

BaFin Perspektiven

Ausgabe 1 | 2019



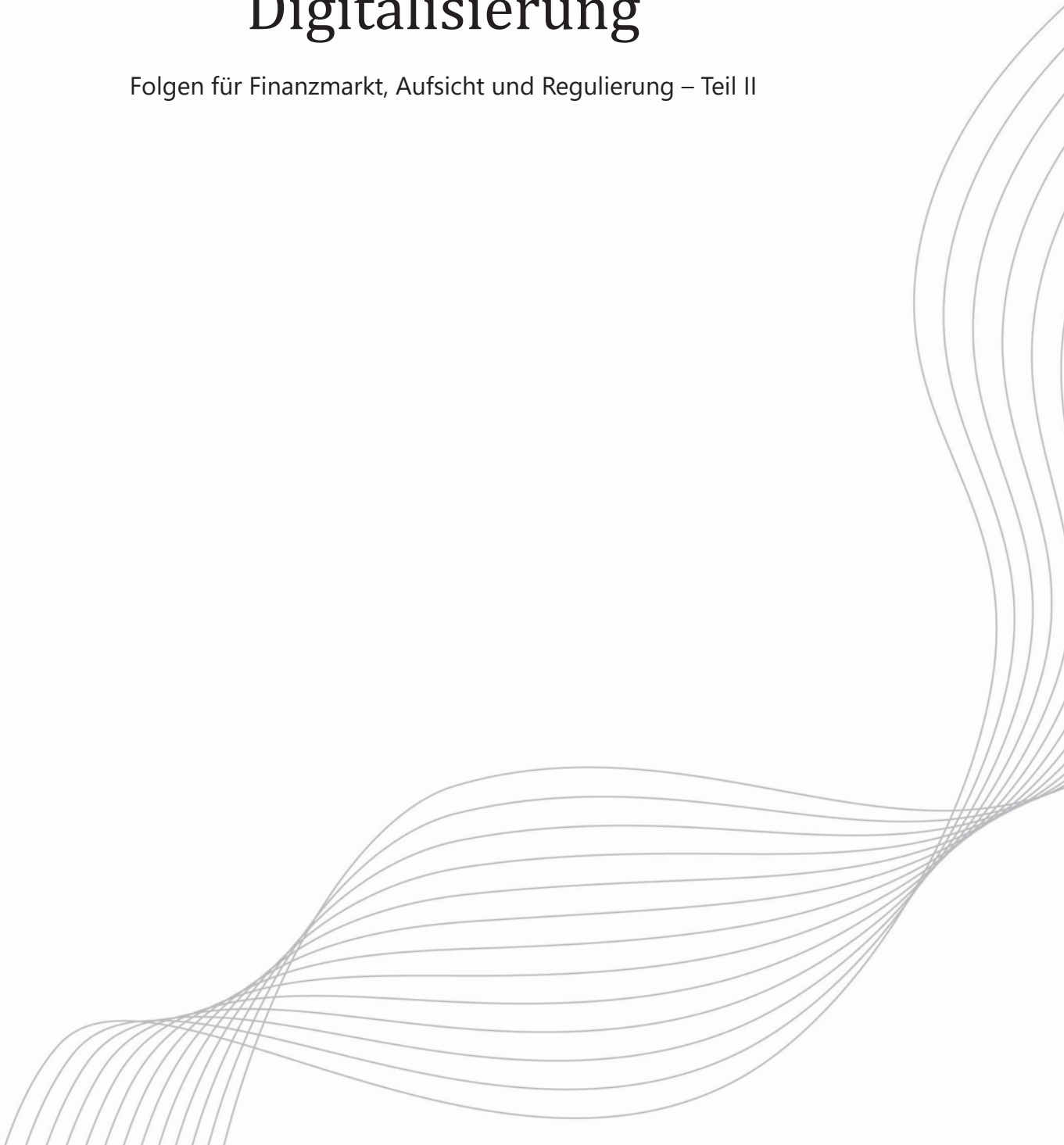
BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

Digitale Transformation

Digitalisierung

Folgen für Finanzmarkt, Aufsicht und Regulierung – Teil II



Inhaltsverzeichnis

| | |
|----------------|----------|
| Vorwort | 8 |
|----------------|----------|

| | |
|---|-----------|
| I. Man muss sich den Chancen, aber auch Risiken der KI stellen | 10 |
|---|-----------|

Staat, Gesellschaft, Wirtschaft, Verwaltung und Wissenschaft müssen sich den Chancen, aber auch den Risiken der künstlichen Intelligenz stellen. Wichtig ist eine gemeinwohlorientierte Nutzung auf Basis der demokratischen Grundordnung.

| | |
|--------------------------------------|-----------|
| Interview mit Dr. Jörg Kukies | 11 |
|--------------------------------------|-----------|

| | |
|---|-----------|
| II. Big Data trifft auf künstliche Intelligenz – Beitrag zu den Ergebnissen der Konsultation des BaFin-Berichts und Interview mit Felix Hufeld | 14 |
|---|-----------|

Zahlreiche Rückmeldungen hat die BaFin zu ihrem Bericht „Big Data trifft auf künstliche Intelligenz – Herausforderungen und Implikationen für Aufsicht und Regulierung von Finanzdienstleistungen“ erhalten. An der Konsultation haben sich Interessensverbände beteiligt, aber auch einzelne Institute, nationale wie internationale Behörden und Vertreter der Wissenschaft. Der Artikel gibt einen Überblick über die Antworten, und BaFin-Präsident Felix Hufeld nimmt im Interview eine erste Bewertung vor. Ein Beitrag von Jörn Bartels und Dr. Thomas Deckers

| | |
|---|-----------|
| 1 Einleitung | 15 |
| 2 Finanzstabilität und Marktaufsicht | 17 |
| 3 Unternehmensaufsicht | 23 |
| 4 Kollektiver Verbraucherschutz | 31 |
| 5 Interview mit BaFin-Präsident Felix Hufeld | 38 |

| | |
|---|-----------|
| III. Wenn Banken IT-Dienstleistungen auslagern | 42 |
|---|-----------|

Die Auslagerung von Aktivitäten und Prozessen ermöglicht es Banken, sich auf ihre Kernkompetenzen zu konzentrieren und ihre Dienstleistungen zu verbessern. Funktionieren kann Auslagerung aber nur, wenn die Institute die Risiken weiterhin unter Kontrolle behalten. Im Zeitalter der Digitalisierung stellt dies Banken und Aufsicht vor neue Herausforderungen. Ein Beitrag von Raimund Röseler und Ira Steinbrecher

| | | |
|-----------|--|-----------|
| 1 | Einleitung | 43 |
| 2 | Standardisierung von IT-Dienstleistungen | 44 |
| 3 | Auslagerung in die Cloud | 44 |
| 4 | Risiken der Auslagerung | 45 |
| 5 | Anforderungen an Auslagerungen an Cloud-Anbieter | 46 |
| 6 | Orientierungshilfe zu Auslagerungen an Cloud-Anbieter | 47 |
| 7 | Diskussion über Weisungsrechte aufgegriffen | 47 |
| 8 | Wie weit kann das Prüfrecht gehen? | 48 |
| 9 | Grenzen der Auslagerung | 49 |
| 10 | Ausblick | 50 |

IV. Das Versicherungskollektiv in Zeiten von Big Data und Artificial Intelligence 52

Die Tarifierung und Preisfestlegung im Versicherungsgeschäft beruht auf einer umfangreichen Basis an Vergangenheitsdaten und Prognosewerten. Mit der zunehmenden Verfügbarkeit von Big Data (BD) und der schnellen, innovativen Entwicklung von Artificial Intelligence (AI) verändern sich auch die Möglichkeiten individueller Tarifierungen. Der vorliegende Beitrag untersucht die Auswirkungen auf den Risikoausgleich im Kollektiv. Ein Beitrag von Prof. Dr. Fred Wagner und Kristina Zentner, M.Sc.

| | | |
|----------|---|-----------|
| 1 | Einleitung | 53 |
| 2 | Definition Versicherung | 54 |
| 3 | Funktionsweise der Versicherung: Das versicherungstechnische Äquivalenzprinzip | 57 |
| 4 | Die digitale Revolution | 59 |
| 5 | Wirkungsweisen von Big Data und Artificial Intelligence in Kalkulation und Tarifierung | 63 |
| 6 | Auswirkungen auf das Versicherungskollektiv | 64 |
| 7 | Würdigung | 66 |
| 8 | Zusammenfassung | 67 |

Der Artikel skizziert die Positionierung der Sparkassen-Finanzgruppe zu wesentlichen Aspekten der digitalen Transformation. Er verdeutlicht die verschiedenen Dimensionen, in denen die Digitalisierung auf die Sparkassen einwirkt und zeigt auf, wie die Institute die damit verbundenen Herausforderungen und Chancen konkret gestalten.

Ein Beitrag von Dr. Joachim Schmalzl und Frank Weigand

| | | |
|----------|---|-----------|
| 1 | Bedeutung der Digitalisierung | 69 |
| 2 | Sparkassen und Digitalisierung | 71 |
| 3 | Die Digitale Agenda der Sparkassen-Finanzgruppe – Leitfaden für die Organisation | 73 |
| 4 | Vertrauen in der digitalen Welt – Cybersicherheit als Wettbewerbsfaktor | 82 |
| 5 | Neue Geschäftsmodelle für die Sparkassen-Finanzgruppe | 84 |
| 6 | Ausblick | 87 |



VI. Unterwegs in die digitale Versicherungswelt – Ein Bericht aus dem

Maschinenraum der Veränderung

88

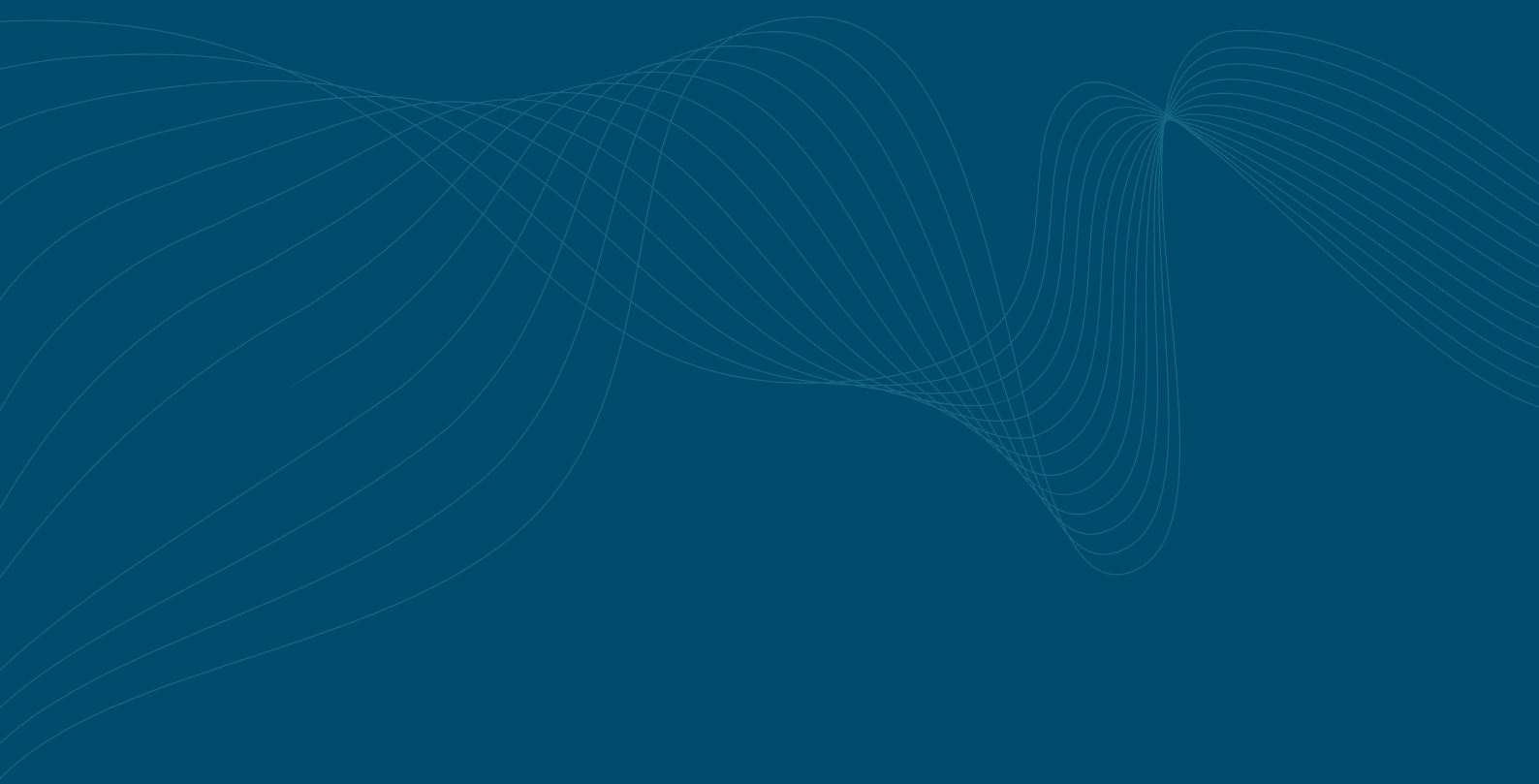
Das Geschäft von Versicherern wird sich grundlegend verändern. Der Vorsitzende der Geschäftsführung des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV), Dr. Jörg von Fürstenwerth, analysiert die sieben möglichen Megatrends und deren Veränderungspotenzial. Ein Beitrag von Dr. Jörg Freiherr Frank von Fürstenwerth

| | | |
|----------|--|------------|
| 1 | Einleitung | 89 |
| 2 | Der Kampf um den Kontakt zum Kunden | 91 |
| 3 | Neue Technologien: Künstliche Intelligenz, Cloud und Blockchain | 93 |
| 4 | Kreative Zerstörung: neue Geschäftsmodelle und Produkte | 95 |
| 5 | Die Prozess-Revolution | 100 |
| 6 | Neue Wettbewerber, mehr Anbietervielfalt | 103 |
| 7 | Wettstreit um Talente | 106 |
| 8 | Agile Aufsicht | 108 |
| 9 | Fazit | 109 |

Impressum

110

Vorwort



Die BaFin widmet eine weitere Ausgabe ihrer BaFinPerspektiven der Digitalisierung – und zwar aus gutem Grund. Die fortschreitende Digitalisierung verändert auch den Finanzmarkt. Der allerdings ist traditionell stark reguliert, denn er lebt mehr als andere Märkte davon, dass man auf seine Funktionsfähigkeit, Stabilität und Integrität vertrauen kann. Eine solide Basis für dieses Vertrauen zu schaffen, ist Aufgabe der BaFin. Sie hat sich daher im August 2018 eine Digitalisierungsstrategie gegeben, in der sie drei Grundfragen formuliert:

- Wie ist aufsichtlich und regulatorisch mit den Marktveränderungen umzugehen, die durch die Digitalisierung ausgelöst werden?
- Wie kann die BaFin sicherstellen, dass die innovativen Technologien und IT-Systeme sowie Daten, die bei den beaufsichtigten Unternehmen genutzt werden, sicher sind?
- Wie muss sich die BaFin angesichts der fortschreitenden Digitalisierung selbst weiterentwickeln – intern und an den Schnittstellen zum Markt?

Die BaFin muss ihre Digitalisierungsstrategie immer wieder überdenken, um am Ball zu bleiben. Dazu pflegt sie den Austausch mit Finanzwirtschaft, Wissenschaft, Politik und anderen Behörden – etwa in der Konsultation zu ihrem Bericht „Big Data trifft auf künstliche Intelligenz“.

In dieser Ausgabe bieten Ihnen Jörn Bartels und Dr. Thomas Deckers, beide BaFin, einen Überblick über die Antworten, und ich nehme eine erste Einordnung vor. Dr. Jörg Kukies, Staatssekretär im Bundesfinanzministerium, erläutert in einem Interview, wie die Bundesregierung das Thema künstliche Intelligenz gestalten will. Mit der Auslagerung von IT-Dienstleistungen durch Banken befassen sich mein Direktoriumskollege Raimund Röseler und Ira Steinbrecher, ebenfalls BaFin. Professor Dr. Fred Wagner, Mitglied unseres Verwaltungsrats, und Kristina Zentner, beide



Universität Leipzig, schreiben über das Versicherungskollektiv in Zeiten von Big Data und Artificial Intelligence. Dr. Jörg Freiherr Frank von Fürstenwerth, Gesamtverband der Deutschen Versicherungswirtschaft, und Dr. Joachim Schmalzl sowie Frank Weigand, Deutscher Sparkassen- und Giroverband, berichten, wie der Versicherungs- und der Sparkassensektor mit den Herausforderungen der Digitalisierung umgehen.

Ich wünsche Ihnen eine interessante Lektüre!

A handwritten signature in blue ink, which appears to read "F. Hufeld". The signature is written in a cursive style with a horizontal line above the first letter.

Felix Hufeld
Präsident der BaFin

I

Staat, Gesellschaft, Wirtschaft, Verwaltung und Wissenschaft müssen sich den Chancen, aber auch den Risiken der künstlichen Intelligenz stellen. Wichtig ist eine gemeinwohlorientierte Nutzung auf Basis der demokratischen Grundordnung.

Man muss sich den Chancen, aber auch Risiken der KI stellen

Interview mit

Dr. Jörg Kukies

Staatssekretär im Bundesministerium der Finanzen (BMF)



Herr Staatssekretär, die Bundesregierung hat in der Sitzung des Digitalkabinetts am 15. November 2018 die nationale KI-Strategie beschlossen. Worum geht es da?

Mit der Strategie setzt die Bundesregierung erstmalig einen Rahmen für eine ganzheitliche politische Gestaltung der weiteren Entwicklung und Anwendung künstlicher Intelligenz (KI) in Deutschland. Mit ihr sollen drei wesentliche Ziele verfolgt werden. Erstens: Deutschland und Europa sollen zu einem führenden Standort für die Entwicklung und Anwendung von KI-Technologien gemacht werden – auch um die künftige Wettbewerbsfähigkeit Deutschlands abzusichern. Zweitens: Es soll eine verantwortungsvolle und gemeinwohlorientierte Entwicklung und Nutzung von KI sichergestellt werden, und, drittens: KI soll im Rahmen eines breiten gesellschaftlichen Dialogs und einer aktiven politischen Gestaltung ethisch, rechtlich, kulturell und institutionell in die Gesellschaft eingebettet werden. Der Staat nimmt zur Erreichung dieser Ziele viel Geld in die Hand.

Investitionen in Höhe von insgesamt drei Milliarden Euro sind vorgesehen.

Die Strategie beinhaltet auch wesentliche Aspekte für die Finanzindustrie und berücksichtigt damit Empfehlungen des FinTechRats beim BMF¹. KI und Big Data ermöglichen Innovationen, die den Finanzmarkt stark verändern. Das alles erfordert technische und fachliche Kompetenzen. Darauf muss auch die Aufsicht entsprechend reagieren. Da ist die BaFin-Studie zu Big Data und künstlicher Intelligenz² ein wichtiger erster Schritt.

¹ Bundesministerium der Finanzen.

² BaFin, Big Data trifft auf künstliche Intelligenz – Herausforderungen und Implikationen für Aufsicht und Regulierung von Finanzdienstleistungen, www.bafin.de/dok/10985478. Die BaFin hat den Bericht unter Mitwirkung von PD – Berater der öffentlichen Hand GmbH, der Boston Consulting Group GmbH und Fraunhofer – Institut für Intelligente Analyse- und Informationssysteme erarbeitet.



© iStock/From2015

Wo sehen Sie die größten Chancen und mögliche Risiken beim Einsatz von Big Data und künstlicher Intelligenz auf dem Finanzmarkt?

Staat, Gesellschaft, Wirtschaft, Verwaltung und Wissenschaft sind aufgefordert, sich den Chancen, aber auch den Risiken der KI zu stellen. Die Bundesregierung hat mit der KI-Strategie eine Grundlage etabliert, um die Voraussetzungen zur Nutzung des Potenzials von KI zu schaffen. Die Entwicklung und der Einsatz von BDAI müssen dabei im Sinne einer menschenzentrierten, gemeinwohlorientierten Nutzung für Wirtschaft und Gesellschaft auf Basis der demokratischen Grundordnung erfolgen.

Das Zusammenspiel von künstlicher Intelligenz und Big Data führt zu autonomen Systemen, die die Digitalisierung derzeit in allen Wirtschaftszweigen rasch voranschreiten lassen. In der nächsten Zeit können diese Entwicklungen auch zu Veränderungen unseres Finanzsystems führen. Auf dem Kapitalmarkt kann man den Einsatz von BDAI bereits beobachten. Aber auch bei Banken und Versicherungen wird BDAI zunehmend als Chance erkannt.

BDAI-Anwendungen könnten auch bei Risikobewertungsmodellen von Instituten zum Einsatz kommen. Auch Versicherungen könnten BDAI zur Unterstützung des Schadensmanagements einsetzen.

Bei dem Einsatz von BDAI-Technologien ist es wichtig, dass die Finanzstabilität und -Integrität nicht verletzt

werden. Hinzu kommt, dass der Verbraucher mitgenommen werden muss. Das bedeutet, dass Verbraucher die Hoheit über ihre personenbezogenen Daten auch in einer BDAI-Welt nicht verlieren dürfen.

Halten Sie es für möglich, dass der vermehrte Einsatz von Big Data und künstlicher Intelligenz neuartige systemische Risiken hervorbringt?

Zum jetzigen Zeitpunkt lassen sich noch keine systemischen Risiken erkennen. Dafür ist der Einsatz von Big Data und künstlicher Intelligenz in der Finanzindustrie noch zu gering. Dies kann sich allerdings schnell ändern. Daher ist es wichtig, dass Aufseher mögliche Risiken für die Stabilität des Finanzsystems im Auge behalten, um diese gegebenenfalls schnell zu adressieren.

Die Anwendung von Big Data und künstlicher Intelligenz löst regelmäßig auch datenschutzrechtliche Fragen aus. Wie sollte aus Ihrer Sicht finanzaufsichtlich damit umgegangen werden?

Bei einer massenhaften und selbstlernenden Auswertung von Daten durch Unternehmen muss gewährleistet sein, dass Kunden noch Herr ihrer Daten bleiben. Mit der im letzten Jahr in Kraft getretenen DSGVO³ sind dafür europaweit wichtige Standards gesetzt worden, d. h. der Kunde muss einwilligen, dass seine Daten zu Preisfindungszwecken verarbeitet werden. Gleichwohl müssen

³ Datenschutz-Grundverordnung.

Kunden noch mehr dafür sensibilisiert werden, dass sie für schnelleren und besseren Service in aller Regel mit ihren Daten bezahlen. Aber auch auf Unternehmensseite muss ein verantwortungsvoller Umgang mit den Kundendaten sichergestellt sein.

Die Bundesregierung hat sich deswegen in ihrer KI-Strategie das Ziel gesetzt, einen Runden Tisch mit Datenschutzaufsichtsbehörden und Wirtschaftsverbänden einzuberufen, um gemeinsam Leitlinien für eine datenschutzkonforme Entwicklung und Anwendung von KI-Systemen zu erarbeiten und Best-Practice-Anwendungsbeispiele aufzubereiten.

Die Einhaltung von Datenschutzbestimmungen obliegt den zuständigen Länderbehörden und dem Bundesbeauftragten für den Datenschutz. Auch kommt bei Vorliegen der entsprechenden Voraussetzungen ein Einschreiten der BaFin im Rahmen der Missstandsaufsicht in Betracht. In besonders extremen Fällen müsste dann wohl auch die Eignung der Geschäftsleitung in Frage gestellt werden.

In der ersten Ausgabe der BaFinPerspektiven hat BaFin-Präsident Felix Hufeld das Problem der ungewollten Diskriminierung durch Big Data und künstliche Intelligenz beschrieben. Wie lässt sich dieses Problem lösen?

Algorithmen liegt erst einmal kein Weltbild zugrunde, sie ziehen ihre Schlüsse aus den Datensätzen. Je nachdem, wie diese Datensätze ausgewählt werden oder wofür die Auswertung genutzt werden soll, kann daraus allerdings eine Diskriminierung folgen. Der FinTechRat hat in seinen Handlungsempfehlungen schon Ende 2017 auf diese Problematik hingewiesen. Zu einem verantwortungsvollen und gemeinwohlorientierten Umgang mit KI gehört auch, dass Unternehmen, die KI einsetzen, dafür sorgen müssen, dass Diskriminierung verhindert wird – notfalls durch menschliche Kontrollmechanismen. Für die Finanzindustrie heißt dies, dass der Einsatz von

KI-Technologie die Geschäftsleitung nicht von ihrer Gesamtverantwortung für die ordnungsgemäße Geschäftsorganisation entbindet.

Big Data und künstliche Intelligenz machen es möglich, unterschiedliche Daten zu verknüpfen. Damit lässt sich möglicherweise auch die maximale Zahlungsbereitschaft von Kunden ausloten – und, bei entsprechender Marktmacht, ausnutzen. Wie stehen Sie dazu?

An das sogenannte Pricing knüpfen sich zahlreiche Fragen, die weit über das Aufsichtsrecht hinausgehen. Wie auch in anderen Bereichen ist die Grenze des Hinnehmbaren dann erreicht, wenn das Unternehmen seine Marktmacht zu Lasten des Verbrauchers ausnutzt. Soweit Pricing auf personenbezogenen Daten aufsetzt, greift auch hier der Schutz der DSGVO.

Mit der KI-Strategie setzt die Bundesregierung sich ambitionierte Ziele. Was erwarten Sie von der BaFin?

Die Bundesregierung will beim weiteren Einsatz von KI in der Verwaltung eine Vorreiterrolle einnehmen und damit zur Verbesserung von Effizienz, Qualität und Sicherheit von Verwaltungsdienstleistungen beitragen. Dazu kann auch die BaFin einen wichtigen Beitrag leisten. Mit ihrer BDAI-Studie hat sie den Grundstein dafür gelegt. Darauf gilt es jetzt aufzubauen. BDAI-Anwendungen können vor allem in den Aufsichtsbereichen einen Mehrwert darstellen, in denen die BaFin über ausreichende strukturierte Daten in ausreichender Qualität verfügt. Da fällt mir etwa das Meldewesen in der Wertpapieraufsicht ein. Die BaFin sollte ambitioniert prüfen, ob die Auswertung großer strukturierter Datenmengen in Zukunft nicht häufiger KI-gesteuert werden kann. Hier wäre dann auch eine Weiterentwicklung der Digitalisierungsstrategie der BaFin anzustreben, um langfristig die Finanzaufsicht weiter zu stärken.

Herr Staatssekretär, wir danken Ihnen für das Interview!

III

Zahlreiche Rückmeldungen hat die BaFin zu ihrem Bericht „Big Data trifft auf künstliche Intelligenz – Herausforderungen und Implikationen für Aufsicht und Regulierung von Finanzdienstleistungen“ erhalten. An der Konsultation haben sich Interessensverbände beteiligt, aber auch einzelne Institute, nationale wie internationale Behörden und Vertreter der Wissenschaft. Der Artikel gibt einen Überblick über die Antworten, und BaFin-Präsident Felix Hufeld nimmt im Interview eine erste Bewertung vor.

Big Data trifft auf künstliche Intelligenz

Beitrag zu den Ergebnissen der Konsultation des BaFin-Berichts und Interview mit Felix Hufeld

Autoren

Jörn Bartels

Referat Strategieentwicklung,
Bundesanstalt für Finanzdienstleistungsaufsicht
(BaFin)

Dr. Thomas Deckers

Referat Finanztechnologische Innovationen,
Bundesanstalt für Finanzdienstleistungsaufsicht
(BaFin)

1 Einleitung

Am 16. Juli 2018 hat die BaFin ihren Bericht „Big Data trifft auf künstliche Intelligenz – Herausforderungen und Implikationen für Aufsicht und Regulierung von Finanzdienstleistungen“¹ (kurz: BDAI-Bericht²) öffentlich zur Konsultation³ gestellt. Im Fokus der Konsultation standen insbesondere die in Kapitel „Perspektive der Aufsicht“⁴ aufgeworfenen strategischen Leitfragen zur Fortentwicklung von Aufsicht und Regulierung in Zeiten der vermehrten Verwendung von Big Data und Artificial Intelligence.

Insgesamt erreichten die BaFin 31 inhaltliche Rückmeldungen. An der Konsultation haben sich Interessensverbände, aber auch einzelne Institute beteiligt. Auch von nationalen wie internationalen Behörden und der Wissenschaft sind Antworten eingegangen. Durch die Bank wurde in den Beiträgen begrüßt, dass die BaFin mit dem Bericht eine sehr offene und breite Diskussion angestoßen habe. Es wurde auch darauf hingewiesen, dass es wichtig sei, etwaige BDAI-bedingte Anpassung von Aufsicht und Regulierung international abzustimmen. Zudem wurde betont, dass auch in Zeiten von BDAI deutsche Finanzdienstleister nicht mit Bigtechs verglichen werden sollten – etwa im Umgang mit Kundendaten.

In diesem Artikel werden die Rückmeldungen zum BDAI-Bericht anlog zu dessen Aufbau in drei übergeordneten Themen zusammengefasst: Finanzstabilität und Marktaufsicht, Unternehmensaufsicht sowie Kollektiver Verbraucherschutz. Zu jedem dieser Themen und zu jedem Unterthema wird zunächst in einer Box die Position aus dem BDAI-Bericht in komprimierter Form wiedergegeben.⁵ Daran anschließend werden die bei der

1 BaFin, Big Data trifft auf künstliche Intelligenz – Herausforderungen und Implikationen für Aufsicht und Regulierung von Finanzdienstleistungen, www.bafin.de/dok/10985478, abgerufen am 23.1.2019. Die BaFin hat den Bericht unter Mitwirkung von PD – Berater der öffentlichen Hand GmbH, der Boston Consulting Group GmbH und Fraunhofer – Institut für Intelligente Analyse- und Informationssysteme erarbeitet.

2 Das Kürzel „BDAI“ steht für „Big Data und Artificial Intelligence“.

3 BaFin, Konsultation des BDAI-Berichts, www.bafin.de/dok/11137698, abgerufen am 23.1.2019.

4 BaFin, a. a. O. (Fn. 1), Seite 166ff.

5 Die in diesem Artikel wiedergegebenen Positionen des BDAI-Berichts finden sich dort überwiegend in Kapitel „Perspektive der Aufsicht“.

Konsultation eingegangenen Rückmeldungen zusammenfassend und anonymisiert dargestellt.⁶

Aufgrund der Diversität der Konsultationsteilnehmer (Unternehmen, Verbände, Behörden, Wissenschaftler) ist es nicht möglich, repräsentative Mehrheiten bei den Antworten anzugeben, da man die Antworten dazu gewichten müsste (zum Beispiel ein einzelnes Unternehmen im Verhältnis zu einem Verband). Zur Vereinfachung wurde daher in diesem Artikel jede Antwort gleich gewichtet.

Dass nicht alle Details der Antworten in diesem Artikel behandelt werden, ist der Notwendigkeit einer verdichteten Darstellung geschuldet. Zu beachten ist auch, dass die BaFin die in diesem Artikel wiedergegebenen Aussagen noch nicht bewertet. Auch gibt dieser Artikel noch keine Antwort auf die Frage, welche der eingegangenen Anregungen in Aufsichtspraxis und Regulierung ihren Niederschlag finden sollten. Dies wird noch Zeit in Anspruch nehmen.

Eine erste Einordnung nimmt BaFin-Präsident Felix Hufeld im Interview zur Konsultation vor.⁷

⁶ Falls passend, wurden zu jedem Thema auch Hinweise berücksichtigt, die sich in Rückmeldungen zu anderen Themenblöcken wiederfanden.

⁷ Vgl. Seite 38f.



2 Finanzstabilität und Marktaufsicht

2.1 Konsultationsergebnisse zur Entstehung neuer Unternehmen und Geschäftsmodelle

In Kürze

Kernaussage aus dem BDAI-Bericht

BDAI-getriebene Innovationen rufen im Finanzsektor neue Anbieter auf den Plan. Die Disaggregation der Wertschöpfungskette kann dadurch weiter voranschreiten, insbesondere, wenn existierende Unternehmen mit neuen Spezialanbietern kooperieren. Das Phänomen BDAI könnte auch neuartige Geschäftsmodelle und Marktteilnehmer hervorbringen, die regulatorisch noch nicht adäquat erfasst werden. Solche Fälle müssen identifiziert und das Spektrum der zu beaufsichtigenden Anbieter und Unternehmen sollte entsprechend erweitert werden.⁸

2.1.1 Allgemeine Marktbeobachtung

Branchenübergreifend sei das Entstehen neuer Wertschöpfungsketten zu beobachten, heißt es in vielen Rückmeldungen. Dabei würden insbesondere solche Unternehmen auf den Markt drängen, die durch den Einsatz von BDAI die Datenverarbeitung auf ein neues Level heben könnten. Einzelne Konsultationsteilnehmer gehen davon aus, dass langfristig im Markt nur bestehen könne, wer die digitale Kundenschnittstelle besetze. Insgesamt sei der Trend zu beobachten, dass Anbieter von Suchmaschinen, sozialen Netzwerken oder Online-(Vergleichs-)Plattformen durch intelligente

Nutzung von Daten in Bereiche vordrängen, die bisher spezialisierten und häufig auch regulierten Anbietern vorbehalten seien. Dazu zählten auch die Daten, die aufgrund der Zweiten Zahlungsdiensterichtlinie (Payment Services Directive 2 – PSD 2) gewonnen werden können.

2.1.2 Level-Playing Field – Finanzmarktregulierung

In der Mehrzahl der eingegangenen Konsultationsantworten wird die bestehende technologie neutrale und prinzipienbasierte Finanzmarktregulierung als grundsätzlich ausreichend angesehen – auch mit Blick auf Fragen der Finanzstabilität. Man sieht zudem das Risiko, dass bei zu schnellen regulatorischen Reaktionen auf neue Technologien die Technologie neutralität auf der Strecke bleiben könne und ein eher regelbasierter Ansatz verfolgt werde. Angeregt wird ein Abbau von regulatorischen Barrieren. Als Beispiel werden bestehende Papieranforderungen angeführt.

In den Antworten wird aber auch betont, dass die Anwendung bestehender Regulierung ausschließlich auf Institute und Versicherungsunternehmen zu Wettbewerbsverzerrungen führen könne. Insbesondere wird eine Diskrepanz zwischen der aufsichtlichen und regulatorischen Erfassung klassischer Geschäftsmodelle und der neuer Geschäftsmodelle gesehen, die auf der Analyse von Finanz- und alternativen Daten zu eigenen Zwecken oder für Dritte beruhen.⁹ Es wird vermutet, dass neue Marktteilnehmer künftig bewusst versuchen, Regulatorik zu vermeiden, um Innovationen vorantreiben zu können. In diesem Zusammenhang wird unter anderem eine Prüfung angeregt, inwieweit neue Vertriebskanäle, zum Beispiel zielgerichtete Marketingmaßnahmen von Plattformanbietern, für eine Beraterhaftung heranzuziehen seien. Vereinzelt wird auch kritisiert, dass neue Player wie Fintechs nicht an der Finanzierung von Aufsichtsbehörden beteiligt seien und dies zu Wettbewerbsverzerrung führe.

Obwohl der erwartete zusätzliche Wettbewerb mit Fintechs und Bigtechs Profite etablierter Anbieter des

⁸ Diese und die weiteren in diesem Artikel wiedergegebenen Positionen des BDAI-Berichts finden sich dort überwiegend in Kapitel „Perspektive der Aufsicht“.

⁹ Vgl. hierzu auch Abschnitt 2.2.

Finanzmarktes kurzfristig schmälern könnte, werden die bisherigen Instrumente zur Beurteilung der Solvenzsituation beaufsichtigter Finanzdienstleister als ausreichend eingestuft. Es wird aber in einzelnen Rückmeldungen darauf hingewiesen, dass sich ein verstärkter Margendruck insbesondere dann entfalten könne, wenn Bigtechs mit kostenlosen und/oder quersubventionierten Finanzdienstleistungen auf den Finanzmarkt drängten.

2.1.3 Level-Playing Field – Wettbewerbspolitik und -aufsicht

Die Digitalisierung verschärfe, so ist in mehreren Rückmeldungen zu lesen, insgesamt die Gefahr von „The-Winner-takes-it-all“-Marktstrukturen. Solche könnten durch monopolistische Strukturen beim Datenzugang entstehen. Für Versicherungsunternehmen sei daher zum Beispiel der Zugang zu Fahrzeugdaten für das Angebot von Telematik-Tarifen wichtig. Eine effektive Wettbewerbspolitik bzw. -aufsicht sei gerade in Zeiten von BDAI mehr denn je eine Grundvoraussetzung für einen dauerhaft leistungsfähigen Finanzmarkt.

Offene Märkte könnten, insbesondere was den Datenzugang angeht, außerdem über eine daraus folgende stärkere Differenzierung der Marktteilnehmer zu einer Minderung systemischer Risiken führen. Außerdem sei ein ausreichender Wettbewerb auch für eine effektive Preisfindung wichtig.¹⁰ In diesem Zusammenhang wird vereinzelt darauf hingewiesen, dass die PSD 2 ein positives Beispiel für die Ermöglichung eines freien Datenzugangs darstelle. Es wird die Idee in den Raum gestellt, ähnlich wie in der PSD 2 Schnittstellen zu den Daten von Bigtechs zu ermöglichen.

Insgesamt wird ein verstärkter Austausch zwischen Wettbewerbsbehörden und der Finanzaufsicht befürwortet.

2.1.4 Level-Playing Field erhalten – Einordnung von Daten als Rechtsgut

In einer Stellungnahme wird gefragt, wie Daten jenseits des Datenschutzrechts als individuelles Rechtsgut/Schutzgut einzuordnen seien. Auf diese rechtspolitisch hochkomplexe Materie müsse eine überzeugende Antwort gefunden werden, um insbesondere primär datenbasierte Geschäftsmodelle adäquat adressieren zu können. Als zielführend sieht man den Ansatz, Parallelen zum Immaterialgüterrecht herzustellen.

2.2 Systemrelevanz und Vernetzung in Zeiten von BDAI

In Kürze

Kernaussage aus dem BDAI-Bericht

Anbieter mit datengetriebenen Geschäftsmodellen könnten aufgrund ihrer Skalierbarkeit und Reichweite schnell an Systemrelevanz gewinnen. Jedoch kann Systemrelevanz auch entstehen, wenn zentrale Daten- oder Plattformanbieter einer Vielzahl von Marktteilnehmern identische oder sehr ähnliche Grundlagen für Prozesse oder Algorithmen zur Verfügung stellen. Systemrelevanz könnte zudem aus der Interaktion verschiedener Marktteilnehmer als Struktur erwachsen. Es stellt sich daher die Frage, ob und wie der bank- und versicherungsfachlich geprägte Begriff der Systemrelevanz weiterentwickelt werden muss, um auch neuen Geschäftsmodellen und Marktstrukturen gerecht zu werden.

¹⁰ Vgl. auch Abschnitt 4.1.

2.2.1 Systemrelevanz neu definieren und adressieren: Ein geteiltes Meinungsbild

Was eine eventuelle Erweiterung des Begriffs der Systemrelevanz angeht, bietet sich in den Antworten ein geteiltes Bild: Auf der einen Seite wird darauf hingewiesen, dass es zum jetzigen Zeitpunkt, in dem sich viele Technologien noch im Entwicklungsstadium befänden, verfrüht, wenn nicht gar innovationshemmend wäre, neue Definitionen und Kriterien festzulegen. Insbesondere sei nicht klar, ob BDAI das Systemrisiko tatsächlich erhöhe oder ob durch die wachsende Zahl von Marktteilnehmern die Abhängigkeit von Banken und Versicherern nicht sogar abnehmen werde. In jedem Fall müsse empirisch klar belegbar sein, dass bestimmte Risiken in einer Weise auftreten könnten, dass sie die Existenz von Instituten tatsächlich gefährdeten.

Auf der anderen Seite halten viele Konsultationsteilnehmer eine Neudefinition der Systemrelevanz mit Blick auf BDAI für wichtig. Vereinzelt wird sie sogar als möglicher Grund für ein Basel-V-Rahmenwerk gesehen. Konzeptionell seien Kategorien wie Vernetzung und Komplexität zwar bereits unter der aktuellen Definition von Systemrelevanz abgedeckt. Da der Grad an Vernetzung und Komplexität aber im Rahmen der Digitalisierung zunähme, sollte ihnen eine stärkere Gewichtung zukommen. Eine internationale Diskussion im Basler Ausschuss für Bankenaufsicht über die Definition und Messung von Vernetzung wird als sinnvoll erachtet. Weiterhin wird gefordert, dass bei der Messung des Systemrisikos nicht nur auf klassische Finanzdienstleister, sondern auch auf aufsichtlich bisher nicht erfasste Fintechs und Bigtechs abzustellen sei. Insbesondere seien auch solche Geschäftsmodelle zu berücksichtigen, die auf einer Monetarisierung von Daten beruhen.



2.2.2 Adressierung bislang unregulierter Anbieter aufgrund ihrer Vernetzung mit dem Finanzmarkt

Bereits einzelne, bislang in vielen Fällen nicht regulierte Unternehmen könnten essenziell für das Funktionieren der Gesamtbranche sein, ist zu lesen. Beispielhaft genannt werden Cloud-Anbieter, Telekommunikationsanbieter, Automobilhersteller (Stichwort „Telematik-Tarife“; siehe Seite 18), Algorithmen- bzw. Code-Anbieter, aber auch Anbieter von Daten oder Bewertungen wie Scorings und Ratings. Entsprechende Unternehmen könnten aufgrund ihres Wissens monopolartige Strukturen gegenüber Verbrauchern und anderen Marktteilnehmern aufbauen. Zudem wird das Problem gesehen, dass es zu prozyklischen Wirkungen kommen könne, wenn viele Finanzdienstleister zum Beispiel auf die Daten und Auswertungen eines zentralen Anbieters zurückgriffen.¹¹

Eine mögliche Systemrelevanz von bisher nicht beaufsichtigten Unternehmen könne etwa durch eine Erweiterung des Begriffs der kritischen Infrastrukturen adressiert werden. Damit könnten für bisher unbeaufsichtigte Daten-, Plattform- und Algorithmenanbieter dieselben technischen Mindestanforderungen geltend gemacht werden wie für regulierte Banken. Außerdem wird gefordert, den Begriff der Systemrelevanz um funktionale und prozessuale Faktoren zu erweitern. So könnten sich Schlüsselunternehmen selbst einfacher identifizieren und Finanzdienstleister könnten dies berücksichtigen.

¹¹ Hier ist einschränkend zu erwähnen, dass in einer weiteren Antwort argumentiert wird, dass zumindest Kreditrisikomodelle geschlossene Systeme einzelner Institute seien, die keine institutsübergreifenden Kaskadeneffekte verursachen könnten.

2.2.3 Ideen zur Anpassung des Outsourcing-Regimes bei fragmentierten Wertschöpfungsketten

Bei immer stärker fragmentierten Wertschöpfungsketten sei darüber hinaus das heutige Outsourcing-Regime, das als Anlaufstelle nur das Finanzinstitut kenne, ggf. nicht mehr ausreichend. Zudem sei zu berücksichtigen, dass Infrastruktur- und Datenanbieter in vielen Fällen auch direkte Wettbewerber auf dem Finanzmarkt seien. Und insbesondere bei Produkten, die über einen fragmentierten Wertschöpfungsprozess erstellt würden, böte sich eine Art digitale Signatur an. Bei dieser Signatur müsse jedes Unternehmen genannt sein, das am Wertschöpfungsprozess beteiligt sei. Insgesamt sei darüber nachzudenken, den aufsichtlichen Fokus vom einzelnen Unternehmen auf die Aufrechterhaltung von ganzen Wertschöpfungsketten zu verschieben. Zur Aufrechterhaltung von Wertschöpfungsketten könnte es eine Maßnahme sein, per Smart Contract für jede Leistung innerhalb einer Wertschöpfungskette eine Back-Up-Partei zu vereinbaren, die die Leistung beim Ausfall eines Unternehmens übernehme.

Eigenkapitalpuffer seien als mitigierende Maßnahme dagegen wenig geeignet, um Schocks, die außerhalb des Finanzsektors entstünden, wie zum Beispiel der Ausfall eines IT-Anbieters, zu absorbieren. Geeigneter seien Maßnahmen, die darauf abzielten, die Eintrittswahrscheinlichkeit zu minimieren. Genannt werden in diesem Zusammenhang technische Mindeststandards oder gezielte Szenarioanalysen sowie die im folgenden Absatz behandelten technischen Begrenzungen von Fehlentwicklungen. Darüber hinaus könnten Volumenbeschränkungen eine sinnvolle Maßnahme darstellen.

2.3 Technische Begrenzung von Fehlentwicklungen

In Kürze

Kernaussage aus dem BDAI-Bericht

Auch außerhalb von Handelsplätzen besteht in stark vernetzten Systemen die Gefahr, dass sich Störungen rasch und unkontrolliert ausbreiten. Es stellt sich die Frage, ob bisher von Handelsplätzen bekannte technische Maßnahmen im Zeitalter von BDAI auch außerhalb von Handelsplätzen erforderlich und sinnvoll anwendbar wären. Beispielsweise könnte über Abkopplungsmechanismen für Datenströme nachgedacht werden, da Datenzulieferungen durch BDAI stark an Bedeutung gewinnen.

2.3.1 Technische Sicherungsmaßnahmen zwar potenziell erforderlich, aber nur bei Gefahr immenser Schäden

Technische Maßnahmen zur Begrenzung von Kaskadeneffekten werden als potenziell erforderlich angesehen. Die Adressierung von Kaskadeneffekten gestaltete sich aber dann schwierig, wenn Teile des Marktes innerhalb der relevanten Kaskade nicht aufsichtlich bzw. regulatorisch erfasst seien. Die Gefahr von Herden- bzw. Kaskadeneffekten wird eher im Bankensektor und am Kapitalmarkt gesehen als im Versicherungssektor, wo zentrale Prozesse – wie Risiko- und Leistungsprüfungen – nur durch den Kunden selbst angestoßen würden. Grundsätzlich sei einmal zu prüfen, wo neue Entwicklungen wie etwa Echtzeitzahlungen in der Realwirtschaft tatsächlich gebraucht würden und das Risiko von Fehlentwicklungen rechtfertigten. Generell begrenze nämlich möglicherweise eine Entschleunigung mit vorgegebenen Mindestzeitfenstern und Rückabwickelbarkeit Fehlentwicklungen.

Technische Sicherungsmaßnahmen seien zum Beispiel dann überlegenswert, wenn bei der Nutzung von BDAI der Grad der algorithmischen Differenzierung zu gering sei. Auch könnten Schnittstellen von Cybernetzwerken ausfindig gemacht werden, um die Gefahr immenser Schäden zu reduzieren. In diesem Zusammenhang könne über den Aufbau redundanter Notfallsysteme nachgedacht werden. Eine Diversifizierung von Datenanbietern wird als weitere (nichttechnische) Maßnahme genannt. Nur in massiven Gefahrensituationen erscheine ein Eingriff in Datenströme gerechtfertigt. Keinesfalls sollten aber zum Beispiel Instrumente wie Volatilitätsunterbrechungen, trotz ggf. genauerer Kalibrierung, von selbstlernenden Algorithmen ausgelöst werden, da in diesem Fall der Zeitpunkt der Unterbrechung für die Marktteilnehmer nicht mehr vorhersagbar wäre.

2.4 Technologie auf Seiten der Aufsicht: Transparenz und Kontrolle über neue Strukturzusammenhänge behalten

In Kürze

Kernaussage aus dem BDAI-Bericht

Eine stärkere Vernetzung könnte das Marktgeschehen komplexer machen, indem beispielsweise ehemals interne Prozesse eines einzigen Akteurs über mehrere – auch bislang unregulierte – Marktteilnehmer verteilt werden. Aufsichtlich und regulatorisch gilt es daher, die sich ändernden Strukturen des dynamischen Marktes und die daraus resultierenden Risiken im Blick zu behalten, zu bewerten und zu adressieren.

2.4.1 Verantwortung beim Menschen, nicht beim Computer – auch bei der Aufsicht

In den Konsultationsantworten wird sehr klar die Erwartungshaltung geäußert, dass auch bei der Aufsicht die letztendliche Verantwortung beim Menschen zu verbleiben habe und nicht auf den Computer übertragen werden könne. Der vermehrte Einsatz von Technologie auf Seiten der Aufsicht wird dennoch in den meisten Antworten als zwingend erforderlich eingeschätzt. Zur Erkennung von Systemrelevanz könnte sich die Aufsicht auch verstärkt externer Daten bedienen und diese mittels Methoden wie Netzwerkanalysen berücksichtigen. Interessante externe Daten seien zum Beispiel Konsumausgaben und Sparverhalten von Haushalten, aber auch Open-Source Daten, welche wiederum auch für die Betrugserkennung von Interesse sein könnten.

2.4.2 Echtzeitdatenzugriff – API-Einsatz bei der Aufsicht

Analysen, die auf einmalig bzw. monatlich oder quartalsweise erhobenen Daten beruhen, verlören aufgrund der steigenden Marktdynamik zunehmend an Relevanz. Die Aufsicht solle sich daher darum bemühen, über Application Programming Interfaces (APIs) einen Zugriff in Echtzeit auf spezifische Unternehmensdaten zu erhalten und damit fortlaufende Analysen – zum Beispiel Geldflussanalysen – durchführen, auch zur Früherkennung neuer Risiken und Geschäftsmodelle. Die Einrichtung von APIs wird auch für den reibungslosen Datenaustausch zwischen verschiedenen (Aufsichts-)Behörden als sinnvoll erachtet. Über das Zusammenspiel von APIs und BDAI lasse sich seitens der Aufsicht auch ein effektiveres Outsourcing-Controlling einrichten. Zudem könnten so auch die Beziehungen der beteiligten Unternehmen in aufsichtlichen Analysen automatisch Berücksichtigung finden.



3 Unternehmensaufsicht

3.1 BDAI-Governance

In Kürze

Kernaussage aus dem BDAI-Bericht

BDAI wird weitere Möglichkeiten der Automatisierung marktüblicher Prozesse schaffen. Zur Ausgestaltung (teil-)automatisierter Prozesse ist es wichtig, die Einbettung in eine wirksame, angemessene und ordnungsgemäße Geschäftsorganisation zu gewährleisten. Die Verantwortung auch für automatisierte Prozesse verbleibt bei der Geschäftsleitung des beaufsichtigten Unternehmens. Um dies sicherzustellen, ist eine angemessene Dokumentation erforderlich. Unter Umständen ist es zudem erforderlich, etablierte Governance-Konzepte wie das Vier-Augen-Prinzip weiterzuentwickeln und auf automatisierte Prozesse zu übertragen.

3.1.1 Bestehende Konzepte weitgehend ausreichend – Auslegungen aber erwünscht

In einer Mehrzahl der Antworten wird der bestehende Aufsichtsrahmen auch bei vermehrtem BDAI-Einsatz grundsätzlich als ausreichend eingestuft. BDAI-Anwendungen bedeuteten nicht zwangsläufig ein höheres Risiko und könnten analog zu bestehenden Prozessänderungen betrachtet werden. Somit könnten sie auch in die bestehende Geschäftsorganisation und die entsprechende Regulierung eingebettet werden.¹² Die

¹² Beispielsweise seien laut Ziffer 164 der Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo) Analysen zu operationellen Risiken vor der Einführung oder wesentlichen Änderung von Produkten, Prozessen und Systemen durchzuführen und die Ergebnisse dieser Analyse in die Entscheidungsfindung einzubeziehen. Im Bankensektor seien die Mindestanforderungen an das Risikomanagement (MaRisk) hinsichtlich Organisation und Dokumentation (AT 5 und AT 6) zu berücksichtigen.

aktuellen Anforderungen ermöglichten zudem, dass die Aufsicht die Prozesse risikoorientiert und strichprobenartig prüfe. Auch bezüglich der Geschäftsleitung seien strenge Anforderungen bereits gesetzlich verankert. Darüber hinaus wird betont, dass der Einsatz von BDAI regelmäßig unter die Outsourcing-Bestimmungen falle, die Verantwortung und Haftung für künstliche Intelligenz jedoch nicht ausgelagert werden könne. Sollte es zunehmend Auslagerungen an Regtechs geben, entstehe das Risiko, dass Risikokultur und Wissen innerhalb der beaufsichtigten Unternehmen geschwächt würden.

Es bestehe aber auch zum Teil Klärungsbedarf, wie bestehende Regeln in Bezug auf BDAI anzuwenden seien. Es böte sich an, dass die Aufsicht Vorschriften in Auslegungen spezifiziere. Ungeachtet der Komplexität der zugrundeliegenden Prozesse dürften aber in keinem Fall aufsichtliche Anforderungen aufgeweicht werden.

3.1.2 Ideen zur Erweiterung bestehender Governance-Konzepte

Konträr zu der oben genannten Meinung gibt es aber auch einige Rückmeldungen, die es explizit für geboten halten, die bestehende Regulierung und Aufsichtspraxis mittelfristig zu überarbeiten. So könne zum Beispiel bei Algorithmen über das Erfordernis der Implementierung und gegenseitigen Kontrolle verschiedener Teilsysteme nachgedacht werden. Dies würde bei lernenden Systemen im Regelfall die Nutzung unterschiedlicher Lernverfahren und möglichst auch unterschiedlicher Trainingsdaten bedeuten. Als hilfreich könne sich auch ein „Outlier-Mining“ erweisen, um potenziell fehlerhafte Entscheidungen aufzuspüren. Zudem stelle sich die Frage, ob die Validierung von BDAI-Algorithmen von der derzeitigen Regulierung (hinreichend) abgedeckt sei.

An einzelnen Stellen seien zudem aufgrund des vermehrten BDAI-Einsatzes Veränderungen der bestehenden Geschäftsorganisationen zu beobachten. So sei es wichtig, die Fehlerkultur im Unternehmen an das fortwährende Lernen und die damit verbundene laufende Veränderung von Algorithmen und Modellen anzupassen. Zudem entwickle sich die bislang rein administrative Aufgabe des Data Quality Managements (DQM) zu einer analytischen



und konzeptionellen Aufgabe weiter und habe künftig eine Schlüsselrolle im Unternehmen. Vorgeschlagen wird außerdem die Schaffung von Algorithmus-Beauftragten, analog zu Datenschutz-Beauftragten, und die Einrichtung einer Datenethikkommission in den Unternehmen. Insgesamt müsse man dabei aber aufpassen, dass es nicht zu einer unklaren Zuordnung von Verantwortung komme.

3.2 Nachvollziehbarkeit und Erklärbarkeit von Algorithmen und Entscheidungen

In Kürze

Kernaussage aus dem BDAI-Bericht

Es liegt in der Verantwortung des beaufsichtigten Unternehmens, die Erklärbarkeit und Nachvollziehbarkeit von BDAI-basierten Entscheidungen zu gewährleisten. Auch bei sehr komplexen Modellen können zumindest Einblicke in die Funktionsweise des Modells und die Gründe für Entscheidungen erzielt werden und Modelle müssen nicht zwangsläufig als Blackbox verstanden werden. Die Aufsicht wird es daher nicht akzeptieren, wenn man ihr ein Modell als unerklärbare Blackbox präsentiert. Aufgrund der Komplexität der Anwendungen ist darüber hinaus zu überlegen, ob künftig neben den Dokumentationsanforderungen auch Prozessergebnisse untersucht werden sollten.

3.2.1 Zwei Ebenen der Erklärbarkeit: Das Modell und die Einzelfallentscheidung

Einleitend wird in den Antworten darauf hingewiesen, dass es bei Erklärbarkeit und Nachvollziehbarkeit zwei Ebenen gebe, an denen man ansetzen könne: Zum einen das generelle Modell, das zur Entscheidungsfindung herangezogen werde, und zum anderen die (Einzelfall-) Entscheidung selbst. Die Erklärbarkeit eines auf maschinellem Lernen basierenden Modells hänge notwendigerweise von der Komplexität der eingesetzten Verfahren und der verwendeten Daten ab. Aufsichtliche Eingriffe oder Regulierungsanpassungen sollten aber nicht ausschließlich in der Komplexität eines Modells bzw. in der Verwendung von BDAI begründet sein. Sie sollten vielmehr immer den jeweiligen Einsatzbereich und die damit erwartete Risikosituation berücksichtigen.

Nachvollziehbarkeit sei insbesondere im Kundenkontakt und damit im Einzelfall wichtig, da Kunden häufig forderten, eine Entscheidung zu begründen. Nur die Begründung versetze Betroffene in die Lage, unzutreffende Daten und darauf basierende Entscheidungen zu korrigieren. Im Sinne eines „Audit-Trails“ müssten einzelne Entscheidungsschritte stets nachvollziehbar sein. Zumindest sollte eine Nachvollziehbarkeit von Entscheidungen immer soweit durchgesetzt werden, dass sie für forensische Zwecke möglich wäre.

3.2.2 Wie sich Erklärbarkeit und Nachvollziehbarkeit herstellen lassen

Erklärbarkeit und Kontrollierbarkeit von Algorithmen und Modellen sowie nachvollziehbare Prozesse lägen im Eigeninteresse der Unternehmen, heißt es in einigen Antworten. Zu nennen seien hier auch die zahlreichen

existierenden (Selbst-)regulierungsmaßnahmen, wie die Product Oversight and Governance Requirements (POG) und das interne Kontrollsystem (IKS). In der Praxis verankere man im Modellfindungs- und Kalibrierungsprozess immer wieder Backtestings und in der folgenden Anwendung Warn- und Alarmsignale, die letztendlich in eine manuelle bzw. menschliche Intervention mündeten. Dass die Möglichkeit (manueller) Korrektur und generell von Revidierbarkeit bestehen müsse, wird in vielen Antworten hervorgehoben. Zudem müssten auch Abschalt-Prozesse für auslaufende oder fehlerhafte BDAI-Anwendungen vorhanden sein.

Zur Herstellung von Nachvollziehbarkeit böte sich zunächst an, bestehende Modelle und solche, die auf BDAI beruhten, parallel auszuführen. Auf diese Weise lasse sich nachvollziehen, welche Einflussfaktoren es gebe. Weiterhin seien komplexe Modelle auch durch einfache Modelle approximierbar. So ließen sich zum Beispiel Approximationen bilden und so Einzelfallentscheidungen lokal durch ein einfaches Modell erklären. Wichtig sei in diesem Zusammenhang die Definition einer Mindestgüte für die Approximation.

3.2.3 Gegenmeinung: Erklärbarkeit und Nachvollziehbarkeit als unangemessene Einschränkung

In einer Reihe von Antworten wird allerdings gegensätzlich argumentiert: Es sei schwer bzw. aufgrund der Natur der BDAI-Verfahren unmöglich, den Entscheidungsweg eines Algorithmus detailliert nachzuvollziehen. Insbesondere bei sehr komplexen Verfahren wie Deep-Learning sei Erklärbarkeit nur sehr schwer darstellbar. Entsprechend bedeute die Forderung nach der Erklärbarkeit von Algorithmen eine unangemessene Einschränkung. Aufgrund der Komplexität der Modelle solle die Validierung der Ergebnisse im aufsichtlichen Fokus stehen. Allerdings sei fraglich, inwiefern etwa der Einsatz von Test-Szenarien zur Überprüfung institutseigener Algorithmen sinnvoll sei. Denn beim Einsatz von Test-Szenarien sei zu beachten, dass das Einbeziehen von vordefinierten Szenarien das Risiko der Überanpassung (Overfitting) auf eben diese Szenarien berge.

Insbesondere sei die Anforderung, jeden Musterkunden – also die Einzelfallentscheidung – nachzurechnen,



realitätsfern. Entgegen der im BDAI-Bericht geäußerten Feststellung sei Erklärbarkeit schon allein aufgrund der komplexen Daten eingeschränkt. Wichtig und technisch möglich sei hingegen, einen Nachweis über die Prognosegüte und die Stabilität der verwendeten Modelle zu erbringen. Ein aufsichtlicher Abnahmeprozesses für BDAI-Anwendungen wird in diesem Zusammenhang abgelehnt, da dadurch die Innovation der Unternehmen stark beeinträchtigt würde. Außerdem wird hierin eine unangemessene Benachteiligung von Finanzunternehmen im Vergleich zu anderen (unregulierten) Unternehmen wie zum Beispiel den Bigtechs gesehen.

3.2.4 Ideen zur aufsichtlichen Überprüfung von BDAI-Modellen

Außerdem stelle sich die Frage, wie sich BDAI-Modelle aufsichtlich überprüfen ließen. Sofern BDAI im signifikanten Umfang in geschäftskritischen Prozessbereichen Anwendungen finde, seien hierzu möglicherweise erweiterte Anforderungen erforderlich, zum Beispiel mit Blick

auf Code-Review-Verfahren, Simulations- und Penetrations-Tests und die Begutachtung von Musterprofilen. Die Anforderungen zur Dokumentation und Erklärbarkeit und Nachvollziehbarkeit für BDAI-Anwendungen sollten zum Beispiel über Best-Practice Leitlinien konkretisiert werden. Eine effektive Aufsicht müsse außerdem über die Betrachtung von Dokumentation und Einzelfällen hinausgehen.

Aufseher müssten komplexe Verfahren wie Deep Learning verstehen und die Anwendungen der Unternehmen im Rahmen eines risikosensitiven Ansatzes selbst testen. Erweitert werden sollten Anforderungen aber nur in Abhängigkeit davon, wie kritisch die jeweiligen Prozesse seien, auch im Hinblick auf den Verbraucher. Für die Finanzaufsicht ergebe sich aus der Verwendung algorithmenbasierter Entscheidungssysteme zudem die Chance, aber auch die Verpflichtung, algorithmenbasierte Entscheidungsprozesse und damit weite Teile der Geschäftspraxis auf Konsistenz mit den aufsichtsrechtlichen Vorgaben und der zivilen Rechtsprechung zu prüfen.



3.3 Genehmigungspflichtige interne Modelle

In Kürze

Kernaussage aus dem BDAI-Bericht

Eine Verwendung von BDAI bei genehmigungspflichtigen Modellen stünde immer unter dem Vorbehalt einer entsprechenden aufsichtlichen Genehmigung im Einzelfall. Über den Einzelfall hinaus ist zu prüfen, ob bestehende gesetzliche (Mindest-) Anforderungen an die verwendeten Daten und die Modelltransparenz mit Blick auf BDAI hinreichend sind oder erweitert werden sollten. Bei dynamischen BDAI-Modellen stellt sich zudem die Frage, bei welchen generellen Anpassungen eine Modelländerung im aufsichtlichen Sinne vorliegen kann, die eine Bank oder ein Versicherer, etwa entsprechend der Modelländerungsrichtlinie bei Versicherungsunternehmen, bei der Aufsicht anzeigen und unter Umständen genehmigen lassen müsste.

3.3.1 BDAI findet noch keine Anwendung bei genehmigungspflichtigen Modellen

Zunächst einmal ergibt sich aus den Antworten, dass BDAI-Ansätze bei genehmigungspflichtigen internen Modellen bisher noch keine Anwendung finden. Da die Stabilität interner Modelle sehr wichtig sei, seien BDAI-Modelle zudem eher bei Support-Anwendungen zu erwarten. Es wird im Übrigen bezweifelt, dass BDAI-Modelle, bei denen aufgrund veränderter Daten automatisiert anzeigepflichtige Modellanpassungen vorgenommen werden, genehmigungsfähig wären.

3.3.2 Gegensätzliche Meinungen zu bestehender Regulierung

Zur Anwendbarkeit von BDAI in genehmigungspflichtigen Modellen gibt es gegenläufige Auffassungen, insbesondere mit Blick auf den Modelländerungsprozess.

Dem einen Lager zufolge sind BDAI-Anwendungen grundsätzlich für den Einsatz in aufsichtlich abzunehmenden Modellen geeignet. Ihr Einsatz berge eine erhebliche Chance, Risiken besser zu modellieren. Es sei nicht zu erwarten, dass man die Definition einer Modellanpassung ändern bzw. zusätzliche Regulierung schaffen müsse. Dies insbesondere deswegen, weil die Anzeigepflicht einer Modellanpassung eher vom Einfluss auf die risikogewichteten Aktiva als von der eingesetzten (BDAI)-Technologie abhängig sei. Auch eine Erweiterung bestehender (Mindest-)Anforderungen an die Erklärbarkeit der Modelle und Daten wird in diesen Antworten für nicht erforderlich gehalten. Eine erneute Einschätzung könne jedoch erforderlich sein, falls der Einfluss von BDAI-Methoden auf die in diesem Zusammenhang relevanten Kenngrößen wesentlich werde. Unter Umständen könne es dann erforderlich sein, die Technischen Regulierungsstandards zu erweitern.

Das andere Lager schlägt vor, die Abnahmepaxis anzupassen. So solle Unternehmen die Möglichkeit gegeben werden, eingesetzte Modelle flexibler anzupassen, ohne zuvor langwierige Abnahmeprozesse für Modelländerungen durchlaufen zu müssen. Die Aufsicht solle schnellere „Validierungsfeedbackloops“ ermöglichen. Wünschenswert sei darüber hinaus, Modelländerungen durch die Neuschätzung von Parametern nicht als Modelländerung zu betrachten, wenn ein modellinhärentes Verfahren die Notwendigkeit der Neuschätzung bestimme. Vereinzelt wird auch die Meinung vertreten, dass eine Veränderung der Parameter bereits heute zumindest im Versicherungssektor keine Modelländerung darstelle. Darüber hinaus wird vorgeschlagen, für die Überwachung von BDAI-Modellen ein automatisiertes regelmäßiges, stark standardisiertes Monitoring auf BDAI-Basis zu etablieren und über entsprechende Berichte die Kommunikation mit der Aufsicht zu erleichtern. Außerdem könne der vermehrte Einsatz von Validierungsinstrumenten wie Stabilitätsanalyse, Sensitivitätsanalyse und Backtesting hilfreich sein.

Schlussendlich wird jedoch auch darauf hingewiesen, dass bei flächendeckendem BDAI-Einsatz zu prüfen wäre, ob dieser durch eine deutliche Verminderung der risikogewichteten Aktiva zu einer (unerwünschten) Kapitalerleichterung oder zu einer Umgehung aufsichtlicher Anforderungen führe.

3.4 Abwehr von Finanzkriminalität und Verhaltensverstößen

In Kürze

Kernaussage aus dem BDAI-Bericht

BDAI kann die Anomalie- und Mustererkennung verbessern, wodurch Compliance-Prozesse wie zum Beispiel die Geldwäscheerkennung und die Betrugsprävention effektiver und effizienter werden könnten. Wird die Geldwäscheerkennung durch den Einsatz von BDAI-Technologien sehr viel effektiver, könnten Täter auf Unternehmen ausweichen, die auf diesem Gebiet nicht so weit entwickelt sind. Es gilt zu beobachten, ob solche Ausweichreaktionen tatsächlich stattfinden. Die Ergebnisse der Algorithmen müssen in einer Weise nachvollziehbar sein, dass die Aufsichtsbehörden sie überprüfen und zuständige Stellen wie Strafverfolgungsbehörden sie verwenden können. Möglicherweise sind hierfür aufsichtlich und regulatorisch Mindeststandards zu entwickeln.

3.4.1 Regulatorik gibt bereits Standards vor – Erweiterungen könnten aber angebracht sein

Die überwiegende Mehrheit der Antwortenden hält es für unangemessen und unverhältnismäßig, den Einsatz von BDAI zur Betrugsabwehr und Geldwäscheverhinderung zu erzwingen. In vielen Antworten wird allerdings befürwortet, allgemeine bzw. Mindeststandards einzuführen, auch über BDAI-Anwendungen hinaus. Solche Standards könnten die Prozesse zur Identifikation von Finanzkriminalität und Verhaltensverstößen effektiver machen bzw. die Identifikation und Vermeidung von Geldwäsche verbessern. Da sich BDAI schnell und individuell weiterentwickle, sollten diese Standards prinzipienbasiert ausgestaltet werden. Zum Beispiel solle die Dokumentation insbesondere bei Sanktions- und Eingriffsmaßnahmen im Einzelnen nachvollziehbar sein, damit sie einer menschlichen Überprüfung standhalten kann. Auch eine aufsichtliche Prüfung der Geldwäscheeffektivität wird vorgeschlagen, zum Beispiel mithilfe von normierten, mindestens jährlich anzupassenden Prüfdatensätzen – analog zum Penetration Testing.

In anderen Antworten wird dagegen darauf verwiesen, dass die bisherige prinzipienbasierte Regulatorik bereits Standards setze und insbesondere mit der Umsetzung der fünften EU-Geldwäsche-Richtlinie ein ausreichender Rahmen vorhanden sei. Zudem seien spezielle BDAI-Standards nicht zwingend erforderlich, da sich diese direkt aus wissenschaftlichen Standards der Machine-Learning-Community ableiten ließen.

3.4.2 Feedbackloops zur Modell-Kalibrierung unerlässlich

Wie effektiv BDAI-Modelle in der Geldwäscheprävention eingesetzt werden könnten, hänge stark davon ab,

ob sie mit verlässlichen Daten kalibriert würden. Für die Modell-Kalibrierung und –Verbesserung sei es daher wichtig, Rückmeldungen zu den Modellvorhersagen im Einzelfall zu erhalten. Aktuelle Feedbacks der Zentralstelle für Finanztransaktionsuntersuchungen (FIU) oder der Strafverfolgungsbehörden seien folglich wünschenswert. Auch sei in diesem Zusammenhang über die Kompatibilität der Datensysteme nachzudenken, was den Datenstandard und die technische Umsetzung ggf. über eine API angehe. Denn nur so sei ein Datenaustausch zwischen Unternehmen und Ermittlungsbehörden ohne Konvertierung möglich.

3.4.3 Vorteile von Pooling-Lösungen, insbesondere für weniger versierte Unternehmen

Darüber hinaus wird ein institutsübergreifendes Datenpooling vorgeschlagen; etwa um kleinere Institute, also solche mit geringerer Datenbasis, zu unterstützen. Dabei könnte auch über ein Pooling von Know-how bzw. der Verwendung gemeinsamer Metriken nachgedacht werden. In der Teilnahme an einem vernetzten Informationspool, in dem geldwäscherelevante Informationen gespeichert und abgerufen werden könnten, sieht man den Vorteil, dass – auch ohne BDAI – ein ganzheitlicher Blick auf das Kundenrisiko ermöglicht würde. Entsprechend wird vereinzelt der Wunsch geäußert, dass Aufsicht bzw. Gesetzgeber solche Know-Your-Customer-Plattformen (KYC-Plattformen) wohlwollend begleiten.

Es wird vorgeschlagen, dass die Aufsicht Unternehmen, deren Geldwäschereerkennung mit Blick auf BDAI weniger weit entwickelt sei, unterstützen solle. Die Unternehmen müssten aber auch bereit sein, mehr in neue Technologien zu investieren. Die Aufsicht solle den Unternehmen klarmachen, was sie von ihnen erwarte.

3.4.4 Mehrdimensionale Herangehensweise bei der Geldwäschebekämpfung

Einige Teilnehmer sprechen sich bei der Geldwäschebekämpfung für eine mehrdimensionale Herangehensweise aus, also zum Beispiel für eine Kombination von BDAI-Analysen mit Peergroup-Vergleichen, öffentlichen

Daten und KYC-Scores. Darüber hinaus wird vereinzelt der Wunsch geäußert, die bei der Geldwäschereerkennung gewonnen Erkenntnisse auch für andere Zwecke – etwa für das Kreditrisikoring – nutzbar zu machen. Demgegenüber wird darauf verwiesen, dass bei der Anwendung von BDAI insbesondere das Willkürverbot beachtet werden müsse. Durch BDAI dürften Merkmale nicht willkürlich verknüpft werden, weil sonst Personen fälschlicherweise strafrechtlich verfolgt würden. Auch eine direkte oder indirekte Diskriminierung, wie sie Art. 3 Absatz 3 Grundgesetz (GG) beschrieben sind, sollte unterbleiben.

3.5 Umgang mit Informationssicherheitsrisiken

In Kürze

Kernaussage aus dem BDAI-Bericht

Das Management von Informationssicherheitsrisiken steht durch die BDAI-bedingt zunehmende Komplexität dieser Risiken vor neuen Herausforderungen. Die von BDAI unterstützte Disaggregation von Wertschöpfungsketten und das wachsende Datenvolumen vergrößern zudem die Angriffsfläche für externe Zugriffe und verringern zugleich die Möglichkeiten eines einzelnen Anbieters, die genutzten und verteilten Daten zu kontrollieren. Zusätzlich kann es bei bestimmten BDAI-Algorithmen auch zu Angriffen durch Datenmanipulation kommen. Beispiele sind Adversarial und Poison Attacks. BDAI ließe sich aber auch in der Abwehr von Informationssicherheitsrisiken nutzen, zum Beispiel bei der Analyse und Entdeckung von Gefahren. Auch bestimmte Verschlüsselungsverfahren, welche die Anwendung von BDAI-Methoden direkt auf verschlüsselten Daten erlauben, könnten genutzt werden, um die Resilienz gegenüber solchen Risiken zu stärken.

3.5.1 Prinzipienbasierte Regulierung für Informationssicherheitsrisiken auch auf BDAI anwendbar

Angemerkt wird, dass Informationssicherheitsrisiken beim Einsatz von BDAI-Techniken zunehmen könnten – und zwar insbesondere durch die zunehmende Vernetzung und die daraus resultierenden vermehrten Angriffspunkte. Dem Grunde nach handele es sich hierbei aber um ähnliche Sicherheitsaspekte, wie sie auch bei anderen Softwarelösungen zu beachten seien. Es wird daher kein (weitgehender) regulatorischer Anpassungsbedarf gesehen. Zahlreiche Regularien, wie die Bankaufsichtlichen Anforderungen an die IT (BAIT) und die Versicherungsaufsichtlichen Anforderungen an die IT (VAIT), aber auch die MaRisk oder bestimmte ISO-Standards fänden bereits heute beim Einsatz von BDAI Berücksichtigung. Vereinzelt wird dennoch gefordert, einzelne Regularien wie etwa die BAIT hinsichtlich BDAI weiter zu konkretisieren. Sollten künftig weitere Ergänzungen erforderlich sein, so sollten diese möglichst prinzipienbasiert ausgestaltet sein und nur bei Bedarf mit regelbasierten Vorgaben ergänzt werden. Insgesamt sei es aber riskant, Standards festzuschreiben, da sich die Informationstechnologie sehr schnell weiterentwickle.

Die Möglichkeit, BDAI zur Bewältigung bzw. Erkennung von Cyberattacken zu nutzen, wird in den Antworten insgesamt bestätigt.

3.5.2 Verschlüsselung ist kein Allheilmittel

Um die Auswirkungen von Schäden bei Sicherheitsvorfällen zu minimieren, sollten Daten prinzipiell möglichst umfassend anonymisiert oder pseudonymisiert werden. Allerdings wird deutlich hervorgehoben, dass die Vorstellung, BDAI-bedingte Datenschutzrisiken könnten durch kryptographische Verfahren abschließend gelöst werden, unrealistisch sei. Verschlüsselungsverfahren könnten auch Schein-Sicherheit suggerieren. Aus technischer Sicht sei nicht zu erwarten, dass maschinelles Lernen auf verschlüsselten Daten außerhalb spezieller Anwendungen erfolgreich nutzbar sein werde. In einer einzelnen Rückmeldung wird vorgeschlagen, den Datenhandel im Sinne einer Monetarisierung von Daten generell zu untersagen, um so neben dem Datenschutz auch die Informationssicherheitsrisiken zu minimieren.



4 Kollektiver Verbraucherschutz

4.1 Ausnutzung der Zahlungsbereitschaft und -fähigkeit der einzelnen Kunden

In Kürze

Kernaussage aus dem BDAI-Bericht

BDAI könnte Anbietern eine kostengünstige (Massen-) Individualisierung von Produkten und Dienstleistungen und der entsprechenden Preise erleichtern. So wären auch kundenindividuell höhere Preise ohne höhere Kosten für die Unternehmen denkbar. Die Individualisierung könnte Preisvergleiche tendenziell erschweren. Zudem könnte sie ermöglichen, bei der Preissetzung die (situative) Zahlungsbereitschaft und -fähigkeit des Kunden auszunutzen, falls diese dem Anbieter bekannt ist. Gerade die BDAI-getriebene Verknüpfung von finanzwirtschaftlichen Transaktions- und Verhaltensdaten mit anderen Daten-(quellen) kann die Einschätzung der Zahlungsbereitschaft erleichtern. Auch außerhalb des regulierten Finanzsektors könnten diese Daten somit theoretisch eine Abschöpfung der Konsumentenrente¹³ begünstigen. Eine BDAI-bedingte Entstehung von wenigen zentralen Kundenschnittstellen („The-Winner-takes-it-all“-Marktstrukturen) könnte diese Entwicklungen durch verbesserten Datenzugriff sowie Auswertungs-Synergien zusätzlich fördern. Verbraucher sind daher stärker dafür zu sensibilisieren, wie ihre (Finanz-) Daten genutzt werden können und welche Bedeutung sie haben.

¹³ Als Konsumentenrente versteht man die Differenz zwischen dem Preis, den ein Verbraucher für ein Produkt oder eine Dienstleistung maximal zu zahlen bereit ist, und dem Preis, den er tatsächlich am Markt zahlen muss.

4.1.1 Abgrenzung von risikoadäquater Preisdifferenzierung und Ausnutzung der individuellen Zahlungsbereitschaft

Abzugrenzen von einer Preissetzung in Abhängigkeit der individuellen Zahlungsbereitschaft seien im Finanzsektor die generell erforderlichen Preisdifferenzierungen aufgrund der individuell entstehenden Risikokosten. Diese Art der Preisdifferenzierung, so ist in den Antworten zu lesen, müsse auch künftig zur risikoadäquaten Bepreisung möglich sein. Es wird auch darauf hingewiesen, dass zum Beispiel der situative Versicherungsschutz regelmäßig auf einen (Mehr-)Jahresbeitrag hochgerechnet werde und teurer sei als langfristiger Versicherungsschutz, da er häufig auf einen Zeitraum mit erhöhten Risiken ausgerichtet werde.

4.1.2 Wettbewerb und langfristige Geschäftsbeziehungen sprechen gegen eine Abschöpfung der Konsumentenrente am Finanzmarkt

Die Möglichkeit, durch den Einsatz von BDAI die Konsumentenrente besser abschöpfen zu können, wird in der Mehrzahl der Antworten verneint. Als Gegenargument wird insbesondere ein intensiver (Preis-)Wettbewerb um den Kunden angeführt. Bei der Vermeidung einer einseitigen Preisgestaltung käme damit vor allem einer effektiven Wettbewerbspolitik bzw. -aufsicht eine Schlüsselrolle zu: Grundvoraussetzung für die Abschöpfung der Konsumentenrente sei ein Marktversagen – also etwa die Bildung von Mono- und Oligopolen bzw. Preisabsprachen und wettbewerbsbeschränkende Absprachen.

Für den Bankensektor fänden darüber hinaus Regelungen wie die Preisangabenverordnung Anwendung. Vermeintlich willkürliche bzw. rein personenabhängige Preisgestaltungen in der Breite des Kundengeschäfts seien daher schwer vorstellbar. Zudem seien für Finanzdienstleister Fairness gegenüber den Kunden und deren Vertrauen von existenzieller Bedeutung für die Kundenbeziehung. Eine faire Preisgestaltung liege daher im eigenen Interesse und sei häufig bereits im Code of

Conduct der Unternehmen angelegt. In anderen Antworten hingegen wird die Position vertreten, dass Verbraucher eine eventuelle Ausnutzung ihrer Zahlungsbereitschaft und -fähigkeit selbst verantworteten, wenn sie ihre Daten freigäben. Der These einer breiten Nutzung der Finanz- und Verhaltensdaten außerhalb des Kerngeschäfts wird zudem entgegengehalten, dass eine solche derzeit nicht zu beobachten sei.

4.1.3 BDAI könnte Transparenz für Produktalternativen erhöhen

Gegen die Abschöpfung der Konsumentenrente spreche auch die verbesserte Möglichkeit, als Kunde über BDAI einen Überblick über verfügbarer Produktalternativen und Preise zu erlangen. Eine von BDAI befeuerte hohe Marktdynamik könne sogar sinkende Preise zur Folge haben. Auch könnten insbesondere Kunden mit geringer Zahlungsbereitschaft durch BDAI-Anwendungen neue Konsummöglichkeiten eröffnet werden.

4.1.4 Verstärkte Marktkonzentration könnte künftig neue Gefahren entstehen lassen

Dagegen wird in einigen Antworten darauf hingewiesen, dass eine teilweise Abschöpfung der Konsumentenrente bereits heute möglich sei, da es nur wenige Online-Plattformen gebe. Wenn Methoden der datenbasierten Preisdifferenzierung breitere Anwendung fänden, könne dies die Informationsasymmetrie zwischen Verbrauchern und Unternehmen verstärken – zu Ungunsten der Verbraucher. Sollten hierbei neue Gefahren entstehen, wäre über die Initiierung von aufsichtlichen oder regulatorischen Maßnahmen nachzudenken. Zudem sollten einheitliche Anforderungen an die Pflicht zur Angabe von Daten gestellt werden, die zur Preisbestimmung herangezogen würden. Ebenso sollten sachgerechte Regelungen für die Nutzung von Daten getroffen werden, die im Internet of Things anfallen.



4.1.5 Verstärkte Verbraucheraufklärung ist nötig

In einigen Antworten wird explizit betont, dass es wichtig und notwendig sei, Verbraucher aufzuklären und auszubilden. Verbraucher müssten nämlich in der Lage sein, aufgeklärtere Entscheidungen zu treffen, was ihre persönlichen Daten und Finanzprodukte angehe. Eine wichtige Rolle spielten dabei unter anderem Verbraucherschutzorganisationen, welche die Kunden über Veränderungen im Marktangebot und mögliche Fallstricke in der Produktauswahl aufklären sollten. Außerdem sei es förderlich, die Datenhoheit der Kunden zu stärken.

4.2 Differenzierung und mögliche Diskriminierung

In Kürze

Kernaussage aus dem BDAI-Bericht

Durch den Einsatz von BDAI kann sich die Gefahr von Diskriminierung erhöhen: Algorithmen könnten Merkmale nutzen, die aus rechtlichen Gründen nicht zur Differenzierung verwendet werden dürfen. Und selbst wenn unzulässige Merkmale nicht genutzt werden, ist eine Approximation möglich, da sehr viele andere Daten zur Verfügung stehen, die Rückschlüsse zulassen. Es besteht zudem das Risiko, dass die Differenzierung auf Basis falscher Annahmen bzw. der daraus resultierenden Schlussfolgerungen der Algorithmen erfolgt, dass also Verbraucher de facto – wenn auch unbeabsichtigt – diskriminiert werden. Bei der Programmierung der Algorithmen und bei der Kontrolle der Ergebnisse müssen Anbieter entsprechend verstärkt darauf achten, dass einzelne Verbraucher nicht diskriminiert werden. Es stellt sich die Frage, welche Kontroll- und Transparenzmechanismen ihnen dabei helfen könnten.

4.2.1 Gefahr indirekter Diskriminierung nimmt zu – Nachweis von Diskriminierungsfreiheit erforderlich

Die Gefahr indirekter Diskriminierung (wie einleitend beschrieben) könne bei der Verwendung von BDAI zunehmen, heißt es in einigen Antworten. Anbieter sollten daher einen Nachweis über die diskriminierungsfreie Funktion ihrer Systeme und die Relevanz der verwendeten Variablen führen. Es wird befürwortet, Algorithmen einer regelmäßigen Prüfung zu unterziehen – unternehmensintern und durch Dritte. In einer Antwort wird sogar ein staatliches Kontrollsystem für alle BDAI-Algorithmen auch außerhalb der Finanzbranche gefordert. Zudem müsse man einer möglichen Diskriminierung bereits bei der Modellentwicklung begegnen, zum Beispiel durch Verwendung von Methoden wie Bias-Correction. Insgesamt sei die Durchsetzung von Diskriminierungsverboten im Kontext von BDAI aber eine technisch anspruchsvolle Aufgabe, für die es noch keine insgesamt befriedigende Lösung gebe. Derzeit sei eine nachträgliche, stichprobenhafte Kontrolle von Einzelfallentscheidungen den einzig gangbaren Weg.

4.2.2 Im Versicherungssektor sind viele Antidiskriminierungsregeln etabliert

Im Versicherungssektor seien bereits – neben allgemeinen Vorgaben wie dem Allgemeinen Gleichbehandlungsgesetz und dem Gendiagnostikgesetz – eine Reihe sektorspezifischer Vorschriften zu beachten. Genannt wird hier insbesondere der Gleichbehandlungsgrundsatz für Lebensversicherungen (§ 138 Absatz 2 Versicherungsaufsichtsgesetz (VAG)) und Versicherungsvertragsgesetz (VvAG) (§ 177 Absatz 1 VAG). Außerdem verfüge die Aufsicht in der Missstandsaufsicht über umfangreiche Instrumente, die als ausreichend angesehen werden. Darüberhinausgehende Mikroregulierung oder Mikrosteuerung von Produktgestaltung und Bepreisungsmodellen wirkten innovationshemmend. Im Übrigen sei unzulässige Diskriminierung im Versicherungssektor leichter zu vermeiden als in anderen Branchen, da, bis auf das Merkmal Geschlecht, jedes Merkmal nur ein differenzierender Faktor sei, solange dieser risikorelevant sei.



4.2.3 Definition von Diskriminierung bzw. Diskriminierungsfreiheit

Diskriminierungsfreiheit bezogen auf ein Merkmal mit nur zwei Ausprägungen (zum Beispiel Raucher/Nicht-raucher) liege dann vor, wenn beide Gruppen die gleiche Erfolgswahrscheinlichkeit für den Abschluss eines Vertrages (zu gleichen Konditionen) hätten. Anders ausgedrückt müssten also zwei Verbraucher mit den gleichen risikorelevanten Eigenschaften den gleichen Preis zahlen. Insgesamt sei es für nicht erhobene Merkmale unmöglich zu garantieren, dass das Ergebnis einer Modellentscheidung unabhängig von diesem Merkmal sei. Wenn das Merkmal allerdings bekannt sei, könne die Modellentscheidung weitestgehend zur Vermeidung von Diskriminierung bereinigt werden. Um eine unzulässige Diskriminierung auszuschließen, ist nach Meinung einiger Konsultationsteilnehmer ein Datensatz erforderlich, der genau das auszuschließende Merkmal enthält.

4.2.4 Weitergehender gesellschaftlicher Diskurs erscheint notwendig

Um gewollte Differenzierung und nicht zu akzeptierende Diskriminierung voneinander abzugrenzen, brauche man künftig einen gesellschaftlichen Diskurs. Auf diese Weise könne man die Akzeptanz der neuen Technologien fördern. Dabei sei aber zu berücksichtigen, dass die durch BDAI ermöglichte weitere Differenzierung Phänomenen wie Moral Hazard und adverser Selektion entgegenwirken könne. Würden diese Möglichkeiten nicht genutzt, könne es zu unfairen Verteilungen bzw. Bedingungen kommen, wenn es sich um risikorelevante Informationen handele. Mit Blick auf Differenzierung wird darauf verwiesen, dass sehr stark segmentierende Tarife in der Vergangenheit wenig erfolgreich gewesen seien. Einige sahen den Grundgedanken des Versicherungsschutzes durch verfeinerte Segmentierung gefährdet.

4.3 Zugang zu Finanzprodukten

In Kürze

Kernaussage aus dem BDAI-Bericht

Gerade eine Verknüpfung von vielfältigen Daten(-quellen) könnte die Risikobeurteilung der Finanzbranche verbessern. Kunden könnten daher künftig damit konfrontiert werden, in größerem Umfang (neue) Daten(-quellen) freizugeben– etwa Social Media Accounts. Es ist also denkbar, dass künftige Datenanforderungen deutlich über die bisher üblichen hinausgehen und der Preis einer Finanzdienstleistung von der Bereitstellung dieser Daten abhängt. Zudem könnten BDAI-Selektionsmechanismen generell einzelnen Verbrauchern den Zugang zu bestimmten Finanzdienstleistungen unverhältnismäßig erschweren. Das kann besonders prekär werden, wenn der Verbraucher durch eine geringere Produktauswahl benachteiligt wird, aber nicht nachvollziehen kann, dass seine personenbezogenen Daten der Grund sind. Es stellt sich daher die Frage, wie der Zugang zu (erschwinglichen) Finanzleistungen erhalten werden kann, wenn Kunden umfangreiche (neue) Datenquellen nicht freigeben können oder wollen.

In diesem Themenblock lag der Schwerpunkt der Konsultationsteilnehmer auf Versicherungsprodukten. Viele Argumente lassen sich aber generell auf Finanzdienstleistungen ausweiten.

4.3.1 Daten sind zur Risikobeurteilung essenziell

In einem Großteil der Antworten wird darauf hingewiesen, dass die Daten-Bereitstellung zur Risikoprüfung im Finanzsektor (zum Beispiel Kreditwürdigkeitsprüfung) unerlässlich sei. So sei das Grundprinzip einer privaten Versicherung, dass sich Prämien am versicherten Risiko orientierten. Denn die private Versicherung basiere – anders als die Sozialversicherung – darauf, dass sich das Versichertenkollektiv lediglich das Zufallsrisiko aufteile. Vom individuellen Risiko hänge daher ab, ob und zu welchen Konditionen ein Kunde (privaten) Versicherungsschutz – bzw., allgemein gesprochen, eine Finanzdienstleistung – erhalten könne.¹⁴ Es wird betont, dass Kunden, die weniger risikorelevante Daten bzw. Informationen offenlegten, über ein anderes Risikoprofil verfügten. Dementsprechend müssten sich die Konditionen von Tarifen in Abhängigkeit der Verfügbarkeit relevanter Daten unterscheiden.

4.3.2 Festlegung risikorelevanter Daten entscheidend

Es wird vorgeschlagen, dass der Gesetzgeber, die Aufsicht oder die Branche (über Selbstverpflichtungen) verbindlich definieren sollte, welche Daten zur sachgerechten Differenzierung tatsächlich erforderlich seien. Staatliche Stellen könnten dann auch sicherstellen, dass Verbrauchern, die in eine Datenverarbeitung über das erforderliche Maß hinaus nicht einwilligen, nicht der Zugang zu Finanzdienstleistungen verwehrt werde. Es sei jedoch unklar, in welche Risikoklasse solche datensparsamen Verbraucher einzuordnen wären, ob es also im Sinne einer Diskriminierungsfreiheit ausreichend sei, wenn diese Kunden nicht gänzlich von einer entsprechenden Dienstleistung ausgeschlossen würden, aber dennoch Dienstleistungen zu ggf. schlechteren Konditionen erhielten. Zu berücksichtigen sei auch, dass die Möglichkeit, durch die Freigabe zusätzlicher Daten den

¹⁴ Kunden mit gleichem Risiko erhielten gleiche Konditionen, Kunden mit unterschiedlichem Risiko unterschiedliche Konditionen. Dies werde im Gleichbehandlungsgrundsatz in § 138 Absatz 2, § 146 Absatz 2, §§ 147 und 161 VAG vorgeschrieben.

Preis für ein Finanzprodukt zu senken, unter Umständen das Recht auf informationelle Selbstbestimmung untergrabe.

4.3.3 Wettbewerb regelt den Zugang zu Finanzprodukten auch für datensparsame Kunden

Der Wettbewerb regle den Zugang zu Finanzprodukten auch für datensparsame Kunden, ist zu lesen. Es sei zunehmend zu beobachten, dass Anbieter einen datensparsamen und bequemen Vertragsabschluss als Leistungsmerkmal herausstellten. In welchem Umfang und in welcher Form Kunden bei Abschluss eines Vertrages Daten bereitstellen müssten, sei somit bereits heute ein Wettbewerbsfaktor. Andererseits wird auch darauf hingewiesen, dass generell ein Spannungsverhältnis zwischen den Vorgaben zur Datensparsamkeit und den Anforderungen der BDAI-Systeme an eine hinreichend große Datenbasis bestehe. Es sei keine Lösung, Unternehmen zu verpflichten, Produkte anzubieten, die nicht mehr dem Marktstandard entsprächen und auf veralteten Technologien beruhten. Diese Produkte wären für Kunden nicht von Interesse, gesetzliche Eingriffe entsprechend obsolet.

4.3.4 Gegenmeinung: Vorschlag zur Ausweitung von Basisprodukten

Um den Ausschluss von Kunden zu verhindern, die sich datensparsam bzw. nichtdigital verhalten, werden auf der anderen Seite gesetzliche Regelungen gefordert, die Anbieter verpflichten, auch analoge Verträge anzubieten. Eindeutig zu definieren, wann ein Vertrag analog bzw. konventionell sei, erscheine jedoch sehr komplex. Der Gesetzgeber könne – analog zur Einführung eines Anspruchs auf Einrichtung eines Basiskontos – eine Basisversorgung garantieren, etwa für die Kranken- und Pflegeversicherung, Privathaftpflichtversicherung, Berufsunfähigkeitsversicherung und Kfz-Haftpflichtversicherung. Dies insbesondere vor dem Hintergrund, dass die zunehmende Differenzierung dazu führen könne, dass bestimmte Kundengruppen nicht mehr oder nur noch zu sehr hohen Preisen versicherbar seien. Dies wäre insbesondere für Kunden problematisch, die das Risiko nicht selbst beeinflussen könnten. Auch könne die

Aufsicht ein Zertifikat für datensparsame Finanzdienstleistungen aufsetzen, welches, sofern als Gütesiegel akzeptiert, die Risiken eines Ausschlusses von datensparsamen Kunden minimieren könne. Demgegenüber wird aber auch davor gewarnt, dass eine spezielle gesetzliche Verpflichtung zu datensparsamen bzw. konventionellen Finanzprodukten suggerieren könne, dass bei anderen (Finanz)produkten das Prinzip der Datensparsamkeit nicht gelte.

4.4 Souveränität der Verbraucher

In Kürze

Kernaussage aus dem BDAI-Bericht

Das Potential von BDAI lässt sich für Finanzdienstleistungen nur nutzen, wenn es gelingt, das Vertrauen der Verbraucher in die wunschgemäße und gesetzeskonforme Nutzung ihrer Daten zu gewinnen und zu erhalten. Die Anbieter sollten dazu insbesondere sicherstellen, dass Verbraucher souveräne Entscheidungen treffen können, indem sie sie angemessen über die potenzielle Reichweite und die Konsequenzen der Nutzung ihrer Daten aufklären und ihnen verlässliche Kontrollmöglichkeiten und wirkliche Wahlfreiheit ermöglichen. Es wird also nicht genügen, Verbrauchern hochkomplizierte Nutzungsbedingungen zur Verfügung zu stellen, welche meist ungelesen akzeptiert werden. Vor allem auch technische (Datenschutz-) Möglichkeiten (z.B. Privacy-preserving-Data-Mining) bzw. ein Privacy-by-design-Konzept, könnten dazu beitragen, das Verbrauchervertrauen in BDAI-Innovationen zu stärken.

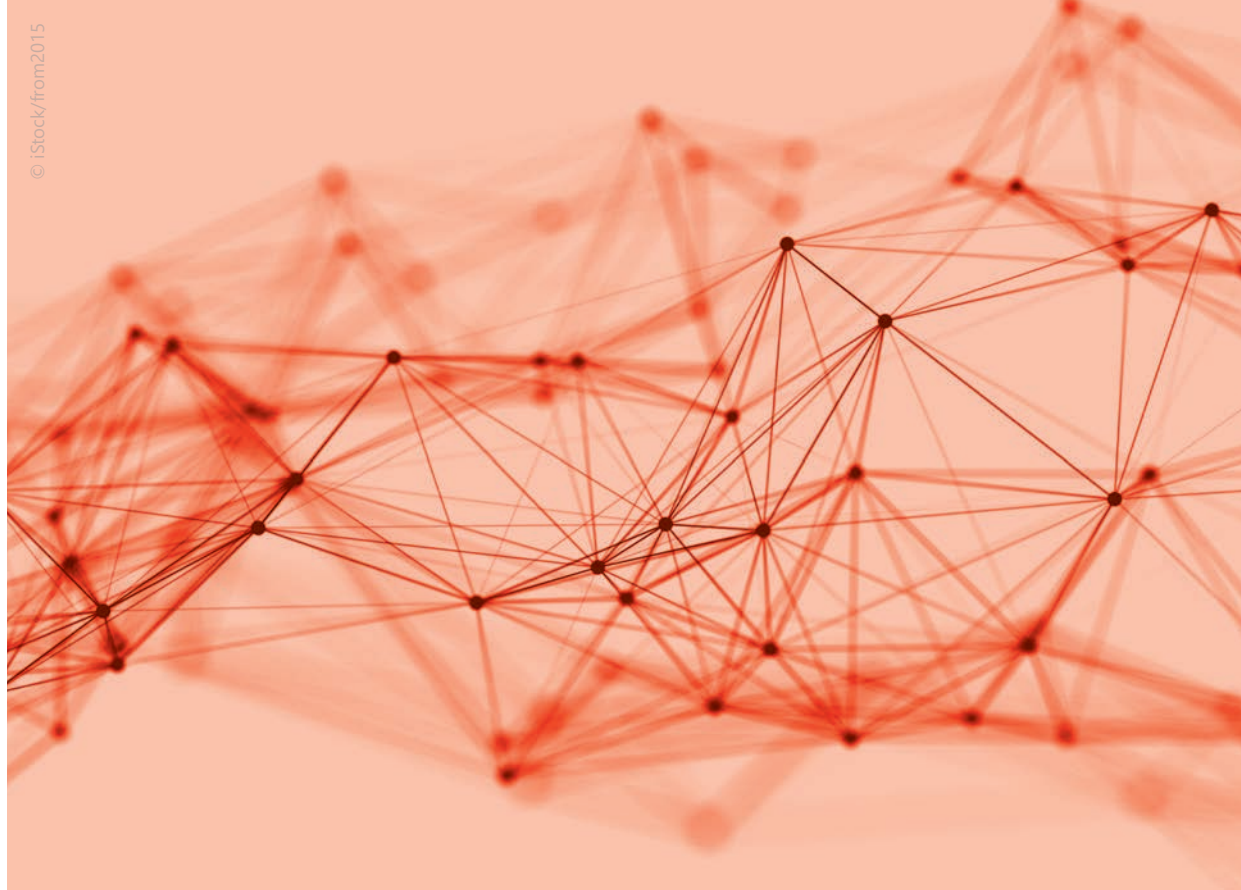
4.4.1 Datensouveränität wird als entscheidendes Thema angesehen

In der Mehrzahl der Antworten wird klarherausgestellt, dass die Datensouveränität der Verbraucher ein sehr relevantes Thema sei – nicht nur mit Blick auf den Finanzmarkt, sondern auch branchenübergreifend. Es sei sicherzustellen, dass Verbraucher über den Zweck der Datenverwendung in verständlicher Weise informiert würden und eine bewusste und sensibilisierte Entscheidung über ihre Datenweitergabe treffen könnten. Wirkliche Wahlfreiheit sei hierfür eine essenzielle Voraussetzung. Problematisch bzw. kontraproduktiv seien hingegen zum Beispiel sozialer und finanzieller Druck, Lock-in- und Netzwerkeffekte. Bei eventuellen regulatorischen Maßnahmen seien diese Faktoren und allgemein eine eingeschränkte Informationsaufnahme- und -verarbeitungskapazität der Verbraucher zu berücksichtigen. In diesem Zusammenhang wird ein Mindestmaß an Datenschutz vorgeschlagen, das auch dann greife, wenn eine Einwilligung vorliege. Sofern aber alle Anforderungen erfüllt seien, solle der Gestaltungsspielraum der Finanzdienstleister nicht weiter eingeschränkt werden.

4.4.2 Finanzaufsicht nicht primär zuständig – Dialog mit anderen Behörden aber nötig

In denselben Antworten wird aber auch betont, dass eine Stärkung der Datensouveränität der Verbraucher nicht in der Zuständigkeit der Finanzaufsicht gesehen werde. Diese solle sich in diesem Punkt auf die Missbrauchsaufsicht konzentrieren bzw. beschränken. Gefragt seien andere Behörden bzw. die Gesellschaft als Ganzes. So wird beispielsweise vorgeschlagen, über digitale Bildung, Verbraucheraufklärung sowie Schul- und Erwachsenenbildung auch über den Wert und Gegenwert beim „Bezahlen mit persönlichen Daten“ aufzuklären. In diesem Zusammenhang wird allerdings auch ein intensiverer Dialog von Finanz- und Datenschutzaufsichtsbehörden für nötig erachtet.¹⁵

¹⁵ Ein intensiverer Austausch wird zudem zwischen Finanzaufsicht und Wettbewerbsbehörden bzw. Wettbewerbsaufsicht gefordert – siehe Abschnitt 2.1.3.



4.4.3 Ideen zur Stärkung bzw. Gewährleistung von Datensouveränität

Datensouveränität könne grundsätzlich durch eine Einhaltung von gesetzlichen Rahmenwerken wie der DSGVO und eine transparente Informationspolitik gegenüber dem Verbraucher gewährleistet werden. Um Verbrauchern einen besseren Überblick über die von ihnen freigegebenen Daten zu gewähren, wird zum Beispiel die Einrichtung eines Datenschutzcockpits vorgeschlagen. Generell sei zu gewährleisten, dass eine Verwendung von personenbezogenen Daten nur über klar definierte und dokumentierte Prozesse erfolgen sollte. Auch solle Verbrauchern ein Ansprechpartner genannt werden, unabhängig davon, wo in der Wirkungskette der Schaden oder ein Problem entstanden sei. Verbraucher bräuchten auch in fragmentierten Wertschöpfungsketten eine lückenlose Haftungshandhabung.

Zudem wird auf die Möglichkeit hingewiesen, dass Industriestandards der Finanzbranche zu De-facto-Minimalanforderung an die Verwendung persönlicher Daten werden könnten, wenn diese vom Kunden akzeptiert bzw. wahrgenommen würden. Der Kunde könne sich so zuverlässige Partner für die Erbringung von Finanzdienstleistungen selber auswählen. Zum Beispiel hätten sich die Versicherer erst kürzlich in Zusammenarbeit mit den Datenschutzbehörden in einem veröffentlichten Code of Conduct zur Datensparsamkeit verpflichtet. Abschließend wurde die Vermutung geäußert, dass es

künftig Dienstleister geben werde, die sich auf die Durchsetzung der informationellen Selbstbestimmung spezialisierten. Solche Anbieter könnten mit Hilfe von BDAI-Methoden ausfindig machen, wo personenbezogene Daten eines Nutzers gespeichert seien. Sofern der Nutzer dies wünsche, könnte der Dienstleister anschließend beantragen, solche Daten zu löschen.

4.4.4 Technische Datenschutzmöglichkeiten

Die Verwendung von Verfahren wie Privacy-Preserving-Data-Mining und eine möglichst umfangreiche Pseudonymisierung bzw. Anonymisierung können, so die generelle Ansicht, das Vertrauen stärken. Die Forderung, Privacy-Preserving-Data-Mining als unbedingt einzuhaltende Grundanforderung zu etablieren, wird aber als problematisch angesehen, da dies oft eine erhebliche Einschränkung bei der Entwicklung von Algorithmen bedeute.¹⁶ Was das Privacy-Preserving-Data-Mining angeht, wird darauf hingewiesen, dass dieses in der Praxis auf eine vertrauenswürdige dritte Partei („Trusted Third Party“) angewiesen sei. Hier könnten Finanzinstitute eine wichtige Rolle einnehmen. Unter Umständen seien aber aufgrund des potentiell hohen Haftungsrisikos auch staatliche Stellen gefordert, die Rolle einer vertrauenswürdigen dritten Partei zu übernehmen.

¹⁶ Hierzu gibt es auch die Gegenmeinung, dass häufig trotz Verwendung dieser Verfahren das BDAI-Potenzial voll genutzt werden könne.

Wir werden künftig nicht mehr nur einzelne Unternehmen betrachten

Interview mit

Felix Hufeld

Präsident der BaFin



Herr Hufeld, die Teilnehmer an der Konsultation der BaFin weisen darauf hin, dass Anbieter von Suchmaschinen, sozialen Netzwerken und Online (Vergleichs-)Plattformen durch intelligente Datennutzung in Bereiche vordrängen, die bisher nur spezialisierten und häufig auch regulierten Anbietern vorbehalten seien. Wie beurteilen Sie diese Aussagen?

Sollten solche und andere technologie- und plattformbasierte Bigtechs regulierte Finanzdienstleistungen anbieten, müssten sie selbstverständlich dieselben aufsichtlichen und regulatorischen Anforderungen erfüllen wie alle anderen Institute. Aber auch wenn sie selbst keine regulierten Finanzdienstleistungen anbieten, weisen die Konsultationsteilnehmer zu Recht darauf hin, dass diese Unternehmen essenziell für das Funktionieren der Gesamtbranche sein können – zum Beispiel als Anbieter von Cloud-Dienstleistungen, von Algorithmen, aber auch von Daten und Bewertungen, wie Scorings und Ratings. Die gab es auch vorher schon, aber wenn dann noch BDAI und automatische Schnittstellen zum Einsatz kommen, kann sich die Auswirkung dieser Dienstleistungen auf den Finanzmarkt noch unmittelbarer entfalten.

Es werden in den Antworten einige interessante Ideen ins Spiel gebracht, wie man diese zunehmende Relevanz für den Finanzmarkt aufsichtlich und regulatorisch aufgreifen könnte. Ein Vorschlag lautet, dass Outsourcer-Unternehmen dann vergleichbare technische Mindestanforderungen erfüllen müssten wie regulierte Banken. Vorgeschlagen wird auch eine Art digitale Signatur am Produkt, die alle bei der Erstellung oder Bereitstellung beteiligten Unternehmen erfasst. Dann könne auch der Kunde klarer erkennen, wer hinter einem Angebot steht. Vor allem nehme man damit – neben dem beteiligten Finanzdienstleister – auch andere Unternehmen entlang der gesamten Wertschöpfungskette in die Verantwortung. Darüber hinaus könne für jede Leistung innerhalb einer Produkt-Wertschöpfungskette eine Back-Up-Partei vereinbart werden, die einspringen müsse, wenn eines der Unternehmen ausfalle. Technische Lösungen wie blockchainbasierte Smart Contracts könnten dabei eine Rolle spielen.

All diese Überlegungen bestätigen die These, die wir in unserem BDAI-Bericht aufgeworfen haben, nämlich, dass wir künftig nicht mehr nur einzelne Unternehmen

regulatorisch und aufsichtlich betrachten, sondern zunehmend Wertschöpfungsketten, die auf mehrere Unternehmen verteilt sind. Der aufsichtliche Fokus würde sich dann auch auf die Aktivitäten von Unternehmen richten, die nicht zum regulierten Finanzsektor zählen, die aber Einfluss auf das Kundenvertrauen und die Integrität des Finanzmarkts als solchen haben können. Damit will ich nicht sagen, dass die BaFin auch Bigtechs, die keine Finanzdienstleistungen erbringen als Ganzes beaufsichtigen sollte. Mir geht es eher um einige Aktivitäten und Verhaltensweisen solcher Unternehmen, um insoweit ein direktes aufsichtliches Mandat zu etablieren.

Lassen Sie uns bei den Wertschöpfungsketten bleiben. Vor allem aus der Verknüpfung von Daten verschiedenen Ursprungs lässt sich Wert schöpfen – etwa an zentralen Kundenschnittstellen auf Plattformen. Wie könnte man dieser steigenden Bedeutung von (Finanz-)Daten Rechnung tragen?

In dieser Frage sind wir uns mit den meisten Antwortenden einig. Die steigende Relevanz von Daten im Zeitalter der Digitalisierung gründet ja auch in dem Umstand, dass Daten aus verschiedenen Quellen verknüpft und in Relation zueinander gebracht werden und man so neue Kenntnisse gewinnen kann. Wer finanzwirtschaftliche Transaktionsdaten und Daten zum Verhalten von Verbrauchern miteinander verknüpft, kann sich ein ziemlich genaues Bild davon machen, wofür Kunden wie viel Geld auszugeben bereit und in der Lage sind. Zusätzlich werden durch das Aufkommen von plattformbasierten Geschäftsmodellen Informationssilos aufgebrochen, und Informationen aus einem Bereich können Auswirkungen auf andere Bereiche haben. Da ist es nur folgerichtig, wenn auch die Behörden, die verschiedene Bereiche des Wirtschaftslebens beaufsichtigen, enger zusammenarbeiten und ihre Informationssilos ebenfalls aufbrechen – natürlich soweit das rechtlich zulässig ist. Aufgrund der vermehrten Anwendung von BDAI sind für uns Finanzaufseher die Datenschutzbehörden und Wettbewerbshüter besonders wichtig. Nicht zu vergessen sind auch unsere Aufsichtskollegen im Ausland.

Natürlich sehen die Marktteilnehmer in der Hebung von Datenschätzen großes wirtschaftliches Potenzial. Aber auch beim Data-Mining müssen wir – wie bei jedem klassischen Schürf-, Abbau und Verwertungsprozess – die damit verbundenen Risiken im Blick behalten. Für uns Aufseher ist vor allem entscheidend, dass Verbraucher und Anbieter darauf vertrauen können, dass der Finanzmarkt stabil ist und dass es dort mit rechten Dingen zugeht. Wir müssen auch bedenken, welche negativen Ausstrahlungseffekte es haben kann, wenn Finanzdaten – auch mit formal juristisch korrekter Einwilligung – außerhalb des Finanzmarktes in Wertschöpfungsprozessen genutzt werden. Gesellschaftliche Errungenschaften wie der Schutz der Privatsphäre und die informationelle Selbstbestimmung sollten nicht unter dem Deckmantel der Innovation ausgehöhlt werden – etwa indem man scheinbar alternativlose Einwilligungen zur Datenfreigabe einholt. Nicht alles was technisch möglich, innovativ und wirtschaftlich kurzfristig sinnvoll ist, ist es auch aus einer ganzheitlichen und nachhaltigen Perspektive.

Lassen Sie uns nochmal auf den Finanzmarkt schauen. Sehen Sie auch hier hinsichtlich der Verwendung von Daten ein wichtiges Thema, das durch BDAI an Relevanz gewinnt?

Mit dem Argument, dass Daten zur Einschätzung des Risikos erforderlich seien, ließe sich bei der Erbringung von Finanzdienstleistungen die Erhebung nahezu aller Daten rechtfertigen. Eine solche Praxis beobachten wir auf dem deutschen Finanzmarkt jedoch bisher nicht. Die Rückmeldungen zu unserer Konsultation haben uns aber eines klar widerspiegelt: Wir müssen uns verstärkt fragen, welche Daten tatsächlich für eine sachgemäße Einschätzung von Risiken erforderlich sind – also für eine sachgerechte und aufsichtlich geforderte Differenzierung. Versicherer, die sich an unserer Konsultation beteiligt haben, haben sich in Zusammenarbeit mit den Datenschutzbehörden bereits in einem veröffentlichten Code of Conduct zur Datensparsamkeit verpflichtet. Interessant finde ich in diesem Zusammenhang aber die grundsätzliche Frage, wo die Grenzen der Datenerhebung und Auswertung bei BDAI liegen sollen.



Ab wann rechtfertigt eine marginale Verbesserung der Risikoeinschätzung die Erhebung zusätzlicher Daten? Bei welchen Daten können wir sagen, dass sie wirklich einen nachhaltigen und wesentlichen Nutzen haben und zugleich ein ausgewogenes Verhältnis zwischen dem erforderlichen Erkenntnisgewinn und anderen Zielen wie der Datensparsamkeit besteht? Ich denke, wir müssen mit allen Beteiligten einen breiten Dialog führen, aber wir müssen uns auch als Gesellschaft fragen, wo wir in der schönen neuen Datenwelt die roten Linien ziehen möchten.

Wenden wir uns der Verantwortung im Rahmen von selbstlernenden Entscheidungsunterstützungssystemen zu. Auch im BDAI-Bericht weist die BaFin darauf hin, dass die letztendliche Verantwortung immer beim Menschen und nie bei der Maschine liegen darf. Dies gilt laut den Konsultationsteilnehmern auch für die Aufsicht. Wie stehen Sie dazu?

Bei der Arbeit an unserem BDAI-Bericht hat uns unter anderem das Fraunhofer Institut für Intelligente Analyse- und Informationssysteme unterstützt. Fraunhofer hat dabei betont, dass die Erfolge des maschinellen Lernens bislang nur in sehr spezifischen Anwendungsbereichen zu finden und dass Ansätze zur generellen Nachbildung

von menschlicher Intelligenz nach wie vor nicht erkennbar seien. Wir werden also auf absehbare Zeit auf ein Zusammenspiel von künstlicher und menschlicher Intelligenz angewiesen sein. Auch bei der Finanzaufsicht wird und muss daher die Verantwortung beim Menschen bleiben. Aufsicht ist und bleibt ein flexibler Prozess, bei dem die Bewertung komplexer Sachverhalte im Vordergrund steht. Künstliche Intelligenz kann uns Aufseher aber unterstützen und ermöglichen, bessere und schnellere Prozesse zu etablieren und Entscheidungen vorzubereiten. In stark datengetriebenen Bereichen – etwa bei Marktmissbrauchsanalysen und eventuell künftig bei der Geldwäscheprävention – wird Aufsicht auf BDAI nicht verzichten können.

In den Rückmeldungen zu unserer Konsultation wird für Entscheidungsunterstützungssysteme, die auf künstlicher Intelligenz basieren, auch eine manuelle bzw. menschliche Intervention gefordert. Andererseits wird aber die Forderung nach der Erklärbarkeit von Algorithmen als unangemessene Einschränkung gesehen. Wie stehen Sie dazu?

Blindes Technik-Vertrauen halte ich für gefährlich. Menschen müssen intervenieren und automatisierte Prozesse müssen sich abschalten lassen können. Wie gesagt,

der Mensch trägt die Letztverantwortung, nicht die Maschine. Das müssen wir uns vor Augen halten, wenn wir neue Verfahren bewerten.

Zur Erklärbarkeit von KI-Systemen haben wir schon in unserem Bericht hervorgehoben, dass man zwischen Erklärbarkeit und Transparenz unterscheiden sollte. Transparenz bedeutet, dass das Verhalten des gesamten Systems vollständig nachvollziehbar ist. Laut Fraunhofer kann diese Forderung oft nicht erfüllt werden, da viele Modelle notwendigerweise sehr komplex seien. Das Kriterium der Erklärbarkeit hingegen sei technisch deutlich leichter zu erfüllen, denn dabei gehe es darum, für eine konkrete Entscheidung des Systems die wesentlichen Einflussfaktoren aufzuzeigen.

Auch in den Antworten zu unserer Konsultation vertritt man die Ansicht, dass sich für uns Aufseher die Frage stelle, ob und wie sich BDAI-Modelle prüfen lassen. Es werden erweiterte Anforderungen für geschäftskritische Prozessbereiche vorgeschlagen, etwa dass Code-Review-Verfahren, Simulations- und Penetrations-Tests und die Begutachtung von Musterprofilen eingesetzt werden. Man fordert uns auch auf, konkrete Anforderungen an Dokumentation und Erklärbarkeit von BDAI-Anwendun-

gen zu formulieren. Aufsichtliche Schnellschüsse werden Sie allerdings nicht erleben. Wir sollten erst einmal den Dialog mit Wissenschaft und Praxis vertiefen und zusehen, dass die Industrie Best-Practices entwickelt. Wenn wir wissen, ob und wie die wirken, können wir in einem weiteren Schritt überlegen, inwieweit wir daraus Standards ableiten.

Wie geht es nach der Konsultation für die BaFin weiter?

Wir haben bereits begonnen, die Rückmeldungen auszuwerten, die wir hier in diesem Artikel zusammengefasst haben. Es kristallisieren sich inhaltliche Stränge heraus, die wir – je nach Dringlichkeit und Bedeutung – priorisieren und abarbeiten möchten. Um dem anspruchsvollen Thema in allen Facetten gerecht zu werden, müssen wir uns hier und da noch intensiver mit der Branche, der Wissenschaft und anderen Behörden austauschen. Das wollen wir in der nächsten Zeit in Angriff nehmen. Wir haben mit unserem BDAI-Bericht und der Konsultation aber schon jetzt etwas erreicht: Wir haben die brennenden Fragen rund um das Thema platziert – auch in der Öffentlichkeit.

Herr Hufeld, wir danken Ihnen für das Interview!

III

Die Auslagerung von Aktivitäten und Prozessen ermöglicht es Banken, sich auf ihre Kernkompetenzen zu konzentrieren und ihre Dienstleistungen zu verbessern. Funktionieren kann Auslagerung aber nur, wenn die Institute die Risiken weiterhin unter Kontrolle behalten. Im Zeitalter der Digitalisierung stellt dies Banken und Aufsicht vor neue Herausforderungen.

Wenn Banken IT-Dienstleistungen auslagern

Autoren

Raimund Röseler

Exekutivdirektor Bankenaufsicht,
Bundesanstalt für Finanzdienstleistungsaufsicht
(BaFin)

Ira Steinbrecher

Referat Grundsatz IT-Aufsicht und Prüfungswesen,
Bundesanstalt für Finanzdienstleistungsaufsicht
(BaFin)

1 Einleitung

Für Unternehmen ist die Auslagerung von Aktivitäten und Prozessen seit jeher ein effizienter Weg der Arbeitsteilung. Bereits im Jahr 1776 hat Adam Smith festgestellt, dass Arbeitsteilung die produktiven Kräfte der Arbeit mehr als alles andere fördern und verbessern dürfte.¹ Auch Banken nutzen die Vorteile von Auslagerungen – und zwar aus vielfältigen Gründen: Bei einem Quervergleich der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) im Jahr 2013 nannten alle Institute Kostenersparnis, Prozessoptimierung und – vor allem bei der Informationstechnologie (IT) – Qualitätssteigerung, Zugang zu Spezialwissen, Nutzen von Synergien und Schonen von Ressourcen. Hauptmotiv für Auslagerungen war für sämtliche Banken die Kostenersparnis.²

In den vergangenen Jahrzehnten wurden die Prozesse und Aktivitäten in den Instituten zunehmend von IT-Systemen unterstützt. Die Digitalisierung ist daher für die Institute nicht neu, vollzog sich jedoch bislang im

Wesentlichen in deren Innern.³ Mit zunehmender Vernetzung der IT-Infrastruktur haben die Möglichkeiten der Arbeitsteilung in der Informationsverarbeitung zwischen Marktakteuren zugenommen. Banken ist es auf diese Weise möglich geworden, IT-Dienstleistungen auszulagern, was dazu führte, dass sie auch Teile des Wertschöpfungsprozesses nicht mehr vollständig selbst erbringen, sondern als IT-Dienstleistungen von Dritten beziehen. Wertschöpfungsketten werden also zunehmend aufgespalten und dezentralisiert.⁴

1 Smith, Der Wohlstand der Nationen, 5. Aufl. 2018, Seite 35.

2 Vgl. BaFinJournal August 2013, Seite 24.

3 Gampe, Digitalisierung und Informationssicherheit im Fokus aufsichtsrechtlicher Anforderungen, in: BaFinPerspektiven, Ausgabe 1/2018, Seite 70.

4 Vgl. hierzu auch Felix Hufeld, Rede vom 28.5.2018, „Digitalisierung – Chancen und Risiken in der Kredit- und Versicherungswirtschaft“, www.bafin.de/dok/10976554, abgerufen am 4.1.2019.

2 Standardisierung von IT-Dienstleistungen

Standardisierte IT-Dienstleistungen ermöglichen den Unternehmen, Skaleneffekte und damit die oben angesprochenen Kosteneinsparungen zu realisieren. Die Nachfrage nach solchen standardisierten Leistungen wird bereits seit einigen Jahren von IT-Dienstleistern, etwa von Rechenzentrenbetreibern, bedient, die solche Dienstleistungen für eine Vielzahl von Kunden bzw. Mandanten anbieten (Mehrmandantendienstleister). Der bereits 2013 von der BaFin analysierte Trend, dass ein Schwerpunkt der Auslagerungen der Banken in der IT liegt,⁵ setzt sich weiter fort. Angesichts der fortschreitenden Digitalisierung und der zunehmenden Bedeutung von Informationstechnologien, insbesondere Finanztechnologien (Fintech), passen die Institu-

tionen ihre Geschäftsmodelle, Prozesse und Systeme an, um solche Technologien zu nutzen. IT zählt daher mittlerweile zu den Aktivitäten, die am häufigsten ausgelagert werden.⁶ Damit einher geht die Beobachtung, dass Auslagerungen – neben dem Streben nach reiner Kostenersparnis – zunehmend eine strategische Dimension zukommt, dass sich Kreditinstitute also durch das Auslagern von Aktivitäten und Prozessen auf ihre Kernkompetenzen konzentrieren und somit ihre Dienstleistungen verbessern wollen.⁷

5 Vgl. a.a.O. (Fn. 2).

6 EBA/GL/2019/02, Seite 6.

7 Vgl. auch PricewaterhouseCoopers (PwC), Fit für die Zukunft – Wie sich bankfachliche Dienstleister erfolgreich für den Business Process Outsourcing Markt 2020 aufstellen, Business Process Outsourcing Studie, Frankfurt am Main, Seite 27.

3 Auslagerung in die Cloud

Ein aktuelles Beispiel für Auslagerungen, bei denen die beiden Dimensionen Kosten und Strategie eine wesentliche Rolle spielen, ist die auffallend zunehmende Nutzung von Cloud-Dienstleistungen.⁸ Die Dienstleistungen von Cloud-Anbietern reichen von der Bereitstellung von Speicherplatz oder Rechnerleistung (Infrastructure as a Service – IaaS) über die Bereitstellung von Entwicklerplattformen (Plattform as a Service – PaaS) etwa zur Einrichtung einer Internetpräsenz, bis hin zur Bereitstellung von Softwareapplikationen bzw. Webanwendungen

(Software as a Service – SaaS)⁹, die auf den Systemen des Cloud-Anbieters laufen. Die Nutzung solcher Cloud-Dienstleistungen bietet Instituten neue Möglichkeiten, Teile ihrer Geschäftsprozesse informationstechnologisch effizienter abzubilden, sich, wie oben beschrieben, auf ihre Kernkompetenzen zu fokussieren oder zum Beispiel neue datengetriebene Big-Data-Geschäftsstrategien zu verfolgen.

8 EBA/GL/2019/02, Seite 6.

9 BaFin Merkblatt, Orientierungshilfe zu Auslagerungen an Cloud-Anbieter, Seite 4, www.bafin.de/dok/11681598, abgerufen am 4.1.2019.

4 Risiken der Auslagerung

Auslagerungen bieten aber nicht nur Vorteile, sondern auch Risiken für die auslagernden Institute. Denn gerade wenn Risiken nicht mehr innerhalb der Organisationsstruktur der Institute liegen, besteht die Gefahr, dass sie nicht mehr vollständig identifiziert und gesteuert werden können.¹⁰ Deshalb haben der deutsche Gesetz-

geber und die deutsche Aufsicht besondere Vorgaben für das Risikomanagement von Auslagerungen entwickelt. Diese Vorgaben sind grundsätzlich technologie-neutral und lassen sich damit auch auf Auslagerungen an Cloud-Anbieter übertragen.

¹⁰ Hufeld, Aufsicht und Regulierung in Zeiten von Big Data und künstlicher Intelligenz, in: BaFinPerspektiven, Ausgabe 1/2018, Seite 16.



© iStock/from2015

5 Anforderungen an Auslagerungen an Cloud-Anbieter

Zunächst gelten für alle Formen der Auslagerungen die Vorgaben der §§ 25a, 25b Kreditwesengesetz (KWG) in Verbindung mit AT 9 der Mindestanforderungen an das Risikomanagement (MaRisk).¹¹ Für wesentliche Auslagerungen, die vom Institut selbst im Rahmen der Risikoanalyse identifiziert werden, gelten unter anderem besondere Anforderungen an die Vertragsgestaltung und die Beendigung des Auslagerungsverhältnisses. Gefordert wird auch, wesentlichen Auslagerungen zu steuern und zu überwachen und klare Verantwortlichkeiten einzurichten. Diese Vorgaben – § 25a, 25b KWG in Verbindung mit AT 9 MaRisk – wurden jedoch vor allem mit

Blick auf individuelle Auslagerungsverhältnisse entwickelt, bei denen Verträge mit entsprechenden Weisungs- und Prüfrechten individuell ausgestaltet werden können.

Wegen der herausragenden Wichtigkeit der IT hat die BaFin im November 2017 die Bankaufsichtlichen Anforderungen an die IT (BAIT)¹² veröffentlicht, die unter anderem im Modul 8 besondere Anforderungen an die Auslagerung und den sonstigen Fremdbezug von IT-Dienstleistungen stellen. Ein zentrales Ziel der BAIT ist es, das Bewusstsein für IT-Risiken in den Instituten und insbesondere auf den Führungsebenen zu schärfen.

¹¹ Rundschreiben 9/2017 (BA) – Mindestanforderungen an das Risikomanagement (MaRisk).

¹² Vgl. u. a. Gampe, Digitalisierung und Informationssicherheit im Fokus aufsichtlicher Anforderungen, in: BaFinPerspektiven 1/2018, Seite 68 ff.



6 Orientierungshilfe zu Auslagerungen an Cloud-Anbieter

Die Auslagerung an Cloud-Anbieter bringt neue Herausforderungen für die Institute und die Aufsicht mit sich. Die BaFin hat daher im November 2018 das Merkblatt „Orientierungshilfe zu Auslagerungen an Cloud-Anbieter“ veröffentlicht.¹³

¹³ Die Orientierungshilfe richtet sich an die im Finanzsektor beaufsichtigten Unternehmen (Kreditinstitute, Finanzdienstleistungsinstitute, Versicherungsunternehmen, Pensionsfonds, Wertpapierdienstleistungsunternehmen, Kapitalverwaltungsgesellschaften, Zahlungsinstitute und E-Geld-Institute). In diesem Artikel wird der Fokus auf Institute gerichtet, wie sie in § 1 Absatz 1b Kreditwesengesetz genannt sind (Kreditinstitute und Finanzdienstleistungsinstitute).

Mit ihrer Orientierungshilfe wollen BaFin und Deutsche Bundesbank transparent machen, wie sie diese Form der Arbeitsteilung und insbesondere verschiedene Vertragsklauseln einschätzen. Darüber hinaus geht es auch darum, bei den beaufsichtigten Unternehmen ein Problembewusstsein zu schaffen, und zwar im Umgang mit Cloud-Diensten und den damit verbundenen aufsichtsrechtlichen Anforderungen. Dazu weist die Orientierungshilfe auf wesentliche Aspekte hin, die beaufsichtigte Unternehmen bei einer Auslagerung an Cloud-Anbieter zum Beispiel bei der Risikoanalyse und der vertraglichen Gestaltung beachten sollten. Die Aufsicht stellt in der Orientierungshilfe allerdings keine neuen Anforderungen, sondern ausschließlich die derzeitige aufsichtliche Praxis dar.

7 Diskussion über Weisungsrechte aufgegriffen

Die BaFin hat in der Orientierungshilfe die aktuelle Diskussion darüber aufgegriffen, inwieweit die Vorgaben des AT 9 MaRisk auch bei der Ausgestaltung von Verträgen für die Auslagerung standardisierter IT-Dienstleistungen einzuhalten sind, etwa was die Vereinbarung von Weisungsrechten angeht: Bei einer Auslagerung muss es einem Institut möglich sein, dem Dienstleister im Hinblick auf die ausgelagerten Aktivitäten und Prozesse und die zugrundeliegenden Kontrollen entsprechend individuelle Weisungen zu erteilen. Bei der Nutzung standardisierter Dienstleistungen kann es aber schwierig werden, individuelle Weisungen zu erteilen, da diese auch Auswirkungen auf die Leistungen haben könnten, die der Cloud-Anbieter für andere Kunden erbringt. In solchen Fällen können daher die Institute von der Möglichkeit Gebrauch machen, die sich in der Erläuterung

zu AT 9 Tz. 7 MaRisk findet. Demnach kann auf eine explizite Vereinbarung von Weisungsrechten verzichtet werden, wenn die vom Auslagerungsunternehmen zu erbringende Leistung hinreichend klar im Auslagerungsvertrag spezifiziert ist. Diese Erleichterungen gelten auch für Auslagerungen an Cloud-Anbieter.



8 Wie weit kann das Prüfrecht gehen?

Über eine weitere zentrale Frage wird diskutiert: Wie weit kann das geforderte uneingeschränkte Prüfungsrecht gegenüber einem Cloud-Anbieter gehen? Die Orientierungshilfe stellt zunächst klar, dass sicherzustellen ist, dass Institute, die Informationen erhalten, die sie für die angemessene Steuerung und Überwachung der mit der Auslagerung verbundenen Risiken benötigen.¹⁴ Um diese Risiken angemessen steuern und überwachen zu können, müssen die Institute in der Lage sein, nicht nur die ausgelagerten Aktivitäten und Prozesse zu prüfen, sondern auch die zugrundeliegenden Kontrollprozesse. Die Cloud-Anbieter müssen ihnen hierfür ein uneingeschränktes Prüfrecht einräumen.

Cloud-Anbieter sehen in der Ausübung der Prüfrechte durch die Institute Risiken für den operativen Betrieb, zum Beispiel für Rechenzentren, wenn eine Vielzahl von Prüfungen zeitgleich durchgeführt werden. Die Orientierungshilfe weist daher auf verschiedene Erleichterungen hin, welche die Institute nutzen können. So kann die Interne Revision einer Bank bei einer wesentlichen Auslagerung gemäß BT 2.1 Tz. 3 MaRisk unter bestimmten Voraussetzungen auf eigene Prüfungen verzichten. Die Revisionstätigkeit ausführen können dann die Interne

Revision des Cloud-Anbieters, die Interne Revision eines oder mehrerer der auslagernden beaufsichtigten Unternehmen im Auftrag der auslagernden Bank (Sammelprüfungen – Pooled Audits), ein vom Cloud-Anbieter beauftragter Dritter oder ein von den auslagernden Instituten beauftragter Dritter.¹⁵

Eine weitere Erleichterung: Ein Institut darf grundsätzlich Nachweise bzw. Zertifikate auf Basis gängiger Standards¹⁶, Prüfberichte anerkannter Dritter oder interne Prüfberichte des Cloud-Anbieters heranziehen, sollte aber Umfang, Detailtiefe, Aktualität und Eignung des Zertifizierers oder Prüfers dieser Nachweise, Zertifikate und Prüfberichte berücksichtigen. Soweit die Interne Revision bei ihrer Tätigkeit solche Nachweise, Zertifikate oder Prüfberichte heranzieht, sollte sie die Nachweise und Belege (Evidenzen) prüfen können, die diesen zugrunde liegen.¹⁷

14 BaFin Merkblatt, Orientierungshilfe zu Auslagerungen an Cloud-Anbieter, Seite 8, www.bafin.de/dok/11681598, abgerufen am 4.1.2019.

15 BaFin Merkblatt, Orientierungshilfe zu Auslagerungen an Cloud-Anbieter, Seite 9, www.bafin.de/dok/11681598, abgerufen am 4.1.2019.

16 Zum Beispiel des Internationalen Sicherheitsstandards ISO/IEC 2700X der International Organization for Standardization und des C-5-Anforderungskatalog des Bundesamtes für Sicherheit in der Informationstechnik.

17 BaFin Merkblatt, Orientierungshilfe zu Auslagerungen an Cloud-Anbieter, Seite 9f., www.bafin.de/dok/11681598, abgerufen am 4.1.2019.

9 Grenzen der Auslagerung

Institute können die beschriebenen Erleichterungen nutzen, um Auslagerungen an Cloud-Anbieter möglichst effizient zu gestalten und auf diese Weise Skaleneffekte möglichst gut zu realisieren. Dennoch hat auch die Auslagerung an Cloud-Anbieter ihre Grenzen. So hat BaFin-Präsident Felix Hufeld schon wiederholt darauf hingewiesen, dass die Letztverantwortung bei der Geschäftsleitung des auslagernden Unternehmens bleibt.¹⁸ Auch die Europäische Bankenaufsichtsbehörde

EBA (European Banking Authority) stellt klar, dass die Geschäftsleitung eines auslagernden Instituts ihre Verantwortung niemals auslagern kann. Auslagerung dürfe nicht dazu führen, dass ein Institut zu einer leeren Hülle wird, der es an Substanz fehlt. Das Management müsse daher sicherstellen, dass ausreichende Ressourcen zur Verfügung stehen, welche die Erfüllung dieser Verantwortung angemessen unterstützen und gewährleisten – einschließlich der Überwachung der Risiken und der Verwaltung der Outsourcing-Vereinbarungen.¹⁹

¹⁸ Vgl. zum Beispiel auch Felix Hufeld, Rede vom 28.5.2018, a. a. O. (Fn. 3); Mußler, FAZ, 8.12.2018, Seite 26.

¹⁹ EBA/GL/2019/02, Seite 7.



© iStock/from2015

10 Ausblick

Unabhängig von der Orientierungshilfe, die den Status Quo der aufsichtlichen Vorgaben und der aktuellen Verwaltungspraxis wiedergibt, stellt sich die Frage, ob es künftig anderer oder dezidierterer Vorgaben für das Management von Risiken bei der Auslagerung von IT-Dienstleistungen bedarf. Internationale Standardsetzer wie die G7, der Basler Ausschuss für Bankenaufsicht (Basel Committee on Banking Supervision – BCBS) und die EBA beschäftigen sich mit Third-Party-Risks bzw. Auslagerungsrisiken. Die deutsche Aufsicht wird laufend prüfen, ob die aufsichtlichen Vorgaben und ihre Verwaltungspraxis angemessen sind, und sie anpassen, wenn notwendig. Die Ausarbeitungen der im Oktober 2018 veröffentlichten „G-7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector“ und die am 25. Februar 2019 veröffentlichten Guidelines on outsourcing arrangements der EBA werden hierbei eine wichtige Rolle spielen.

Daneben stellt sich die Frage, ob und inwieweit es sinnvoll und zielführend ist, konkrete Anforderungen an Mehrmandantendienstleister im Allgemeinen und Cloud-Anbieter im Besonderen zu stellen, um insbesondere deren potentiell systemischer Bedeutung für den Finanzsektor Rechnung tragen zu können. Ein erster Ansatzpunkt für künftige regulatorische Überlegungen könnten Wohlverhaltensregeln bzw. ein Verhaltenskodex sein, wie er zum Beispiel bereits auf dem Gebiet des Datenschutzes für Cloud-Anbieter vorgesehen ist.²⁰

Um die Frage nach der weiteren Entwicklung der aufsichtsrechtlichen Vorgaben beantworten zu können, wird man vor allem die Erfahrungen mit der Anwendung der bestehenden Vorgaben im Blick haben müssen: So dürften die erlaubten Sammelprüfungen für die einzelnen teilnehmenden Institute einen höheren Koordinationsaufwand bedeuten, was letztendlich auch Einfluss darauf hat, wie viele Institute gemeinsam prüfen können. Verschiedene Institute haben in den vergangenen Monaten

bereits erste Erfahrungen mit derartigen Sammelprüfungen gemacht.

Die deutsche Aufsicht beobachtet daher die Nutzung des Instruments Sammelprüfungen auch mit Blick auf die Durchführbarkeit und mögliche Konsequenzen für Verwaltungspraxis und Regulierung. Gleiches gilt für die Frage, inwieweit das Heranziehen von Prüfberichten und Zertifikaten auf Basis gängiger Standards ausreicht, um Risiken effektiv zu managen.

Aus aufsichtlicher und regulatorischer Sicht besonders interessant sind die Risiken, die mit der Auslagerung auf Mehrmandantendienstleister verbunden sein können. Diese Art der Auslagerung führt zu einer stärkeren Vernetzung des Finanzsektors mit IT-Dienstleistungsunternehmen und zu einer zunehmenden Komplexität des Marktgeschehens. Dadurch können neue Risiken entstehen, zum Beispiel an den Schnittstellen zwischen den Marktteilnehmern. Da diese Risiken nicht in der eigenen Organisationsstruktur der beaufsichtigten Banken entstehen, besteht die Gefahr, dass diese sie nur unvollkommen identifizieren und steuern können. Aufsichtlich und regulatorisch gilt es daher, die Struktur dieses dynamischen Marktes und die daraus resultierenden Risiken zu bewerten und, wenn nötig, aufsichtlich zu mitigieren.²¹

Risiken können auch entstehen, wenn eine Vielzahl von Instituten an eine begrenzte Zahl von Mehrmandantendienstleistern auslagert. Die EBA hat darauf hingewiesen, dass Konzentrationen von Auslagerungen auf wenige Dienstleister im Extremfall dazu führen können, dass gleich mehrere Institute nicht mehr oder nicht mehr störungsfrei Finanzdienstleistungen erbringen können. Wenn Dienstleister, zum Beispiel auf dem Gebiet der Informationstechnologie und der Finanztechnologie, ihre Leistungen nicht mehr erbringen können, kann dies sogar systemische Auswirkungen haben.²² Mit anderen

²⁰ Data Protection Code of Conduct for Cloud Service Providers Revised v1.0 vom 22.06.2016; Der Code wurde von der Cloud Select Industry (C-SIG) entwickelt, der von der Europäischen Kommission (DG Connect und DG JUST) einberufen wurde. Der Kodex besteht aus einer Reihe von Anforderungen für Cloud-Anbieter.

²¹ BaFin, Big Data trifft auf künstliche Intelligenz – Herausforderungen und Implikationen für Aufsicht und Regulierung von Finanzdienstleistungen, Seite 14ff., www.bafin.de/dok/10985478, abgerufen am 4.1.2019.

²² EBA/GL/2019/02, Seite 14f.

Worten: Der gesamte Finanzmarkt kann darunter leiden. Die Überwachung und das Management solcher Konzentrationsrisiken sind besonders relevant für IT-Dienstleistungen, die auf nur wenige Anbieter ausgelagert werden können.²³

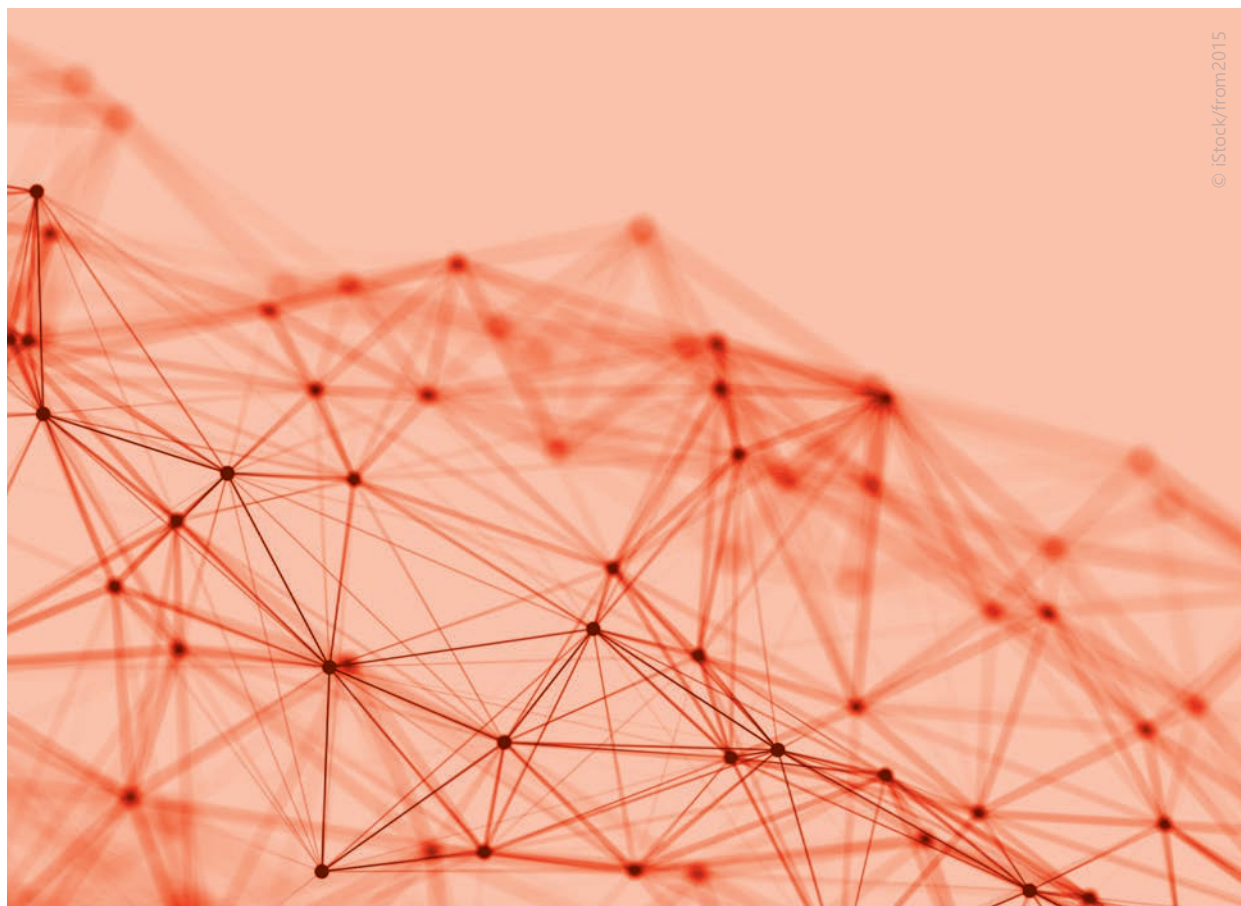
Die BaFin denkt derzeit intensiv darüber nach, wie die beschriebenen Risiken bei Auslagerungen an Mehrmandantendienstleister angemessen überwacht werden können. Grundsätzlich beaufsichtigt sie Dienstleister – also auch Mehrmandanten- bzw. IT-Dienstleister – nicht. Um sich ein besseres Bild von solchen Mehrmandantendienstleistern machen zu können, müsste sie von diesen direkt Informationen anfordern und ihnen gegenüber unmittelbar Prüfungen anordnen können. Nach

derzeitiger Praxis macht die Aufsicht diese Rechte lediglich über die beaufsichtigten Institute geltend. Zu prüfen ist, ob dieser Ansatz dauerhaft tragfähig ist.

Was aber tun, wenn sich Mehrmandantendienstleister nicht nur auf die von der BaFin beaufsichtigten Unternehmen spezialisieren? In solchen Fällen geht es nicht mehr nur um Risiken für den deutschen Finanzdienstleistungssektor. Dann können Risiken für die gesamte Wirtschaft entstehen – und zwar über die nationalen Grenzen hinaus. Eine Kontrolle solcher Dienstleister sollte nicht auf die nationalen Finanzaufsichtsbehörden beschränkt sein. Regulierung und Aufsicht müssen mehr denn je auf multilateraler Ebene stattfinden – auch, um ein echtes Level-Playing-Field zu schaffen.²⁴

23 a.a.O. (Fn. 21).

24 a.a.O. (Fn. 3).



IWV

Die Tarifierung und Preisfestlegung im Versicherungsgeschäft beruht auf einer umfangreichen Basis an Vergangenheitsdaten und Prognosewerten. Mit der zunehmenden Verfügbarkeit von Big Data (BD) und der schnellen, innovativen Entwicklung von Artificial Intelligence (AI) verändern sich auch die Möglichkeiten individueller Tarifierungen. Der vorliegende Beitrag untersucht die Auswirkungen auf den Risikoausgleich im Kollektiv.

Das Versicherungskollektiv in Zeiten von Big Data und Artificial Intelligence

Autoren

Prof. Dr. Fred Wagner

Institut für Versicherungslehre,
Universität Leipzig

Kristina Zentner, M.Sc.

Institut für Versicherungslehre,
Universität Leipzig

1 Einleitung

Big Data und Artificial Intelligence (BDAI) sind inzwischen stark diskutierte Schlagwörter, die mit einer großen disruptiven Kraft und einem hohen Veränderungspotenzial für bestehende Geschäftsmodelle in Verbindung gebracht werden. Insbesondere steigen damit die Möglichkeiten zur Individualisierung von Produkten und Preisen, von Kundenansprachen und der Automatisierung aller möglichen Unternehmensprozesse.

Die Entwicklungen gehen auch an der Versicherungswirtschaft nicht vorbei. So ergeben sich unter anderem Nutzungspotenziale bei der Risikoselektion, der (individualisierten) Prämienkalkulation und Tarifierung. Dabei treten nicht nur Fragestellungen hinsichtlich der Datensicherheit und des Datenschutzes auf. In der Diskussion stehen zugleich Aspekte der Zuverlässigkeit und Zulässigkeit von Big-Data-Nutzungen und einer möglichen Benachteiligung von Versicherungsnehmern mit schicksalsbedingt höheren Risiken. Zu guter Letzt stellt sich vielen die Frage, inwiefern der Risikoausgleich im Kollektiv und damit das Versicherungsprinzip bei individueller Prämienkalkulation und Tarifierung überhaupt noch funktioniert.

Um es vorwegzunehmen: Dem Versicherungskollektiv und dem Risikoausgleich schaden individualisierte Versicherungsprämien, die auf Basis von Big Data und Artificial Intelligence viel genauer ermittelt werden können, grundsätzlich nicht – im Gegenteil. Wie sich diese digitalen und technologischen Entwicklungen genau auf den Risikoausgleich im Kollektiv auswirken, wird im Folgenden analysiert.



2 Definition Versicherung

„Versicherung ist die Deckung eines im Einzelnen ungewissen, insgesamt geschätzten Mittelbedarfs auf der Grundlage des Risikoausgleichs im Kollektiv und in der Zeit.“

Dieter Farny¹

Diese Begriffsbeschreibung umfasst sowohl die wesentlichen Merkmale als auch das eigentliche Geschäftsmodell eines Versicherungsunternehmens. Ein hinreichendes Verständnis des Konzepts von privatwirtschaftlich organisiertem Versicherungsschutz setzt eine tiefgehende Erläuterung der einzelnen Definitionsbestandteile voraus.

„Deckung eines (...) insgesamt geschätzten Mittelbedarfs“

Eine wesentliche Eigenschaft des Versicherungsgeschäfts ist die Stochastizität. Die Stochastik beschäftigt sich vereinfacht mit Wahrscheinlichkeitsverteilungen von Ereignissen und deren Ergebnissen.² Auf Basis von Erfahrungen der Vergangenheit sowie mit Hilfe des Gesetzes der großen Zahl³ werden Wahrscheinlichkeitsverteilungen mit Erwartungswerten und Streuungen von Ergebnissen zufälliger Ereignisse in die Zukunft projiziert. Je mehr Einzelwerte der Ermittlung zugrunde liegen, desto zuverlässiger sind die Wahrscheinlichkeitsverteilungen. Beispielhaft sei das Ergebnis beim Auswerfen eines Würfels genannt. Zwar ist das einzelne Wurfresultat vom Zufall geprägt; allerdings ist der Erwartungswert für die Augenzahl stets 3,5 und die Streuung der Ergebnisse reicht von 1 bis 6. Die Wahrscheinlichkeit, bei nur einem Auswerfen die Augenzahl von 3,5 zu erreichen, ist null. Je häufiger aber das Zufallsexperiment wiederholt werden soll und anschließend ein Durchschnitt zu errechnen ist,

desto zuverlässiger wird die Schätzung, nahe am Erwartungswert von 3,5 auszulaufen.

In einem Versicherungsgeschäft werden meist die wirtschaftlichen Folgen des Eintritts unerwünschter realer Ereignisse, also von Gefahren, gedeckt. So werden beispielsweise in der verbundenen Hausratversicherung⁴ die Gefahren Einbruchdiebstahl, Leitungswasser, Sturm und Feuer abgesichert. Die wirtschaftlichen Folgen werden als Risiken⁵ bezeichnet und sind in Geld bemessene Schäden bzw. Mittelbedarfe, um die eingetretenen Ereignisse gegenzufinanzieren.⁶ Der einzelne Versicherungsnehmer erhält also eine im Versicherungsvertrag festgelegte Entschädigungszahlung, wenn sich eine der versicherten Gefahren und damit ein wirtschaftliches Risiko konkretisiert. Weil dies aber vom Zufall abhängt, ist die auszahlende Leistung im Vorfeld unbekannt. Auf Basis statistischer Vergangenheitswerte sowie unter Einbezug von Risikofaktoren (zum Beispiel Wohnadresse, Bauweise) werden Erwartungswerte für die Schadenhäufigkeit und die Schadenhöhe in einem Bestand versicherter Risiken kalkuliert, und ein vom Versicherer insgesamt zu deckender Mittelbedarf wird geschätzt. Und wie beim Würfelbeispiel wird die Schätzung umso genauer, je mehr Zufallsexperimente ein Kollektiv umfasst, d. h. je mehr Risiken (= einzelne Versicherungsverhältnisse) in den Bestand einbezogen sind.

Für eine zuverlässige Schätzung ist allerdings eine weitgehende Homogenität der versicherten Ereignisse bzw. Risiken erforderlich. Denn eine Schätzung von Durchschnittsschäden aus heterogenen Risiken bei einem Versicherer A würde für die unterdurchschnittlich

1 Farny: Versicherungsbetriebslehre, 5. Aufl. 2011, Seite 8.

2 Schmidt: Versicherungsmathematik, 3. Aufl. 2009, Seite 292f. oder Kamps, in: Roberts/Mosena/Winter (Hrsg.), Gabler Wirtschaftslexikon, 17. Aufl. 2010, Seite 2886.

3 Albrecht, in: Wagner (Hrsg.), Gabler Versicherungslexikon, 2. Aufl., Seite 364.

4 Siehe hierfür Andersch, in: Wagner (Hrsg.), Gabler Versicherungslexikon, 2. Aufl. 2017, Seite 962f.

5 Vgl. Albrecht, in: Wagner (Hrsg.), Gabler Versicherungslexikon, 2. Aufl. 2017, Seite 754.

6 Nicht in allen Versicherungsgeschäften werden Gefahren im Sinne negativer realer Ereignisse versichert. Es gibt auch die Fälle von Versicherungen sehr erwünschter Ereignisse, wie die Langlebigkeit, die allerdings ebenfalls Mittelbedarfe mit sich bringen – im genannten Beispiel etwa zur Finanzierung des weiteren Lebensunterhalts. Der wirtschaftliche Schaden ist in diesem Fall die Finanzierungslücke, die ohne eine Deckung des Mittelbedarfs durch Versicherungsleistungen entstehen würde. Zur Vereinfachung wird im Folgenden aber durchweg von (versicherten) Schäden und Schadenfällen gesprochen.

schadenexponierten Risiken zu einer überhöhten Kalkulation des Mittelbedarfs und damit auch zu überhöhten Versicherungsprämien führen. Umgekehrt würden überdurchschnittlich schadenexponierte Risiken zu gering kalkuliert und bepreist. Die Konsequenz wäre unter Konkurrenzbedingungen mit einem richtig kalkulierenden Wettbewerber B und bei entsprechender Markttransparenz eine Antiselektion von überhöhten Risiken zu Durchschnittsprämien bei Versicherer A.

„im einzelnen ungewiss“

Ein funktionsfähiges Versicherungsgeschäft bedingt die Ungewissheit des Eintritts jedes einzelnen Versicherungsfalls, da sonst ein elementares Kriterium der Versicherbarkeit⁷ von Risiken nicht erfüllt ist. Ein sicheres Ereignis ist nicht sinnvoll versicherbar, weil schon die Risikoprämie der Höhe des (sicheren) Schadens entsprechen müsste; hinzu kämen noch die Administrationskosten. Und ein Ereignis, das sicher nicht eintritt, bedarf keines Schutzversprechens. Der Schadeneintritt muss also vom Zufall geprägt sein. Dies bedeutet, dass sowohl der Versicherungsnehmer als auch das Versicherungsunternehmen im Vorfeld nicht wissen, ob, in welcher Höhe und/oder wann der individuelle Schaden entsteht. Um Informationsasymmetrie und damit die gegenseitige Übervorteilung bei der Versicherungsentscheidung zu vermeiden, sollte der Grad an Ungewissheit auf beiden Seiten in etwa gleich hoch sein. Allerdings ist das Versicherungsgeschäft in der Realität stark von Informationsasymmetrien geprägt.⁸ In der Regel kennt der Versicherungsnehmer sein persönliches Risiko viel besser als der Versicherer und kann dieses sogar beeinflussen. Versicherungsunternehmen können solche Informationsasymmetrien mit Hilfe von Antragsfragen, Besichtigungen und (im Personengeschäft) ärztlichen Untersuchungen sowie Obliegenheiten⁹ verringern. Zudem besitzen die Versicherer umgekehrt aufgrund ihrer

umfangreichen Statistiken einen Informationsvorsprung über die Wahrscheinlichkeitsverteilungen von Schäden, den sie in Form von überhöhten Risikoprämien gegenüber den Versicherungsnehmern ausspielen könnten. Da allerdings die Preistransparenz in Zeiten von Vergleichsportalen sowie Online-Maklern steigt, würde solch ein Verhalten durch die Mechanismen des Wettbewerbsmarkts tendenziell sanktioniert.

Risikoausgleich im Kollektiv

Im Vordergrund eines Versicherungsvertrags steht der Transfer einer Wahrscheinlichkeitsverteilung¹⁰ von Schäden vom Versicherungsnehmer auf das Versicherungsunternehmen. Da ein Versicherungsunternehmen diverse Schadenereignisse einer Vielzahl von Versicherungsnehmern deckt, hat es auch eine Vielzahl von Risiken in seinem Versicherungsbestand, die sich untereinander ausgleichen.

Erneut greift hier das Würfelbeispiel, um den Risikoausgleich im Kollektiv zu erklären. Bei einem fairen Würfel ist die Wahrscheinlichkeit für alle möglichen Würfelresultate, also für das Erreichen der verschiedenen Augenzahlen 1, 2, ... 6, gleich hoch. Da bei einer Reihe von Zufallereignissen (also einzelnen Würfelvorgängen) voneinander unabhängige Ergebnisse entstehen, werden sich gegenüber dem Erwartungswert tendenziell höhere und niedrigere Würfelresultate untereinander ausgleichen, so dass sich das Durchschnittsergebnis entsprechend der ursprünglichen Schätzung bei 3,5 einpendeln wird – und dies umso zuverlässiger, je häufiger gewürfelt wird (Gesetz der großen Zahl, s. o.). Genauso verhält es sich bei versicherten Risiken in der Realität. Eine weitere Voraussetzung ist allerdings die Unabhängigkeit der Risiken untereinander. Wenn keine Unabhängigkeit vorliegt, wie zum Beispiel bei Sturmschäden innerhalb einer abgegrenzten Region, können sich schadenbelastete und schadenfreie Risiken nicht mehr untereinander kompensieren, und der Risikoausgleich misslingt.

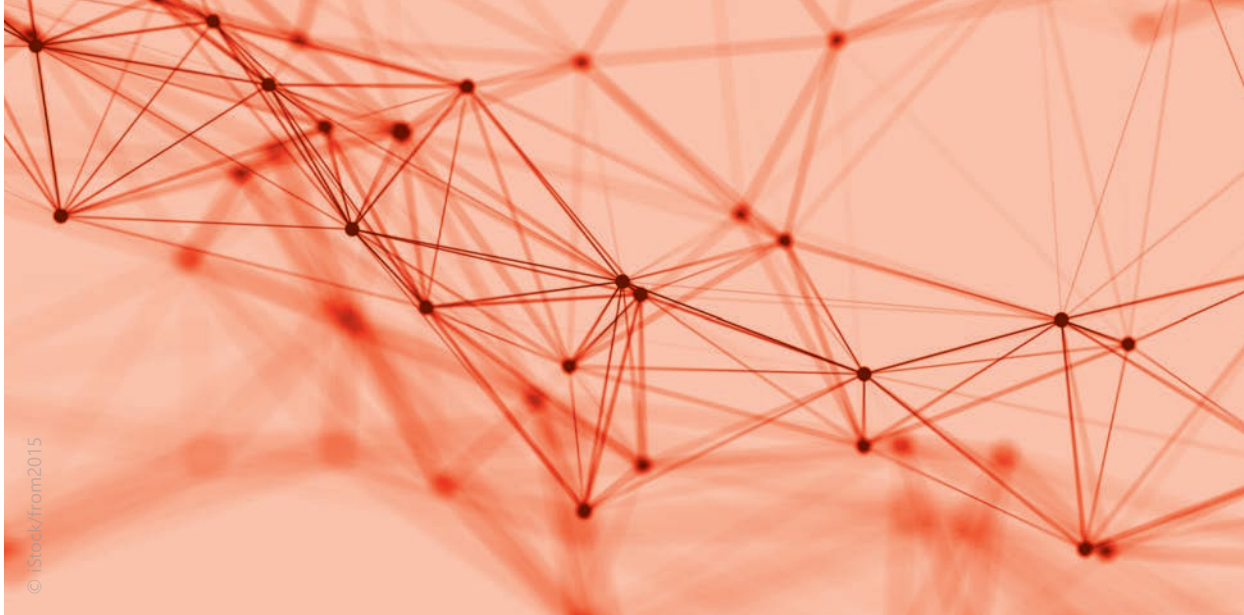
Während für das Schätzkollektiv die Homogenität der Einzelrisiken also von großer Bedeutung ist (s. o.), gilt

7 Wagner/Elert/Luo, in: Wagner (Hrsg.), Gabler Versicherungslexikon, 2. Aufl. 2017, Seite 985.

8 Weiterführende Literatur zu den Phänomenen von Informationsasymmetrien, siehe Akerlof, The Market for "Lemons": Quality Uncertainty and the Market Mechanism, The Quarterly Journal of Economics, 3/1970, pp. 488 et seq.

9 Vgl. hierzu Beckmann/Schirmer, in Wagner (Hrsg.), Versicherungslexikon, 2. Aufl., 2017, Seite 621.

10 Vgl. Schmidt, in: Wagner (Hrsg.), Gabler Versicherungslexikon, 2. Aufl. 2017, Seite 1036.



dies allerdings nicht für den Risikoausgleich im Kollektiv. Hier liegt häufig ein Missverständnis über das Versicherungsprinzip vor. Auch heterogene Risiken, gemessen am Schadenerwartungswert, können sich untereinander ausgleichen, vorausgesetzt, sie werden jeweils mit der richtigen Versicherungsprämie unterlegt. Beispielsweise können in ein Kollektiv von Risikolebensversicherungen auch Versicherte unterschiedlichen Alters und damit unterschiedlicher Sterbewahrscheinlichkeiten aufgenommen werden, wenn unter sonst gleichen Umständen ältere Versicherte eine risikoadäquat höhere Prämie als jüngere Versicherte zahlen. Der Risikoausgleich wird dann nicht gestört. Vorab muss jedoch bei der Schätzung des Risikos und damit bei der Prämienkalkulation passend nach dem Alter der Versicherten differenziert werden.

Risikoausgleich in der Zeit

Der Risikoausgleich im Kollektiv umfasst als Betrachtungszeitraum immer nur eine begrenzte Zeitperiode und funktioniert typischerweise nie perfekt. Innerhalb einer Periode bleiben regelmäßig Über- oder Unterschäden übrig, die sich über die Zeit allerdings tendenziell ebenfalls wieder ausgleichen. Anders ausgedrückt: Perioden mit Unterschäden gleichen Perioden mit Überschäden aus. Damit ist der Risikoausgleich in der Zeit erklärt, der zugleich die Langfristigkeit des Versicherungsgeschäfts erfordert und prägt. Ideale Voraussetzungen für den Risikoausgleich in der Zeit sind konstante Eigenschaften aller Einzelrisiken im Versicherungsbestand und zudem eine gleichbleibende Bestandszusammensetzung. Dies bedeutet, dass der Schadenerwartungswert und die Schadenstreuung möglichst keinem Änderungsrisiko unterliegen oder sich die Änderungsrisiken innerhalb des Gesamtkollektivs tendenziell wieder ausgleichen. Ein über die Zeit konstantes Gesamtkollektiv ist in der Praxis allerdings kaum gegeben, da der Versicherungsbestand von Zu- und Abgängen sowie einer sich verändernden Risikolandschaft geprägt ist. Wegen der Grenzen des

Risikoausgleichs im Kollektiv und in der Zeit verbleibt immer ein versicherungstechnisches Risiko für das Versicherungsunternehmen.

Versicherungstechnisches Risiko

Das versicherungstechnische Risiko beschreibt die Möglichkeit, dass der kollektive Schadeneffektivwert den kollektiven Schadenerwartungswert übersteigt und der Versicherer hierdurch Verlustrisiken oder sogar dem Risiko des Ruins unterliegt, da die eingenommenen Risikoprämien ggf. nicht ausreichen, um die eingetretenen Schäden zu bezahlen.¹¹ Das versicherungstechnische Risiko kann ursächlich in das Zufalls-, Änderungs- und Irrtumsrisiko unterteilt werden.¹²

Das Zufallsrisiko tritt ein, wenn der Schadeneffektivwert vom Schadenerwartungswert abweicht, weil sich zufällig überdurchschnittlich viele und/oder hohe Schäden ereignet haben.¹³

Dem Änderungsrisiko liegt der mögliche Fall zugrunde, dass sich die Risikoverhältnisse im Zeitablauf gegenüber den ursprünglich bei der Prämienkalkulation zugrunde gelegten Annahmen in ungünstiger Weise ändern und der Schadeneffektivwert deswegen am Ende den Schadenerwartungswert übersteigt.¹⁴

Die Bedeutung des Irrtumsrisikos geht aus seiner Bezeichnung bereits hervor. Das Irrtumsrisiko konkretisiert sich bei fehlerhaften Schätzannahmen.¹⁵

11 Vgl. Farny, *Versicherungsbetriebslehre*, 5. Aufl. 2011, Seite 82f.

12 Vgl. ebenda.

13 Vgl. Albrecht, a. a. O., (Fn. 3), Seite 1094.

14 Vgl. Albrecht, a. a. O., (Fn. 3), Seite 37f.

15 Vgl. ebenda, Seite 469f.

3 Funktionsweise der Versicherung: Das versicherungstechnische Äquivalenzprinzip

Die konzeptionelle Grundlage zur Berechnung der Risikoprämien¹⁶ ist das versicherungstechnische Äquivalenzprinzip. Nach dem versicherungstechnischen Äquivalenzprinzip entspricht die Risikoprämie dem Schadenerwartungswert des in Deckung genommenen Risikos.

In einer weiteren Differenzierung lassen sich das kollektive und das individuelle versicherungstechnische Äquivalenzprinzip voneinander unterscheiden. Bei einer Prämienermittlung nach dem individuellen versicherungstechnischen Äquivalenzprinzip ist die Höhe der vom Versicherungsnehmer zu zahlenden Risikoprämie gleich der Höhe seines ganz individuellen Schadenerwartungswerts. Nach dem kollektiven versicherungstechnischen Äquivalenzprinzip entspricht die Gesamtheit der Risikoprämien aus einem Versicherungsbestand dem kollektiven Gesamtschadenerwartungswert. Das individuelle versicherungstechnische Äquivalenzprinzip schließt gleichsam das kollektive versicherungstechnische Äquivalenzprinzip mit ein; denn wenn jeder Versicherungsnehmer die Risikoprämie für den Anteil seines Schadenerwartungswerts am Gesamtkollektiv erbringt, entspricht die Summe der individuellen Risikoprämien auch dem aggregierten Schadenerwartungswert eines Kollektivs.¹⁷ Umgekehrt muss die durch die Anzahl der Versicherungsnehmer geteilte kollektive Risikoprämie nicht gleich dem individuellen Schadenerwartungswert sein. Bei heterogenen Risiken liegt dann eine Durchschnittsprämie für unterschiedliche, d.h. teils überdurchschnittlich und teils unterdurchschnittlich schadenexponierte, Risiken vor, für die jeweils unterdeckende bzw. überdeckende Versicherungsprämien eingefordert würden – mit den Folgen von Antiselektion, wie folgt:

Angenommen seien mehrere auf einem transparenten Versicherungsmarkt unter Konkurrenzbedingungen agierende Versicherungsunternehmen. Auf diesem erhebt Versicherer 1 Risikoprämien, die an die individuellen

Schadenerwartungswerte angeglichen sind, und ein anderer Versicherer 2 durchschnittliche Risikoprämien für seinen Versicherungsbestand. Nutzenmaximierende, rationale Versicherungsnehmer mit unterdurchschnittlichen Risiken (also solchen mit einem gegenüber dem Durchschnitt geringeren Schadenerwartungswert) schließen in diesem Fall ihren Versicherungsvertrag bei Versicherer 1 mit entsprechend geringeren Risikoprämien ab. Versicherungsnehmer mit überdurchschnittlichen Risiken (also solchen mit einem gegenüber dem Durchschnitt erhöhten Schadenerwartungswert) entscheiden sich für Versicherer 2 mit der durchschnittlichen Risikoprämie, da diese immer noch unter ihrem eigentlichen Schadenerwartungswert liegt. Passt Versicherer 2 seine Risikoprämie nicht schnell genug an das neu zusammengesetzte Kollektiv an, läuft er Gefahr, in den Ruin zu fallen.

Nach bisherigem Stand kann eine Risikoprämie allenfalls näherungsweise nach dem individuellen versicherungstechnischen Äquivalenzprinzip kalkuliert werden. Für eine weitere Annäherung fehlen derzeit eine zuverlässige Datenbasis sowie informationstechnische Verarbeitungsprozesse. Als Datenbasis dienen grundsätzlich Informationen über Risikomerkmale, die im Wesentlichen drei Anforderungen erfüllen müssen:

1. Es muss ein statistisch signifikanter Zusammenhang zwischen den Ausprägungen der Risikomerkmale einerseits und dem Verlauf der Schadenverteilung¹⁸ (mit dem Schadenerwartungswert und der Schadenstreuung) andererseits vorliegen.
2. Der Zusammenhang muss plausibel sein, um Scheinkorrelationen auszuschließen.
3. Die Ausprägungen der Risikomerkmale müssen für das Versicherungsunternehmen operativ erfassbar sein.

¹⁶ Im Weiteren wird ohne Betriebskosten, Kapitalkosten und Sparanteile argumentiert.

¹⁷ Vgl. auch Albrecht, a. a. O., (Fn. 3), Seite 1021f.

¹⁸ Vgl. Albrecht, in: Wagner (Hrsg.), Gabler Versicherungswörterbuch, 2. Aufl. 2017, Seite 822.

Zugunsten der Erfassbarkeit dominieren heute sogenannte „objektive Risikomerkmale“¹⁹, deren Ausprägungen von außen tendenziell leicht und zuverlässig erhoben werden können. Beispiele sind in der Kfz-Versicherung die Typklasse des Automobils, der Wohnort des Halters (Regionalklasse), die Dauer des Führerscheinbesitzes etc. Mit über 100 Risikomerkmale, die marktweit verwendet werden, sind die Kfz-Versicherer schon heute in der Lage, das versicherungstechnische Äquivalenzprinzip bis in kleinste Tarifzellen herunterzubrechen, denen jeweils nur wenige, teils sogar nur einzelne Risiken angehören. Vermutlich ist sogar die Anzahl der Tarifzellen, die mit den gegebenen Risikomerkmale nach den Regeln der Kombinatorik gebildet werden können, deutlich höher als die marktweite Zahl der versicherten Risiken. Aus der Summe der Einzelprämien, die auf diese Weise ermittelt werden, dürfte hochgerechnet für das Kollektiv eine Gesamtprämie resultieren, die dem versicherungstechnischen Äquivalenzprinzip in hohem Maße genügt. Dennoch bleibt das individuelle versicherungstechnische Äquivalenzprinzip unvollkommen erfüllt. Es fehlt vor allem an der Erhebung und Verarbei-

19 Vgl. Farny, a.a.O. (Fn. 1), Seite 31f.

tung subjektiver Risikomerkmale, die insbesondere für die Einstellungen, Fähigkeiten und Verhaltensweisen der Autofahrer stehen und die für die Schadenträchtigkeit besonders relevant sind – bis heute aber nicht oder kaum erfasst werden konnten. Vielfach dienen vor diesem Hintergrund die objektiven Risikomerkmale als unvollkommene Ersatzmerkmale für die subjektiven Risikomerkmale²⁰. Konkreter ausgedrückt: Die Typklasse des Fahrzeugs, der Wohnort des Halters und die Dauer des Führerscheinbesitzes sind nicht dafür verantwortlich, ob der Autofahrer unterwegs einen Unfall verursacht. Sie sind aber statistisch signifikante, plausible und gut erfassbare Indizien für die Einstellungen, Fähigkeiten und Verhaltensweisen des Versicherungsnehmers im Straßenverkehr. Im Durchschnitt mögen diese Zusammenhänge stimmen; in den Einzelfällen dürften jedoch vielfach Abweichungen von den plausiblen Annahmen und den statistischen Werten vorliegen.²¹

20 Vgl. ebenda.

21 Unbenommen bleibt dabei, dass auch die objektiven Risikomerkmale teils hohe Relevanz besitzen. So beeinflusst die Typklasse des Kfz über dessen Ausstattungsmerkmale (z. B. Assistenzsysteme) auch unmittelbar die Eintrittswahrscheinlichkeit von Unfällen, die der Fahrer zu verantworten hat.



4 Die digitale Revolution

4.1 Grundlagen zur Digitalisierung

Die Geschwindigkeit und Dynamik, mit denen der technische, vor allem der informationstechnische Fortschritt voranschreitet, ist beeindruckend und herausfordernd zugleich. Oft ist inzwischen die Entwicklung neuer Datengrundlagen, Technologien und möglicher Prozesse schneller als die Bereitschaft und Fähigkeit von Unternehmen und ganzen Branchen, diese in einem rechtlich teils noch ungeklärten Umfeld anzuwenden. Die Begeisterung, das Interesse und manchmal schlichtweg die Normalität, mit der die neuen Technologien in der breiten Bevölkerung und von Konsumenten angewandt werden, fördern die Weiterentwicklungen umso mehr. Das Anspruchsdenken bzw. die Erwartungshaltung an digitale Anwendungen lässt sich selbst bei öffentlichen Verwaltungen und in Schulen beobachten.²²

Der Begriff Digitalisierung an sich meint zunächst nur die Transformation von Ziffern, Buchstaben, Texten, Bildern, Videos und anderen Datentypen in ein digitales Format, ferner deren Speicherung und Verarbeitung mittels unterschiedlicher Computertechnologien.²³ Auch in der deutschen Versicherungswirtschaft bedarf es einer zügigen und erfolgreichen Fortentwicklung entsprechender digitaler Fähigkeiten, möchte sie im Verhältnis zu anderen Branchen sowie international wettbewerbsfähig bleiben. Als für Versicherungsunternehmen bedeutsame Treiber werden nachfolgend die Faktoren Big Data und Artificial Intelligence dargestellt und deren potenzielle Auswirkungen auf das Versicherungskollektiv grundlegend untersucht.

22 Bundeszentrale für politische Bildung, URL: <https://www.bpb.de/gesellschaft/bildung/zukunft-bildung/213441/digitalisierung-und-schule>, abgerufen am 3.12.2018.

23 Vgl. Hofer, a.a.O (Fn. 3), Seite 228f.

4.2 Big Data

Big Data steht für die Verfügbarkeit großer digitaler Datenmengen und deren technologische Auswertungsmöglichkeiten. Der Trend zu Big Data wird durch die zunehmenden Speicherkapazitäten und die steigende Verarbeitungsgeschwindigkeit neuer Computertechnologien getrieben und beschleunigt.²⁴

Zur Charakterisierung von Big Data können vier Dimensionen von Kriterien herangezogen werden: Volume, Velocity, Variety und Value.²⁵

Volume beschreibt Big Data mit der verfügbaren Datenmenge und der Maßgröße Byte. Die jährlich generierte digitale Datenmenge wird in den nächsten Jahren rasant wachsen. Wurden 2016 16,1 Zetabyte²⁶ an digitalen Daten weltweit generiert, soll sich diese Zahl bis zum Jahr 2025 verzehnfachen.²⁷ Das Kriterium Velocity steht für die Geschwindigkeit der Datenerzeugung und -verarbeitung. Die Datenvielfalt ist Gegenstand des Kriteriums Variety. Damit sind nicht lediglich unterschiedliche Dateiformate (zum Beispiel Bilder, E-Mails, Word- und PDF-Dateien, Videos) gemeint, sondern auch ihr Strukturierungsgrad. Daten sind unstrukturiert, wenn sie keiner formalisierten Ordnung entsprechen. Dies ist in der Regel bei Bildern und E-Mails der Fall. Semi-strukturierte Daten weisen entweder keine fest typisierte, sondern lediglich eine versteckte Struktur auf, oder sie sind insgesamt unterschiedlich strukturiert. Mit der Struktur sind neben den Dateiformaten, die mit der Unternehmensdatenbank kompatibel sein müssen, auch die Strukturen der Feldtypen (Beispiel: Titel_Quelle_Datum) gemeint, die eine Datei in einer Datenbank näher beschreiben.²⁸

24 Vgl. Hofer, a. a.O (Fn. 3), Seite 157.

25 Vgl. <https://www.ibmbigdatahub.com/infographic/four-vs-big-data>, abgerufen am 3.12.2018.

26 1 Zetabyte entsprechen ca. 10²¹ Byte.

27 Siehe hierzu eine Studie von Statista GmbH, <https://de.statista.com/statistik/daten/studie/267974/umfrage/prognose-zum-weltweit-generierten-datenvolumen/>, abgerufen am 3.12.2018.

28 Deutsches Institut für Vertrauen und Sicherheit im Internet, Big Data, 2016, Seite 26.

Die Investitionen in Informationstechnologien zur Speicherung und Verarbeitung von Big Data sollen sich selbstverständlich amortisieren und den Unternehmenswert steigern. Anders ist die Sammlung, Speicherung und Auswertung von Big Data aus unternehmerischen Gesichtspunkten nicht sinnvoll. Diese Zielsetzung ist im Kriterium Value enthalten.²⁹

Bei der Nutzung extern beschaffter Daten sind deren Qualität und Aussagekraft zu überprüfen. Außerdem

ist zu beachten, dass bei personenbezogenen Daten die betroffene Person nach Artikel 15 Absatz 1 lit. g der europäischen Datenschutz-Grundverordnung (DSGVO)³⁰ über ein Auskunftsrecht der Datenherkunft verfügt.

Der Übergang von herkömmlichen Datenbeständen und deren Auswertungen hin zu Big Data ist fließend. Traditionell verfügen Versicherungsunternehmen über große Datenbestände mit langen Historien, die zum Beispiel aus den Antragserhebungen und Schadenerfahrungen

29 Fasel/Meier, Big Data – Grundlagen, Systeme und Nutzungspotenziale, 2016, Seite 6.

30 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).



hervorgehen. Vielfach liegen diese Daten allerdings in verteilten Datenbanksystemen und wurden/werden nicht zusammengefügt. Auch die Datenqualität – im Sinne von laufender Aktualisierung und Harmonisierung – ist meist verbesserungswürdig. Inzwischen können auch Daten über subjektive Risikomerkmale mittels Smart Gadgets verfügbar gemacht werden. Und zunehmend bestehen Möglichkeiten, Daten aus externen Quellen zu erlangen. Dazu zählen spezielle Datenprovider, Websites und das Social Web.³¹ Insbesondere gegenüber den US-Bigtechs (Google, Amazon, Facebook, Apple, kurz Gafa & Co.) und anderen Branchen besteht allerdings ein großer Rückstand, weil noch kaum Open Data und Daten in Echtzeit erfasst werden. Open Data sind „ungefilterte und maschinenlesbare elektronische Daten, die jedem öffentlich, zweckfrei und unverbindlich zur Verfügung gestellt werden“.³² Sie kommen in der Regel von der Bundesverwaltung und umfassen zum Beispiel Informationen über den Verkehr, den Tourismus oder das Wetter.³³ Wie allen anderen Unternehmen aus sämtlichen Branchen steht es auch Versicherungsunternehmen frei, zusätzlich Open Data für die Optimierung ihrer Produkte, Services und Geschäftsprozesse, zum Beispiel als Tarifierungsgrundlage, zu integrieren.

Daneben können Echtzeitdaten dazu beitragen, Aktivitäten und Verhaltensweisen von Versicherungsnehmern und Versicherten zu entschlüsseln, um unter anderem auf die Risikoverhältnisse zu schließen. Echtzeitdaten werden heute schon in großen Mengen etwa von Smartphones und Wearables über die Nutzer erfasst und von den Herstellern ausgewertet. Automobilhersteller sind in der Lage, das Fahrverhalten der Kraftfahrzeugführer in Echtzeit zu messen. Die Frage wird sein, wer in Zukunft vom Souverän dieser Daten (das sollte immer der gemessene Bürger selbst sein) legitimiert wird, solche Daten für welche Zwecke verwenden zu dürfen.

31 Seufert, in: Fasel/Meier, a. a. O. (Fn. 28), Seite 52.

32 Termer, F. (2018): Open Data bringt Mehrwert für Unternehmen, <https://www.bitkom.org/Presse/Presseinformation/Open-Data-bringt-Mehrwert-fuer-Unternehmen.html>, abgerufen am 3.12.2018.

33 Vgl. Bundesministerium für Wirtschaft und Energie, Open Data: Mit öffentlichen Daten digitale Wirtschaft fördern, <https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/open-data.html>, abgerufen am 3.12.2018.

Versicherer wären mit personalisierten Echtzeitdaten wiederum zum Beispiel in der Lage, auch den subjektiven Risikomerkmale deutlich näher zu kommen.

Die Versicherungswirtschaft macht im Spielfeld von Big Data inzwischen aber auch Fortschritte. So werden in der Kraftfahrzeugversicherung vermehrt Pay-as-you-drive- und Pay-how-you-drive-Tarife entwickelt und angeboten. Bei Pay-as-you-drive-Tarifen wird die Versicherungsprämie kilometergenau je tatsächlich gefahrenen Kilometer berechnet, während bei Pay-how-you-drive-Tarifen das persönliche Fahrverhalten analysiert wird und Gegenstand der individuellen Prämienkalkulation ist.³⁴

Weitere Entwicklungslinien in anderen Versicherungszweigen stellen Pay-as-you-live-Tarife dar. Hier werden Daten über das persönliche alltägliche Verhalten mittels Wearables, wie zum Beispiel Smart Watches, ausgelesen oder ebenfalls durch Smartphones oder Technologien im Smart Home³⁵ an das Versicherungsunternehmen übermittelt. Allerdings sind die Versicherer mit diesen Konzepten insgesamt noch eher zurückhaltend.³⁶

Der Umgang mit Big Data ist an technische, personelle und intellektuelle Voraussetzungen geknüpft. Die Kunst liegt in der Generierung von Smart Data, die weitere Gütekriterien erfüllen, wie zum Beispiel datenschutzrechtliche Anforderungen und gesellschaftliche Akzeptanz.

Um Big Data effizient und sinnvoll innerhalb der Risikoanalyse und Versicherungstarifizierung nutzen zu können, bieten die Entwicklungslinien der künstlichen Intelligenz neue Ansätze.

34 Vgl. GDV, Positionen. Den Fahrer im Blick, <http://positionen.gdv.de/den-fahrer-im-blick/>, abgerufen am 3.12.2018.

35 Vgl. OECD Digital Economy Papers, Consumer Policy and the smart home, 2018, Nr. 268, <https://www.oecd-ilibrary.org/docserver/e124c34a-en.pdf?expires=1543255258&id=id&accname=guest&checksum=FFC7F6B9DB075CE596466A4198B8CDD4>, abgerufen am 3.12.2018.

36 Weiterführend ist das Positionspapier des GdV zu den Anforderungen an Smart Home Installationen sowie Geräten des „Internet der Dinge“ vom 29.5.2017, <https://www.gdv.de/resource/blob/8254/346747549f0b20cd6a28b6a806a04152/anforderungen-smart-home-iot--900514353-data.pdf>, abgerufen am 3.12.2018.



4.3 Artificial Intelligence

Eine allgemeingültige Definition von Intelligenz ist kaum zu finden. Als charakteristisch für menschliche Intelligenz werden zum Beispiel praktische Problemlösungsfähigkeiten, verbale Fähigkeiten und soziale Kompetenzen genannt.³⁷

Mit Artificial Intelligence (deutsch: künstliche Intelligenz) ist die Fähigkeit von Aufgabenlösungen durch Computertechnologien gemeint, über die sonst nur Menschen aufgrund ihrer intellektuellen Verarbeitungsfähigkeiten verfügen.³⁸ Ohne Anspruch auf Trennschärfe können nach Intelligenzstufen eine schwache künstliche Intelligenz und eine starke künstliche Intelligenz unterschieden werden.³⁹

Auf Basis schwacher künstlicher Intelligenz sind computergetriebene Maschinen in der Lage, Lösungen zu entwickeln, die sich auf bestimmte, angelernte Aufgaben beschränken. Beispiele sind Navigationssysteme und die Korrekturfunktionen in elektronischen Schriftmedien.

Von starker künstlicher Intelligenz wird gesprochen, wenn Maschinen menschliche Intelligenz nachbilden und breitere kognitivere Leistungen erzielen.⁴⁰ Dies trifft dann zu, wenn Maschinen logische Schlüsse ziehen können, stetig dazulernen oder kluge Entscheidungen unter Unsicherheit treffen.

Für die Entwicklung künstlicher Intelligenz wurden und werden die neuronalen Netze, also Netzwerke aus Nervenzellen, des menschlichen Gehirns untersucht, mittels moderner Technologien modelliert und somit stückweise imitiert. Im Fall einer starken künstlichen Intelligenz wird computerbetriebenen Maschinen die Fähigkeit zum Lernen (Machine Learning⁴¹) und damit verbunden zur Urteilsbildung und Problemlösung übermittelt.⁴² Deep Learning ist ein Teilaspekt des Machine Learnings, bei dem Maschinen Fähigkeiten zur Prognosestellung und zum Fällen eigener Entscheidungen entwickeln.⁴³

37 Sternberg, *Advances in the psychology of Human influence*, 5. Aufl., 1989, pp. 91 et seq.

38 <https://www.britannica.com/technology/artificial-intelligence>, abgerufen am 3.12.2018.

39 Buxmann/Schmidt (Hrsg.), *Künstliche Intelligenz – Mit Algorithmen zum wirtschaftlichen Erfolg*, Seite 40.

40 National Science and Technology Council, 2016, https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf, abgerufen am 3.12.2018.

41 Machine Learning (zu Deutsch: Maschinelles Lernen) bedeutet, dass Maschinen trainiert werden, bestimmte Aufgaben auf Basis von Erfahrungen zu lösen. Vgl. Buxmann/Schmidt (Hrsg.), *Künstliche Intelligenz – Mit Algorithmen zum wirtschaftlichen Erfolg*.

42 Ertel, *Grundkurs Künstliche Intelligenz*, 4. Aufl., 2016.

43 <https://www.bigdata-insider.de/was-ist-deep-learning-a-603129/>, abgerufen am 3.12.2018.

5 Wirkungsweisen von Big Data und Artificial Intelligence in Kalkulation und Tarifierung

Artificial Intelligence ermöglicht erstmals eine sinnvolle und effiziente Nutzung von Big Data. Innovative Prozesse, die auf die Leistung künstlicher Intelligenz zurückgreifen, wie etwa Entwicklungen im Bereich Smart Data Analytics, können große, unstrukturierte Datenmengen nutzbar machen, indem sie sie filtern, selektieren, sortieren und in ein einheitliches Format transformieren. Unter Einsatz künstlicher Intelligenz anstelle von menschlicher Intelligenz können teure Mitarbeiterkapazitäten gespart und anderweitig eingesetzt werden. Zudem kommt es bei der Bearbeitung großer Datenmengen mit künstlicher Intelligenz zu keinen Ermüdungserscheinungen. Die Bearbeitung erfolgt somit schneller und fehlerfreier.

Mit Hilfe von Pattern-Analysen, also Mustererkennungen, wird es unter anderem möglich, die Zusammenhänge zwischen Echtzeitdaten einerseits und Verhaltensausprägungen sowie Schadenpotenzialen andererseits zuverlässig und effizient zu erforschen. Damit werden auch die Analyse und Auswertung von subjektiven Risikomerkmale entscheidend vorangebracht.

Auf Basis dieser Erkenntnisse und einer Dunkelverarbeitung von Big Data kann somit unter anderem eine

Echtzeittarifierung ermöglicht werden. Beim Versicherer eingehende verhaltensbasierte Daten aus den Sensoren eines Kraftfahrzeugs, von der Smart Watch oder anderen Fitnessstrackern sowie aus einem Smart Home können mittels intelligenter, automatisierter Prozesse unverzüglich analysiert und in einem personalisierten Versicherungstarif mit individueller Prämie verarbeitet werden. Auch Bonus-Malus-Regelungen könnten bei bestimmten, im Vorfeld definierten Verhaltensweisen, automatisiert und unverzüglich umgesetzt werden. Der erhebliche Zugewinn an Verarbeitungskapazität, -geschwindigkeit und -flexibilität kann schließlich zu nahezu gänzlich individualisierten Versicherungsprämien führen. Außerdem können künstlich intelligente Prozesse durch die akribische Analyse von Big Data vorhandene Informationsasymmetrien, die zulasten des Versicherers gehen, verringern.

Zum heutigen Stand müssen die notwendigen Voraussetzungen für den Einsatz künstlicher Intelligenz in Versicherungsunternehmen allerdings teilweise erst noch geschaffen werden. Zunächst muss den Versicherungsnehmern der in der Weitergabe von Daten liegende Nutzen aufgezeigt werden. Daten, die bereits im



Versicherungsunternehmen über viele ältere Systeme verteilt sind, müssen datenschutzkonform zentralisiert und zur Analyse zur Verfügung gestellt werden. Zu beachten ist ferner, dass das Versicherungsunternehmen den Versicherungsnehmern nach Artikel 13 Absatz 2 lit. f DSGVO mitteilen muss, welche Logik der automatisierten Entscheidungsfindung zugrunde liegt. Das wird per se problematisch, denn zumindest starker künstlicher Intelligenz liegt kaum noch ein nachvollziehbarer Algorithmus zugrunde, der aufgedeckt und kommuniziert werden könnte.

In der Folge wird künstliche Intelligenz nach den geltenden Regeln die menschliche Intelligenz bei der Tarifierung nicht gänzlich ersetzen können. Zwar können damit die Anforderungen der statistischen Signifikanz und (zusammen mit den digitalen Möglichkeiten der Datengewinnung) die Probleme der Erfassbarkeit von Verhaltensweisen und subjektiven Risikomerkmale überwunden werden, wie aufgezeigt. Allerdings stellt sich mit ihr verstärkt das Problem der Plausibilisierung.

Nach Auffassung der Aufsichtsbehörde, soweit verlautete, müssen die Versicherer auch stets in der Lage sein, die Logik der Algorithmen gemäß Artikel 13 Absatz 2 f DSGVO zu erklären und ggf. gewisse ethische und rechtliche Grundsätze zu überprüfen (zum Beispiel die Einhaltung des Verbots der Tarifierung nach Geschlecht und Nationalität).⁴⁴ Noch scheint Skepsis angebracht, ob diese Anforderungen mit dem Einsatz künstlicher Intelligenz überhaupt vereinbar sind. Wird die Nutzung künstlicher Intelligenz vor diesem Hintergrund (aufsichts-)rechtlich eingeschränkt, stellt sich wiederum die Frage, ob deutsche Versicherungsunternehmen (und die deutsche Wirtschaft schlechthin) im internationalen und branchenübergreifenden Wettbewerb entscheidende Nachteile erleiden und ins Hintertreffen geraten. Schon heute sind die Entwicklungszentren für künstliche Intelligenz eher in den USA, China und Indien, aber nicht in Deutschland lokalisiert.

⁴⁴ Vgl. Frank Grund, Rede vom 13. November 2018, „Neue Herausforderungen für Aufsicht und Branche“, abgerufen am 3.12.2018.

6 Auswirkungen auf das Versicherungskollektiv

Ziel des Einsatzes von Big Data und Artificial Intelligence in der Tarifierung von Versicherungsunternehmen ist also die Ermittlung einer Versicherungsprämie, die näher am individuellen Schadenerwartungswert des einzelnen Versicherungsnehmers bzw. Risikos liegt. Eine Prämie, die sich dem individuellen versicherungstechnischen Äquivalenzprinzip annähert, kann auch als fairer bzw. leistungsgerechter empfunden werden.

Eine individuell versicherungstechnisch äquivalente Prämie wird sich naturgemäß für Versicherungsnehmer

mit unterdurchschnittlich hohen Risiken als vorteilhaft und für Versicherungsnehmer mit überdurchschnittlich hohen Risiken als nachteilig erweisen – bei Letzteren insbesondere dann, wenn deren ungünstige Risikomerkmale nicht durch anderes Verhalten positiv beeinflusst werden können (zum Beispiel Gendispositionen in der Personenversicherung). Bei individuellen und verhaltensabhängigen Versicherungsprämien wird sich zunehmend die Frage stellen, welche Faktoren, Eigenschaften und Verhaltensweisen in die Tarifierung einbezogen werden dürfen und welche eher nicht.



© iStock/From2015

Außerdem bleibt derzeit noch zu hinterfragen, ob die Zusammenhänge zwischen konkreten Verhaltensweisen und ihren Einflüssen auf die individuell erwarteten Schäden bereits hinreichend erforscht sind. Zum Beispiel ist noch näher zu untersuchen, wie genau sich das Geschwindigkeits-, Beschleunigungs- und Bremsverhalten in einem Kraftfahrzeug tatsächlich auf die Gefahrenpotenziale auswirken. Bei Pay-as-you-live-Tarifen ist etwa zu untersuchen, welche Lebensmittel für welche Personengruppen wirklich gesundheitsfördernd oder -schädigend sind oder welche Intensität und Dauer welcher Sportaktivitäten langfristig das körperliche und geistige Wohlergehen fördern oder stören – und das Ganze sowohl mit Blick auf die statistische Signifikanz als auch auf die Plausibilität. Falsche oder zumindest nicht weitestgehend treffende Schlussfolgerungen können zu einer ungerechtfertigten Benachteiligung bestimmter Versicherungsnehmergruppen führen.

Soweit die Tarifierung auf Basis von Big Data und Artificial Intelligence zu individuellen Prämien führt, ist der Risikoausgleich im Kollektiv allerdings grundsätzlich unbeschadet. Vor dem Hintergrund der Tatsache, dass bei Ermittlung einer Prämie nach dem individuellen versicherungstechnischen Äquivalenzprinzip zwingend auch das kollektive versicherungstechnische Äquivalenzprinzip erfüllt ist, ist die kollektive Versicherungsprämie auch bei individueller Tarifierung auskömmlich genug, um die insgesamt erwarteten Schäden zu decken. Damit ist dem verbreiteten Missverständnis eindeutig entgegenzutreten, dass bei einer individualisierten Prämie der Kollektivgedanke und damit das Versicherungsprinzip nicht mehr erfüllt seien. Das Gegenteil – siehe oben – ist richtig: „Versicherung ist die Deckung eines im Einzelnen ungewissen, insgesamt geschätzten Mittelbedarfs auf der Grundlage des Risikoausgleichs im Kollektiv und in der Zeit“. Auch und gerade mit einer versicherungstechnisch richtig kalkulierten individuellen Versicherungsprämie funktioniert der Risikoausgleich im Kollektiv und wird Antiselektion

vermieden. Risikotheoretisch wird damit zudem eine faire Prämie festgelegt. Ob diese Prämie auch in der allgemeinen Öffentlichkeit als fair im Sinne von gerecht beurteilt wird, ist eine andere Frage, die hier nicht zu erörtern ist.⁴⁵

Ein signifikanter Vorteil durch den Einsatz von künstlicher Intelligenz und damit verbundener Dunkelverarbeitung bei der Tarifierung von Versicherungsverträgen können die sinkenden Betriebs- und Verwaltungskosten sein. Wie bei allen Innovationen muss hier allerdings zuerst eine gewisse Amortisationszeit eingerechnet werden. Von sinkenden Kosten profitiert wiederum das gesamte Versicherungskollektiv, da sich die Kostenvorteile in geringeren Prämien widerspiegeln sollten.

Große Herausforderungen bei der Nutzung von Big Data und Artificial Intelligence liegen derzeit noch in der Einhaltung von Anforderungen des Datenschutzes. Insbesondere die DSGVO mit den Erfordernissen der Datenminimierung⁴⁶ gemäß Artikel 5 Absatz 1 c DSGVO, Speicherbegrenzung⁴⁷ gemäß Artikel 5 Absatz 1 e DSGVO und Zweckbindung⁴⁸ gemäß Artikel 5 Absatz 1 b DSGVO beschränken die faktischen Einsatzmöglichkeiten. Mangels bislang klar abgesteckter Regelungen besteht die Herausforderung in der Praxis derzeit schon allein darin, den rechtlich zulässigen Spielraum für die Nutzung von verfügbaren Daten und deren Analyse auszuloten.

45 Siehe dazu näher Wagner, *Geschäft oder Gewissen? Vom Auszug der Versicherung aus der Solidargemeinschaft*, 2017.

46 Die erhobenen Daten müssen auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

47 Die Identifizierung der jeweiligen Person darf nur solange möglich sein, wie es für den Zweck der Datenerhebung notwendig ist.

48 Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

7 Würdigung

Grundsätzlich kann durch den Einbezug von Big Data und mit Hilfe des Einsatzes künstlicher Intelligenz der Risikoausgleich im Kollektiv durch eine noch fundiertere Ermittlung individueller Risikoprämien verbessert werden. Zudem bestehen vielerlei Kostenoptimierungspotenziale, die zugunsten des Versicherungskollektivs gehen. Wichtig ist, dass der Individualisierungsgrad der Tarifierung Hand in Hand mit dem Tempo geht, in dem die gesellschaftliche Akzeptanz dieser Technologien und der damit zusammenhängenden Geschäftsmodelle zunimmt.

Inwiefern der steigende Individualisierungsgrad den Solidargedanken gefährdet und insofern die Gerechtigkeitsempfindungen beim Verbraucherschutz, in der Politik und Öffentlichkeit stört, ist ausdrücklich keine Wesensfrage des Geschäftsmodells in der privaten Versicherungswirtschaft. Privatversicherung folgt nicht dem Solidarprinzip nach den Kriterien „Gesund für Krank, Reich für Arm, Stark für Schwach“, wie es im Kern für die Säulen des Sozialversicherungssystems gilt, sondern dem Prinzip des Risikoausgleich im Kollektiv.⁴⁹ Nichtsdestotrotz müssen auch privatwirtschaftliche Versicherungsunternehmen die Erwartungshaltungen erfüllen, und bei nicht ausreichender Berück-

sichtigung von Solidarität in der Tarifikalkulation werden sie mit Kritik konfrontiert. Ein prominentes Beispiel ist die Debatte um die versicherungstechnisch richtigen, aber unbezahlbar hohen Versicherungsprämien in der Hebammenhaftpflichtversicherung.

Der Problematik hoher Prämienbelastungen bestimmter, überdurchschnittlich hoher Risiken im Versicherungskollektiv steht jedoch auch die Möglichkeit gegenüber, dass damit positive Steuerungswirkungen entfaltet werden. Soweit nämlich unerwünschte Verhaltensweisen der Versicherungsnehmer oder Versicherten das überhöhte Risiko begründen, führt die damit verbundene Versicherungsprämie möglicherweise dazu, solche Verhaltensweisen zu korrigieren oder einzustellen. Wenn zum Beispiel mit Hilfe von Big Data, künstlicher Intelligenz und Echtzeitverarbeitung einem Autofahrer bei Anzeichen von überhöhter Geschwindigkeit im Display seiner Armaturen ein signifikanter Prämienzuschlag angezeigt wird, könnte dies ad hoc zu einer Anpassung des Fahrverhaltens und auch auf Dauer zu erwünschten Verhaltensanpassungen führen. Derartige Konsequenzen stören vermutlich auch nicht den Solidargedanken, sondern stärken im Gegenteil die Verantwortung für das eigene Verhalten im Versicherungskollektiv und damit auch die versicherungstechnische Solidarität. Die Grenzziehung ist jedoch schwierig und liegt im Graubereich zwischen den verhaltensgesteuerten und schicksalhaften Merkmalen der Versicherungsnehmer und ihren versicherungstechnischen Risiken.

⁴⁹ Siehe dazu Wagner, *Geschäft oder Gewissen? Vom Auszug der Versicherung aus der Solidargemeinschaft*, 2017.

8 Zusammenfassung

Der Einbezug von Big Data und Artificial Intelligence kann insgesamt Vorteile mit sich bringen – sowohl für den Versicherer als auch für den Versicherungsnehmer. Im Wettbewerb um die Nutzung und Einsatzmöglichkeiten stehen die Versicherungsunternehmen allerdings unter anderem den Technologieriesen wie Amazon, Apple, Facebook und Google gegenüber, die zum einen viel geübter darin sind, Daten zu sammeln und zu verarbeiten, und bei denen zum anderen auch die gesellschaftliche Akzeptanz hierfür höher ist. Zudem erweisen sich die meist noch verteilten Datenbanken, die verbesserungswürdige Datenqualität und die vielfach veralteten IT-Systeme als Nachteile von Versicherungsunternehmen bei der Umsetzung der vielversprechenden und potenzialträchtigen Technologien. Die Versicherungsunternehmen werden gezwungen sein und sollten das Mögliche daransetzen, sich den Innovationen gegenüber zu öffnen und sie zu ihren Vorteilen auszuschöpfen. Dabei den Gleichschritt mit den rechtlichen Rahmenbedingungen, insbesondere dem Datenschutz, ferner mit den ökonomischen Möglichkeiten (Investitionskosten!) und nicht zuletzt mit der gesellschaftlichen Akzeptanz zu halten, wird nicht einfach.

Eine Herausforderung wird auch darin bestehen, ein tiefergehendes Vertrauen beim Kunden zu schaffen und Souveränität im Umgang mit den Daten zu beweisen. Die Generierung echter und für den Kunden spürbarer Mehrwerte wird weiter in den Vordergrund rücken, damit es sich für den Kunden lohnt, Daten über subjektive Merkmale preiszugeben.

Der vorliegende Beitrag hat sich – seinem Titel folgend – auf die Auswirkungen von Big Data und Artificial Intelligence auf das Versicherungskollektiv konzentriert und darauf weitgehend beschränkt. Ausgeblendet wurden weitere vielversprechende Einsatzmöglichkeiten im Versicherungsunternehmen, wie beispielsweise bei der Betrugserkennung, generell im Schadenmanagement, darüber hinaus bei der gesamten Prozessoptimierung und zudem für die Generierung kundenzentrierter Mehrwertleistungen über den reinen Versicherungsschutz hinaus. Diese Aspekte eröffnen zusätzliche, vermutlich sogar erheblich größere und entscheidende Zukunftspotenziale – mehr noch: sie dürften für die einzelnen Versicherungsunternehmen überlebenswichtig sein.



W

Der Artikel skizziert die Positionierung der Sparkassen-Finanzgruppe zu wesentlichen Aspekten der digitalen Transformation. Er verdeutlicht die verschiedenen Dimensionen, in denen die Digitalisierung auf die Sparkassen einwirkt und zeigt auf, wie die Institute die damit verbundenen Herausforderungen und Chancen konkret gestalten.

Standortbestimmung Digitalisierung Sparkassen

Autoren

Dr. Joachim Schmalzl

Geschäftsführendes Vorstandsmitglied,
Deutscher Sparkassen- und Giroverband, Berlin

Frank Weigand

Abteilungsleiter, Digitale Innovationen,
Deutscher Sparkassen- und Giroverband, Berlin

1 Bedeutung der Digitalisierung

Die Digitalisierung wird häufig auch als Digitale Revolution bezeichnet. Revolution meint in der Literatur meist eine „drastische, zu schwerwiegenden und tiefgreifenden sozialen und politischen Strukturveränderungen führende Umwälzung“.¹ Das beschreibt die Reichweite der Digitalisierung sehr zutreffend. Denn was in der ursprünglichen Definition ziemlich unspektakulär als das Umwandeln analoger Werte wie Text oder Musik in digitale Formate, also Daten, daher kommt², ist tatsächlich ein drastischer Kontinuitätsbruch, der die ganze Gesellschaft betrifft.³

Die Digitalisierung verändert Privatleben, Politik und Wirtschaft. Erst in den zurückliegenden Jahren erreicht dies ein breites Bewusstsein, doch die Digitalisierung ist kein neues Phänomen. Der Beginn des digitalen Zeitalters lässt sich mit der Entstehung des World Wide Web Anfang

der 1990er Jahre recht gut verorten. In den zurückliegenden 15 Jahren hat nicht nur das klassische Internet eine rasante weltweite Akzeptanz gefunden. Mit dem Aufkommen der Smartphones und damit der mobilen Nutzung hat das Web den Lebensalltag vieler Menschen massiv verändert. Es beginnt sogar Werte und Normen von Gesellschaften und Staatengemeinschaften zu wandeln.⁴

Auf politischer Ebene wurde die Digitalisierung im europäischen Umfeld erstmals 2010 in der „Digital Agenda for Europe“ strategisch bewertet. Auf nationaler Ebene erarbeitete die Enquete-Kommission „Internet und digitale Gesellschaft“ zwischen 2010 und 2013 Empfehlungen für den deutschen Bundestag. Daran schloss sich die „Digitale Agenda 2014 – 2017“ an, die Grundsätze der Digitalpolitik formulierte. Inzwischen ist die Digitalisierung Chefsache.⁵ Der Koalitionsvertrag der laufenden

1 Hillmann: Wörterbuch der Soziologie, 4. Aufl. 1994, Seite 737.

2 Gartner, IT Glossary, <https://www.gartner.com/it-glossary/digitization/>, abgerufen am 12.12.2018.

3 McAfee, Andrew and Brynjolfsson, Erik, The Second Machine Age, 2014, Seite 9ff.

4 Lemke, Einführung in das digitale Zeitalter, 2014, Seite 19.

5 Die Bundesregierung, Digitalisierung wird Chefsache, <https://www.bundesregierung.de/breg-de/aktuelles/digitalisierung-wird-chefsache-1140420>, abgerufen am 12.12.2018.

Bundesregierung setzt einen deutlichen Schwerpunkt in diesem Bereich.

In der Wirtschaft führt die Digitalisierung zu einer Vielzahl von neuen, datengetriebenen Geschäftsmodellen. Es ist eine strukturelle Veränderung, weil Technologieunternehmen traditionelle Unternehmen bei der Leistungserbringung ablösen. Während 2006 mit Microsoft nur ein Technologiekonzern unter den wertvollsten Unternehmen zu finden war⁶, stellten Unternehmen aus traditionellen Branchen 2017 nur noch drei der zehn Höchstplatzierten. Mit JP Morgan befindet sich nur noch eine Bank in der Liste.⁷

Viele Branchen haben sich bereits komplett gewandelt – etwa die Musikindustrie – oder befinden sich mitten in einer tiefgreifenden Veränderung – so wie die Finanzbranche. Die in der Vergangenheit geführten Diskussionen darüber, ob die Digitalisierung die Finanzbranche nachhaltig berührt, sind der Frage gewichen, wie man den Herausforderungen der Digitalisierung aktiv begegnet und sich zukunftsfähig aufstellt, um auch in Zukunft relevant zu bleiben.

Wo aber steht die Branche aktuell? Darüber gehen die Ansichten weit auseinander. Der im Monitoring-Report „Wirtschaft DIGITAL 2018“ des Bundeswirtschaftsministeriums ermittelte Index zum Digitalisierungsgrad deutscher Unternehmen weist bei den Finanz- und Versicherungsdienstleistungen mit 61 Punkten einen überdurchschnittlichen Wert gegenüber dem Gesamtindex (54 Punkte) aus. Damit gilt die Branche als digital fortgeschritten. Die Kreditwirtschaft selbst erwartet bis 2023 einen weiteren Digitalisierungsschub.⁸ Der Index basiert auf einer Befragung hochrangiger Entscheider der Wirtschaft.

Eine Vielzahl aktueller Studien und Publikationen sieht den Digitalisierungsgrad der Kreditinstitute hingegen als noch nicht ausreichend, um die bekannten und kommenden Herausforderungen erfolgreich zu meistern. Insbesondere die traditionelle Rolle als Intermediär wird als gefährdet angesehen.⁹ Digitale Anwendungen haben das Potential, bestehende Geschäftsmodelle zu disruptieren oder aber massiv zu verändern.¹⁰

Experten sehen zudem die Gefahr, dass die Kreditwirtschaft die Digitalisierung primär als Mittel zur Erzielung von Produktivitäts- und Effizienzgewinnen begreife und wie bisher zu langsam agiere. Oft wird auch der Vorwurf erhoben, Banken nähmen die Digitalisierung nicht ernst und würden die Herausforderung durch die Onlinekonkurrenz belächeln.¹¹ Die Branche unterschätze den durch die neuen Technologien hervorgerufenen und erforderlichen fundamentalen Wandel weiterhin und laufe Gefahr, in Zukunft zunehmend erhebliche Marktanteile an digitale Plattformen, nicht traditionelle Wettbewerber und Fintechs zu verlieren.¹²

Die Aufgabe für die Kreditwirtschaft besteht also darin, das veränderte Nutzerverhalten der Kunden, neue Technologien und nicht zuletzt neue Wettbewerber aus dem Technologieumfeld in ihre Strategie einzubinden.

6 The Economist, <https://www.economist.com/special-report/2016/09/17/the-rise-of-the-superstars>, abgerufen am 7.1.2019.

7 FAZ, Technologie schlägt Industrie, <http://www.faz.net/aktuell/wirtschaft/diginomics/das-sind-die-wertvollsten-unternehmen-der-welt-15364862.html>, abgerufen am 12.12.2018.

8 BMWi, Monitoring-Report Wirtschaft DIGITAL 2018, Kurzfassung, Seiten 5,8,9.

9 Vgl. McKinsey, Banks in the changing world of financial intermediation, <https://www.mckinsey.com/industries/financial-services/our-insights/banks-in-the-changing-world-of-financial-intermediation>, abgerufen am 12.12.2018.

10 Vgl. FAZ, Banken spüren wachsende Konkurrenz aus dem Internet, <http://edition.faz.net/faz-edition/finanzen/2018-11-10/fb7fb16b905ef973ea03ef35e18be74d/?GEP=s1>, abgerufen am 12.12.2018.

11 Wohlfahrt, Welt, <https://www.welt.de/wirtschaft/bilanz/article169443724/Die-sechs-groessten-Irrtuemer-von-Banken.html>, abgerufen am 12.12.2018.

12 Finextra, <https://www.finextra.com/newsarticle/32860/most-banks-will-be-made-irrelevant-by-2030---gartner>, abgerufen am 12.12.2018.

2 Sparkassen und Digitalisierung

2.1 Geschichte

Im Geschäftsmodell der Sparkassen hat Digitalisierung schon seit vielen Jahrzehnten eine wichtige Aufgabe. Denn der Fertigungsprozess im Bankgeschäft besteht „im Wesentlichen aus der Verarbeitung von Informationen.“¹³ In jedem der vier relevanten Subprozesse „Akquisition“, „Vereinbarung von Geschäften“, „Abwicklung von Geschäften“ und „Bereitstellung von Informationen“ spielt Informationstechnologie eine wichtige Rolle.

Viele Jahre blieb die schrittweise Digitalisierung zum Beispiel im Zahlungsverkehr für die Kunden weitgehend unsichtbar. Dies änderte sich 1983 mit der offiziellen Einführung des ersten deutschen Onlinedienstes BTX durch die Deutsche Bundespost. Bereits ab 1984 konnten Kunden bei vielen Sparkassen Bankgeschäfte am Computer von zuhause aus durchführen, Kontostände abrufen oder Überweisungen ausführen.¹⁴ Aber erst mit der Entwicklung des World Wide Web, das den Boom des Internets begründete, gewann das Onlinebanking für Sparkassen und ihre Kunden rasant an Bedeutung.

Ab Mitte der 1990er Jahre waren die Sparkassen mit ersten eigenen Websites und browserbasierten Onlinebanking-Angeboten im Internet vertreten.¹⁵ Zum Start waren dies noch virtuelle Visitenkarten mit reinen Informationsinhalten, die jedoch stetig um Interaktionselemente wie erste Selbstberatungsangebote ergänzt und durch eine Vielzahl weiterer Service- und Transaktionselemente ausgebaut wurden.

Wesentlich für das Geschäftsmodell der Sparkassen war schon immer die Nähe zu ihren Kunden. Mit der Einführung des Giroverkehrs und dem dadurch entstehenden Bedarf an Auszahlungsstellen war das flächendeckende

Filialnetz in den Fünfziger und Sechziger Jahren noch einmal dichter geworden, so dass die Menschen es gewohnt waren, ein umfassendes Beratungsangebot in direkter Nachbarschaft zu finden. Mit dem Internet ergab sich daraus die Anforderung, mit gleicher Qualität Dienstleistungen auch online zu erbringen. Hieraus entstand die Multikanalstrategie der Sparkassen. Kundenwünsche sollten über verschiedene Kanäle auch außerhalb der Filialen und der bereits etablierten Selbstbedienungs (SB)-Bereiche erfüllt werden. Dabei ergänzen das Internet und die Telefonie den Kanal-Mix.

2.2 Aktueller Status der Digitalisierung in der Sparkassen-Finanzgruppe

Heute nutzen fast 19 Millionen Kunden mit über 40 Millionen Konten die Möglichkeit, ihre Bankgeschäfte mit den Sparkassen online zu erledigen. Dabei wird der Zugang über mobile Endgeräte wie Smartphones und Tablets immer wichtiger. Ihr Anteil am Gesamtvolumen aller Transaktionen belief sich 2017 bereits auf über 30 Prozent. Die Websites der Sparkassen verzeichnen pro Jahr 2,5 Milliarden Besucher und gehören damit zu den am stärksten genutzten Internetangeboten in Deutschland.¹⁶

Schon längst beschränken sich die digitalen Angebote nicht nur darauf, Informationen und Services online anzubieten, sondern dienen zunehmend auch als Vertriebskanal für die Vermittlung von Bankprodukten. Eine immer wichtigere Rolle übernehmen die Online-Präsenzen auch als zentrale Anlaufpunkte in der Kundenkommunikation über E-Mail, Audio- und Videochats oder Messenger-Dienste.

Lange Jahre war der Online-Vertrieb ein das Filialgeschäft ergänzender Vertriebsweg, der weitgehend

13 Rebstock/Weber/Daniel, Informationstechnologie in Banken, 2012 und Moormann/Fischer, Handbuch Informationstechnologie in Banken, 1. Aufl. 1999, Seiten 6, 7.

14 Sparkassenhistorisches Dokumentationszentrum des Deutschen Sparkassen- und Giroverbandes, Geschichte der Sparkassen-Finanzgruppe, Seite 5.

15 Kreissparkasse Köln, Technischer Fortschritt, <https://www.ksk-koeln.de/unternehmen/unternehmensprofil/ueberblick-zahlen/innovation-technik-fortschritt.aspx>, abgerufen am 12.12.2018.

16 DSGVO, Rundschreiben Jahreszahlen zu digitalen Kanälen, 2018/151, 2018.



isoliert stattfand. Qualifizierte persönliche Beratung war die Domäne der Berater vor Ort. Erste Versuche einiger Sparkassen mit digitalen Beratungsteams, blieben zunächst eine Ausnahme. Inzwischen steht die Beratung über digitale Kanäle zunehmend im Fokus der weiteren Entwicklungen. Sie ist fester Bestandteil der Vertriebsstrategie der Sparkassen. Kunden sollen alle wichtigen Leistungen in allen Kanälen erhalten und medienbruchfrei zwischen den Zugangswegen wechseln können.

Wir gehen davon aus, dass Beratungskompetenz auch zukünftig ein entscheidender Erfolgsfaktor im Wettbewerb ist. Auch in der digitalen Welt besteht sichtbar Bedarf an qualitativ hochwertiger Beratung von Menschen für Menschen gerade bei komplexen finanziellen Sachverhalten. Deshalb bleibt bei den Sparkassen diese Beratung nicht auf die Filiale begrenzt.

Der Treiber für diese und die weitere Ausrichtung der Sparkassen sind die zunehmenden und rasant steigenden digitalen Bedürfnisse der Kunden. In der Vergangenheit wurde stark auf die technikgetriebene Erweiterung digitaler Lösungen und auf die kostengetriebene Optimierung und Zentralisierung von Prozessen und IT-Infrastruktur gesetzt. Jetzt rückt der Mensch in den Mittelpunkt.

Wir sehen eine klare Wechselwirkung: Aus neuen technischen Möglichkeiten entstehen Neugier und andere

Erwartungen. Verändertes Verhalten wiederum macht immer neue digitale Angebote möglich und nötig. Das gilt beim Konsumieren von Musik oder Videos über Angebote wie Spotify und Netflix anstatt über CDs oder im Fernsehen, beim Einkaufen im Internet oder in der Kommunikation über WhatsApp oder FaceTime. Genauso ändert sich auch die Art und Weise, wie Bankgeschäfte erledigt werden, nämlich zunehmend online. Die Institute werden zwar weiterhin über Filialen physisch präsent sein, aber die Gewichte zwischen den verschiedenen Kanälen verschieben sich.

Die neuen Wettbewerber, zum Beispiel Fintechs und andere Technologieunternehmen, beobachten wir intensiv, analysieren sie bezüglich ihrer Stärken und Leistungsversprechen und leiten daraus Impulse für unsere Maßnahmen ab.

Die Mitarbeiter und Führungskräfte der Sparkassen sind zugleich Adressaten und Mitwirkende unserer Digitalisierungsstrategie. Der technologische Wandel hat unmittelbaren Einfluss auf die zukünftige Arbeitswelt aller Sparkassenmitarbeiter und auf die Arbeitswelt der Berater mit Kunden im Besonderen. Die Vermittlung digitaler Kompetenz ist dabei von besonderer Bedeutung, damit weiter hochqualitative Beratungsleistungen erbracht werden können und Mitarbeiter den digitalen Wandel annehmen.

3 Die Digitale Agenda der Sparkassen-Finanzgruppe – Leitfaden für die Organisation

Die unterschiedlichen Aspekte der Digitalisierung wurden Ende 2016 in der „Digitalen Agenda“ der Sparkassen zusammengefasst. Damit erhielten die Institute eine Orientierung und Hilfeleistung bei der Bewältigung der praktischen Herausforderungen. Erarbeitet wurde die Digitale Agenda von der „Task-Force-Digitalisierung“, an der unterschiedliche Institute und weitere Unternehmen der Sparkassenfinanzgruppe beteiligt waren.¹⁷ Ziel war es, ausgehend von der Ist-Situation „die notwendigen Erweiterungen zu definieren, um die Aufstellung der Organisation gezielt zu verändern oder auszubauen und damit für die Herausforderungen und die Chancen der Digitalisierung gut gerüstet zu sein.“¹⁸

Die Maßnahmen der digitalen Agenda setzen auf dem Selbstverständnis der Sparkassen auf, für ihre Kunden der zentrale Kontaktpunkt für alle Finanzdienstleistungen zu sein. Wesentliches Unterscheidungsmerkmal zum Wettbewerb ist weiterhin die persönliche und regionale Nähe. Die Mitarbeiter werden als Alleinstellungsmerkmal gesehen. Kundenzufriedenheit und Kundenerlebnisse werden durch ein leistungsgerechtes Portfolio verbessert.

Mit der digitalen Agenda wird der Anspruch deutlicher dokumentiert, digitale Lösungen konsequenter auf Kundenbedürfnisse auszurichten. Kunden sollen und können den für sie selbst in der jeweiligen Situation geeigneten Kontaktpunkt wählen. Das zentrale Element dafür ist die Multikanalstrategie. Dabei ist es entscheidend, nicht einfach nur in allen relevanten Vertriebswegen vertreten zu sein, sondern diese auch eng miteinander zu verzahnen. Während das Multikanalangebot der Sparkassen im Privatkundenbereich schon einen guten Reifegrad hat, muss das Angebot für das

Firmenkundengeschäft flächendeckend umgesetzt und auch konzeptionell und funktionell weiter ausgebaut werden.

Abgeleitet aus der Geschäftsstrategie der Sparkassen umfasst die Digitale Agenda auch die Mitarbeiterperspektive und Fragen der betriebswirtschaftlichen Effizienz. Denn ein stetiger und rascher Wandel muss betrieblich leistbar sein, Kompetenzen müssen mitwachsen. Beides soll durch fokussierte Maßnahmen ermöglicht bzw. ausgebaut werden. Marktrelevante digitale Lösungen der Sparkassen-Finanzgruppe sollen künftig schneller definiert, erarbeitet und von Sparkassen eingesetzt werden, damit private Kunden, Firmenkunden und Kommunen in ganz Deutschland diese Lösungen dann auch nutzen können.

Die Digitale Agenda formuliert ein Ambitionsniveau in den folgenden Dimensionen:

Innovation

Die Sparkassen-Finanzgruppe hat den Anspruch gegenüber marktführenden Treibern der Digitalisierung im Finanzdienstleistungsmarkt zumindest fast follower, bei gezielten Themen auch Vorreiter zu sein. Gegenüber dem klassischen Wettbewerb will man regelmäßig Vorreiter sein.

Ökonomie

Die Chancen der Digitalisierung zur Kostensenkung und Ertragssteigerung sowie zur Rationalisierung und Prozessautomation werden konsequent genutzt.

Relevanz

Die Sparkassen sind für ihre Kunden der zentrale Kontaktpunkt für alle Finanzdienstleistungen. Sie nutzen die Digitalisierung, um als attraktive Arbeitgeber Arbeitsplätze in der Region zu sichern. Die digitale Kompetenz wird auch zum Nutzen der kommunalen Träger und der Öffentlichkeit eingesetzt.

¹⁷ An der Erstellung waren Vertreter folgender Institute/Institutionen beteiligt: Förde Sparkasse, Stadtparkasse München, NordLB, BayernLB, Rheinischer Sparkassen- und Giroverband (RSGV), Ostdeutscher Sparkassenverband (OSV), Sparkassenversicherung Baden-Württemberg, Deutscher Sparkassenverlag (DSV-Gruppe), Finanz Informatik (FI) und Deutscher Sparkassen und Giroverband (DSGV).

¹⁸ DSGV, Digitale Agenda, 2017, Zielsetzung, Seite 1.

Weiterhin werden in der digitalen Agenda folgende Grundüberzeugungen als Leitplanken definiert:

- Die Sparkassen verstehen sich weiterhin als Multi-kanalbanken, wir wollen keine (Online-) Direktbank werden.
- Die Mitarbeiter sollen auch in der digitalen Welt relevant bleiben und dort digitale Kompetenz ausstrahlen.
- Neue, relevante und vom Kunden honorierte Wertschöpfungen werden gebraucht.
- Wir bieten allen unseren Kunden bedarfsgerechte und einfache Lösungen an.
- Sparkassen sind eine datennutzende Organisation. Dabei stellen wir den Schutz der Privatsphäre unserer Kunden über die eigenen wirtschaftlichen Interessen.
- Die IT-Sicherheit unserer Systeme hat höchste Priorität.

Um das definierte Ambitionsniveau zu erreichen und die Leitplanken messbar zu machen, wurden in der digitalen Agenda verschiedene Instrumente für die Sparkassen geschaffen. Sie helfen bei der Standortbestimmung und zeigen konkrete Maßnahmen auf, wie die bereits heute zur Verfügung stehenden Digitalisierungskonzepte und -lösungen konsequent genutzt werden können.

Die Digitale Agenda setzt aber auch Impulse,

- wie der Kontakt zum Kunden zukünftig gestaltet wird,
- welche Innovationen dazu nötig sind,
- und wie die Gruppe – auch gemeinsam mit den Kunden – konkurrenzfähige Angebote schneller entwickeln, bereitstellen und diese laufend verbessern kann.

Nachfolgend werden die einzelnen Instrumente näher erläutert.



3.1 Die Kundenperspektive in der digitalen Agenda

3.1.1 Innovationsmanagement und Kundenzentrierung

„Der Kunde ist König“ ist keine Erfindung der Digitalisierung, sondern war schon immer Anspruch erfolgreicher Wirtschaftsunternehmen. Kundenzentrierung hat bei den Sparkassen eine lange Tradition. Im Kern ist das gesamte Geschäftsmodell der Sparkassen kundenzentriert, da dies Auftrag und den Wurzeln der Sparkassen entspricht. Tatsächlich beruht ein wesentlicher Teil der gesellschaftlichen Gestaltungskraft der Digitalisierung darauf, dass sie das Leben der Menschen im Alltag einfacher und bequemer macht und der Nutzen dieser Revolution für den Einzelnen direkt spürbar wird.

In der filialorientierten Welt waren allein die Berater die Mittler und Übersetzer zwischen den Kunden und den unterstützenden IT-Systemen. In der digitalen Welt agieren die Kunden direkt mit der IT. Systeme müssen daher möglichst selbsterklärend, ohne Aufwand und ohne Expertenwissen nutzbar sein. Die Finanzwirtschaft und gerade auch die Sparkassen haben hier zwar aufgeholt. Es ist aber nicht zu leugnen, dass weiterhin Verbesserungsbedarf besteht.

Das bedeutet auch, dass klassische produktzentrierte Vorgehensweisen bei der Entwicklung neuer Angebote nach dem Wasserfallmodell hinterfragt werden müssen. Denn erfolgreiche Digitalunternehmen nehmen in kurzer Folge neue Releases, Updates oder Features in Betrieb. Sie können so in kürzester Zeit auf Kundenreaktionen wiederum selbst reagieren. Da ist es nicht mehr ausreichend, in teilweise mehrjährigen Planungs- und Umsetzungsprozessen neue Produkte in den Markt zu bringen – und darauf zu hoffen, dass die ursprünglich getroffenen Annahmen auch tatsächlich noch stimmen. Dies gilt umso mehr, als sich neue Technologien und Nutzertrends mit hoher Geschwindigkeit weiter entwickeln. Je länger also die Produktionszeiten, desto höher die wirtschaftliche Unsicherheit.

Die Sparkassen-Finanzgruppe begegnet diesen Herausforderungen auf unterschiedlichen Ebenen. Wichtig ist

zunächst ein besseres Wissen über die aktuellen Technologietrends in und außerhalb der Finanzbranche und über die Erfolgsfaktoren erfolgreicher Anbieter. Dazu wurden an verschiedenen Stellen der Finanzgruppe Innovationshubs gegründet. Exemplarisch hierfür steht der von der Finanz Informatik initiierte und getragene S-Hub, der in Hamburg beheimatet ist. Weitere Institutionen wie der Deutschen Sparkassenverband, der Deutsche Sparkassen- und Giroverband (DSGV) und eine Reihe von engagierten Sparkassen unterstützen den S-Hub zusätzlich mit finanziellen Mitteln und Mitarbeitern.

Die Aufgabe des S-Hubs besteht neben dem Erkennen von Trends und dem Bewerten existierender Fintech-Lösungen (Markt-Screening) vor allem darin, mit Kunden gemeinsam neue Produktideen zu entwickeln und Prototypen zu erstellen: sozusagen von Kunden für Kunden.

Hierbei setzt der S-Hub konsequent auf agile Methoden wie den Design-Thinking-Ansatz. In den vergangenen 18 Monaten wurden in product-discoveries mehr als 20 Prototypen entwickelt, von denen einige derzeit zu realen Produkten ausgebaut werden. Ziel ist es dabei, möglichst früh im Entstehungs- und Entwicklungsprozess Kundenfeedback zu bekommen, um so das Risiko zu minimieren, am Kundenbedarf vorbei Produkte zu entwickeln. Anfang 2019 hat der S-Hub für die Sparkassen eine zentrale tester-community gestartet, die das frühzeitige Testen von Prototypen deutlich erweitern wird.

Aber nicht nur in der Phase der Ideengenerierung und Prototypisierung kommen agile Arbeitsweisen zum Einsatz. Auch bei der Weiterentwicklung der Kernsysteme zum Beispiel bei der Internet-Filiale¹⁹ werden Projekte vermehrt mit agilen Elementen zum Beispiel aus SCRUM umgesetzt, soweit dies mit den regulatorisch abgesteckten Rahmenbedingungen vereinbar ist. Auch die Entwicklung und Verprobung dezentraler Innovationsideen durch einzelne Sparkassen ist bewusst erwünscht und wird gefördert.²⁰

¹⁹ Die Internet-Filiale ist der Onlineauftritt der Sparkassen inklusive Online-Banking-Zugang.

²⁰ DSGV, Digitale Agenda, 2017, Seite 15.

Voraussetzungen für die Umsetzung kreativer Innovationen sind dabei immer, dass diese nicht erkennbar Recht, ethische Grundsätze, die Marke, das Selbstverständnis, die Reputation, das Regionalprinzip oder die Geschäftsstrategie der Sparkassen verletzen. Hierfür wurden in der Gruppe gemeinsame Leitlinien entwickelt.

3.1.2 Die Finanzplattform, das digitale Ökosystem der Sparkassen

Mit der Internet-Filiale und der Sparkassen-App verfügen die Sparkassen über Online-Kontaktpunkte, die von 17 Millionen Kunden regelmäßig für die Erledigung ihrer Bankgeschäfte und den Kontakt zu den Sparkassen genutzt werden. Die Sparkassen haben den Anspruch, auch in der Plattformökonomie die direkte Kundenschnittstelle zu behalten bzw. auszubauen und nicht auf den Status eines reinen Infrastrukturdienstleisters etwa für die Angebote von Fintechs zurückzufallen.

Das Girokonto wird deshalb in eine digitale Plattform eingebettet und zum Ökosystem ausgebaut, das das digitale Zuhause aller Nutzer (Privat- und Firmenkunden) für ihre finanziellen Bedürfnisse ist und das Leben einfacher gestalten will. Der Begriff Nutzer wird hier bewusst verwendet, denn diese Plattform steht nicht nur Kunden der Sparkassen-Finanzgruppe offen, sondern perspektivisch auch Kunden anderer Institute. Die Finanzplattform will dabei auch ein regionales und überregionales Serviceangebot außerhalb des Kerngeschäfts bieten.

Die Weiterentwicklung der derzeit bei den Sparkassen im Einsatz befindlichen Internet-Filiale 6 zur Finanzplattform findet iterativ und verstärkt auch mit direkter und ständiger Einbeziehung von Kunden statt. Im August 2018 wurde den Kunden auch dort die Multibankfähigkeit (Multibanking) zur Verfügung gestellt und damit der Grundstein für den weiteren Ausbau der Plattform gelegt.²¹ Denn Kunden können nun auch solche Konten im Onlinebanking der Sparkasse verwalten, die sie nicht bei der Sparkasse führen. Im Dezember 2018 wurde die Multibankfähigkeit um schreibende Geschäftsvorfälle wie

21 In der Sparkassen-app ist die Multibankfähigkeit seit der ersten Version fester Funktionsbestandteil.

Überweisung und Daueraufträge, sowie um erste Funktionalitäten eines persönlichen Finanz-Managements erweitert. Im ersten Halbjahr 2019 werden zudem erste Komponenten aus Kooperationen mit Fintechs flächendeckend von Sparkassen in ihre Onlineauftritte integriert.

Neben dem eigenen Ökosystem wollen die Sparkassen auch in den Ökosystemen anderer Anbieter erlebbar sein. Dafür gibt es bereits umgesetzte Beispiele, zum Beispiel die Einbindung der Filial- und Geldautomatenadressen der Sparkassen in Google Maps und andere Navigationssysteme, oder die Platzierung von Immobilienangeboten in den großen Internetportalen.

3.1.3 API²²-Strategie der Sparkassen-Finanzgruppe

Mit dem Home Banking Interface (HBCI) bzw. dessen Weiterentwicklung, den Financial Transaction Services (FinTS), verfügt die deutsche Kreditwirtschaft bereits seit 1996 über leistungsfähige Schnittstellen. Hierüber können primär Privatkunden mit Drittanbieterprodukten auf ihre Bankdaten zugreifen. Über diese Schnittstellen kann vor allem auch die Multibankfähigkeit hergestellt werden.²³

Der Funktionsumfang von FinTS wurde über die Jahre immer weiter ausgebaut. Die fachlichen Spezifikationen decken inzwischen mehr als 130 Geschäftsvorfälle aus allen Bereichen ab.²⁴ Auch für das Geschäft mit Firmenkunden existiert eine Reihe von Schnittstellenstandards, von denen der bekannteste der Electronic Banking Internet Communication Standard (EBICS) ist. Es hatte 2008 das bis dahin gebräuchliche File Transfer, Access and Management (FTAM) Protokoll abgelöst.²⁵

22 Application-Program-Interfaces (API), zu deutsch Programmierschnittstellen, ermöglichen die Anbindung von Software an bestehende Systeme durch Nutzung auf freigegebene Funktionen, Content oder sonstige Daten. Vgl. z.B. EBA Working Group on Electronic Alternative Payments, Understanding the business relevance of open APIs and Open Banking for Banks, Version 1, May 2016, Seite 7.

23 FinTS, <https://www.hbci-zka.de>, abgerufen am 12.12.2018.

24 FinTS, <https://die-dk.de/zahlungsverkehr/electronic-banking/fints/>, abgerufen am 12.12.2018.

25 DFÜ-Verfahren EBICS, <https://die-dk.de/zahlungsverkehr/electronic-banking/dfu-verfahren-ebics/>, abgerufen am 12.12.2018.



Während in der Vergangenheit vor allem klassische Bankingsoftware-Produkte diese Schnittstellen nutzen, so wird FinTS heute im Sparkassenbereich vor allem von Smartphone-Apps für iOS²⁶ oder Android²⁷ Geräten verwendet, um hierüber Kunden mobiles Banking zu ermöglichen. Gerade mobiles Banking gewinnt immer mehr an Bedeutung. So nutzen bereits mehr als 30 Prozent der Onlinebanking-Kunden der Sparkassen den Zugang zum Konto regelmäßig über ihr Smartphone. Daneben wurde und wird die FinTS-Schnittstelle aber immer mehr auch von Internetunternehmen oder Drittdiensten verwendet, um darauf aufbauend ihre Leistungen anbringen zu können.

Mit der Zweiten Zahlungsdiensterichtlinie (Payment Service Directive II – PSD 2) ergeben sich für die Sparkassen neue Herausforderungen und Anforderungen sowohl in der Beziehung zu den Kunden (und dort vor allem im Zugang zum Onlinebanking) als auch in der Beziehung zu Wettbewerbern wie Fintechs und vor allem zu internationalen Tech-Giganten. Aus Sicht der Sparkassen liefert die PSD 2 aber auch einen wichtigen Beitrag zur Rechtsicherheit, weil sie festlegt, wie Dritte auf Onlinebankingdaten zugreifen können. Dasselbe gilt für die Anfang 2018 von der Europäischen Kommission veröffentlichten „Regulatory Technical Standards on Strong Customer Authentication and common Secure Communication (RTS)“. Die RTS konkretisieren die

Anforderungen der PSD 2. Beide Regelwerke stellen klar, dass screen-scraping²⁸ verboten ist. Dadurch und durch die Vorgaben zur starken Kundenauthentifizierung (SCA) leisten sie einen wichtigen Beitrag zur Sicherheit von Onlinetransaktionen. Gleichzeitig trägt die PSD 2 mit den definierten Ausnahmeregeln von der SCA dem Bedürfnis vieler Kunden nach einer gesteigerten Nutzerfreundlichkeit Rechnung.

Die Sparkassen begreifen die PSD 2 deshalb auch als Chance, ihre digitalen Dienstleistungen über ihr Online-Angebot kundenfokussiert aufzuwerten. Die Einführung des Multibanking in der Finanzplattform der Institute ist hier ein erster Schritt. Die gesetzlich festgelegte Verpflichtung zur Öffnung von Schnittstellen auch für andere Branchen (zum Beispiel für Technologie-Konzerne) wäre ein wichtiger Schritt zur Gleichbehandlung.

Die Sparkassen-Finanzgruppe hat bereits von Beginn an aktiv an der Schaffung der PSD-Schnittstellen mitgewirkt, indem sie die Entwicklung der NextGenPSD2-API der europäischen Standardisierungsinitiative Berlin Group maßgeblich begleitet hat.²⁹ Die Spezifikationen setzen einen länderübergreifenden Standard für eine

26 Betriebssystem des Unternehmens Apple für deren mobile Geräte (Iphone und Ipad).

27 Betriebssystem des Unternehmens Google für mobile Geräte.

28 Press release European Commission, Payment Services Directive (PSD2), Regulatory Technical Standards (RTS) enabling consumers to benefit from safer and more innovative electronic payment , http://europa.eu/rapid/press-release_MEMO-17-4961_en.htm, abgerufen am 12.12.2018.

29 Pressemeldung Berlin Group, PSD2 Access to Bank Accounts, <https://www.berlin-group.org/psd2-access-to-bank-accounts>, abgerufen am 12.12.2018.

Schnittstelle um, die die Vorgaben der PSD 2 erfüllt und den Datenaustausch mit Kontoinformationsdienstleistern, Zahlungsauslösedienstleistern und Drittkartene-mittenten gesetzeskonform ermöglicht. Die ersten Tests werden, wie rechtlich vorgegeben,³⁰ ab dem 14. März 2019 ermöglicht. Der Live-Betrieb ist ab dem 14. September 2019 geplant.

Neben den rechtlich vorgegebenen Schnittstellen aus der PSD 2 und der etablierten FinTS-Infrastruktur arbeitet die Sparkassen-Finanzgruppe an einer umfassenden API-Infrastruktur für alle Anwendungsbereiche.

Bereits heute ermöglicht das Kernbankensystem der Sparkassen, One-System-Plus (OSPlus) eine Reihe von Möglichkeiten zur Integration solcher Angebote zum Beispiel durch Single-Sign-On-Mechanismen und den Zugriff auf bankfachliche Prozesse und Daten. Die künftige API-Infrastruktur wird neben öffentlichen

Schnittstellen, die frei genutzt werden können, auch weiterhin private APIs anbieten, die nach definierten Rahmenbedingungen zertifizierten Vertragspartnern zur Verfügung gestellt werden könnten.

Die vertraglichen, inhaltlichen und technischen Rahmenbedingungen für den künftigen Zugang zur API-Infrastruktur werden derzeit unter Einbeziehung verschiedener Interessengruppen definiert. Dies könnte zu einer schnelleren Integration von Marktlösungen beitragen. Es wäre damit aber auch leichter, marktfähige Prototypen außerhalb der traditionellen Entwicklungszyklen des zentralen Rechenzentrums in kurzer Taktung zu entwickeln. Produktinnovationen in Form von MVP³¹, die gleichwohl den rechtlichen und regulatorischen Anforderungen genügen, könnten so möglichst schnell auf Kundenakzeptanz getestet, in einzelnen Sparkassen verprobt und bei Erfolg flächendeckend in der Gruppe eingeführt werden.

30 EBA, Payment services and electronic money, <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money>, abgerufen am 12.12.2018.

31 „MVP“ = Minimum viable Product bedeutet, erste minimal funktionsfähige Iteration eines Produkts, das entwickelt werden muss, um mit minimalem Aufwand den Kunden-, Markt- oder Funktionsbedarf zu decken und handlungsrelevantes Feedback zu gewährleisten.



3.1.4 Fintechs – Partner oder Konkurrenten?

In den vergangenen Jahren sind auf dem Markt der Finanzdienstleistungen viele neue Anbieter aufgetreten, die über das Internet Finanzdienstleistungen anbieten. Diese von den Medien oftmals als Fintechs bezeichneten Unternehmen, bei denen es sich oftmals um Startups handelt, haben deutlich an Bedeutung zugenommen.³²

Typisch für Fintechs ist vor allem ihre hohe Technologiekompetenz. Gezielt lösen sie einzelne Prozesse aus der Wertschöpfungskette der traditionellen Kreditinstitute heraus und optimieren diese für die digitale Welt. Dazu wählen sie von vornherein eine andere Vorgehensweise, als es bestehende Finanzdienstleister bislang taten.

Fintechs haben den Anspruch, sich bei der Entwicklung digitaler Lösungen maximal an den Kundenbedürfnissen auszurichten und diese in jeder Phase der Entwicklung einzubeziehen. Sie arbeiten dabei automatisch mit kurz getakteten Entwicklungszyklen, um Fehl- oder Neuentwicklungen schnell erkennen und umsteuern zu können. Damit unterscheiden sie sich in ihrer Vorgehensweise deutlich von den klassischen Entwicklungsverfahren, die die Sparkassen typischerweise verwenden. Im Ergebnis sind Fintechs oftmals schneller mit digitalen Lösungen am Markt. In Einzelfällen ist aber auch eine höhere rechtliche und, damit verbunden, auch eine höhere wirtschaftliche Risikobereitschaft zu beobachten (zum Beispiel bei der Geldwäsche-Prüfung).

Die Sparkassen nehmen für sich in Anspruch, schon immer ein kundenorientiertes Geschäftsmodell zu haben, mitunter sieht man dies aber nicht jeder technischen Lösung an. Sie haben schon früh die neue Konkurrenz durch Fintechs erkannt. Die erste Phase des Gegeneinanders, die vor allem in der Fachöffentlichkeit hochstilisiert

wurde, ist allerdings längst vorbei. Tatsächlich sehen wir viele Ansätze dafür, wie beide Seiten voneinander profitieren können: Fintechs punkten mit ihrer unzweifelhaft gegebenen Digitalkompetenz, die sich in kurzem time to market und der oft hohen Qualität der Kunden-Front-Ends zeigt. Kreditinstitute bringen neben ihrer großen Kundenbasis und den langjährigen Kundenbeziehungen die persönliche Nähe und hohe Qualität im Beratungsprozess, gut funktionierende und skalierende Supportstrukturen sowie eine ausgeprägte regulatorische Kompetenz ein.

Bei der Zusammenarbeit zwischen Sparkassen und Fintechs nimmt der unter der Überschrift „Innovationsmanagement und Kundenzentrierung“ (siehe Seite 75) beschriebene Innovationshub eine wichtige Rolle ein. Der Hub nutzt dabei die gleichen Vorgehensweisen wie Digitalunternehmen zur gemeinsamen Erarbeitung von Produktideen mit Kunden. Sie laden hierzu auch gezielt im Rahmen von Trendscoutings ausgewählte Fintechs ein, ihre Expertise und Lösungen einzubringen. Hieraus sind bereits erste Kooperationen entstanden. Mehr als 230 Sparkassen nutzen beispielsweise die Videolegitimation als Prozess erleichterung etwa im Kontoeröffnungsprozess und setzen dabei auf bewährte Lösungen von Fintechs. Auch für den Kontoumzug haben die Institute externe Lösungen integriert.

Die partnerschaftliche Zusammenarbeit mit Fintechs wollen die Sparkassen weiter ausbauen. Beispielsweise durch ihre Mitarbeit im Fintech-Rat der Bundesregierung oder als Fördermitglied im Bundesverband Deutsche Startups.

Zur Sicherung der partnerschaftlichen Zusammenarbeit in der Zukunft sehen die Sparkassen die Notwendigkeit für eine europäische Standardisierung auf Basis gesetzlicher Vorgaben, für die im Moment noch das gemeinsame Verständnis fehlt. Insbesondere kann die Entwicklung und Nutzung von Schnittstellen zu Konten- und Bankdaten nur dann ausreichend vorangebracht werden, wenn das rechtliche Umfeld eine Refinanzierung der notwendigen Infrastrukturen durch deren Mit-Nutzer möglich macht.

³² Der Begriff Fintech wird in diesem Zusammenhang nicht einheitlich verwendet. Das Europäische Parlament, die Europäische Kommission und die European Banking Authority verstehen darunter neue Vertriebswege und Produkte in der Finanzwirtschaft. Deshalb beziehen sie Startups und etablierte Institute in ihre Überlegungen mit ein. (European Parliament's report on FinTech, April 2017; EU-KOM Fintech Action Plan März 2018; EBA Fintech Road Map FAQ, März 2018).

3.2 Die Sparkassenperspektive in der digitalen Agenda

Neben der Kundenperspektive konzentriert sich die Digitale Agenda auf die digitale Fitness der Sparkassen. Hierfür stellt sie verschiedene Instrumente bereit, die der Sparkasse zunächst dabei helfen sollen, ihren Status Quo zu erfassen – um sie dann dabei zu unterstützen, sich weiter zu verbessern.

Nachfolgend werden diese Instrumente vorgestellt.

- Digitale Mindeststandards – Wo steht die Sparkasse im Vergleich zum Durchschnitt der Gruppe?
- Digitalisierungskompass – Digitales Nachschlagewerk für Sparkassen, das konkrete und institutsindividuelle Handlungsempfehlungen gibt.
- Evidenzstelle – Zentrales Informationsangebot für den Austausch von digitalen Ideen und Innovationen

3.2.1 Digitale Mindeststandards

In den Digitalen Mindeststandards ist festgehalten, welche tatsächliche Nutzung digitaler Lösungen in den Dimensionen Kunden, Sparkasse und Mitarbeiter von den Instituten erwartet wird. Die hierfür definierten Messkriterien sind so formuliert, dass sie mit zentral bereitgestellten Lösungen und Unterstützungsmaßnahmen erreicht werden können. Der Durchschnitt des erreichten Digitalisierungsgrads aller Sparkassen ergibt den Mindeststandard. Der Standard ist also keine feste Größe, sondern er wächst mit.

Die Mindeststandards werden einmal jährlich ermittelt. Was heute Durchschnitt ist, gilt dann morgen als Mindest-Soll. Damit wird eine fortlaufende dynamische Entwicklung des Niveaus im Konsens sichergestellt.

3.2.2 Digitalisierungskompass

Jede Sparkasse kann auf Basis der eigenen erreichten Werte bei den Mindeststandards festlegen, ob und wenn ja, in welchen Aspekten sie sich im Thema Digitalisierung

weiterentwickeln will. Das Instrument Digitalisierungskompass zeigt dabei für den konkreten Handlungsbedarf mögliche Lösungsansätze auf. Der Digitalisierungskompass ist als digitales Nachschlagewerk gestaltet, der die Sparkassen auch im Veränderungsprozess und Kulturwandel zur Digitalisierung unterstützt.

3.2.3 Evidenzstelle

Mit der Evidenzstelle wurde ein webbasiertes Informationsangebot geschaffen, das den Sparkassen einen zentralen Überblick über die bestehenden, verfügbaren oder in Entwicklung befindlichen Innovationsideen und vorhandenen digitalen Lösungen der Sparkassen-Finanzgruppe und ihrer Dienstleister liefert. Dies schließt ausdrücklich Lösungen ein, die einzelne Institute in eigener Initiative gefunden haben oder mit anderen weiterentwickeln möchten.

Die Evidenzstelle funktioniert als Plattform. Sie soll Ideengeber, mögliche Investoren und Umsetzer zusammenbringen und dadurch die Entwicklung weiterer Investitionen unterstützen. Gleichzeitig entsteht Evidenz darüber, was es schon gibt. Das soll helfen, Parallelentwicklungen in der Gruppe möglichst zu vermeiden.

Nutzer der Evidenzstelle können ihre Projektvorhaben auch überprüfen lassen – etwa hinsichtlich rechtlicher und Markenfragen sowie bezüglich regulatorischer Rahmenbedingungen.

3.2.4 Digitale Mitarbeiterkompetenz

Die fortschreitende Digitalisierung wird die Arbeitswelt und damit das Arbeitsumfeld der Mitarbeiter in Sparkassen substantiell verändern. Die Sparkassen sehen auch in der zukünftigen digitalen Welt einen Bedarf für hochqualifizierte persönliche Beratung, während reine Service-tätigkeiten zunehmend durch automatisierte Prozesse abgelöst werden könnten. Auch hier gilt: Die Kunden entscheiden, welche Dienstleistungen sie mit welchen Leistungsmerkmalen auf welchem Weg nutzen wollen.

Um in dieser Veränderung erfolgreich zu sein, müssen die Mitarbeiter und Führungskräfte der Sparkassen auch digitale Kompetenz aufbauen. Das umfasst neben einem



selbstverständlichen Umgang mit den Sparkassen-eigenen Digitalangeboten auch eine stärkere Bereitschaft zu ständiger Veränderung. Daher sind die Fortbildung von Mitarbeitern und der offene Umgang mit den notwendigen Veränderungen erfolgsentscheidend.

Die Sparkassen-Finanzgruppe adressiert den notwendigen Kulturwandel durch eine Reihe von Maßnahmen auf zentraler und dezentraler Ebene. Der Status Quo der digitalen Kompetenz wird durch die Mitarbeiterperspektive in den Digitalen Mindeststandards (siehe 3.2.1, Seite 80) sichtbar gemacht.

Beschäftigte werden durch eine Reihe von Schulungsmaßnahmen weiter qualifiziert. Bei Neueinstellungen und bei der Auswahl von Nachwuchskräften gewinnen die digitalen Fähigkeiten von Bewerbern an Gewicht. Die gruppeneigenen Ausbildungskonzepte und Schulungsangebote werden immer stärker digitalisiert und den Mitarbeitern über elektronische Medien zum Beispiel auf Tablets zugänglich gemacht. Besondere Bedeutung hat für die Sparkassen auch die Reform des Berufsbildes Bankkaufmann/-frau.³³

³³ DSGVO, Finanzbericht 2017, Seite 199.

3.2.5 Automatisierung

Ein weiterer wichtiger Aspekt der Digitalisierung sind die Automation von Prozess- und Entscheidungsschritten und, damit verbunden, die Reduktion notwendiger manueller Aktivitäten von Mitarbeitern und Kunden.

Die Vorteile der Automatisierung liegen auf der Hand. Prozesse laufen kundenorientierter, schneller, weniger fehleranfällig und kosteneffizienter. Banken und Sparkassen hinken hier anderen Branchen noch hinterher. In den vergangenen Jahren haben die Sparkassen bzw. ihr zentraler Dienstleister die Finanzinformatik die Prozessautomation gezielt ausgebaut, sowohl für den Bereich interner Prozesse als auch mit Blick auf direkt von Kunden über die Internetplattformen ausgelöste Geschäftsvorfälle. Ziel ist es, möglichst viele komplett fallabschließende und damit medienbruchfreie Geschäftsvorfälle umzusetzen bzw. Prozesse durch Automatisierung bestmöglich zu verschlanken. In diesem Sinne werden weitere Anstrengungen unternommen und neue Technologien wie zum Beispiel Robotic-Process-Automation (RPA) genutzt. Im laufenden DSGVO-Projekt „Betriebsstrategie der Zukunft“ ist es das Ziel, den Verwaltungsaufwand der Sparkassen unter anderem durch intensivere Nutzung und gezielte Neuentwicklung geeigneter Automatisierungsmaßnahmen spürbar zu verringern.

4 Vertrauen in der digitalen Welt – Cybersicherheit als Wettbewerbsfaktor

Mit zunehmender Digitalisierung wird die Widerstandsfähigkeit gegenüber Cyberrisiken (Cyber-Resilience) immer wichtiger. Cyberrisiken gehören inzwischen zu den Top-Geschäftsrisiken.

Die Internet-Filiale der Sparkassen, das Onlinebanking und die Sparkassen-Apps zählen aufgrund ihrer hohen Kundenakzeptanz und Nutzungsintensität zu den attraktivsten Hacker/Cybercrime-Angriffszielen in Deutschland. Im ersten Halbjahr 2018 waren insgesamt 12.000 Meldungen zu Cyberattacken zu verzeichnen, mitunter 1.000 pro Woche.

Die Sicherheit der für die Digitalisierung eingesetzten IT-Systeme ist deshalb für die Sparkassen von höchster Priorität und ein entscheidender Wettbewerbsfaktor. Die Kunden vertrauen den Sparkassen, mit ihren Daten und letztlich mit ihrem Geld nicht nur sorgfältig umzugehen, sondern diese auch vor dem unberechtigten Zugriff Dritter zu schützen. Cybersicherheit trägt wesentlich zu diesem Vertrauen bei.

Die Sparkassen-Finanzgruppe stellt sich der Herausforderung, die operativen, technischen, finanziellen und reputationsrelevanten Aspekte von Cyberrisiken in ihrem Risikomanagement adäquat sicherzustellen. In den vergangenen Jahren sind umfassende organisatorische Maßnahmen umgesetzt sowie erhebliche Investitionen getätigt worden, um zum Beispiel die mehrstufige Sicherheitsarchitektur der Finanz Informatik sowie die Informationssicherheitssysteme und -prozesse der Sparkassen kontinuierlich weiter zu entwickeln.

Cybersicherheit ist eine essentielle Querschnittsdisziplin und integraler Bestandteil der Strategien der Sparkassen-Finanzgruppe. Nicht zuletzt über den „Sicheren IT-Betrieb“ (SITB) sind die eigenen Maßnahmen der Sparkassen für eine hohe Vertraulichkeit, Integrität und Sicherheit von Daten und Prozessen, mit den Vorkehrungen für eine hohe Verfügbarkeit und Ausfallsicherheit von Systemen und den Informationssicherheitssystemen der zentralen Dienstleister abgestimmt.





Cybersicherheit bedeutet aber auch, mit Partnern, Marktakteuren und Netzwerken zusammen zu arbeiten, die sich für mehr Sicherheit im Internet einsetzen. Deshalb arbeitet das zentrale Cyber-Abwehrteam der Sparkassen-Finanzgruppe sehr eng mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und anderen staatlichen Institutionen zusammen, um Cyberbedrohungen präventiv entgegenzuwirken. Im Jahr 2017 hat das zentrale Cyber-Abwehrteam 170.000 Hinweise zu gefährlichen Schadprogrammen, Trojanern und Phishing-Seiten an Anti-Viren-Hersteller übermittelt und so die Schutzwirkung der von vielen Sparkassen und deren Kunden eingesetzten Anti-Viren-Systeme verbessert.

Entsprechend der wachsenden Cyberbedrohungslage haben Gesetzgeber und Aufsichten die Anforderungen an Informationssicherheitsrichtlinien und Informationssicherheitsprozesse von Banken und Sparkassen kontinuierlich angepasst und konkretisiert. Die PSD 2, die vorrangig durch das Zahlungsdienstenaufsichtsgesetz (ZAG) abgebildet wird und die Mindestanforderungen an das Risikomanagement (MaRisk) der BaFin – ergänzt um das Rundschreiben 10/2017 (BA) „Bankaufsichtliche Anforderungen an die IT (BAIT)“ – sind hier maßgeblich.

Die Sparkassen-Finanzgruppe folgt der ISO27xxx-Reihe von Standards zur Informationssicherheit. Darüber

hinaus werden all diese gesetzlichen und regulatorischen Vorgaben für die Informationssicherheit und für ein standardbasiertes Informationssicherheits-Managementsystem für die Institute der Sparkassenfinanzgruppe mit dem „Sicheren IT-Betrieb“ verbindlich abgebildet.

Zur Umsetzung dieser gesetzlichen und regulatorischen Vorgaben ist eine Vielzahl von Maßnahmen erforderlich. Das zentrale Cyber-Abwehrteam der Sparkassen-Finanzgruppe unterstützt die Sparkassen und Landesbanken bei der Umsetzung. Das Cyber-Abwehrteam umfasst eine Meldestelle, die Hinweise zu Cyberattacken entgegennimmt, ein Lagezentrum, das die Auswirkungen der Attacken übergreifend darstellt, sowie eine spezielle Abweereinheit, die den Angriffen entgegenwirkt. Ergänzend hierzu wurde ein zentrales Betrugsabwehrteam für die Institute der Sparkassen-Finanzgruppe in der Finanzinformatik etabliert.

Die Sparkassen-Finanzgruppe geht für 2019 von einer vergleichbaren hohen Zahl von Cyberangriffen aus. Es ist auch damit zu rechnen, dass im Zuge der PSD 2 mehr Kontenzugriffe (Access to Account) durch Drittparteien (Kontoinformationsdienste beziehungsweise Zahlungsauslösedienste) erfolgen und damit auch die Zahl der Angriffe und Betrugsversuche durch gezielte Phishing- und Social Engineering-Attacken steigen wird.

5 Neue Geschäftsmodelle für die Sparkassen-Finanzgruppe

Aktuell sind vor allem BigData und künstliche Intelligenz und Blockchain Gegenstand intensiver Diskussionen und Analysen, wenn es um die Betrachtung neuer Geschäftsfelder für die Finanzwirtschaft geht.

5.1 BigData/Künstliche Intelligenz (BDAI)

BigData und künstliche Intelligenz (Artificial Intelligence – AI) – sind entscheidende Technologien in der Digitalisierung, weil sie zwei wesentliche Erwartungen an den Nutzen des digitalen Wandels einlösen helfen: Sie erhöhen die Geschwindigkeit, mit der Anfragen und Aufträge erledigt werden können. Und mit ihnen lassen sich interne Prozesse, Prüfungen und Bewertungen optimieren. Es wird allgemein davon ausgegangen, dass BDAI einen wesentlichen Beitrag dazu leisten kann, Wertschöpfungsketten massiv zu verändern und wesentliche Effizienzsteigerungen zu erreichen.³⁴

Die kundenorientierte Nutzung von Daten prägt und verändert die Finanzdienstleistung. Die Sparkassen haben hier eine starke Ausgangsbasis. Mit Daten von mehr als 50 Millionen Kunden verfügen sie über einen großen Datenschatz. Datenanalysen („Sparkassen Data Analytics“ – SDA) und datenbasierte Anwendungsfälle machen es ihnen möglich, Kundenbedürfnisse und Verhaltensmuster besser zu verstehen. Darauf aufbauend können Services und Mehrwerte für die Kunden zum Beispiel durch individuelle Beratungsansätze verbessert oder sogar erst ermöglicht werden. Eine weitere Ausbaustufe ist die next best action, mit der den Kunden in jeder Situation und auf jedem Kanal zur richtigen Zeit genau die Lösung angeboten werden kann, die ihrem Bedarf entspricht.

Dabei achtet die Sparkassen-Finanzgruppe mit ihren Datenanalyseverfahren strengstens darauf, nur auf die

innerhalb der rechtlichen Grenzen nutzbaren Daten zuzugreifen, zu deren Nutzung die Kunden in Form der bewusst ausführlichen Einwilligungserklärung auch explizit zugestimmt haben. Beides leitet die Strategie der Institute: die gesetzlichen und aufsichtsrechtlichen Anforderungen, insbesondere die Datenschutz-Grundverordnung (DSGVO) einzuhalten, und die Interessen der Kunden beim Umgang mit ihren Daten zu wahren. Die schon jetzt hohe Zustimmungsquote von 30 Prozent zeigt das den Sparkassen entgegengebrachte Vertrauen.

In der Vergangenheit wurden Daten mit klassischen statistischen Verfahren (zum Beispiel multivariate Analysen) ausgewertet, um etwa mit Score-Karten Ausfallwahrscheinlichkeiten oder Produktaffinitäten zu ermitteln. In den vergangenen Jahren ist die Rechenleistungsfähigkeit der IT-Systeme stark gestiegen. Damit gewinnen auch Systeme und Verfahren an Bedeutung, die auf künstlicher Intelligenz aufsetzen.

Neue Algorithmen und Machine Learning sollen dabei nicht nur eine automatische und ständige Optimierung von bestehenden Verfahren bieten, sondern darüber hinaus auch ganz neue Anwendungsfälle und Einsatzgebiete erschließen. Voraussetzung hierfür ist sowohl das Training mit bestehenden Daten als auch die Schaffung von kontinuierlichen Kreisläufen. In diesen closed loops werden die Ergebnisse von Auswertungen und die tatsächlich eingetretenen Ereignisse in das System zurückgegeben, um es über diesen Abgleich treffsicherer zu machen.

Die Sparkassen-Finanzgruppe beschäftigt sich in verschiedenen Feldern mit dem Thema künstliche Intelligenz. So sind insbesondere auch in Bereichen wie der Cybersicherheit heute schon neuronale Netze im Einsatz, um Schäden abzuwenden oder zu minimieren. Auch in der Automatisierung von Geschäftsprozessen zum Beispiel bei der Erkennung und Zuordnung eingehender Korrespondenz über unterschiedliche Kanäle sehen wir Anwendungsfälle, die in Projekten verprobt werden. Im direkten Kundenkontakt werden ebenfalls erste Erfahrungen mit Bots und Voice Services gesammelt. So setzen erste Sparkassen Chatbot-Systeme ein, die nicht nur Kundenfragen zu Standardproblemen beantworten,

³⁴ BaFin, Big Data trifft auf künstliche Intelligenz – Herausforderungen und Implikationen für Aufsicht und Regulierung von Finanzdienstleistungen, Seite 66ff.



sondern sich auf Basis der durchgeführten Dialoge auch selbständig optimieren.³⁵

Aktuell erarbeitet der DSGVO für die Sparkassen-Finanzgruppe eine umfassende Strategie zur künstlichen Intelligenz, die neben der rechtlichen und wirtschaftlichen Betrachtung auch ethische Grundsätze behandeln wird und damit der Gruppe eine Orientierung für das Themenspektrum geben soll.

Der DSGVO hat sich zudem intensiv mit der BaFin-Studie „BigData trifft auf künstliche Intelligenz – Herausforderungen und Implikationen für Aufsicht und Regulierung von Finanzdienstleistungen“ auseinandergesetzt und sich aktiv im Rahmen der durchgeführten Konsultation an dem von der BaFin gestarteten Dialog beteiligt.³⁶

Mit Blick auf die vielfältigen Anwendungsgebiete und die aktuell erkennbaren neuen Geschäftsmodelle zum Beispiel im Umfeld von Bonitätsbewertungen,

Sentiment-Analysen und automatisierter Kundenansprache sieht die Sparkassen-Finanzgruppe neben den großen Chancen auch die Notwendigkeit, eventuelle Risiken konzeptionell zu beobachten, zu analysieren und sie zeitnah in das regulatorische System einzubinden. Dabei halten wir es in diesem Kontext für sinnvoll, dass auf Basis von BDAI entstehende Geschäftsmodelle und Unternehmen nach dem Grundsatz „Gleiche Regeln für gleiche Risiken“ behandelt werden und damit aus Gründen der Wettbewerbsgleichheit wie auch des Verbraucherschutzes eine uneingeschränkte Gleichbehandlung erfolgt.

5.2 Blockchain

Die Blockchain und insbesondere die Distributed-Ledger-Technologie haben das Potenzial, ein digital noch stärker vernetztes, globales Ökosystem hervorzubringen. Schon jetzt bricht die Digitalisierung einste feste System- und Prozessgrenzen auf und dezentralisiert Wertschöpfungsketten. Blockchain und Distributed Ledger können dies noch deutlich verstärken und so die Entwicklung neuer dynamischer und digitaler Wertschöpfungsnetzwerke (Öko-Systeme) befördern.

Die Entwicklungen im Bereich der Blockchain-Technologien und -Anwendungen haben sich im Jahr 2017

³⁵ IT-Finanzmagazin, Berliner Sparkasse setzt Beta-Version des KT-Chatbot „fred knows“ ein; nun sei er allgemein verfügbar, <https://www.it-finanzmagazin.de/berliner-sparkasse-ki-chatbot-64861/>, abgerufen am 12.12.2018.

³⁶ BaFin, Konsultation des BDAI-Berichts, www.bafin.de/dok/11137698, abgerufen am 12.12.2018.

deutlich intensiviert. Neue Blockchain-basierte Geschäftsmodelle, Anwendungen und Konsortien entstehen aktuell mit hoher Dynamik. Immer mehr Banken und Versicherungen erkennen konkrete Potenziale dieser Technologie und investieren in entsprechende Projekte oder beteiligen sich an Konsortien. Die Kombination privater bzw. konsortialer Blockchains mit dem Konzept der Smart Contracts stehen hierbei besonders im Fokus.

In der Sparkassen-Finanzgruppe sind seit dem Jahr 2015 eine Reihe von Initiativen gestartet worden, um den Stellenwert der Blockchain zu evaluieren und prototypische Blockchain-basierte Geschäftsmodelle und Anwendungen auf ihre Eignung hin zu testen. Ein Beispiel ist der Aufbau einer Blockchain-basierten Plattform für Schuldschein-Emissionen durch die Landesbank Baden-Württemberg (LBBW) in den Jahren 2017 (Daimler) und 2018 (Telefonica Deutschland).

Blockchain-basierte Schuldschein-Emissionen ermöglichen in Echtzeit unmittelbare, sichere und nachvollziehbare Finanztransaktionen, da die Aktualisierung von Datensätzen nur im Konsens erfolgt. Die dezentrale Speicherung der Datenblöcke sowie die kryptografische Signierung machen die Transaktionsprozesse transparenter, sicherer und effizienter. Allerdings zeigen diese Beispiele auch die aktuellen rechtlichen Restriktionen auf, um Blockchain-Schuldschein-Transaktionen als wirkliche Option für die Unternehmensfinanzierung zu etablieren. Dafür müsste die Möglichkeit der Verbriefung von Schuldverschreibungen mittels digitaler Urkunden rechtlich einwandfrei bestätigt sein. Bei den aktuellen Blockchain-basierten Schuldschein-Transaktionen wurde daher auch aus Gründen des sogenannten Skripturprinzips zur rechtskonformen Abbildung der Anleihebedingungen parallel der konventionelle Emissionsweg beschritten.

Nach der Abwicklung dieser Schuldschein-Transaktionen über die Blockchain-Technologie haben LBBW und die Börse Stuttgart unter der Marke „Debtvision“ einen Marktplatz zur vollständigen Digitalisierung des Schuldscheinprozesses gegründet. Zahlreiche institutionelle Investoren, wie Sparkassen, Banken, Versicherungen und Pensionskassen haben sich bereits an die Plattform angeschlossen. In den nächsten Monaten soll die

Blockchain in die Plattform eingegliedert und damit die komplette Wertschöpfungskette auf diese innovative Technologie übertragen werden.

Die NordLB hat im Jahr 2017 gemeinsam mit der Fraunhofer Gesellschaft einen Blockchain-Prototyp zur Prozessoptimierung für Dokumentenakkreditive entwickelt. Sie hat sich im September 2018 an JP Morgans „Interbank Information Network“ (IIN) angeschlossen. IIN basiert auf der Blockchain-Datenbank „Quorum®“ von JP Morgan und ist speziell auf den internationalen Zahlungsverkehr ausgerichtet.

Im Jahr 2018 startete darüber hinaus eine institutsübergreifende Initiative mit BayernLB, Helaba, LBBW und S-Servicepartner Berlin, um eine Blockchain-basierte Plattform für die Institute der Sparkassen-Finanzgruppe zu etablieren, auf dessen Basis Handels-/ Finanzierungsprozesse sowie alternative Finanzprodukte im Bereich Trade Finance innovativ digitalisiert und effizienter unterstützt werden können.

In all diesen Entwicklungen steht die Sparkassen-Finanzgruppe im engen Austausch mit den europäischen Sparkassen, besonders mit der Ersten Bank Group, Caixa-Bank und Swedbank, die ebenso Blockchain-Initiativen betreiben.

Nichtsdestotrotz befindet sich die Blockchain-Technologie technisch und wirtschaftlich immer noch am Anfang. Die bislang in der Finanzwirtschaft identifizierten Anwendungen sind aktuell mehrheitlich in der Konzept- oder Erprobungsphase. Entsprechend weit sind sie noch vom kommerziellen Einsatz im Massen-/Mengen-geschäft entfernt. Dennoch treiben insbesondere Potenziale zur Verbesserung der Prozess-Transparenz und -Effizienz die Entwicklung. Wir sehen zum Beispiel eine Möglichkeit, die Blockchain als effizienten Weg für Meldungen an die Aufsichtsbehörden zu nutzen, um beispielsweise die Richtigkeit und Vollständigkeit von Transaktionen und Geschäftsvorfällen nachzuweisen.

6 Ausblick

Die Digitalisierung stellt die Sparkassen vor eine Vielzahl von Herausforderungen in unterschiedlichen Dimensionen, die sie auf zentraler und dezentraler Ebene mit einer Vielzahl an Maßnahmen adressieren. Die Digitale Agenda der Sparkassen hat dabei das Ambitionsniveau festgelegt und Instrumente geschaffen, die den Instituten dabei helfen sollen, auch in Zukunft relevant zu bleiben.

Es zeigt sich, dass die Digitalisierung kein statisches Ziel ist. Vielmehr ist Digitalisierung ein Prozess, der es erfordert, zeitnah auf Veränderungen nicht nur zu reagieren, sondern diese aktiv gestalten zu können. Von besonderer Bedeutung sind dabei auch die rechtlichen und

regulatorischen Rahmenbedingungen. Sie haben einen entscheidenden Anteil daran, ob die Institute künftig auch mit den teilweise in Deutschland noch nicht regulierten Technologiekonzernen, die zunehmend finanznahe Dienstleistungen anbieten, mithalten können – oder ob sie sich unter ungleichen rechtlichen Bedingungen bewähren müssen.

Die Sparkassen sehen die Digitalisierung bewusst als Chance, um sich zu verändern und ihr Geschäftsmodell weiterzuentwickeln und dabei den Kern – die Nähe zu Kunden – zu wahren. Vor allem das Kundenerlebnis entscheidet über die Akzeptanz in der digitalen Welt.



WVI

Das Geschäft von Versicherern wird sich grundlegend verändern. Der Vorsitzende der Geschäftsführung des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV), Dr. Jörg von Fürstenwerth, analysiert die sieben möglichen Megatrends und deren Veränderungspotenzial.

Unterwegs in die digitale Versicherungswelt

Ein Bericht aus dem Maschinenraum der Veränderung

Autor

Dr. Jörg Freiherr Frank von Fürstenwerth

Mitglied des Präsidiums,

Vorsitzender der Geschäftsführung

Gesamtverband der Deutschen

Versicherungswirtschaft e.V. (GDV)

1 Einleitung

Die vorherrschende Meinung kommt dieser Tage nicht ohne die These aus, dass Unternehmen in einer Zeit tiefgreifender Veränderungen nur dann zu einem zukunftsfähigen Geschäftsmodell finden, wenn sie in jeder Hinsicht agil sind. Agilität ist zu einem der Leitbegriffe des digitalen Diskurses geworden. Nur agile Unternehmen seien in der Lage, eine angemessene Antwort auf die Disruption ihrer Geschäftsmodelle zu finden. Versicherungsunternehmen scheinen nach landläufiger Ansicht sogar vor ganz besonders hohen Hürden zu stehen, haben sie doch nicht gerade den Ruf, an der Spitze der Veränderung zu marschieren. Nicht ganz zu Recht. Deswegen soll an dieser Stelle ein etwas genauerer Blick in den Maschinenraum der Veränderung gewährt werden.

Der allerdings mit einem Blick über den Tellerrand beginnt: Denn wenn es in jüngster Zeit ein Symbol für die Dynamik der Veränderung von Geschäftsmodellen und Märkten gegeben hat, dann steht dafür der Name Cebit. Das Konzept der Messe hat der Dynamik der Digitalisierung nicht mehr standgehalten. Die Cebit

ist Geschichte – und ein mahnendes Beispiel dafür, das Tempo des Wandels nicht zu unterschätzen.¹

Die Zeichen der Zeit müssen schnell erkannt und analysiert, Handlungsfelder abgesteckt und die notwendigen, mitunter bitteren Maßnahmen mit Agilität und vor allem mit Mut umgesetzt werden. Beispielhaft zeigt sich das am Wettlauf um die Vorherrschaft bei Künstlicher Intelligenz (KI). KI gilt vielen heute als wichtigste Technologie seit der Dampfmaschine.² Auch wenn an ihr und den notwendigen Algorithmen bereits seit 70 Jahren geforscht wird, bieten erst heute die Rechenleistungen moderner Computersysteme die Möglichkeiten, die Technologie voll auszuschöpfen – mit Blick auf den Horizont wäre hier der Quantencomputer zu nennen.

1 Schnurer, NDR.de – Für Hannover ist das Ende der Cebit ein Desaster, https://www.ndr.de/nachrichten/niedersachsen/hannover_weserleinegebiet/Fuer-Hannover-ist-Ende-der-Cebit-ein-Desaster,cebit4234.html, abgerufen am 5.12.2018.

2 Vgl. Reuters, Altmaier – Künstliche Intelligenz nach Airbus-Vorbild vorantreiben, <https://de.reuters.com/article/deutschland-k-nstliche-intelligenz-idDEKBN1O30H1>, abgerufen am 5.12.2018.

Um auf dem globalen Zukunftsmarkt nicht den Anschluss zu verlieren, haben die Mitgliedstaaten der Europäischen Union (EU) Milliarden Euro mobilisiert. Der Plan der EU-Kommission sieht Maßnahmen in vier Schlüsselbereichen vor: „Steigerung der Investitionen, Verfügbarkeit von mehr Daten, Förderung von Talenten und Vertrauensbildung.“³

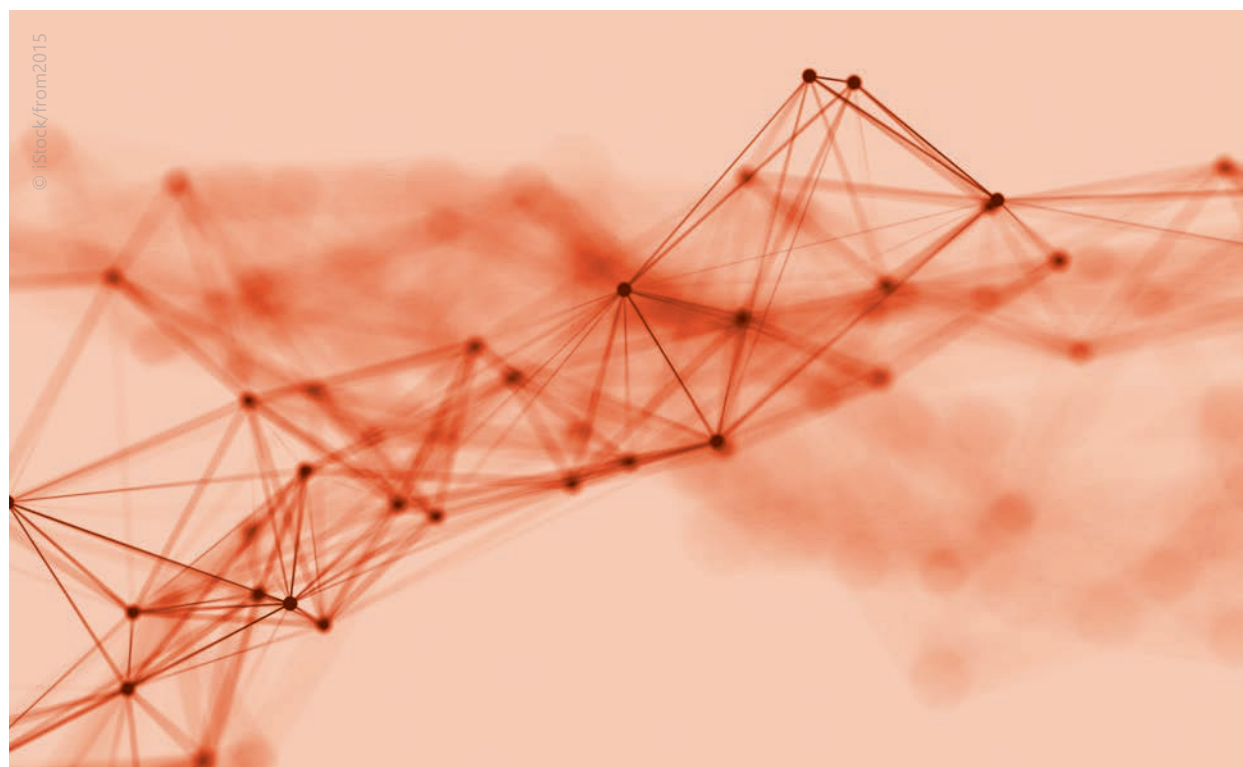
Schon im November 2018 hatte die Bundesregierung ihre KI-Strategie veröffentlicht. Demnach sollen 100 neue Professuren für KI geschaffen und bis zum Jahr 2025 etwa drei Milliarden Euro bereitgestellt werden. Forschung ist allerdings nicht alles, gilt es doch die Ergebnisse im internationalen Wettbewerb auch in tragfähige, möglicherweise grundlegend neue und damit disruptive Geschäftsmodelle und neue Lösungen

3 Vgl. Pressemeldung Europäische Kommission, Mitgliedstaaten und Kommission arbeiten gemeinsam an Förderung künstlicher Intelligenz « Made in Europe », http://europa.eu/rapid/press-release_IP-18-6689_de.htm, abgerufen am 5.12.2018.

für Wirtschaft und Gesellschaft zu transferieren. Und KI ist dabei nur einer von vielen digitalen Trends, die die Ökonomie mit wachsender Dynamik von links auf rechts krepeln, alte Märkte auf den Kopf stellen und völlig neue entstehen lassen könnten – und natürlich macht die Versicherungswirtschaft hier keine Ausnahme.

Aktuell lassen sich sieben Megatrends erkennen, die das Potenzial haben, das Geschäft von Versicherern nachhaltig zu verändern – gleichermaßen behaftet mit Chance und Risiko:

- Der Kampf um den Kontakt zum Kunden
- Neue Technologien: Künstliche Intelligenz, Cloud und Blockchain
- Die kreative Zerstörung, neue Geschäftsmodelle und Produkte
- Die Prozess-Revolution
- Neue Wettbewerber, mehr Anbietervielfalt
- Der Wettstreit um Talente
- Eine agile Aufsicht



2 Der Kampf um den Kontakt zum Kunden

Verbraucher sind verschieden

Die Finanz- und Staatsschuldenkrise nach 2008 war ein wichtiger Hebel für ein grundsätzlich erneuertes Verbraucherbild⁴, noch nie stand Verbraucherschutz höher im Kurs als heute. Die Versicherer nehmen die Herausforderung an und begreifen die Digitalisierung dabei als große Chance: Sie folgen dem erneuerten, differenzierten Verbraucherleitbild und setzen darauf, die unterschiedlichen Bedürfnisse der Kunden besser zu erfüllen. Die Digitalisierung beschert unserer Branche neue Möglichkeiten, anders, individuell und intensiver als je zuvor mit den Kunden in Kontakt zu treten.

Das Web verstärkt den Wettbewerb – allerdings nicht zwingend die Transparenz

Das Web überflutet Kunden mit Daten und saugt sie gleichzeitig bei ihnen ab. Neuigkeiten über digitale Tools, wie Sprachassistenten, Chatbots, Roboadviser und Apps dominieren die Berichterstattung. Manche Kunden vertrauen diesen Tools sogar schon mehr als Menschen. Fakt ist, dass immer mehr Verbraucher Informations- und Vergleichsplattformen suchen. Auch die Versicherer gehen dorthin, wo sich die Kunden aufhalten. Deshalb werden branchenübergreifende Kooperationen beim Vertrieb von Versicherungsschutz zunehmen. Auch predictive analytics, das Erstellen von Vorhersagen anhand von Daten, werden – über kurz oder lang – eine Rolle im Vertrieb von Finanzdienstleistungen spielen. Im Vergleich zu traditionellen Vermittlern können sie den Bedarf der Kunden nach Versicherungsschutz oft schneller erkennen oder gezielter wecken und auch komfortabel bedienen. Der Wettbewerbsdruck wird dadurch steigen – die Transparenz im Markt allerdings nicht zwingend, denn Altruismus ist auch im World Wide Web die Ausnahme. Vergleichsportale zum Beispiel erwecken zumeist zwar den Anschein, sie sind aber nicht uneigennützig. Sie verfolgen ein klares Geschäftsinteresse und decken normalerweise nicht den gesamten Markt ab. Das sollte sich jeder, der diese Portale nutzt, klarmachen. Und das sollte deshalb auch deutlich erkennbar sein.

⁴ Vgl. GDV, Verbraucherleitbild, <https://www.gdv.de/resource/blob/23930/5ee58e2831202f286c8c6bbec9d4609c/verbraucherleitbild-des-gdv-1016934987-data.pdf>, abgerufen am 5.12.2018.

Vernetzung digitaler Kommunikation und persönlicher Beratung

Viele Kunden kaufen Versicherungsschutz im Internet. Andere nehmen stattdessen – online vorinformiert – persönlich Kontakt zu einem Vermittler ihres Vertrauens auf. Wieder andere informieren sich analog und kaufen online. Die Customer Journey ist individuell, situativ und vor allem flexibel.⁵ Die Präferenz für Digitales ist längst keine Frage des Alters der Kunden mehr. Die effiziente Integration von digitaler Kommunikation und persönlicher Beratung ist ein Muss für jeden im Vertrieb und die große Chance, sich im Wettbewerb um den Kunden zu profilieren. Denn die persönliche Beratung ist für viele Menschen und in vielen Bereichen nach wie vor unverzichtbar. Dann zählen die persönliche Beziehung zum Kunden sowie Qualifikation und Professionalität. Empathie, Erreichbarkeit, Bequemlichkeit, Prozessgeschwindigkeit und Vernetzung gehören zusammen. Effizienter Datenfluss ist unverzichtbar. Das lässt die herkömmliche Differenzierung nach Vertrieb, Betrieb, Schaden und Leistung aus Sicht des Kunden verschwimmen.

Papier ist geduldig... und bleibt uns erhalten

Um die Dynamik bestmöglich nutzen zu können, gilt es, alle Prozesse im Unternehmen – von der Antragstellung bis zur Schadenregulierung – elektronisch abbilden zu können. Aber es ist schwer, vom Papier loszukommen. Die EU-Versicherungsvertriebsrichtlinie IDD (Insurance Distribution Directive) sieht den Papierversand von Dokumenten als Standardfall vor, von dem nur unter bestimmten Umständen abgewichen werden darf. Oft ertnen Versicherer aber absolutes Unverständnis, wenn sie Briefe an ihre Kunden schicken – schon allein wegen des Zeitverzugs (fairerweise sei aber auch erwähnt, dass es vielen Kunden nach wie vor wichtig ist, ein Stück Papier in der Hand zu halten).

⁵ Institut für Versicherungswirtschaft Universität St. Gallen & Synpulse Schweiz AG, Denken Sie noch in Kanälen oder erreichen Sie Ihre Kunden schon? Die Customer Journey in einer multioptionalen Welt, <https://www.ivw.unisg.ch/~media/internet/content/dateien/institute-undcenters/ivw/studien/pm-customer%20journey%20mfz-studie-2016.pdf>, abgerufen am 5.12.2018.



Gleiche Regeln für alle

Im Wettbewerb um den Kunden muss gelten: gleiche Regeln für alle. Das gilt für die etablierten Anbieter in unserer Branche ebenso wie für neue. Seit Februar 2018 gibt es für den Versicherungsvertrieb ein neues Regelwerk, die schon erwähnte IDD. Diese EU-Richtlinie ist vom Gesetzgeber umgesetzt – nun müssen sich auch alle Marktteilnehmer an diese Regeln halten. Denn nicht alles, was digital daherkommt, geschieht zum Vorteil des Kunden. Die EU-Kommission plant jedenfalls eine Verordnung zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten. Hier geht es auch darum, mehr Transparenz in Kriterien zu bringen, die für Rankinglisten als Ergebnis von Suchanfragen gelten. So soll Willkür beim Auslisten von Anbietern verhindert werden. Auch das Bundeskartellamt hat sich in einer Sektoruntersuchung mit Vergleichsplattformen auseinandergesetzt.⁶

⁶ Vgl. Bundeskartellamt, Sektoruntersuchung Vergleichsportale - Konsultation, https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Sektoruntersuchungen/Sektoruntersuchung_Vergleichsportale_Konsultation.html, abgerufen am 6.12.2018.

Verbraucher sollen frei wählen können

Verbraucher haben in Deutschland die Wahl zwischen verschiedenen Zugangswegen zum Versicherungsschutz. Sie können direkt beim Versicherer abschließen. Sie können aber – und das tun die meisten – auch einen Versicherungsvermittler einschalten, der mit Provision vergütet wird. Oder sie entscheiden sich für einen Versicherungsberater, der auf Honorarbasis arbeitet. Die Koexistenz dieser Möglichkeiten ist ein wichtiges Gut. Kein Vergütungssystem sollte diskriminiert werden.

Mit der Digitalisierung geht eine neue Vielfalt einher. Das ist die eigentliche unternehmerische Herausforderung. Denn einerseits ist ein klarer Trend zur Standardisierung erkennbar. Gleichzeitig zeigt sich aber auch ein Trend zu immer maßgeschneiderteren Lösungen. Die Digitalisierung macht beides möglich und beides immer besser. Es scheint insofern paradox, ist aber Realität und dürfte Wirklichkeit bleiben: Das persönliche Gespräch wird gerade in dieser Welt der Vielfalt eine wichtige Rolle sowohl beim Abschluss von Versicherungen als auch beim Aufbau und vor allem dem Erhalten einer guten Beziehung zum Kunden spielen.

3 Neue Technologien: Künstliche Intelligenz, Cloud und Blockchain

Technologiesprünge eröffnen Chancen für die Versicherungswirtschaft

An dieser Stelle soll vor allem von den Chancen geredet werden: Der technische Fortschritt bietet vielfältige Möglichkeiten, die Bereitstellung von Versicherungsprodukten zu verbessern. Alle Teile der Wertschöpfungskette sind betroffen. Die Potenziale sind reichhaltig, zusätzliche Datenquellen stehen zur Verfügung, es gibt neue Analysemethoden für Risikobewertung und Tarifierung, die Automatisierung von Geschäftsprozessen ist in vollem Gang, junge Köpfe prägen per Start-up-Kultur neuartige Marketing- und Vertriebsstrategien. Dies alles befeuert einen intensiven Innovationswettbewerb, dessen Ziel es ist, effiziente und kostengünstige Prozesse, bessere Produktlösungen sowie Services und möglichst optimierte Kundenzugänge bereitzustellen.

Schlüsselbereiche von KI sind Prozessautomatisierung, Risikoanalyse und Kundenkontakt

Die Versicherungswirtschaft eignet sich ganz besonders für den Einsatz von KI, da hier große Datenmengen verarbeitet werden und die Prozesse in Teilen von Wiederholungen, aber auch semantischen Besonderheiten geprägt sind. Absehbar wird KI in drei Schlüsselbereichen eine wesentliche Rolle spielen: Erstens wird KI zur Automatisierung der Versicherungsprozesse beitragen. Zweitens wird KI einen wertvollen Beitrag bei der Risikoanalyse leisten. Drittens wird KI den Kundenkontakt effizienter gestalten.

Schon heute hilft KI: Kunden erhalten ihre Versicherungsleistung nicht innerhalb von Tagen, sondern binnen Stunden. Roboadvice und Sprachassistenten sind für die Kunden rund um die Uhr mit hoher Beratungsqualität verfügbar.⁷ Schäden können reduziert oder gar verhindert werden, indem zum Beispiel Wetterdaten rechtzeitig mit Unwetterwarnungen an Kunden gesendet werden. Durch Datenverknüpfung können Versicherer ihre Kunden in neuen Lebenssituationen, etwa Heirat und Geburt, noch besser auf Doppel-Versicherungen oder Versicherungslücken hinweisen. Adressänderungen

oder die Archivierung von bearbeiteten Versicherungsfällen lassen sich von intelligenten Systemen im Hintergrund abwickeln, was die Verwaltungskosten reduziert und damit auch dem Kunden Geld spart.

Neben der Optimierung des Versicherungsprozesses und der Schadenregulierung wird KI auch die Datenverarbeitung und Analytik verbessern – angesichts der Datenmengen, die etwa durch das Internet der Dinge (IoT) verfügbar werden, ist das ein enormer Fortschritt. Im Ergebnis steigt das Risikoverständnis bei den Kunden, und Versicherer können schneller innovative und maßgeschneiderte Leistungen bieten.

Cloud-Computing in der Versicherungswirtschaft auf dem Vormarsch

Das Cloud-Computing macht weiterhin große Fortschritte, hieraus ergeben sich interessante Möglichkeiten für Optimierungs- und Kostenreduktionsprogramme. Cloud-Dienstleister bieten verschiedene Servicemodelle: Eine Servicestufe ist die Infrastructure as a Service (IaaS) und bedeutet, dass in einem externen Rechenzentrum virtualisierte Computerhardware wie Rechner, Speicher und Netzwerke genutzt werden. Eine weitere ist die Platform as a Service (PaaS) und damit die Cloud als Entwicklungsumgebung. Mit PaaS entwickeln Nutzer eigene Softwareanwendungen oder testen sie in einer vom Cloud-Provider bereitgestellten Umgebung. Bei Software as a Service (SaaS) wird die Anwendung selbst aus der Cloud bezogen. Alle drei Varianten sowie etwaige Unterkategorien müssen den Unternehmen unter Wahrung eines hohen Sicherheitslevels im ordentlichen Geschäftsverkehr zugänglich sein – wollen sie im internationalen Wettbewerb bestehen.

Blockchain bietet großes Potenzial im E-Government-Bereich

Das Interesse an der Blockchain-Technologie hält – wenn auch aus veränderten Blickwinkeln – unvermindert an. Nach anfänglichem Hype an den Märkten, insbesondere ausgelöst durch den Aufstieg der Kryptowährung Bitcoin, geht es nun vermehrt um konkrete Anwendungen und die erforderliche Anpassung des Rechtsrahmens. Denn Blockchain ist die Technologie und Bitcoin nur eine mögliche Anwendung.

⁷ Vgl. GDV, Hey, Computer, was geht ab?, <https://www.gdv.de/de/themen/positionen-magazin/hey--computer--was-geht-ab--39074>, abgerufen am 5.12.2018.

Gerade für die Versicherungswirtschaft hat die Distributed Ledger Technologie (DLT) erhebliches Potenzial – dies immer dann, wenn eine Reihe von Partnern über einen längeren Zeitraum zu unterschiedlichen Zeitpunkten ein berechtigtes Interesse an der lückenlosen und verbindlichen Historie einer Sache oder Person hat und dies nachweisen kann. Zu nennen wären hier beispielsweise der bauliche Zustand eines Hauses und die Gebäudeversicherung oder der Kilometerstand eines Autos und die Kraftfahrtversicherung, aber auch der über vielleicht einige Jahrzehnte laufende Rentenversicherungsvertrag wie bei der Riester-Rente. Denn gerade im E-Government-Bereich bietet die Blockchain die Möglichkeit, private und staatliche Stellen wie Grundbuchämter, Zulassungsstellen und die Zulagenstelle für Altersvermögen kosteneffizient, verbindlich und sicher zu vernetzen. Mit entsprechend intelligent gebauten Blockchain-Lösungen würden sich die Vertrags- und Bestandssysteme bei allen beteiligten Partnern smarter und die Prozessketten einfacher gestalten lassen.

Moderner Rechtsrahmen zur Anwendung neuer Technologien im globalen Wettbewerb

Damit die Chancen der digitalen Technologien genutzt werden können, kommt es auf einen modernen Regulierungs- und Aufsichtsrahmen an. Regulierung muss innovationsfreundlich sein. Dazu gehören Technologieneutralität, Prinzipien- und Risikobasierung und der Verzicht auf übermäßige Vorgaben.

So kommt es immer wieder zu der Forderung nach einem Algorithmen-TÜV. Von Seiten des Verbraucherschutzes wird bemängelt, dass die Entscheidungen etwa einer einfachen KI nicht nachvollziehbar und intransparent seien, quasi eine Blackbox. Bereits heute besteht für Kunden – im Falle einer negativen oder ablehnenden Entscheidung durch ein vollautomatisiertes System – die Möglichkeit, die Kriterien zu erfahren und eine manuelle Nachprüfung einzufordern. Die Forderung nach einem Algorithmen-TÜV mag auch deshalb verwundern, da die Nutzung von Algorithmen in der Versicherungswirtschaft grundsätzlich nicht neu ist. Innovativ ist heute der Einsatz von teil- und vollautomatisierten Prozessketten, bei denen auch KI zum Einsatz kommt. Mit diesen können beispielweise Adressänderungen

oder Archivierungsvorgänge zentral über intelligente Systeme gesteuert werden.

Bei aller Euphorie ist ein verantwortungsvoller Umgang mit der KI-Technologie angezeigt. Insofern ist es wichtig, dass sich alle Player zu einem breiten gesellschaftlichen Dialog über die Verwendung von KI bekennen. Hierbei ist darauf zu achten, dass die Interessen sowohl der betroffenen Verbraucher als auch der Unternehmen angemessen berücksichtigt werden. Gleichwohl darf die Nutzung neuer Technologien nicht mit übereilten Rufen nach Regulierung gebremst werden. Eine auf die nationale Ebene beschränkte Regulierung könnte überdies zu Nachteilen für deutsche Unternehmen im internationalen Wettbewerb führen.

Blockchain: Der Staat ist gefordert

In einem Sondierungsprojekt haben die Versicherer unter dem Dach des Gesamtverbands der Deutschen Versicherungswirtschaft e.V. (GDV) geeignete Einsatzszenarien für die Blockchain lokalisiert und analysiert. Ein wesentliches Ergebnis: Damit sich die Blockchain durchsetzen kann, ist auch der Staat gefordert. Denn noch ist unsicher, wie sich die möglichen Blockchain-Anwendungsfälle mit dem geltenden Rechtsrahmen vereinbaren lassen. In der gerade mit viel Aufwand in Europa verankerten Datenschutz-Grundverordnung (DSGVO) steht das „Recht auf Vergessenwerden“ der grundsätzlichen technischen Konstruktion der Blockchain entgegen. Darüber hinaus darf es bei Blockchain-Lösungen im Versicherungsbereich keine Rechtsunsicherheit bezüglich der Anerkennung von Transaktionen und Identitäten geben.

4 Kreative Zerstörung: neue Geschäftsmodelle und Produkte

Ein Paradebeispiel für die Umwälzungen, die in Technik, in Gesellschaft, aber natürlich auch in Politik und Wirtschaft bevorstehen, ist die Revolution der Mobilität. Die Versicherungsbranche widmet sich dem Thema intensiv, es geht sie natürlich auch ökonomisch (Kfz-Versicherung) unmittelbar an. Im November 2018 hat der Verband über Realität und Vision auf einem Kongress in Berlin intensiv debattiert. Den Grundstein für den Einsatz von automatisierten Fahrsystemen hat dabei die Bundesregierung mit der Reform des Straßenverkehrsgesetzes im Jahr 2017 gelegt. Das Land, in dem das Auto erfunden wurde, müsse den Anspruch haben, auch beim autonomen Fahren an der Spitze zu stehen, betonte dazu ein Vertreter der Bundesregierung im Rahmen des Kongresses.

Digitale Transformation im Straßenverkehr

Tatsächlich arbeiten fast alle Autohersteller intensiv an Lösungen, die Fahraufgaben ohne Eingriffe des Fahrers

bewältigen können. Blickt man in die Zukunft des assistierten, automatisierten und in der letzten Evolutionsstufe, des autonomen Fahrens, könnte man zu dem Schluss kommen: Viele Versicherungen werden eines Tages überflüssig – etwa wenn eine fehlerfreie Technik den ersehnten unfallfreien Verkehr beschert. Aus der „Vision Zero“ – keine Toten und Schwerverletzten im Straßenverkehr – würde Realität. Tatsächlich?

Vor diesem Hintergrund hat der GDV eine interdisziplinäre Projektgruppe aus Ingenieuren, Mathematikern, Versicherungsexperten und Unfallforschern gebildet. Sie sollten ein ebenso realistisches wie fundiertes Bild der zu erwartenden Auswirkungen des assistierten und automatisierten Fahrens erarbeiten. Die eingehende Analyse der Experten und die daraus abgeleitete Prognose für den Einfluss auf die Schadenentwicklung bis ins Jahr 2035 zeigen:



Moderne Fahrerassistenzsysteme und automatisierte Fahrfunktionen

- machen Autofahren sicherer, verhindern in der Praxis aber deutlich weniger Schäden als in der Theorie,
- setzen sich nur mit starker Verzögerung durch und senken die Schäden daher nur langsam,
- führen im Schadenfall zu höheren Reparaturkosten und
- wirken sich auf Kfz-Haftpflichtschäden stärker aus als auf Kaskoschäden.

Die Studie des GDV belegt: Bis 2035 werden die Entschädigungsleistungen der Kfz-Versicherer durch die neuen Systeme nur um sieben bis maximal 15 Prozent sinken.⁸ Die neue Technik, die längst noch nicht perfekt ist, macht Reparaturen teurer, verhindert in der Praxis weniger Schäden als erhofft und gerät bei Steinschlag, Hagel oder Marderbissen an ihre Grenzen. Auch in digitalen Zeiten bleibt Versicherungsschutz also unverzichtbar.

Das intelligente Haus wird selbst zum Risiko

Dasselbe gilt für das smarte Eigenheim und die zunehmende Nutzung von intelligenten Geräten im Haushalt: Wenn man den Versprechungen der Hersteller glaubt, gehören im intelligenten Haus Schäden der Vergangenheit an, haben Einbrecher keine Chance mehr und der Kühlschrank füllt sich von selbst. Nichts davon ist zumindest derzeit auch nur annähernd Realität.

Für die Einordnung hilft ein Blick über den Tellerrand: Bevor die vermeintlich neue Technik in unseren Wohnungen Einzug gehalten hat, wurden praktisch alle Komponenten im industriell/gewerblichen Bereich eingesetzt. Beispiele: Gebäudeüberwachung mit Kameras und Bewegungserkennung, elektronische Schlösser, Brandmeldeanlagen, Leckage-Sensoren. Sie haben geholfen, die Schadenlast bei immer höheren Sachwerten im Griff zu halten. Die Welt gänzlich von Schäden zu befreien, ist auch ihnen aber nicht gelungen. Und das, obwohl diese Komponenten für ein anspruchsvolles Arbeitsumfeld entworfen wurden und entsprechend teuer in

Anschaffung und Wartung über den Lebenszyklus hinweg sind. Versicherung überflüssig? Wohl eher nicht.

Und damit nicht genug: Die moderne Technik dient leider allzu oft als Einfallstor für zusätzliche Gefahren. Denn schon die Cybersicherheit vieler Produkte für den privaten Anwender ist höchst fragwürdig. Kurze Lebenszyklen der Geräte, fehlende Updates, Backdoor-Zugänge – die Liste der problembehafteten Komponenten ließe sich beliebig fortsetzen.

Dies hat Auswirkungen für die Käufer unsicherer Produkte und für Dritte. Der Einbrecher des 21. Jahrhunderts muss sich nicht mehr hinter Büschen verstecken und das Haus ausspähen; es genügt der Zugriff auf die gehackte Überwachungskamera, die praktischerweise auch den PIN-Code des smarten Türschlosses aufgezeichnet hat. Und während man sich über den Komfort der intelligenten Rollladensteuerung freut, greift diese unbemerkt als Teil eines Botnetzes den eigenen Arbeitgeber an. Spätestens am Beispiel des Mirai-Botnetzes⁹ sollte jedem deutlich geworden sein, wie leicht sich Internet of Things (IoT)-Geräte als Angriffsvehikel nutzen lassen – beispielsweise für Distributed Denial of Service Attacks (DDoS)-Attacks.¹⁰

Gefahren erkennen und eingrenzen

Natürlich können in der Verbindung von intelligenter und sicherer Haustechnik mit Konzepten der Wohngebäude- bzw. Hausratversicherung große Chancen liegen. Schäden wie austretendes Leitungswasser können früher erkannt und eingedämmt werden, zum Beispiel durch das automatische Schließen des Hauptwasserhahns. Entsprechende Produktentwicklungen der Versicherer werden intensiv vorangetrieben. Das Problem dabei: Weder für Verbraucher noch für Versicherer ist derzeit klar erkennbar, welche Geräte in Bezug auf Sicherheit und Support empfehlenswert sind. Niemand hat einen

8 Vgl. GDV, Automatisiertes Fahren – Weniger Unfälle, teurere Reparaturen, <https://www.gdv.de/de/medien/aktuell/weniger-unfaelle-teurere-reparaturen-8286>, abgerufen am 28.1.2019.

9 Symantec Corporation, Mirai Botnet, <https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks>, abgerufen am 24.1.2019.

10 Symantec Corporation, Distributed Denial of Service Attack, <https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html>, abgerufen am 24.1.2019.

Überblick, welche Geräte einen Nutzen im Sinne eines Sicherheitsgewinns mit sich bringen und welche nicht.

Daher hat die Versicherungswirtschaft an die Geräte-kategorie Smart Home beziehungsweise Internet der Dinge bereits im Jahr 2017 konkrete Anforderungen gestellt.¹¹ Wenn die Risiken dieser Geräte auf Dauer tragbar sein sollen, müssen sich Produkt- und Supportphilosophie der Hersteller grundlegend ändern. Andernfalls steuern wir vor dem Hintergrund des exponentiellen Zuwachses intelligenter und vernetzter Geräte auf einen Sicherheits-GAU sondergleichen zu. Allein in den nächsten zwei Jahren wird sich die Zahl dieser Geräte verdoppeln – auf dann weltweit etwa 20 Milliarden Stück (siehe Abbildung 1).

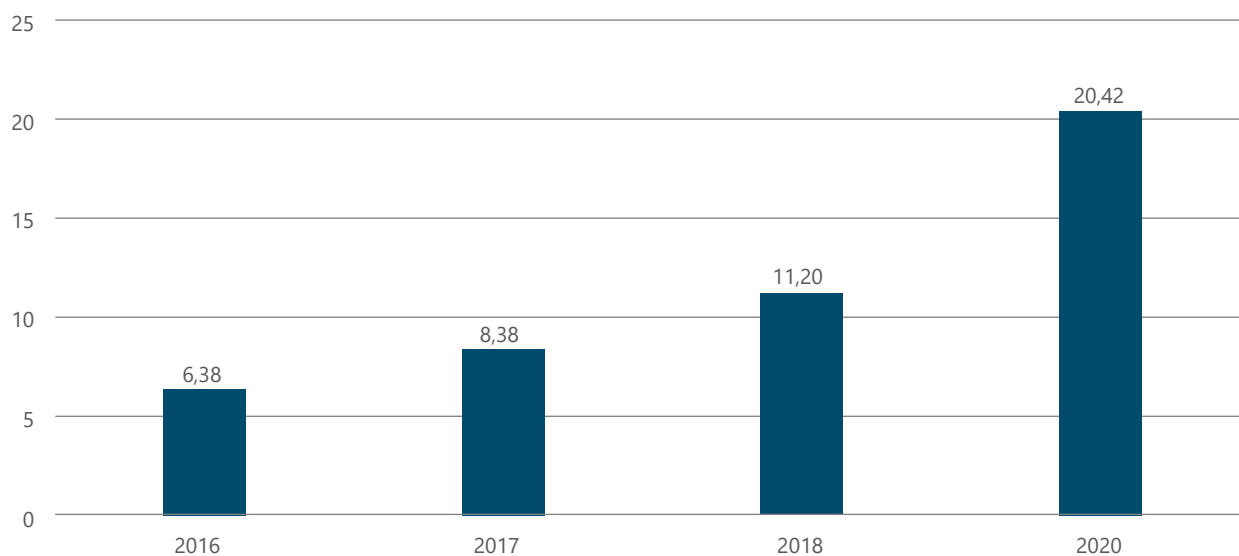
Die Versicherungswirtschaft begrüßt daher ausdrücklich die Veröffentlichung der Technischen Richtlinie „Secure

Broadband Router“ (TR-03148)¹² durch das Bundesamt für Sicherheit in der Informationstechnik (BSI). Denn der Breitband-Router ist die zentrale Sicherheitsinstanz in allen Privathaushalten. Wird der Router kompromittiert, stehen Smart Home und Daten des Betroffenen Cyberkriminellen offen. Ein wichtiges Ziel der Technischen Richtlinie ist es, die Sicherheitseigenschaften für alle Anwender – damit auch die Versicherer – transparent zu machen. Dies können Hersteller durch eine geeignete Kennzeichnung am Gerät unterstützen. Die Technische Richtlinie ist daher ein wichtiger Schritt in Richtung eines IT-Sicherheitskennzeichens, wie es die Bundesregierung in der Cyber-Sicherheitsstrategie von 2016 und im Koalitionsvertrag vorgesehen hat. Die Versicherungswirtschaft unterstützt die Planungen des BSI, auch für weitere Geräte des Internets der Dinge und des Smart Homes Mindestanforderungen an deren IT-Sicherheit zu formulieren.

11 GDV, Smart Home – Versicherer warnen vor Cyberrisiken im digitalen Zuhause, <https://www.gdv.de/de/medien/aktuell/versicherer-warnen-vor-cyberrisiken-im-digitalen-zuhause-8258>, abgerufen am 5.12.2018.

12 Bundesamt für Sicherheit in der Informationstechnik, BSI TR-03148 Sichere Breitband Router, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03148/tr03148_node.html, abgerufen am 5.12.2018.

Abbildung 1: Internet der Dinge – über 20 Milliarden installierte Geräte im Jahr 2020



Quelle: <https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016>.

Neue Produkte und Geschäftsmodelle

Die Digitalisierung verändert nicht nur einzelne Marktsegmente, sie schafft sogar ganz neue: Der GDV hat unverbindliche Musterbedingungen für Cyber-Versicherungen entwickelt, die speziell kleine und mittlere Unternehmen schützen können.¹³ Sie richten sich sowohl an Arztpraxen oder Anwaltskanzleien als auch an Handwerksbetriebe und Industrielieferer. Die Versicherung leistet hier nicht nur bei Datenklau und Betriebsunterbrechungen, sondern übernimmt auch Kosten für IT-Forensiker oder Krisenkommunikation.

Die zur Ermittlung des Cyberrisikos erforderlichen Auskünfte des Kunden sind andere, als für den Abschluss einer üblichen Betriebshaftpflicht- oder Gebäudeversicherung. Damit Versicherer vor Abschluss eines Vertrages das individuelle Risiko eines Kunden, Opfer einer Cyberattacke zu werden, besser einschätzen können und das zu versichernde Unternehmen mögliche Schwachstellen seiner IT-Sicherheit leichter erkennt, hat der GDV auch unverbindliche Risikofragen entwickelt. Anzahl und Inhalt der Fragen sind abhängig von der jeweiligen Risikokategorie und den Geschäftsfeldern des Unternehmens und ob es beispielsweise mit sensiblen Daten umgeht, vernetzt produziert oder E-Commerce betreibt.

Es werden bei Bedarf auch neue Arten von Risikodeckungen möglich: Kurzzeitversicherungen etwa, die nach dem On-demand-Prinzip situativ abgeschlossen werden können. Beispiele sind eine tageweise zubuchbare Erweiterung des Fahrerkreises bei der Kfz-Versicherung und eine Unfallversicherung speziell für den Skiurlaub.

Gleichzeitig sind bei den Versicherern viele Ansätze innovativer Erweiterungen des Geschäftsmodells zu beobachten: Neben der Geldleistung im Versicherungsfall wird der Kunde zunehmend beim Umgang mit Risiken unterstützt oder erhält direkte Hilfeleistungen. Dazu gehören etwa Hinweise zu einer Verbesserung des

Fahrverhaltens und schnelle Hilfe bei einem Unfall in der Kfz-Versicherung sowie Hilfen beim Management chronischer Krankheiten in der Krankenversicherung. Versicherer werden dadurch noch stärker als bisher zum Partner im Umgang mit Risiken. Versicherer machen Angebote, die risikoarmes Verhalten durch besonders günstige Tarife belohnen. Dazu erheben sie auf freiwilliger Basis schon heute Daten, etwa zum Fahrverhalten und zum Grad körperlicher Bewegung. Die Unternehmen belohnen umsichtiges Fahren und aktive Bewegung – als wesentlichen Beitrag zu moderner Schadenprävention.¹⁴

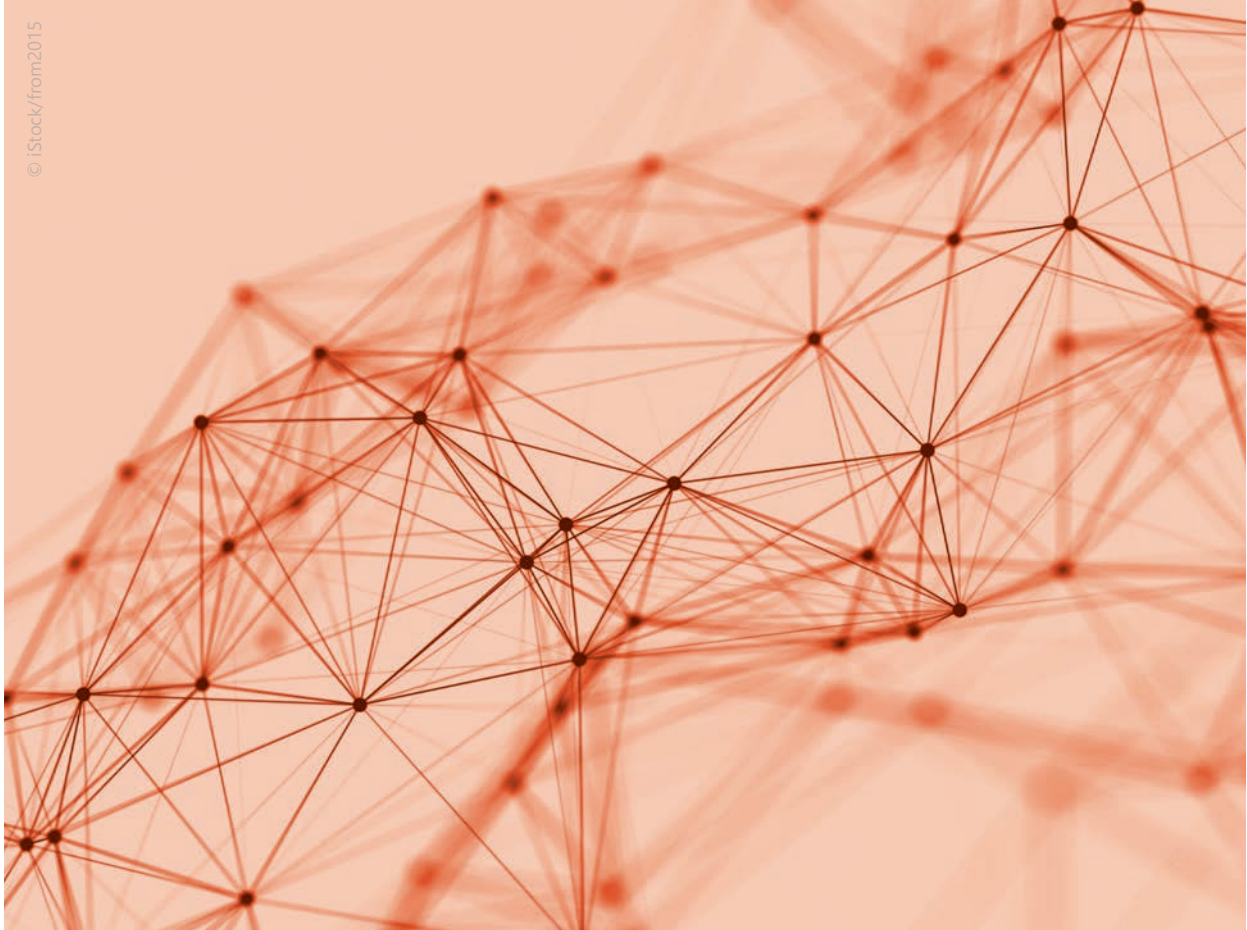
Eine der womöglich weitreichendsten Innovationen, die durch die digitalen Technologien ermöglicht wurden, ist die Sharing Economy – direkte Transaktionen zwischen Privatpersonen, das sogenannte Peer-to-Peer über Internetportale, die lediglich als Vermittler agieren. In einigen Bereichen haben derartige Portale bereits eine hohe Marktdurchdringung erreicht, etwa bei Kurzzeitvermietungen von privaten Wohnungen. Auch im Bereich der Kreditvermittlung gewinnen Peer-to-Peer-Plattformen an Bedeutung.

Im Versicherungsbereich sind Peer-to-Peer-Plattformen dagegen erst in Anfängen zu finden. So gibt es am deutschen Markt für einige Sparten der Schaden-/Unfallversicherung Ansätze bei der Übernahme kleiner Schäden innerhalb von Kleingruppen von Versicherten. Entstehen keine Schäden, erhalten die Kunden eine Beitragserstattung. Größere Schäden werden weiterhin durch Versicherer als Risikoträger gedeckt.

Anzeichen der Ausweitung einer Peer-to-Peer-Absicherung auf höhere Risiken gibt es im Privatkundengeschäft bisher jedoch nicht – und im Gewerbetündergeschäft erst recht nicht. Im Zuge des weiteren Innovationswettbewerbs ist aber zu erwarten, dass

13 Vgl. GDV, Medieninformation – GDV stellt Musterbedingungen für Cyberversicherung vor, <https://www.gdv.de/de/medien/aktuell/gdv-stellt-musterbedingungen-fuer-cyberversicherung-vor-8270>, abgerufen am 5.12.2018.

14 Zu Erweiterungen des Geschäftsmodells und neuen Produktansätzen, vgl. etwa Wiener, Theis, Vier Gründe, warum die Versicherungswirtschaft wichtiger wird, in: GDV Makro und Märkte kompakt, Nr. 15, <https://www.gdv.de/resource/blob/26204/b0ce16220de8b51d62f31e6f54fdeebe/makro-und-maerkte-kompakt---vier-gruende--warum-die-versicherungswirtschaft-wichtiger-wird-data.pdf>, abgerufen am 6.12.2018.



neue Produktangebote, die Peer-to-Peer-Elemente integrieren, auf den deutschen Versicherungsmarkt kommen könnten.

Ein möglicher Wettbewerbsvorteil dieser Produkte kann darin bestehen, dass in der Kleingruppe ein Gemeinschaftsgefühl entsteht, welches eine deutlich geringere Betrugsneigung hervorbringt und damit positive Auswirkungen auf die Schadenentwicklung haben kann. Dennoch ist es unwahrscheinlich, dass Versicherungsrisiken verstärkt oder gar vollständig von Peer-to-Peer übernommen werden. Dem stehen die Besonderheiten des Versicherungsgeschäfts entgegen. Dazu gehört ein hohes Schadenpotenzial, etwa in der Haftpflichtversicherung. Außerdem sei an den langfristigen Charakter insbesondere vieler Personenversicherungsverträge erinnert. Mit ihnen verbunden ist die notwendige Gewähr der versprochenen Leistungen auch bei ungünstigen Entwicklungen, damit die Versicherung für den Einzelnen ihren Zweck erfüllt, Stichwort „mögliche Nachschusspflicht“. Dementsprechend stellen sich beim Peer-to-Peer-Angebot auch noch zahlreiche rechtliche Fragen.

Um diese beschriebenen Potenziale produktiv nutzen zu können, müssen Versicherer Spielraum für Innovation und Rechtssicherheit haben. So müssen diese vereinbaren dürfen, dass im Ermessen der Kunden risikorelevante Daten aus vernetzten Endgeräten für Versicherungs- und Serviceangebote genutzt werden können. Die Datenhoheit der Versicherungsnehmer, etwa

beim automatisierten Fahren, ist dabei Voraussetzung für einen funktionierenden Wettbewerb um die besten Lösungen.

Appell für eine neue Risikokultur

Ein grundsätzlicher Appell zum Thema Sicherheit im Netz: Die Gesellschaft braucht nicht weniger als eine neue Risikokultur für den Cyber-Space: erstens und ganz grundlegend die Bereitschaft der Wirtschaft, diese Risiken ernst zu nehmen und entsprechend zu handeln; zweitens ein gemeinsames Verständnis über einen Grad an IT-Sicherheit, der ein Unternehmen zuverlässig schützt, aber nicht wirtschaftlich überfordert und drittens natürlich Versicherungen, die das verbleibende Risiko decken und den Unternehmen im Ernstfall nicht nur mit Geld, sondern auch mit Know-how zur Seite stehen. Mit der Veröffentlichung der unverbindlichen Musterbedingungen für diese neuen Produkte durch den GDV wird sich der junge Markt hoffentlich dynamisch entwickeln. Den ersten Schritt allerdings – das Risiko erkennen und es ernst nehmen – muss jedes Unternehmen selbst gehen, wenn es nicht Opfer des derzeitigen kriminellen Goldrausches im World Wide Web werden will.

Die Absicherung von Risiken bleibt den Versicherern folglich als zentrales Geschäftsmodell erhalten. Die Digitalisierung hilft aber, Versicherungen individueller und passgenauer zu gestalten. Neue Daten und Analysetechniken erlauben eine exaktere Risikobewertung und erweiterten Versicherungsschutz.

5 Die Prozess-Revolution

Hoher Automatisierungsgrad in der Versicherungswirtschaft

Standardisierte und automatisierte Prozesse bilden einen wesentlichen Grundpfeiler für die Digitalisierung des Versicherungsgeschäfts. Wenn der Versicherungskunde individualisierte, smarte und sekundenschnelle Reaktionen von seinem Versicherer erwartet, so ist jenes für Versicherungsunternehmen nur durch eine konsequente und durchgängige Automatisierung und Beschleunigung ihrer Prozesse zu erreichen. Und dies gilt für sämtliche Sparten, Fachbereiche und Geschäftsprozesse der Unternehmen.

Programme legen automatisch Akten an, verwandeln eingescannte Schreiben in maschinenlesbaren Text, prüfen Rechnungen auf Plausibilität oder lösen eigenständig Zahlungen aus.¹⁵ Während in der Schaden- und Unfallversicherung im Jahr 2013 nur knapp jedes achte

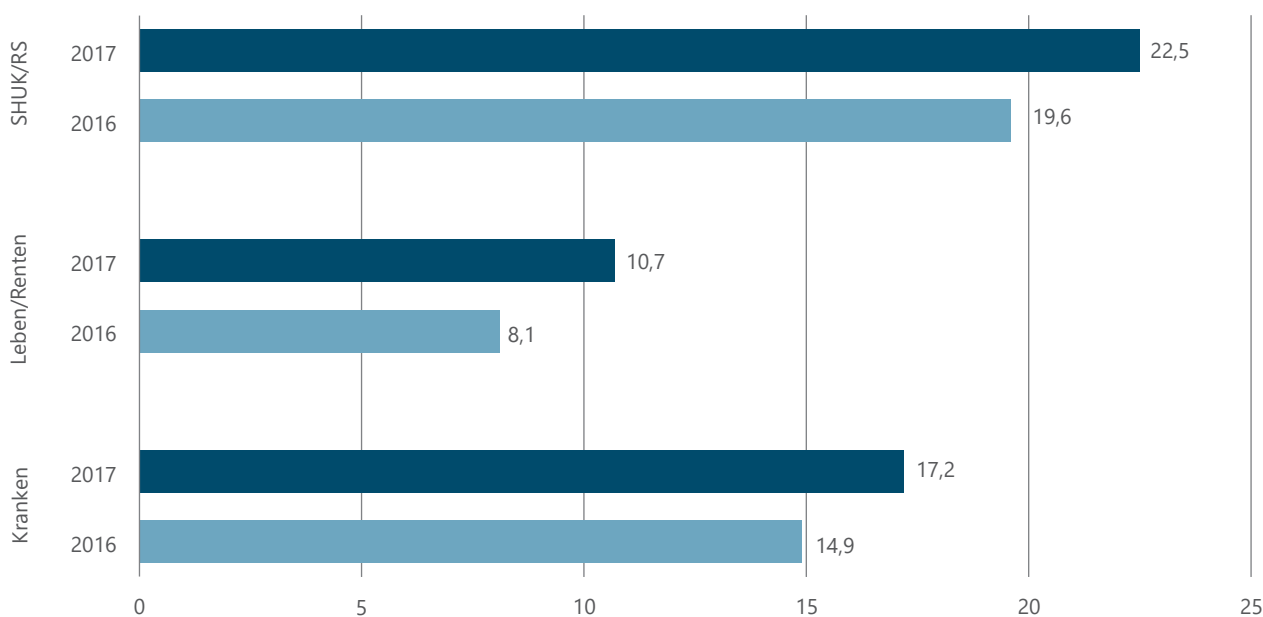
Kundenanliegen von Anfang bis Ende vollautomatisiert bearbeitet werden konnte, ist es heute bereits jedes vierte. Auch in der Lebensversicherung stieg der Anteil der vollautomatisierten Bearbeitung, und zwar von vier auf elf Prozent (siehe Abbildung 2). 2017 gab die Branche insgesamt 4,45 Milliarden Euro für Informationstechnologie aus.

Selbst der World Insurance Report 2018 von Capgemini bescheinigt den deutschen Versicherern einen vorbildlichen Stand beim Einsatz digitaler Technologien zur Automatisierung.¹⁶ Besonders deutlich wird das im Bereich der robotergesteuerten Prozessautomatisierung (RPA) über alle drei Versicherungssegmente (Sach-, Lebens- und Krankversicherung) hinweg. Die große Mehrheit der deutschen Versicherer (89 Prozent) hat RPA-Systeme zumindest pilotiert (36 Prozent) oder bereits vollständig im Einsatz (53 Prozent). Aber auch bei der Implementierung anderer Automatisierungstechnologien (unter anderem

¹⁵ Vgl. GDV, Digitale Schadenbearbeitung – Feinjustiert, <https://www.gdv.de/de/themen/positionen-magazin/feinjustiert-38876>, abgerufen am 5.12.2018.

¹⁶ Vgl. Capgemini, World Insurance Report 2018, <https://worldinsurance.report.com/>, abgerufen am 6.12.2018.

Abbildung 2: Vollautomatisierte Verarbeitung nach Sparten*



* in Prozent

Quelle: GDV



© iStock/from2015

Künstliche Intelligenz, Machine Learning/Deep Learning und Blockchain) zählen deutsche Versicherer nach Einschätzung von Capgemini zu den Vorreitern im internationalen Vergleich.¹⁷

KI als Treiber der Prozess-Revolution

Für die Verbesserung von Geschäftsprozessen bieten KI-Lösungen ein enormes Potenzial und sind damit wesentliche Werkzeuge bei der Prozess-Revolution in den Unternehmen. KI-Systeme sind aber immer nur so gut wie die Daten und Informationen, mit denen sie gefüttert und trainiert werden. Leistungsfähige KI-Lösungen sollten daher mit allen Informationen, die ein Versicherer bisher gesammelt hat, versorgt werden können. Und natürlich mit allen weiteren Fakten, zum Beispiel zu Produkten, die das Unternehmen anbietet. Dieses Inputmanagement entscheidet letztlich, wie gut die Ergebnisse sind, die eine KI im Versicherungseinsatz abliefern. Am Ende profitieren Verbraucher wie Unternehmen von einer fairen und verantwortungsbewussten Nutzung dieser Verfahren, wie sie etwa bei Chatbots zum Einsatz kommen.¹⁸ Man denke auch an den neuen Rentenrechner des GDV: Spielerisch, mit mathematischer Genauigkeit, berechnet das Tool binnen einer Minute mögliche Vorsorgelücken.¹⁹

Wie das Beispiel der Schrifterkennung und -auswertung mittels KI zeigt, ist dies ein durchaus aufwendiger Weg: Schriftliche und digitale Dokumente wie E-Mails, unterzeichnete Verträge auf Papier, Web-Formulare, Fax-Sendungen oder PDF-Dateien beispielsweise für die Schadenabwicklung müssen dafür dem KI-System zugeführt werden. Bevor eine KI aus einem solchen Datenmix Informationen und Wissen generieren kann, müssen alle Fakten mittels Natural Language Processing (NLP) maschinengerecht aufbereitet werden. In einem nächsten Schritt muss das System die Bedeutungszusammenhänge der Fachbegriffe lernen, um sie künftig richtig zuzuordnen und interpretieren zu können.

Erst durch diese begriffliche Anreicherung der Fakten und der Regeldefinition für die Verarbeitungsalgorithmen versteht das System den Kontext, kann Texte richtig interpretieren und daraus Handlungsoptionen ableiten. So kann das KI-System dann aus den unstrukturierten und verteilt liegenden Texten die Informationen herauslesen. Diese Anlernphase ist entscheidend für die Güte der Informationen im späteren Einsatz. Und diese Lernphase muss durch Menschen didaktisch gestaltet und sinnvoll strukturiert werden. Denn nur wenn diese Lernphase gut organisiert ist, wird das System auch eigenständig intelligenter und kann durch die Anwendung seines Wissens Muster und Gesetzmäßigkeiten selbst ableiten und künftig anwenden.

¹⁷ Vgl. IT Finanzmagazin, Deutsche Versicherer bei Automatisierungstechnologien über dem weltweiten Durchschnitt, <https://www.it-finanzmagazin.de/deutsche-versicherer-bei-automatisierungstechnologien-ueber-dem-weltweiten-durchschnitt-71261/>, abgerufen am 5.12.2018.

¹⁸ Vgl. GDV, a.a.O. (Fn. 7), abgerufen am 6.12.2018.

¹⁹ Vgl. GDV, Neuer Rentenrechner – In 60 Sekunden zur individuellen Altersvorsorge, <https://www.gdv.de/de/medien/aktuell/in-60-sekunden-zur-individuellen-altersvorsorge-32892>, abgerufen am 5.12.2018.

Moderne Zahlungsdienstleister als Partner der Prozess-Revolution

Die Prozesse rund um Zahlung und Auszahlung sind – mit dem E-Commerce vergleichbar – zentrale Erfolgsfaktoren für die Digitalisierung in der Versicherungswirtschaft. Der Kunde erwartet für die Bezahlung seiner



Prämien und die Auszahlung seiner Leistungen höchstmöglichen Komfort, idealerweise gepaart mit umfassender Flexibilität und maximaler Sicherheit. Die Branche bietet alternative Zahlverfahren allerdings noch zurückhaltend an. Das liegt nicht zuletzt daran, dass die am Markt agierenden Zahlungsdienstleister – ob klassisches Kreditinstitut oder neu am Markt tätiger Zahlungsdienstleister – ihre Angebote bisher primär an den Bedürfnissen des E-Commerce ausrichten. Die Versicherungswirtschaft und deren Produktpalette sind jedoch nicht ohne Weiteres mit anderen Branchen vergleichbar. So ist die Bezahlung eines online bestellten Artikels im E-Commerce etwas anderes, als wiederkehrende Prämienforderungen aus einem Versicherungsvertrag zu begleichen. Zudem erwarten die Versicherer von einem modernen Zahlungsdienstleister nicht nur die reine Abwicklung einer Zahlung. Es geht ihnen auch um die Kombination des Bezahlvorgangs mit weiteren prozessualen Mehrwerten, um dadurch die Digitalisierungsprozesse in den Unternehmen zu unterstützen und den Automatisierungsgrad zu erhöhen (zum Beispiel: sichere Kundenidentifizierung/-authentifizierung, E-Invoicing-Services mit verlinkter Bezahlungsfunktion, Erteilung eines rechts-sicheren elektronischen Lastschriftmandats). Auf diese Weise können Zahlungsdienstleister zu starken Partnern bei der Prozessautomatisierung und Digitalisierung der Versicherer werden.

Mit der Zweiten Zahlungsdienstleistungsrichtlinie (Payment Services Directive – PSD 2) und dem von ihr verfolgten Open-Banking-Ansatz wurde die Grundlage für diese Entwicklung geschaffen. Für Banken, Sparkassen und neue Zahlungsdienstleister eröffnet sich nun gleichermaßen die Chance, sich zu einem Zahlungsdienstleister

im eigentlichen Wortsinne zu entwickeln. Die entstehenden offenen API-Ökosysteme (Application Programming Interface) ermöglichen die Schaffung von innovativen Mehrwertangeboten rund um Konto und Zahlung und den Umbau in Richtung einer digitalen Bankenplattform. Diese Entwicklung hin zu digitalen Payment-Ökosystemen wird von der deutschen Versicherungswirtschaft aufmerksam verfolgt und begrüßt. Sie bietet auch für die Versicherer die Möglichkeit, die eigenen Zahlungsverkehrs- und Abrechnungsprozesse effizienter, digitaler und kundenfreundlicher zu gestalten.

Sicherheit und Standards entscheidend für Interoperabilität und den Unternehmenserfolg

Entscheidend für den Erfolg ist das Vertrauen der Kunden: Ihre Daten sind unverzichtbare Ressource im Kerngeschäft. Ihre Sicherheit und Integrität stehen an erster Stelle. Unabhängig davon, ob Daten und Algorithmen intern oder extern etwa durch Cloud-Computing verarbeitet werden, müssen geeignete Sicherheitsmaßnahmen ergriffen werden, um die IT-Sicherheit zu gewährleisten.

Zur Sicherstellung einer zukünftigen Handlungsfähigkeit muss Interoperabilität und Sicherheit zwingend von Beginn an mitgedacht und nach dem Motto „Security by Design“ in IT-Systemen und Geschäftsprozessen eingebaut werden. Denn gerade die vollautomatisierte End-to-End-Bearbeitung birgt noch für alle Versicherungssparten erhebliche Kosteneffizienzpotenziale. Die bereits angestoßenen Optimierungsmaßnahmen gilt es weiter mit hohem Engagement voranzutreiben und mittels einer idealerweise technikneutralen und modernen Gesetzgebung zu flankieren.

6 Neue Wettbewerber, mehr Anbietervielfalt

Marktpositionen verschieben sich

In den vergangenen Jahren sind zahlreiche neuartige Wettbewerber in den deutschen Versicherungsmarkt eingetreten, etwa die Insurtech-Startups. Die allermeisten dieser neuen Player beschränken sich auf Teile der Wertschöpfungskette, wie den Vertrieb oder IT-Services.²⁰ Einige Insurtechs haben mittlerweile aber auch eine Versichererlizenz erhalten. Über einen stärkeren Markteintritt der großen Technologie-Konzerne oder anderer branchenfremder Konzerne wird spekuliert. Die neue potenzielle Konkurrenz befeuert den Wettbewerb und die Innovationsdynamik und erhöht den Anpassungsdruck auf traditionelle Versicherer.

Die verschiedenen Anbietertypen – etablierte Versicherer, Insurtech-Startups sowie Newcomer aus anderen Branchen wie etwa Technologieunternehmen – verfügen dabei jeweils über spezifische Stärken. Insurtechs können ihre Angebote ohne Altlasten voll auf die digitale Welt zuschneiden. Die Bigtechs zeichnen sich durch ihre Expertise im Umgang mit neuen Technologien und ihren umfangreichen Datenpool aus. Traditionelle Versicherer dagegen profitieren von ihren gewachsenen Kundenbeziehungen und ihrer umfassenden Versicherungs- und Regulierungskompetenz. Sie stehen aber vor der Herausforderung, ihre Strategie und ihren Geschäftsbetrieb an die neuen Gegebenheiten anzupassen.

²⁰ Vgl. etwa Institut für Versicherungswirtschaft Universität St. Gallen, The Current InsurTech Landscape: Business Models and Disruptive Potential, Institut für Versicherungswirtschaft Universität St. Gallen, https://www.ivw.unisg.ch/~media/internet/content/dateien/instituteundcenters/ivw/studien/ab-insurtech_2017.pdf, abgerufen am 5.12.2018.

Markteintritte und -austritte sowie Unternehmens- transaktionen werden zunehmen

Den Wettbewerbern eröffnen sich dabei ganz unterschiedliche strategische Optionen, um sich am Markt zu behaupten. Zu beobachten ist, dass Versicherer ganz unterschiedliche strategische Wege gehen. Die





traditionell sehr vielfältige Anbieterlandschaft am deutschen Versicherungsmarkt differenziert sich damit weiter aus. Dies wird durch die zunehmende Bedeutung von Kooperationen – sowohl zwischen Versicherern und Firmen anderer Branchen als auch zwischen mehreren Versicherern – verstärkt. Im Wettbewerbsprozess ist für die nächsten Jahre mit erheblichen Verschiebungen in den Marktpositionen zu rechnen. Nicht alle Versicherer werden sich am Markt behaupten können. Markteintritte und -austritte sowie Unternehmenstransaktionen werden zunehmen.

Extreme Veränderungen der Anbieterlandschaft mittelfristig unplausibel

Vor diesem Hintergrund hat der GDV im Rahmen einer Projektgruppe untersucht, wie sich durch die tiefgreifenden Veränderungen mittelfristig – bis ca. 2025 – die Anbieterlandschaft am deutschen Versicherungsmarkt wandeln könnte.²¹

Aus den vorliegenden Informationen lassen sich fünf Extremszenarien als langfristig theoretisch denkbare Entwicklung für die Anbieterlandschaft identifizieren:

- Neuartige Versicherer (Insurtechs oder die Versicherungstöchter von Technologieunternehmen) verdrängen die bisherigen Anbieter.

- Die traditionellen Versicherer passen sich erfolgreich an und behalten ihre dominante Marktstellung.
- Versicherer werden zu reinen Risikoträgern, die Kundenschnittstelle wird von anderen Unternehmen – wie etwa Internetplattformen – bedient.
- Durch die neuen Möglichkeiten der digitalen Vernetzung fragmentiert sich die Wertschöpfungskette.
- Es kommt zu einer Disintermediation der Versicherer als Risikoträger, zum Beispiel durch Peer-to-Peer-Portale.

Bei aller Unsicherheit über die zukünftige Entwicklung und die möglichen verschiedenen Entwicklungspfade: Ergebnis der Analysen des Verbandes ist, dass sich voraussichtlich keines der Extremszenarien einstellen wird. Stattdessen ist zu erwarten, dass sich in der zukünftigen Anbieterstruktur am Versicherungsmarkt Elemente aus allen Szenarien wiederfinden werden. In der mittelfristigen Entwicklung dürften sich die verschiedenen Extremszenarien allerdings sehr unterschiedlich niederschlagen (siehe Abbildung 3, Seite 105).

Vieles spricht dafür, dass etablierte Versicherer durch erfolgreiche Anpassungen an die neue Welt auch in den nächsten Jahren eine starke Marktposition behalten werden. Gleichzeitig ist allerdings auch zu erwarten, dass sich einige neuartige Versicherer erfolgreich am Markt behaupten. Angesichts der zunehmenden Bedeutung von Kooperationen und Internetportalen an der Schnittstelle zum Kunden könnten Versicherer in Zukunft häufiger als bisher die Rolle eines reinen Risikoträgers übernehmen. Der Disintermediation – dem Ersetzen der Versicherer in ihrer Rolle als Risikoträger durch andere

²¹ Vgl. GDV, Volkswirtschaftliche Themen und Analysen Nr. 8, Anbieterlandschaft am Versicherungsmarkt: Ein Ausblick, <https://www.gdv.de/resource/blob/33376/29aaed518cba2d28d01aba3906c18f81/anbieterlandschaft-download-data.pdf>, abgerufen am 6.12.2018.

Modelle der Risikoübernahme – dürften dagegen auf absehbare Zeit enge Grenzen gesetzt sein. Auch eine starke Fragmentierung der Wertschöpfungskette scheint angesichts der in vielen Bereichen bestehenden Größenvorteile wenig plausibel.

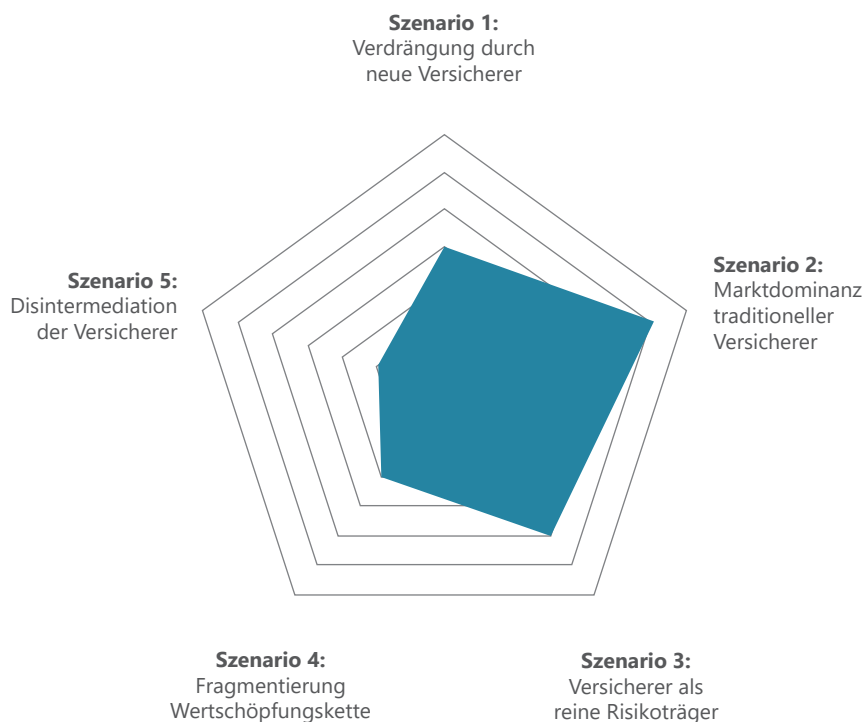
Aus heutiger Sicht spricht sehr vieles dafür, dass der deutsche Versicherungsmarkt auch mittelfristig durch eine breite Auswahl an Angeboten und Anbietern gekennzeichnet bleiben wird. Hierfür sprechen Markteintritte ebenso wie Anpassungen innerhalb der Gruppe der etablierten Anbieter. Eine hohe Leistungsfähigkeit in allen Segmenten des Versicherungsmarkts unter den zukünftigen Gegebenheiten kann allerdings nicht alleine durch den Wettbewerbsprozess und die kontinuierliche Anpassung der Anbieter gewährleistet werden. Auch Staat und Aufsicht sind gefordert. Über eine effektive Wettbewerbspolitik und einen sachgerechten Regulierungsrahmen muss ein fairer Wettbewerb zwischen herkömmlichen und neuen Geschäftsmodellen und allen

Gruppen von Anbietern – auch über die Branchengrenzen hinaus – sichergestellt sein. Monopolstellungen muss entgegengewirkt werden.

Zentrale Grundsätze für den Regulierungsrahmen sind die Gewährleistung eines Level Playing Fields für alle Anbieter und die konsequente Anwendung des Proportionalitätsprinzips in der Aufsicht.²² Regulierung muss effizient und effektiv erfolgen und darf die Nutzung der Chancen der neuen Welt nicht unnötig beeinträchtigen, etwa durch nicht mehr zeitgemäße Vorgaben. Nur dann kann der Wettbewerb auf dem Versicherungsmarkt auch in bewegten Zeiten als ständiges Entdeckungsverfahren für die besten Lösungen im Sinne von Kunden und Gesellschaft wirken.

²² Vgl. GDV, Solvency II – Wer soll das stemmen ?, <https://www.gdv.de/de/themen/positionen-magazin/wer-soll-das-stemmen--39638>, abgerufen am 5.12.2018.

Abbildung 3: Bandbreite mittelfristig plausibler Entwicklungen – Ranking der erwarteten Relevanz der Extremszenarien



Quelle: GDV

7 Wettstreit um Talente

IT-affine Mitarbeiter als Schlüssel zum digitalen Unternehmen

Mit Fug und Recht verlangen die Kunden, dass Versicherer die Chancen der Digitalisierung nutzen und ihre Produkte und Services kontinuierlich weiterentwickeln: bequemer, einfacher, innovativer, schneller, günstiger. Tun es die Versicherer nicht, werden es eben neue Wettbewerber tun – und die sind agil wie nie zuvor; auch auf dem Arbeitsmarkt.

Dass es gerade in Zeiten technologischer Sprünge auf die Qualifikation der Mitarbeiter ankommt, ist keine ganz neue Entdeckung. Umso häufiger wird die Frage nach den negativen Wirkungen der Digitalisierung auf die Zahl der Arbeitsplätze in der Versicherungswirtschaft gestellt. Wahrscheinlich dürften zuallererst die klassische Sachbearbeitung oder die Kundenservicecenter betroffen sein. Hier zeigen sich die Wirkungen der Prozessoptimierung oder des Einsatzes von Robotics, künstlicher Intelligenz und Blockchain. Doch die Digitalisierung löst auch Gegeneffekte aus, es bedarf bereits jetzt neuer Mitarbeiterinnen und Mitarbeiter mit neuen Fähigkeiten. Um diese Digital Natives für ein

Versicherungsunternehmen zu gewinnen, müssen sich diese selbst zu digitalen Unternehmen wandeln. Dabei dürfte sich weniger der Wille zur Digitalisierung, sondern die Verfügbarkeit von IT-affinen Mitarbeitern als Nadelöhr im Erneuerungsprozess des Versicherungsunternehmens herausstellen.

Die Branche steht hier vor einer großen Herausforderung. Eine aktuelle GDV-Studie belegt, dass sich der Stellenaufbau in der IT zwar fortsetzt, dieser aber bei Weitem nicht den gestiegenen Bedarf an qualifiziertem internen IT-Personal deckt. Dies wiederum erhöht den Druck, alte IT-Systeme konsequent abzuschalten und durch neue zu ersetzen, was den Wert der hierfür erforderlichen qualifizierten Digital Natives steigert.

Im digitalen Unternehmen werden gut ausgebildete Querdenker benötigt, die sich für die Versicherungswirtschaft begeistern lassen. Insofern fordert die Digitalisierung von Versicherern einen Spagat: Beschäftigte mit Erfahrung mitzunehmen in die neue Arbeitswelt und gleichzeitig attraktiv zu sein für neue Mitarbeiter mit neuen Qualifikationen. Wer den Weg in die Zukunft



© iStock/From2015



mitgehen will, der muss multimedial denken, in den sozialen Netzwerken ebenso zu Hause sein wie im klassischen Versicherungsgeschäft und vor allem: Er muss den Kulturwandel wollen. Und der Kulturwandel nimmt Fahrt auf: mehr Trial and Error, Coworking-Spaces, gar ein hauseigenes Basketballfeld – auch die neue Arbeitswelt spiegelt eine Branche im digitalen Umbruch wider.²³

Moderne Arbeitswelten zulassen und fördern

Arbeitszeitmodelle müssen der Digitalisierung Rechnung tragen und noch flexibler werden, als sie ohnehin schon sind. Denn je orts- und zeitflexibler sich die Menschen in der Branche einbringen können, umso mehr steigern sie in der digitalisierten Arbeitswelt ihre Einsatz- und Beschäftigungsmöglichkeiten. Allerdings setzt das deutsche Arbeitszeitgesetz einer flexibleren Arbeitswelt der Zukunft enge Grenzen. Die nationalen und europäischen Gesetzgeber sind deshalb gefordert: Das deutsche

Arbeitszeitgesetz, aber auch die Europäische Arbeitszeitrichtlinie müssen grundsätzlich überarbeitet und an die Erfordernisse gegenwärtiger Produktionsbedingungen angepasst werden.

Die Tarifverträge für die private Versicherungswirtschaft haben einen sehr hohen Verbreitungsgrad. Dies liegt vor allem daran, dass sie den Betriebsparteien (Unternehmen und Betriebsräten) zahlreiche Gestaltungsmöglichkeiten belassen. Dies gilt auch für die Gestaltung der Arbeitszeit. Allerdings werden nicht alle Facetten einer flexiblen Arbeitszeitgestaltung ausgeschöpft. Außerdem ist der Geltungsbereich der Tarifverträge äußerst weit gezogen und erfasst auch deutlich übertariflich bezahlte Angestellte, die nicht leitende Angestellte im Sinne der gesetzlichen Definition sind. Die Tarifvertragsparteien der Branche sind aufgerufen, hier für mehr Flexibilität zu sorgen. Ziel muss es sein, die tarifliche Arbeit so flexibel zu gestalten, dass auch und gerade die neuen Wettbewerber auf dem Markt, wie etwa Insurtechs den Flächentarifvertrag als sinnvolles Gestaltungsinstrument der Arbeitsbedingungen in der Branche wahrnehmen und die Tarifbindung anstreben.

²³ Vgl. GDV, Karriere – Ziemlich geile Aufgaben, <https://www.gdv.de/de/themen/positionen-magazin/ziemlich-geile-aufgaben-39582>, abgerufen am 5.12.2018.

8 Agile Aufsicht

Regulierungsziele und Aufsichtspraxis sind zumeist technikneutral. Doch sie sind seit Jahrzehnten von der analogen Welt geprägt. Agile Unternehmen in hoch regulierten Wirtschaftszweigen benötigen gleichfalls eine agile Aufsicht, um auf dem Weg in die digitale Zukunft Schritt halten zu können – mit den Erwartungen der Kunden, mit anderen Branchen und im internationalen Wettbewerb. Agil ist, wer schnell auf Veränderungen reagieren kann.²⁴ Agil ist, wer flexibel ist, wer eine ausgeprägte Anpassungsfähigkeit aufweist, wer – aus eigenem Antrieb – beweglich ist. Allein eine Aufsicht auf digitaler Augenhöhe zu den beaufsichtigten Unternehmen kann diese in die Lage versetzen, ihre Geschäftsprozesse und Produkte in der gebotenen Geschwindigkeit zu verändern, ohne Einbußen bei bestehenden Verbraucherschutzstandards oder der Stabilität des Finanzsystems.

Offenheit für neue Technologien und konsequente Anwendung des Proportionalitätsprinzips

Was erwarten Versicherer also von einer agilen, digitalen Aufsichtsbehörde? Natürlich Offenheit für neue Technologien, nicht blind und bedingungslos, doch stets mit dem Blick auf die Chancen und nicht nur fokussiert auf potenzielle Bedrohungen. Wir wünschen uns die konsequente Vermeidung von Doppelregulierung und redundanten Berichtspflichten und die konsequente Anwendung des Proportionalitätsprinzips.²⁵ Das heißt im Kern: Handlungsspielraum eröffnen, um digitales Geschäft und IT nach risiko- und geschäftsbezogenen Kriterien individuell anpassen zu können.

Daher ist es gut zu sehen, dass in keinem der Veränderungsprozesse der vergangenen 50 Jahre die deutsche Finanzaufsicht – in ihrer jeweiligen Struktur – so konsequent und rasch, ja agil, agiert wie auf den technologischen Wandel. Mit ihrer Studie „Big Data trifft auf künstliche Intelligenz – Herausforderungen und Implikationen für Aufsicht und Regulierung von Finanzdienstleistungen“²⁶

hat die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) eine gründliche Analyse der Herausforderungen und Implikationen für Aufsicht und Regulierung von Finanzdienstleistungen erarbeitet. Damit hat die BaFin nicht nur national, sondern auch auf europäischer und internationaler Ebene eine Vorreiterrolle eingenommen.

Digitalisierungsstrategie der BaFin – ein Schritt in die richtige Richtung

Wie auch die Unternehmen arbeitet die BaFin agil an ihrer Digitalisierungsstrategie. Das ist gut so, erleichtert es doch die Kommunikation zwischen Unternehmen und Aufsicht. Im Kern wird sich die BaFin aus Sicht der Unternehmen in ihrer Strategie vier Fragen zu stellen haben:

- Wie geht sie mit Marktveränderungen um, die der technologische Fortschritt in den Produkten und Prozessen verursacht?
- Wie positioniert sich die Finanzaufsicht vor allem vor dem Hintergrund der Aufgaben des BSI zum Handlungsfeld „IT-Aufsicht und -Sicherheit“?
- Wie plant die BaFin selbst ihren Weg in die digitale Welt, die Transformation in eine digitale Aufsichtsbehörde?
- Wie kann mit Digitalisierung das Meldewesen zwischen Versicherungsunternehmen und Aufsicht effizienter gestaltet werden?

Die Einrichtung des Referats Finanztechnologische Innovationen und der Gruppe IT-Aufsicht/Zahlungsverkehr/Cybersicherheit sind daher ebenso wie die geplante Bestellung eines Chief Digital Officers bei der BaFin sicher die richtigen Schritte und Signale. Entscheidend ist der enge Dialog zwischen Aufsicht und beaufsichtigten Unternehmen.

²⁴ Vgl. Agile Unternehmen, Was ist agil und evolutionär im Kontext von Unternehmen?, <https://agile-unternehmen.de/was-ist-agil-definition/>, abgerufen am 6.12.2018.

²⁵ Vgl. GDV, Solvency II – Wer soll das stemmen?, a.a.O. (Fn. 22).

²⁶ BaFin, Big Data trifft auf künstliche Intelligenz – Herausforderungen und Implikationen für Aufsicht und Regulierung von Finanzdienstleistungen, www.bafin.de/dok/10985478, abgerufen am 6.12.2018.

9 Fazit

Die hier genannten sieben Gamechanger sind nur ein Teil der Herausforderungen, die mit der digitalen Revolution verbunden sind. Denn die digitale Agenda ist global, sie ist umfassend, und sie betrifft alle Wirtschaftszweige. Für die hochregulierte Versicherungsbranche heißt das, dass sie sich natürlich auch um die richtigen Rahmenbedingungen kümmern muss: Um Datenschutz und Urheberrecht, um digitale Infrastruktur und technische Standards. Und natürlich braucht sie auch faire und agile Regulierung – um nur ein paar der wesentlichen Aspekte zu nennen.

Und doch geht es nicht nur um die harten Themen. Wenn die Branche bei der Digitalisierung vorne dabei sein will, braucht sie vor allem eine Veränderung, die das kreative Potenzial entfesselt.

Dies aber ist zuvorderst eine Frage der Unternehmenskultur. Mit einem technokratischen Managementverständnis, dem es zuallererst um die Risikominimierung

und Prozesskontrolle geht, lässt sich diese Veränderung nicht mehr steuern. Die digitale Transformation erfordert vielmehr einen Such- und Lernprozess, bei dem Versuch und Irrtum, Planung und Exekution mehr oder weniger parallel verlaufen. Deshalb ist eine Unternehmenskultur erforderlich, die Eigeninitiative, Selbstorganisation, Kreativität, Teamarbeit und interdisziplinäres Arbeiten fördert. Die Branche braucht das nicht nur, weil sie damit bessere Lösungen zustande bringt für die digitale Welt, sondern vor allem auch als Arbeitgeber, um die innovativsten Köpfe zu überzeugen. Dazu muss die Branche attraktive Angebote machen, Karrierechancen auch für das neue Verständnis von Arbeiten, von Eigenverantwortung, von Dynamik und diversen Teams anbieten. Die Versicherungsbranche braucht eine Unternehmenskultur, in der frei und neu gedacht wird. Das freilich ist eine Kultur, die man sich nicht kaufen kann. Sondern die man sich in einem manchmal mühsamen Veränderungsprozess erarbeiten muss. Und dies ist die vielleicht größte Aufgabe, vor der die Versicherungsbranche steht.



Impressum

Herausgeber

Bundesanstalt für
Finanzdienstleistungsaufsicht (BaFin)
Gruppe Kommunikation
Graurheindorfer Straße 108 | 53117 Bonn
Marie-Curie-Straße 24 – 28 | 60439 Frankfurt am Main
www.bafin.de

Redaktion und Layout

Referat Öffentlichkeitsarbeit und Reden
Redaktion: Ursula Mayer-Wanders (Leitung)
Tel.: +49 (0)228 4108-2978
Jens Valentin
Tel.: +49 (0)228 4108-2363

E-Mail: perspektiven@bafin.de

Designkonzept

werksfarbe.com | konzept + design
Humboldtstraße 18, 60318 Frankfurt
www.werksfarbe.com

Bonn und Frankfurt am Main | 28. Februar 2019
ISSN 2625-5952

Bezug

Die Schriftenreihe BaFinPerspektiven erscheint auf der Internetseite der BaFin jeweils in deutscher und englischer Sprache. Die englische Ausgabe erscheint unter dem Titel „BaFinPerspectives“. Mit dem Abonnement des Newsletters der BaFin werden Sie über das Erscheinen einer neuen Ausgabe per E-Mail informiert. Den BaFin-Newsletter finden Sie unter:
www.bafin.de » [Newsletter](#).

Disclaimer

Bitte beachten Sie, dass alle Angaben sorgfältig zusammengestellt worden sind, jedoch eine Haftung der BaFin für die Vollständigkeit und Richtigkeit der Angaben ausgeschlossen ist.

Ausschließlich zum Zweck der besseren Lesbarkeit wird in den BaFinPerspektiven auf die geschlechtsspezifische Schreibweise verzichtet. Alle personenbezogenen Bezeichnungen sind somit geschlechtsneutral zu verstehen.

Die Beiträge und Interviews in den BaFinPerspektiven unterliegen dem Urheberrecht. Nachdruck und Verbreitung sind nur mit schriftlicher Zustimmung der BaFin – auch per E-Mail – gestattet.

Satz

Naumilkat – Agentur für Kommunikation und Design
Jahnstraße 84
40215 Düsseldorf

Druck

W. Kohlhammer Druckerei GmbH & Co. KG
Augsburger Straße 722
70329 Stuttgart

Bundesanstalt für
Finanzdienstleistungsaufsicht (BaFin)
Gruppe Kommunikation
Graurheindorfer Straße 108, 53117 Bonn
Marie-Curie-Straße 24 – 28, 60439 Frankfurt am Main
www.bafin.de