auf allen Stufen. Und schliesslich ist an die Einführung spezifischer Versicherungslösungen zu denken.

Rolf H. Weber, em. Professor für Wirtschaftsrecht an der Universität Zürich und Rechtsanwalt in Zürich (Bratschi Wiederkehr Buob AG).

44 Communication (Fn. 3), 15.

45 Vgl. dazu den Hinweis bei Melinda Florina Lohmann, Roboter als Wundertüten – eine zivilrechtliche Haftungsanalyse, AJP 2017, 152, 161.