www.jusletter-it.eu

Alexander Duisberg

Machine Learning und rechtliche Rahmenbedingungen

Regelungsbedarfe und Gestaltungsmöglichkeiten

Machine Learning stands for the core technology of Artifical Intelligence that like no other topic will characterize the digital changes in the years to come. The resource « data » that feeds the self learning systems raises questions of disposal rights and privacy respecting processing. Furthermore questions of liability are paramount. The article discusses some of the essential regulation needs and design possibilities. (as)

Category: Articles
Region: Germany
Field of law: Artificial Intelligence & Law; Big Data, Open Data & Open Government; Data Protection; Robotic; Damage. Compensation for Damages.

Citation: Alexander Duisberg, Machine Learning und rechtliche Rahmenbedingungen, in: Jusletter IT 26 September 2018

Inhaltsübersicht

I. Exponentielle Veränderungen durch Datenwachstum und Analytics

[Rz 1] Machine Learning – als Teilbereich und prägnanter Begriff der «Künstlichen Intelligenz» – wird die kommenden Jahre wie kein anderes Technologie-Thema prägen. Digitale Assistenten (Amazon Alexa, Google Assistants, Duplex Features etc.), selbstlernende und -ausführende Spiele wie AlphaGo oder teilautonome Systeme wie z.B. selbstfahrende Fahrzeuge und Transportdrohnen sind bereits Teil unserer Realität oder werden dies in wenigen Jahren sein, sodass man sich schon bald – wie etwa in Hinblick auf das Smartphone – verwundert die Augen reiben wird, wie wir ohne sie in der Vergangenheit zurechtkamen. Die Durchschlagskraft erfolgreicher Technologien (nicht alle setzen sich durch!) und ihrer extrem hohen Skalierung in kurzer Zeit besteht in der disruptiven Veränderung, wie wir kommunizieren, arbeiten und unser Leben gestalten.

1. «Rohstoff» Daten

[Rz 2] Alle zugrundeliegenden Geschäftsmodelle basieren auf einer besonders starken Datenzentrik. Mit Big Data und Analytics (einschließlich der Herbeiführung von Korrelation durch heterogene Datenquellen) lassen sich innovative Geschäftsmodelle entwickeln und realisieren. Dabei spielt die Kunden- und Nutzerakzeptanz – nicht nur im Verbraucherumfeld – eine, wenn nicht die entscheidende Rolle.

[Rz 3] Schon deswegen ist die sorgfältige rechtliche Prüfung der Rahmenbedingungen und Absicherung der Risiken unverzichtbar. Dazu muss man sich aber zum Teil von bekannten Denkmustern lösen bzw. klären, ob und wie man mit den existierenden Regelwerken angesichts der non-deterministischen Natur des Machine Learning zu vernünftigen und belastbaren Ergebnissen kommen kann.

2. Mehrwert durch non-deterministische Software-Programmierung

[Rz 4] Anders als bei der herkömmlichen, binär-deterministischen Software-Programmierung (wenn Voraussetzung A eintritt, wird Rechenoperation B ausgelöst und ist damit entscheidungslogisch das Rechenergebnis C vorbestimmt) ist beim Machine Learning im Zeitpunkt der Kodierung und Initiierung des Algorithmus «im Betrieb» eben ganz bewusst noch nicht vorhersehbar, «was dabei herauskommt». Vielmehr verbessert sich die Präzision der erzielten Ergebnisse mit Erhöhung des Datendurchsatzes, so dass es zu unvorhergesehen Erkenntnissen und Entscheidungen kommt, die den «Mehrwert» erzeugen. Damit eben dieser «Mehrwert» aber nicht «aus der rechtlich zulässigen Bahn» schlägt, sind eine Reihe von Vorüberlegungen zu den Anwendungsvoraussetzungen und korrigierenden Eingriffspflichten des Betreibers bzw. des für das Machine Learning Verantwortlichen anzustellen.

II. Datensouveränität und Geschäftsgeheimnisse – Determinanten des Machine Learning

[Rz 5] Mit dem Stichwort «Big Data» verbinden sich im Kern zwei unterschiedliche rechtliche Betrachtungsebenen – zum einen das Thema der «Datensouveränität» bzw. der Zugriffs- und Verfügungsbefugnisse über Datensammlungen und zum anderen das Thema der Compliance vorwiegend mit Blick auf den Datenschutz.

1. Daten als nicht-rivale Güter

[Rz 6] In den vergangenen Jahren ist die Frage der Datensouveränität oftmals unter dem leicht irreführenden Begriff «Dateneigentum» diskutiert worden – in der Annahme, dass man ein solches begründen oder erschaffen müsse (wenn es denn de lege lata, wie wohl weitgehend unbestritten, nicht bestehe), um vernünftige Voraussetzungen für den Aufbau der Datenökonomie, des unternehmensübergreifenden Datenaustauschs und damit auch innovativer Geschäftsmodelle zu schaffen.[1] Der Blick auf die nicht-rivale Nutzbarkeit von Daten hat nach und nach vor Augen geführt, dass man nicht in den tradierten Mustern des Sacheigentums und des damit verbundenen Schutzbedarfs knapper Güter verharren darf: Die Nutzbarkeit bzw. Nutzung eines Datums durch einen Verkehrsteilnehmer schließt – im Gegensatz zu beweglichen Gütern und dem dahinter stehenden Schutzgedanken des Sacheigentums – grundsätzlich nicht die Nutzung durch weitere Verkehrsteilnehmer aus. Zudem ist nicht erkennbar, wie mit der sich entwickelnden Komplexität und Veränderung der Wertschöpfung – von der hergebrachten linearen Wertschöpfungskette hin zur Nutzung von Daten in Ökosystemen und Plattformen und ggf. darauf aufbauenden mehrseitigen Märkten – der Zuweisungsgehalt eines «Dateneigentums» vorab und umfassend zugunsten einer Kategorie von Marktteilnehmern (Datenerzeuger vs. Inhaber von Rohdaten vs. Veredler

[1] Siehe bspw. der Bericht der Arbeitsgruppe «Digitaler Neustart» der Konferenz der Justizministerinnen und Justizminister der Länder vom 15. Mai 2017, abrufbar unter www.justiz.nrw.de/JM/schwerpunkte/digitaler_neustart/zt_bericht_arbeitsgruppe/bericht_ag_dig_neustart.pdf (alle Websites zuletzt besucht am 31. August 2018); Alexander Duisberg, Datenhoheit und Recht des Datenbankherstellers – Recht am Einzeldatum vs. Rechte an Datensammlungen, in: Daten als Wirtschaftsgut, Smart-Data-Begleitforschung, FZI Forschungszentrum Informatik, Berlin 2017, abzurufen unter www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/2017-11-22_smartdata_daten_wirtschaftsgut.html.

von Daten vs. Betreiber von Datenverarbeitungssystemen vs. Betreiber von Plattformen vs. Betreiber von Datenmarktplätzen auf Plattformen etc. pp.) sinnvoll und umfassend für jedermann *a priori* entschieden werden könnte. Phänomene wie «open data» (einschließlich der von der PSI Richtlinie (EU) 2003/37 verfolgten Ansätze zur Öffnung von Datenbeständen der öffentlichen Hand), Umsetzungen für den Austausch von Maschinendaten wie im Industrial Data Space[2] und das Generalthema der «shared economy» stehen stellvertretend für eine Vielzahl der auf Datenteilhabe basierenden Innovationspotenziale. Entsprechend gilt es, die Weichen in Richtung einer möglichst offenen, innovationsorientierten Rechtskultur zu stellen und zu fragen, ob mögliche Ausschließlichkeitsrechte an Daten hier innovationshindernd wirken würden.

2. Zugang zu den Datenbeständen der Big Player?

[Rz 7] Dementsprechend hat sich die Diskussion maßgeblich verlagert zu der Frage, ob in bestimmten Industriebereichen und Anwendungen das Risiko eines Marktversagens bestehen könnte und damit die – wettbewerbsrechtliche, nicht zivilrechtliche – Frage im Raum steht, ob (i) es für bestimmte Situationen notwendig sein könnte, mittels Regulierung einen allgemeinen Zugang zu Datenbeständen dominanter Marktteilnehmer zu eröffnen bzw. (ii) ob – soweit es um die Teilhabe an Datenbeständen und Datensammlungen geht – ggf. mittels nicht-diskriminierender, ausgewogener bzw. «fairer» Vertragsbedingungen eine Marktbalance für die Nutzbarkeit von Datenbeständen monolithischer Dateninhaber einzufordern ist.[3]

3. Vertragliche Gestaltung des Datenaustauschs

[Rz 8] Im Ergebnis ist damit die Gestaltung des Datenaustauschs bzw. die Bereitstellung der Datensammlungen für das Machine Learning im Wesentlichen der Vertragsfreiheit zwischen Dateninhabern (Datengebern) einerseits und den Betreibern des Machine Learning (Datennutzern) andererseits überlassen. Während die Herausbildung vertraglicher Standards im Bereich von Maschinendaten – auch unter besonderer Berücksichtigung des Rechts des Datenbankherstellers[4] – in vielen Sektoren noch weitgehend am Anfang steht, sind darin jedenfalls Anforderungen an die Datenqualität wie auch die Compliance bzw. rechtlich unbedenkliche Nutzbarkeit von Daten zu regeln, und entweder durch nähere Gewährleistungs- und Haftungsregeln abzusichern – oder gerade umgekehrt im Sinne einer Risikoverlagerung auf den Betreiber des Machine Learning auszuhandeln.

---

2 Eine Übersicht über Ziele und Architektur des Industrial Data Space geben Boris Otto [et al.] in ihrem Whitepaper Industrial Data Space, Fraunhofer Gesellschaft, München 2016, abrufbar unter www.fit.fraunhofer.de/content/dam/fit/de/documents/Industrial-Data-Space_whitepaper.pdf.

3 Bemerkenswert insoweit die finale Position des Rates zur EU Verordnung «Free flow of non-personal data» vom 28. Juni 2018, 2017/0228 (COD), in der ausdrücklich «data ownership» durch die Postulate «access to and reuse of data» ersetzt werden (ebenda, unter Ziffer (1)).

4 Die Bedeutung dieses Schutzrechts für den Aufbau der Datenökonomie wird bislang weithin unterschätzt. Eine vertiefte Aufbereitung der relevanten Themen würde diesen Beitrag überschreiten; daher bspw. Matthias Leistner, Datenbankschutz, in: Jürgen Basedow / Klaus J. Hopt / Reinhard Zimmermann (Hrsg.), Handwörterbuch des Europäischen Privatrechts, Band 1, Tübingen 2009, 298 ff.; ausführlich matthias Leistner, Der Rechtsschutz von Datenbanken im deutschen und europäischen Recht, München 2000.

4. Neue Regeln für Geschäftsgeheimnisse

[Rz 9] Ein besonderes Augenmerk verdient dabei die Relevanz des Schutzes bzw. der ggf. erfolgenden Offenbarung von Geschäftsgeheimnissen. Mit der Trade Secrets Richtlinie (EU) 2016/943 zeichnet sich ein Paradigmen-Wechsel für das deutsche Recht ab. Nachdem jahrzehntelang ein fragmentierter Rechtsschutz um die deutsche Normen §§ 17–19 gegen den unlauteren Wettbewerb (UWG), §§ 823, 826, 1004 des bürgerlichen Gesetzbuches (BGB) einschließlich umfangreicher Judikatur herangewachsen war,[5] wird nunmehr im Zuge der Umsetzung ein konsolidiertes Gesetz über den Schutz von Geschäftsgeheimnissen erlassen werden.[6] Dabei liegt mit der Richtlinie die folgenreiche Änderung schon in der Definition des «Geschäftsgeheimnisses»: In der Formulierung des deutschen Regierungsentwurfs (§ 2 Nr. 1) ist eine Information dann als Geschäftsgeheimnis einzustufen, wenn sie «a) weder [...] allgemein bekannt oder ohne weiteres zugänglich ist und daher von wirtschaftlichem Wert ist und b) Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist» [Unterstreichung durch den Verfasser]. Zum einen leitet sich also der wirtschaftliche Wert einer geheimen Information, verkürzt gesagt, aus dem Umstand der Geheimheit ab. Zum anderen ist der Schutzbereich erst dann eröffnet, wenn der rechtmäßige Inhaber der Information angemessene Maßnahmen zur Geheimhaltung getroffen hat. Damit werden die Anforderungen an Geschäftsgeheimnisse weiter konkretisiert und gegenüber der bisherigen Rechtslage tendenziell verschärft bzw. an äußere Merkmale geknüpft, die in der Form bisher nicht zu erfüllen waren. Wer mithin Daten für Machine Learning einem anderen überlässt, muss sich also in Zukunft vorher sorgfältig mit der Frage befassen, ob in den Daten, so wie er sie bisher geheim gehalten und geschützt hat, Geschäftsgeheimnisse liegen, oder eben nicht. Nur wenn dies zu bejahen ist, kann der Dateninhaber auch gegenüber dem Betreiber des Machine Learning den Schutz von Geschäftsgeheimnissen geltend machen und diese – dann wiederum vor der Weiterverwendung im Verhältnis zu Dritten – durch vertragliche Abreden mit dem Datennutzer bzw. Betreiber des Machine Learning absichern.

III. Datenschutz und pseudonyme Datennutzung – Lösungsansätze nach der DSGVO

1. Datenminimierung und Zweckbindung nach DSGVO als neue Herausforderungen

[Rz 10] Mit der Datenschutzgrundverordnung (DSGVO) ist ein einheitlicher, hoher Datenschutzstandard mit erheblicher Ausstrahlungswirkung über die EU hinaus geschaffen worden. Zu der Weiterentwicklung der bestehenden Rechtsinstitute, der massiven Verstärkung des Sanktionsrahmens und der die Dokumentationspflichten erheblich ausweitenden Rechenschaftspflicht («Accountability») sind mit Blick auf Big Data zwei Themenstellungen von besonderem Interesse: der Grundsatz der Datenminimierung (Art. 5 Abs. 1 (c) DSGVO), der in einem natürlichen Spannungsverhältnis zu den Anforderungen an den Durchsatz großer Datenmengen steht, mit de-

5 Zur bisherigen Rechtslage siehe etwa Helmut Köhler, in: Helmut Köhler / Joachim Bornkamm / Jörn Feddersen, Gesetz gegen den unlauteren Wettbewerb, 36. Aufl., München 2018, Rn. 53–56a; Ansgar Ohly, in: Ansgar Ohly / Olaf Sosnitza, Gesetz gegen den unlauteren Wettbewerb, 7. Aufl., München 2016, Vorbemerkungen vor §§ 17–19 Rn. 10; Ansgar Ohly, Der Geheimnisschutz im deutschen Recht: heutiger Stand und Perspektiven, GRUR 2014, 1.

6 Siehe RegE des GeschGehG vom 18. Juli 2018, abrufbar unter www.bmjv.de.

nen das Machine Learning erst realisiert werden kann, sowie die Zweckbindung (Art. 5 Abs. 1 (b) DSGVO), die als zentrales Gebot jedem Verantwortlichen die inneren Grenzen der varianten Datennutzung aufzeigt. Man mag angesichts der weiten Definition personenbezogener Daten fragen, wo dann der Raum für Big Data Anwendungen und Wertschöpfung aus weitreichender Datenanalyse liegt: oder anders gefragt: Ob wir uns – noch dazu im globalen Wettbewerb – der Möglichkeiten berauben, in diese zentralen, zukunftsweisenden Technologien einzusteigen, bevor der Wettbewerb um die besten Anwendungen begonnen hat.[7] Die Schlussdiskussion um die Verabschiedung des Wortlauts der DSGVO Ende 2015 zeigt, dass gerade mit Blick auf die Big Data Thematik heftig gerungen wurde.[8]

2. Die Verarbeitung von nicht personenbezogenen Daten

[Rz 11] Die entscheidende Frage für den Datenschutz bei Machine Learning Anwendungen ist, ob und inwiefern die zu verarbeitenden Daten einen Personenbezug aufweisen.

[Rz 12] Die Verarbeitung von Daten ohne Personenbezug lässt das Datenschutzrecht definitionsgemäß von vornherein nicht zur Anwendung kommen: Sensordaten, die im maschinellen Umfeld ohne jede Verknüpfung zu an einem Fertigungsprozess beteiligten Personen vorliegen, Messdaten ohne jeden Kontext zu Personen, reine Finanzdaten von Unternehmen usw. Hier liegt im Kern der breite Anwendungsbereich von Big Data Anwendungen und Machine Learning, der – jedenfalls soweit die Nicht-Anwendbarkeit des Datenschutzrechts geprüft wurde – ohne jede weitere Maßgaben aus der DSGVO umgesetzt werden kann. Doch auch hier ist fortlaufende Sorgfalt geboten. Zum einen sind die Anforderungen an eine erfolgreiche Anonymisierung von Daten sehr hoch.[9] Zum anderen: Was heute an anonymen Daten dem Machine Learning zugrunde gelegt wird, kann morgen aufgrund der Korrelation mit anderen Datenquellen möglicherweise einen Personenbezug aufweisen. Daher ist aus der Compliance-Sicht in jedem Fall die Hinzuziehung des Datenschutzbeauftragten bzw. eine datenschutzrechtliche Prüfung der Anwendbarkeit der DSGVO in dem konkreten Modell des Machine Learning zu empfehlen.

3. Pseudonymisierung eröffnet Spielraum

[Rz 13] Die nächste Stufe der Verarbeitung liegt in der Verarbeitung pseudonymer Daten – hier findet das Datenschutzrecht Anwendung. Hier findet sich in Art. 6 Abs. 4 DSGVO eine bemerkenswerte Regelung: Danach ist die Verarbeitung personenbezogener Daten für variante Zwecke (d.h. sachlich anverwandte, ähnliche gegenüber den ursprünglich festgelegten Zwecken der Verarbeitung) u.a. zulässig, wenn der Verantwortliche die Daten pseudonymisiert bzw. durch Pseudonymisierung für eine ausreichende datenschutzrechtliche Absicherung bzw. Garantie sorgt, so dass der veränderte Verarbeitungszweck als mit dem ursprünglichen vereinbar i.S.d. Art. 5 Abs. 1

---

7 Siehe auch die Meldung der FAZ zum IT-Gipfel 2016: «Merkel: Beim Datenschutz nicht übertreiben», FAZ online, aktualisiert am 17. November 2016, abrufbar unter www.faz.net/aktuell/wirtschaft/netzwirtschaft/angela-merkel-warnt-auf-it-gipfel-vor-zu-strengem-datenschutz-14532201.html.

8 Die Dokumentation zum legislativen Verfahren findet sich beim Europäischen Parlament unter der Verfahrensnummer 2012/0011(COD), abrufbar unter www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2012/0011(COD)&l=EN

9 Siehe Opinion 05/2014 WP 216 der Art 29 WP vom 10. April 2018.

(b) DSGVO gilt.[10] Damit eröffnet sich immerhin ein gewisser, wenn auch nicht übermäßiger Bewegungsspielraum zur Zweckvarianz. Allerdings steht hierzu – wie insgesamt zu der Frage, welche Möglichkeiten die pseudonymisierte Datenverarbeitung nach der DSGVO bietet – in vieler Hinsicht eine weiterführende Konkretisierung durch den Europäischen Datenschutz aus. Im Ergebnis ist aus der Sicht der Innovationspotenziale des Machine Learning zu wünschen und zu verlangen, dass der Betreiber des Machine Learning über die Fertigkeiten verfügt zu erkennen, wenn als Folge des Machine Learning sich neue, aus den zunächst bereit gestellten Datenquellen nicht unmittelbar herzuleitende Personenbezüge generieren. Hier muss der Betreiber des Machine Learning letztlich als Verantwortlicher in die vollen datenschutzrechtlichen Pflichten eintreten und – soweit ihm dies möglich ist – beispielsweise vor einer weitergehenden Verwertung die Personenbezüge aus neu gefundenen Korrelationen entfernen bzw. sich jedenfalls um eine die weitere Verarbeitung absichernde Rechtsgrundlage kümmern

IV. Haftung für selbstlernende Systeme und quasi-autonome maschinelle Entscheidungen

[Rz 14] Wenn das Machine Learning als Datenverarbeitung mittels nicht-deterministisch programmierter Algorithmen zu verstehen ist und darauf Anwendungen und Systeme beruhen, so stellt sich in besonderer Weise die Haftungsfrage für die Folgen «autonom lernender», ergebnisoffener Entscheidungen der Maschinen. Wer haftet, wenn der Computer seine Entscheidungen «in die falsche Richtung» trifft bzw. es zu Schäden und Störungen und Schäden an Rechtsgütern Dritter kommt – ist es der Software-Programmierer, der Inhaber der Maschine, der Betreiber des Systems, der Nutzer einer Anwendung oder womöglich eine gesamtschuldnerische Gemeinschaft denkbarer Haftungssubjekte?[11]

1. Die e-Person als Lösung für die Haftungsfrage?

[Rz 15] Zunächst ist nach allgemeinen zivilrechtlichen Grundsätzen – sowohl für die vertragliche als auch die deliktische Haftung – festzuhalten, dass auch für autonome Systeme die Zurechnung des Handlungsunrechts an eine natürliche oder juristische Person unverändert zu treffen ist: Der Weg zur Haftung der «e-Person», also die Ausstattung eines autonomen Systems mit einer eigenen Rechtspersönlichkeit und einer dahinter stehenden Haftungsmasse wird zwar ernsthaft diskutiert,[12] führt aber derzeit nicht zu einer Enthaftung anderer Haftungssubjekte. Dabei ist erkenntnistheoretisch zugrunde zu legen, dass zwar das konkrete Ergebnis bzw. die konkrete Entscheidung eines autonomen Systems nicht vorhersehbar sein mag, aber jedem System zunächst und vorab eine menschlich bestimmte Zielsetzung zugrunde liegt. Anders gesagt: Nur der

10 Benedikt Buchner / Thomas Petri, in: Jürgen Kühling / Benedikt Buchner, Datenschutzgrundverordnung, Kommentar, 2. Aufl., München 2018, Art. 6 Rn. 183, 191.

11 Interessant auch der systemische Ansatz von Indra Spiecker gen. Döhmann, in dem eine von ihr so genannte Graduelle Gesamtschuldnerschaft zur Anwendung käme (CR 2016, 698 (703)).

12 Aufschlussreich Louisa Specht / Sophie Herold: Roboter als Vertragspartner? MMR 2018, 40 (43) m.w.Nw.

Mensch vermag autonom die Ziele seines Handelns zu bestimmen, eine Maschine vermag dies nicht.[13]

2. Mehrere Akteure: Wer haftet?

[Rz 16] Allerdings ist mit dieser Vorüberlegung das Zurechnungsproblem im Fall eines konkreten, unvorhergesehenen Ergebnisses eines autonomen Systems nicht ohne Weiteres gelöst: Soll etwa der Software-Programmierer für die Ergebnisse des Algorithmus haften, den er entwickelt, den aber ein ganz anderer für die von ihm gesetzten, aber auch nur maßvoll kontrollierten oder eben im Ergebnis kaum kontrollierbaren Systeme eingesetzt hat? Die Frage zu stellen, heißt sie offenkundig zu verneinen. Wenn aber der Betreiber eines Systems aufgrund der Entscheidungslogik des programmierten Algorithmus keine Möglichkeit hat, das System schadensverhindernd zu bremsen oder abzustellen, muss er dann haften, obwohl er die konkrete Entscheidung weder vorhersehen noch während des konkreten Verlaufs zum Schadensereignis in diese hätte eingreifen können? Bei dieser Frage wird es schon schwieriger, zumal wenn man das Haftungsrisiko nicht als allgemeines Lebensrisiko auf den Geschädigten abwälzen kann oder möchte.[14]

3. Neue Herausforderungen in der Produzenten- und Produkthaftung durch Machine Learning

[Rz 17] Nimmt man die bestehenden Kategorien des Haftungsrechts zur Hand, so sind wichtige Fixpunkte zu beachten: Bei der Produkthaftung nach § 1 ff. ProdHaftG haftet der Hersteller verschuldensunabhängig für Schäden, die durch Konstruktions-, Herstellungs- und Instruktionsfehler entstehen. Die Haftung entfällt, wenn das Produkt zum Zeitpunkt des Inverkehrbringens nach dem Stand der Technik gefahrlos genutzt werden konnte, § 1 Abs. 2 Nr. 4 ProdHaftG.

[Rz 18] Im Rahmen der deliktischen Produzentenhaftung nach § 823 Abs. 1 BGB steht der Hersteller dafür ein, dass von dem in Verkehr gebrachten Produkt keine Gefahren für die Rechtsgüter Dritter ausgehen. Kommt es doch dazu, d.h. hat das Produkt einen schadensursächlichen Fehler, trifft ihn die Beweislast, dass er das Produkt sorgfältig mit Blick auf etwaige Gefahrenquellen geprüft hatte.[15] Dabei treffen den Hersteller auch nach Inverkehrbringen Produktbeobachtungspflichten, wenn sich Fehler bzw. Gefahrenquellen erst nachträglich zeigen.[16] Wie fällt aber die Bewertung aus, wenn ein selbstlernendes System zum Zeitpunkt des Inverkehrbringens unter allen Gesichtspunkten objektiv fehlerfrei war und erst danach aufgrund des Machine Learning zur Gefahrenquelle wird? Im Ergebnis dürfte alles dafür sprechen, dass hier eine Produktbe-

---

13 Anders wäre dies möglicherweise bei einer so genannten AGI (artificial general intelligence), von deren Entwicklung wir aber je nach Einschätzung noch Jahre bis Jahrzehnte entfernt sind; siehe näher bei Matt Turck, Frontier AI: How far are we from artificial «general» intelligence, really?, abrufbar unter https://hackernoon.com/frontier-ai-how-far-are-we-from-artificial-general-intelligence-really-5b13b1ebcd4e.

14 Die Beispiele sind uferlos, aber es bestehen natürlich erhebliche Unterschiede zwischen den Horrorszenarien der außer Kontrolle geratenen «Killer-Drohne», die ihre menschlichen Ziele aufgrund von Bewegungs- und Wärmesensorik unaufhaltsam ansteuert und vernichtet, und dem Verspätungsschaden, den ein Passagier aufgrund der nicht rechtzeitigen Beförderung eines unvorhergesehen von der vorgesehenen Linienführung abweichenden, autonomen fahrenden Busses erleidet.

15 Siehe nur Christian Förster, in: Beck scher Online-Kommentar BGB, 46. Aufl. 2018, BGB § 823 Rn. 663–668.

16 Gerhard Wagner, in: Münchener Kommentar zum Bürgerlichen Gesetzbuch, 7. Aufl., München 2017, BGB § 823 Rn. 840.

obachtungspflicht greifen muss, um die Nutzer auf solche Gefahren hinzuweisen oder auch zu intervenieren, um die Gefahrenquelle, soweit möglich, abzustellen. Nur: Ergibt sich diese Pflicht aus der geltenden Produzentenhaftung[17] oder bedarf es hier einer gesetzlichen Erweiterung? Die Produzentenhaftung greift jedenfalls auch dann, wenn die Gefahr von einer reinen Softwareanwendung ausgeht, da im Rahmen des § 823 BGB keine hohen Anforderungen an die Produkteigenschaft gestellt werden.[18]

4. Diskussion um europäische Robotik-Regelungen

[Rz 19] Fragen der Haftung für Machine Learning Systeme werden in Zukunft voraussichtlich zum Grossteil nach europäischen Regelungen entschieden werden. In einer Parlamentsentschließung vom 16. Februar 2017 (P8_TA(2017)0051)[19] hat das Europäische Parlament die Kommission aufgefordert, einen Vorschlag für eine Richtlinie zu zivilrechtlichen Regelungen im Bereich Robotik («Civil Law Rules on Robotics») zu unterbreiten. Dieser Vorschlag solle u.a. eine Begriffsbestimmung und Klassifikation verschiedener Kategorien intelligenter Roboter, eine zentrale Registrierung solcher Roboter, Regelungen zur Interoperabilität, eine Robotik-Charta und einen Verhaltenskodex für Robotikingenieure enthalten – und der Vorschlag soll nach den Vorstellungen des Parlaments Fragen zur zivilrechtlichen Haftung von Robotern und Anwendungen künstlicher Intelligenz behandeln. Dabei lässt das Parlament die Idee der «e-Person» zwar anklingen, allerdings eher als langfristige Perspektive. Das Parlament legt der Kommission nahe, sich Gedanken über die Art der Haftung der beteiligten natürlichen und juristischen Personen zu machen: Es könne etwa verschuldensunabhängig gehaftet werden («strict liability») oder nach dem Risikomanagementansatz. Die Haftung zwischen den Beteiligten untereinander solle sich danach bemessen, inwiefern sich die Autonomie des Roboters ausgewirkt hat bzw. wie lange er bereits von seinem Benutzer «trainiert» worden ist. Das Parlament plädiert ferner für ein Pflichtversicherungssystem, an dem sich – je nach Ausgestaltung – Hersteller, Eigentümer und/oder Benutzer beteiligen müssten. Diese Versicherung könne dann durch einen Fonds ergänzt werden, der einspringt, wenn die Versicherung nicht ausreicht. Seit dem 16. Mai 2017 gibt es eine Antwort der Kommission auf den Beschluss des Parlaments (P8_TA-PROV(2017)0051), wonach die

17 So zumindest für autonome Systeme allgemein Malte Grützmacher, CR 2016, 695 (696) und Susanne Horner / Markus Kaulartz, CR 2016, 7 (12); für Software ausführlicher Johannes Droste: Produktbeobachtungspflichten der Automobilhersteller bei Software in Zeiten vernetzten Fahrens, CCZ 2015, 105 (107).

18 Für Software Johannes Droste: Produktbeobachtungspflichten der Automobilhersteller bei Software in Zeiten vernetzten Fahrens, CCZ 2015, 105 (107); allgemein zum Produktbegriff gerhard Wagner, in: Münchener Kommentar zum Bürgerlichen Gesetzbuch, 7. Aufl., München 2018, § 823 BGB, Rn. 784. Als Beispiel für problematische Softwareanwendungen und entsprechende Beobachtungspflichten sei der im Jahre 2016 erprobte Chat-Bot «Tay» genannt, der sich selbstlernend innerhalb weniger Stunden in einen Verbreiter rechtswidriger Inhalte verwandelte und den der Betreiber Microsoft umgehend stilllegte (Patrick Beuth, Twitter-Nutzer machen Chatbot zur Rassistin, vom 24. März 2016, abrufbar unter www.zeit.de/digital/internet/2016-03/microsoft-tay-chatbot-twitter-rassistisch). Hier griff allerdings keine Produkthaftung, sondern die Betreiberhaftung für Plattforminhalte (kompakt zu dieser Haftung etwa Louisa Specht, Ausgestaltung der Verantwortlichkeit von Plattformbetreibern zwischen Vollharmonisierung und nationalem Recht, ZUM 2017, 114 (116f.)). Das Beispiel zeigt lediglich, dass die Gefahrenlage in kürzester Zeit durch eine fehlgeleitete Softwarefunktionalität exponentiell ansteigen kann.

19 Entschließung des Europäischen Parlaments vom 16. Februar 2017 mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103(INL)), Dok. P8_TA(2017)0051, abrufbar unter www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0051+0+DOC+PDF+V0//DE. Kritische Würdigungen der Entschließung geben: Melinda Lohmann, Ein europäisches Roboterrecht – überfällig oder überflüssig? ZRP 2017, 168; Oliver Kessler, Intelligente Roboter – neue Technologien im Einsatz, MMR 2017, 589; Jan-Philipp Günther, Europäische Regelungen im Bereich Robotik – alles noch Science Fiction?, DB 2017, 651.

Kommission momentan – nachdem mehrere öffentliche Konsultationen zum Abschluss gekommen sind – weitere legislative Schritte in Betracht ziehen dürfte. Die weitere Entwicklung bleibt abzuwarten.

5. Autonomes Fahren: Mensch-Maschine-Interaktion in kritischen Situationen

[Rz 20] Das Beispiel der Haftung des Fahrzeugführers bei hoch- und vollautomatisierten Fahrfunktionen zeigt einen interessanten Regelungszusammenhang: Gemäß dem mit Wirkung zum 21. Juni 2017 eingeführten § 1a des Strassenverkehrsgesetzes (StVG) dürfen Fahrzeuge mit hoch- oder vollautomatisierten Fahrfunktionen ausgestattet und nach den einschlägigen Anwendungen zugelassen werden. Bemerkenswert ist dabei insbesondere § 1 Abs. 4 StVG, der die Rolle des Fahrzeugführers in Übereinstimmung mit einer entsprechenden Änderung des Wiener Übereinkommens über den Straßenverkehr[20] erweitert: «*Fahrzeugführer ist auch derjenige, der eine hoch- oder vollautomatisierte Fahrfunktion im Sinne des Absatzes 2 aktiviert und zur Fahrzeugsteuerung verwendet, auch wenn er im Rahmen der bestimmungsgemäßen Verwendung dieser Funktion das Fahrzeug nicht eigenhändig steuert*.» Die Aufgabe des Fahrzeugführers verändert sich mithin und ist nicht mehr abschließend durch die traditionelle Steuerung des Fahrzeugs beschrieben. Anders gesagt: Der Computer steuert das Fahrzeug und der Fahrzeugführer übernimmt eine veränderte Aufgabe. Entsprechend formuliert § 1b StVG für die Schnittstelle der Mensch-Maschine-Interaktion veränderte Rechte und Pflichten des Fahrzeugführers. Auch wenn er sich von der unmittelbaren Überwachung der Fahrzeugsteuerung herausnehmen darf, muss er «*wahrnehmungsbereit bleiben*» (§ 1b Abs. 1 StVG), um bei entsprechenden Hand-over Signalen des Fahrzeugs oder «*offensichtlichen Umständen*» einer Fehlfunktion der betreffenden Fahrfunktion die Kontrolle über das Fahrzeug gemäß den Anforderungen wieder zu übernehmen (§ 1b Abs. 2 StVG). Dieses Konzept einer verantwortlichen Mensch-Maschine-Interaktion wird auf der Beweisebene durch den Event Data Recorder gemäß § 63a StVG abgesichert, so dass für jeden Fahrverlauf nachträglich festgestellt werden kann, ob der Fahrzeugführer seinen Übernahmepflichten genügt hat bzw. ob ein ordnungsgemäßes Verhalten des Fahrzeugführers zu einer entsprechenden Enthaftung gemäß § 18 Abs. 1 Satz 2 StVG führt. Im Einzelnen sind etliche Details klärungsbedürftig bzw. werden – wie z.B. hinsichtlich der Anforderungen an die «Wahrnehmungsbereitschaft» – womöglich erst durch Rechtsprechung und verhaltenspsychologische Gutachten konkretisiert.[21] Im Ergebnis kommt darin aber jedenfalls zum Ausdruck, dass der kritische Punkt der Mensch-Maschine-Interaktion näher zu regeln ist und einer technischen Umsetzung zugänglich sein muss, um Verantwortlichkeiten, Eingriffspflichten und Haftungszurechnung sinnvoll zu gestalten.

---

20 Mit Wirkung zum 23. März 2016 wurde ein Absatz 5^{bis} in den Artikel 8 des Übereinkommens eingefügt, der unter bestimmten Voraussetzungen auch autonome Fahrzeuge für vereinbar mit den Vorschriften des Abkommens erklärt (Gesetz zur Änderung der Artikel 8 und 39 des Übereinkommens vom 8. November 1968 über den Straßenverkehr, BGBl. II S. 1306). S. dazu auch Benjamin von Bodungen / Martin Hoffmann: Das Wiener Übereinkommen über den Straßenverkehr und die Fahrzeugautomatisierung (Teil 1) (SVR 2016, 41).

21 So ist die Wahrnehmungsbereitschaft nicht statisch bzw. linear hochzurechnen. Sie dürfte zu Beginn einer Fahrt höher liegen und bei längerer Nutzung bzw. Gewöhnung an die automatisierte Fahrfunktion im Fahrtverlauf absinken. Entsprechend würde sich die Frage stellen, ob das Fahrzeug die Hand-over Signale im Fahrtverlauf vorsorglich kürzer takten bzw. deutlicher ausgestalten muss, und nach welchen (ggf. zu individualisierenden?) Kriterien dies erfolgen sollte. Vgl. allgemein zur Problematik, Jan-Erik Schirmer, Augen auf beim automatisierten Fahren! Die StVG-Novelle ist ein Montagsstück, NZV 2017, 253 (255); Reinhard Greger, Haftungsfragen beim automatisierten Fahren, NZV 2018, 1 (3).

V. Fazit

[Rz 21] Mit dem Machine Learning baut sich die nächste Stufe in der Vernetzung der Dinge und Beeinflussung oder sogar Steuerung einer Vielzahl von Lebenssachverhalten durch künstliche Intelligenz auf. Aus rechtlicher Sicht ist dabei das Grundverständnis zum Umgang mit dem Rohstoff Daten zu einem Grossteil entwickelt. Vertragliche Rahmenbedingungen und Musterverträge zur Überlassung von Datensammlungen (unter Berücksichtigung des Rechts des Datenbankherstellers) und der Absicherung von Geschäftsgeheimnissen, die den Daten ggf. innewohnen, weisen den Weg weit mehr als die – inzwischen abklingende – Debatte um ein vermeintliches «Dateneigentum». Soweit darüber hinaus Marktungleichgewichte bestehen, mögen diese unter engen Voraussetzungen durch regulierende Maßnahmen zu «data access», «portability» bzw. «reuse of data» aufgefangen werden.

[Rz 22] Dazu tritt die große Herausforderung des Datenschutzes. Im Ergebnis ist die Verarbeitung nicht-personenbezogener, anonymisierter Daten mit Blick auf den überragenden Grundsatz der Zweckbindung der Verarbeitung personenbezogener Daten der «einfachere Weg» – wobei auch hier eine fortlaufende Sorgfaltspflicht gilt. Denn was heute anonym ist, kann durch Machine Learning eben schon morgen aufgrund der Korrelation mit anderen Datenquellen einen Personenbezug aufweisen. Ansonsten ist mit der Verarbeitung pseudonymisierter Daten ein Spielraum eröffnet, der noch der weiteren Konkretisierung durch den Europäischen Datenschutzausschuss gerade auch mit Blick auf das Machine Learning bedarf.

[Rz 23] Hinsichtlich der Haftung für Entscheidungen auf Machine Learning basierender Systeme kann der bestehende Haftungsrahmen mit vielen sich stellenden Fragen einigermaßen verlässlich umgehen. Allerdings besteht Regelungsbedarf gerade in kritischen Anwendungen, bei denen autonome Systeme unmittelbare Gefahren – insbesondere im Zusammenwirken mit Menschen bzw. im Rahmen der Mensch-Maschine-Interaktion – begründen.

Dr. Alexander Duisberg ist Partner bei Bird & Bird in München. Dr. Duisberg ist einer der führenden Experten Deutschlands im Technologie- und Datenschutzrecht.