Regulierung von künstlicher Intelligenz für FinTech-Anwendungen

Stand der Diskussion in der Schweiz und im Ausland

Cornelia Stengel | Gino Wirthensohn | Luca Stäuble*

New methods of artificial intelligence represent one of the greatest promises and most prospective developments of digitalisation. Artificial intelligence has already enabled numerous innovative applications in the areas of image recognition, medicine, language and mobility, and it is also increasingly being used in the financial market, on which this article focuses. In addition to great opportunities, new methods always entail risks, which are usually countered with regulation, especially in the financial market. This article presents – without claiming to be exhaustive – various possible applications for artificial intelligence in connection with financial services and highlights the question of necessity as well as the status of the discussions surrounding its regulation in Switzerland and abroad.

Inhaltsübersicht

I. Einleitung

Neue Methoden künstlicher Intelligenz stellen eines der grössten Versprechen und eine der aussichtsreichsten Entwicklungen der Digitalisierung dar. Im Bereich der Bilderkennung, der Medizin, der Sprache oder der Mobilität hat künstliche Intelligenz bereits zahlreiche innovative Anwendungen ermöglicht und auch auf dem Finanzmarkt, auf welchen dieser Beitrag fokussiert, kommt sie zunehmend zum Einsatz. Neuartige Methoden bergen neben grossen Chancen immer auch Risiken, welchen gerade auf dem Finanzmarkt üblicherweise mit Regulierung begegnet wird.[1]

Der vorliegende Beitrag stellt – ohne Anspruch auf Vollständigkeit – verschiedene Einsatzmöglichkeiten für künstliche Intelligenz in Zusammenhang mit Finanzdienstleistungen vor und beleuchtet die Frage der Notwendigkeit sowie den Stand der Diskussionen rund um deren Regulierung in der Schweiz und im Ausland.

II. Begriff und Definition

Für den Begriff «künstliche Intelligenz» (englisch: «Artificial Intelligence», häufig auch abgekürzt: «KI» oder «AI») existiert keine exakte, allgemein gültige und akzeptierte Definition.[2] Die Bezeichnung lässt

* Prof. Dr. iur. *Cornelia Stengel,* Rechtsanwältin; MLaw *Gino Wirthensohn;* MLaw *Luca Stäuble,* Rechtsanwalt.

1 Bundesanstalt für Finanzdienstleistungsaufsicht BaFin, Big Data und künstliche Intelligenz, Prinzipien für den Einsatz von Algorithmen in Entscheidungsprozessen, 2021, 3 ff.

2 Staatssekretariat für Bildung, Forschung und Innovation SBFI, Herausforderungen der künstlichen Intelligenz, Bericht der interdepartementalen Arbeitsgruppe «Künstliche Intelligenz» an den Bundesrat, 13. Dezember 2019, 7; *Rainer Kessler/Jutta Sonja Oberlin,* Künstliche Intelligenz: Quo Vadis?, Compliance Berater CB 2020, 89 ff., 90.

häufig mehr vermuten, als tatsächlich dahintersteckt. Denn eine Abbildung menschlicher Intelligenz oder auch nur Ansätze dazu sind nach wie vor nicht absehbar.[3] Vielmehr wird der Begriff in der Regel und auch im vorliegenden Beitrag vereinfachend zur Bezeichnung unterschiedlicher Systeme verwendet, welche sich durch die folgenden strukturellen Elemente in unterschiedlicher Ausprägung auszeichnen[4]:

– Auswertung grosser Mengen von Daten in hoher Komplexität in einer Form, welche mit herkömmlichen Methoden nicht möglich wäre, insbesondere durch selbstständig lernende Algorithmen;
– Erstellung von Vorhersagen als wesentliche Grundlage (automatisierter) Entscheidungen;
– Simulation von Fähigkeiten, die mit menschlicher Kognition in Verbindung gebracht werden;
– weitgehend autonomes Agieren.[5]

Daneben wird im vorliegenden Zusammenhang auch häufig von «maschinellem Lernen» gesprochen. Selbstständig lernende Algorithmen, sogenannte «Algorithmen des maschinellen Lernens» (englisch: «Machine Learning»), sind die Methoden von künstlicher Intelligenz, um Muster in Datensätzen zu erkennen und darauf basierend Voraussagen machen zu können.[6] Systeme, die auf maschinellem Lernen beruhen, fällen Entscheidungen entsprechend nicht auf der Basis von Kausalitäten im Rahmen strukturierter «wenn-dann-Schemata», sondern gestützt auf statistische Zusammenhänge.[7]

Art. 3 Abs. 1 i.V.m. Anhang 1 des jüngst veröffentlichten Vorschlags der EU-Kommission für eine Verordnung zur Regulierung künstlicher Intelligenz umschreibt den Begriff «System der künstlichen Intelligenz» als «eine Software, die mit einer oder mehreren der [nachfolgenden] Techniken und Konzepte entwickelt worden ist und im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren[8]:»

«a) Konzepte des maschinellen Lernens, mit beaufsichtigtem, unbeaufsichtigtem und bestärkendem Lernen unter Verwendung einer breiten Palette von Methoden, einschließlich des tiefen Lernens *(Deep Learning);*

b) Logik- und wissensgestützte Konzepte, einschließlich Wissensrepräsentation, induktiver (logischer) Programmierung, Wissensgrundlagen, Inferenz- und Deduktionsmaschinen, (symbolischer) Schlussfolgerungs- und Expertensysteme;

c) Statistische Ansätze, Bayessche Schätz-, Such- und Optimierungsmethoden.»[9]

III. Einsatzmöglichkeiten: KI in FinTech

Auf dem Finanzmarkt werden Methoden künstlicher Intelligenz schon länger eingesetzt und die Anwendungsfälle nehmen weiter zu, da ihr Einsatz beispielsweise Kostensenkungen durch Automatisierungen oder Qualitätssteigerungen durch massgeschneiderte Lösungen für Kundinnen und Kunden verspricht.[10] Nachfolgend wird exemplarisch eine Auswahl von Einsatzmöglichkeiten für Methoden von künstlicher Intelligenz im Finanzmarkt beschrieben.[11]

Methoden künstlicher Intelligenz können eingesetzt werden, um die Entscheidungsfindung bei der *Kreditvergabe* zu verbessern, indem unter Berücksichtigung alternativer Datenquellen[12] bessere Prognosen über die Rückzahlungsfähigkeit einer Kredit-

3 Bundesanstalt für Finanzdienstleistungsaufsicht BaFin, Big Data trifft auf künstliche Intelligenz, Herausforderungen und Implikationen für Aufsicht und Regulierung von Finanzdienstleistungen, 2018, 7; SBFI KI 2019 (Fn. 2), 7 f.

4 Elemente gemäss: SBFI KI 2019 (Fn. 2), 7.

5 BaFin BDAI 2018 (Fn. 3), 7, Fn. 1: «Vereinfacht kann Artificial Intelligence als ein Zusammenspiel von Massendaten, ausreichenden Rechenressourcen und maschinellem Lernen aufgefasst werden».

6 SBFI KI 2019 (Fn. 2), 7.

7 *Florent Thouvenin/Alfred Früh,* Automatisierte Entscheidungen, Grundfragen aus der Perspektive des Privatrechts, SZW 2020, 3 ff., 6 f.; *Rolf H. Weber/Simon Henseler,* Regulierung von Algorithmen in der EU und in der Schweiz, Zeitschrift für Europarecht EuZ 2020, 28 ff., 29 (m.w.H.).

8 Art. 3 Vorschlag für eine Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, COM(2021) 206 final, 21. April 2021.

9 COM(2021) 206 final, 21. April 2021, Anhang 1.

10 SBFI KI 2019 (Fn. 2), 79.

11 Weitere Anwendungsfälle im Bankensektor z.B. in: Hong Kong Monetary Authority HKMA/PwC, Reshaping Banking with Artificial Intelligence, Dezember 2019, 41 ff.

12 *«Alternative data»:* Daten, welche nicht zu den «klassischen» Finanzdaten wie Ausgaben und Zahlungsvorgänge gehören, beispielsweise demografische Daten oder Daten zum Lebensstil; vgl. z.B. Hong Kong Monetary Authority HKMA/PwC 2019 (Fn. 11), 57.

nehmerin oder eines Kreditnehmers gemacht werden können.[13] So können beispielsweise die Benutzung des Smartphones (z.B. Uhrzeit von Telefongesprächen)[14] oder das Verhalten in sozialen Netzwerken Rückschlüsse auf das Zahlungsverhalten geben.[15] Eine Studie der Federal Reserve Bank of Philadelphia hat ergeben, dass eine hohe Korrelation zwischen dem Zahlungsverhalten und dem Verhalten ausserhalb des Finanzbereichs besteht und viele Kreditnehmerinnen und Kreditnehmer bei einem auf traditioneller Risikoeinstufung basierenden Verfahren ein schlechteres Profil ausweisen als bei einem Verfahren, welches alternative Datenquellen mitberücksichtigt.[16] Auch die automatisierte Auswertung von IT-Systemen eines kreditbeantragenden Unternehmens, beispielsweise des Warenwirtschafts- oder Buchhaltungssystems, durch Methoden künstlicher Intelligenz ermöglicht eine genauere Entscheidungsfindung oder kann sogar den Kreditbedarf eines Unternehmens antizipieren, was ein proaktives Angebot von massgeschneiderten Kreditprodukten ermöglicht.[17]

KI-Systeme können darüber hinaus auch Anlageentscheidungen in der *Vermögensverwaltung* unterstützen.[18] Dies geschieht beispielsweise, indem wichtige Erkenntnisse aus grossen Datenmengen wie Medienberichterstattungen und Marktforschungen, aber auch alternativen Daten wie z.B. Satellitenbildern, gewonnen werden.[19] Quantitative Modellierungsprozesse können automatisiert und Algorithmen genutzt werden, um die Portfoliogewichtung in Echtzeit anzupassen.[20] Auch für die Individualisierung eines Portfolios auf das Risiko- und Interessensprofil einer Anlegerin oder eines Anlegers können Methoden künstlicher Intelligenz eingesetzt werden. So können Anbieter individuellere Portfolios zusammenstellen, welche z.B. Social-Impact-Investing-Faktoren[21] als Teil der Investmentstrategie berücksichtigen.[22] *Robo Advisors*[23] der vierten Generation verwenden selbstlernende Algorithmen.[24] Dabei wird das menschliche Urteilsvermögen für die Auswahl von Investmentprodukten durch selbstlernende künstliche Intelligenz ersetzt.[25]

Künstliche Intelligenz kann ebenfalls mittels Einsatzes von *Chatbots* in der Kundeninteraktion verwendet werden.[26] Diese digitalen Gesprächspartner können gestützt auf Sprach- oder Texteingaben von Kundinnen und Kunden schnellere und konsistentere Antworten als menschliche Ansprechpartner liefern.[27] Chatbots können auch für den internen Einsatz, wie z.B. als Mitarbeiter-Helpdesk, genutzt werden. So soll ein trainierter Chatbot einer Bank bereits 87% der Anfragen verstehen können.[28]

Insbesondere im *RegTech*[29]-Bereich gibt es verschiedene weitere Anwendungsfälle für künstliche Intelligenz, wie z.B. bei der *Geldwäschereibekämpfung*[30] in den Bereichen *Kundenrisikoeinstufung* oder

13 *Henri Arslanian/Fabrice Fischer,* The Future of Finance, The Impact of FinTech, AI, and Crypto on Financial Services, Cham 2019, 183.

14 *Elizabeth Dwoskin,* Lending Startups Look at Borrowers' Phone Usage to Assess Creditworthiness, Smartphones allow lenders' apps to detect subtle patterns of behavior that correlate with repayment or default, WSJ vom 1. Dezember 2015, abrufbar unter: <https://www.wsj.com/articles/lending-startups-look-at-borrowers-phone-usage-to-assess-creditworthiness-1448933308> (zuletzt besucht: 17.9.2021).

15 *Hans Kuhn,* Vertrauen, Kredit und Kreditsicherheiten, SZW 2017, 792 ff., 798.

16 *Julapa Jagtiani/Catharine Lemieux,* Fintech Lending: Financial Inclusion, Risk Pricing, and Alternative Information, Federal Reserve Bank of Philadelphia, WP No. 17-17, 6. Juli 2017; siehe dazu auch *Kuhn* (Fn. 15), 798.

17 *Arslanian/Fischer* (Fn. 13), 184.

18 *Arslanian/Fischer* (Fn. 13), 185.

19 Financial Stability Board FSB, Artificial intelligence and machine learning in financial services, Market developments and financial stability implications, 1. November 2017, 5, 10; *Arslanian/Fischer* (Fn. 13), 186.

20 *Arslanian/Fischer* (Fn. 13), 186.

21 Soziale bzw. ökologische Wirkung: <*https://wirtschaftslexikon.gabler.de/definition/impact-investing-120058*> (zuletzt besucht: 7. Juli 2021).

22 *Arslanian/Fischer* (Fn. 13), 186.

23 Zur Definition: *Lucie Fryzek/Pascal Zysset,* Rechtlicher Rahmen für Robo Advisor, Jusletter 18. Mai 2020, N 3 m.w.H.

24 Deloitte, The expansion of Robo-Advisory in Wealth Management, 2016, 3.

25 *Damir Tokic,* BlackRock Robo-Advisor 4.0, When artificial intelligence replaces human discretion, Strategic Change 27(4), 2018, 285 ff.

26 Financial Stability Board FSB 2017 (Fn. 19), 14.

27 Hong Kong Monetary Authority HKMA/PwC 2019 (Fn. 11), 50.

28 Hong Kong Monetary Authority HKMA/PwC 2019 (Fn. 11), 51 m.w.H.

29 Zur Definition: *Franca Contratto,* «RegTech», Digitale Wende für Aufsicht und Compliance, Jusletter 15. August 2016, N 5 f.

30 Financial Stability Board FSB 2017 (Fn. 19), 10, 11; Schweizerische Bankiervereinigung, Leitfaden im Umgang mit Daten im Geschäftsalltag 2021, 17.

Transaktionsmonitoring.[31] So hat das Institute of International Finance erhoben, dass insbesondere bei der Geldwäschereibekämpfung die Verwendung von KI weit verbreitet ist – sowohl bereits operativ als auch für künftige und Pilotprojekte.[32] In der Schweiz müssen Finanzintermediäre gemäss Art. 6 Abs. 2 GwG Hintergründe und den Zweck einer Transaktion abklären, wenn diese z.B. ungewöhnlich erscheint oder die Transaktion oder die Geschäftsbeziehung mit einem erhöhten Risiko behaftet ist. Diese so genannte Transaktionsüberwachung ist gemäss Art. 20 Abs. 2 GWV-FINMA mit einem informatikgestützten System zu betreiben. KI-Lösungen können dabei verdächtige Transaktionen erkennen und insbesondere die Anzahl sogenannter *False-Positives*[33] reduzieren, womit das Personal vermehrt für die Abklärungen von höheren Risikofällen einsetzbar ist.[34] Ein Transaktionsmonitoring kann ebenfalls zur Identifikation von betrügerischen Zahlungen eingesetzt werden. Mittels Verwendung einer KI-Lösung konnte im Rahmen einer Studie die Betrugserkennungsrate von 85% auf 90% erhöht werden.[35]

Auch die *Versicherungsbranche* bedient sich Methoden künstlicher Intelligenz für Analyseinstrumente.[36] So können beispielsweise auf der Basis eingereichter Bilder automatisch Schäden an Fahrzeugen bewertet werden, um Reparaturkosten zu bestimmen.[37] Auch für personalisierte Versicherungsangebote oder Betrugserkennung kann künstliche Intelligenz eingesetzt werden.[38] Die der Versicherungsindustrie eigene, umfangreiche Bearbeitung von Kundendaten birgt zudem grosse Potenziale im Bereich *Big Data Analytics*.[39]

IV. Rechtsrahmen Schweiz

1. «Grundsätzlich geeigneter allgemeiner Rechtsrahmen in der Schweiz»?

Die dargestellten Einsatzmöglichkeiten von Methoden künstlicher Intelligenz im Finanzmarkt zeigen das grosse Potenzial und die Chancen dieser Entwicklung deutlich auf. So können Anwendungen, die auf künstlicher Intelligenz basieren, einerseits für die Optimierung, d.h. Steigerung von Effektivität und Effizienz interner Prozesse eingesetzt werden wie beispielsweise zur Betrugs- und Geldwäschereiprävention. Auf der anderen Seite ermöglicht ihr Einsatz im Endkundengeschäft innovative Geschäftsmodelle (z.B. *Chatbots, Robo Advice* oder auch *Open Banking*). Beide Aspekte führen auf Seiten des Unternehmens zu Kosteneinsparungen, weil es – nach erfolgreicher Implementierung solcher Methoden – für die entsprechenden Tätigkeiten keine bzw. weniger Mitarbeiter und Mitarbeiterinnen einsetzen muss und somit seine Ressourcen besser allokieren kann.[40] Schliesslich lassen sich mit dem Einsatz von sophistizierten Anwendungen der künstlichen Intelligenz in der Regel qualitativ bessere bzw. präzisere Ergebnisse erzielen, was sich positiv sowohl auf die Reputation (durch eine Verbesserung der Compliance) als auch insgesamt auf die Wettbewerbsfähigkeit (durch eine Verbesserung der Produkte und Dienstleistungen) des betreffenden Unternehmens auswirkt.

Neue Methoden bergen aber immer auch Risiken, welchen gerade auf dem Finanzmarkt üblicherweise mit Regulierung begegnet wird.

Bei den Risiken, die in Zusammenhang mit dem Einsatz künstlicher Intelligenz bisweilen identifiziert wurden, handelt es sich um Herausforderungen wie sie aus dem Bereich der Statistik bekannt sind, welche jedoch durch den Einsatz von Methoden der künstlichen Intelligenz verstärkt werden. So kann insbesondere die Nachvollziehbarkeit bzw. Erklärbarkeit bestimmter Vorhersagen bzw. Ergebnisse lei-

31 Weitere RegTech-Anwendungsfälle in: Financial Stability Board FSB 2017 (Fn. 19), 19 ff.; Hong Kong Monetary Authority HKMA/PwC 2019 (Fn. 11), 53 ff.

32 Institute of International Finance IIF, Machine Learning in Anti-Money Laundering, Summary Report, Oktober 2018, 3.

33 Diese können bis zu 98% der Treffer ausmachen: *<https://www.forbes.com/sites/tomdavenport/2020/10/23/the-future-of-work-now-ai-driven-transaction-surveillance-at-dbs-bank/?sh=3ee0cdde3f7f>* (zuletzt besucht: 9. Juni 2021).

34 Institute of International Finance IIF 2018 (Fn. 32), 3.

35 *Cristina Soviany,* The benefits of using artificial intelligence in payment fraud detection, A case study, Journal of Payments Strategy & Systems, Volume 12 Number 2, 2018, 102 ff., 110.

36 FINMA, Risikomonitor 2020, 16 f.

37 *Arslanian/Fischer* (Fn. 13), 187.

38 Accenture, Machine Learning In Insurance, 2018, 6 ff.

39 *Thomas Puschmann/Rolf H. Weber,* Neuerfindung des Finanzsektors?, SZW 2017, 79 ff., 91 mit einer Übersicht von Fintech-Innovationen im Versicherungsbereich und den entsprechenden rechtlichen Herausforderungen.

40 Vgl. auch die Übersicht bei SBFI KI 2019 (Fn. 2), 79.

den oder auch die Qualität von Vorhersagen und Ergebnissen an sich, weil diese stark von der Qualität der (Trainings-)Daten und Algorithmen abhängt. Dabei handelt es sich in erster Linie um *technische* Herausforderungen. Je nach Anwendungsgebiet können insbesondere die fehlende Nachvollziehbarkeit bzw. Erklärbarkeit von Ergebnissen sowie die autonome Handlungsfähigkeit von KI-Systemen aber auch *rechtliche* Herausforderungen mit sich bringen.[41]

Ein im Jahr 2019 verfasster Bericht der interdepartementalen Arbeitsgruppe «Künstliche Intelligenz» des Staatssekretariats für Bildung, Forschung und Innovation (SBFI) an den Bundesrat beschäftigte sich mit ebendiesen Herausforderungen, welche die Anwendung künstlicher Intelligenz in den verschiedensten Themenbereichen mit sich bringt.[42] Die Arbeitsgruppe kam zum Schluss, dass der bestehende generelle Rechtsrahmen in der Schweiz zum damaligen Zeitpunkt grundsätzlich geeignet gewesen sei, mit den neuen Anwendungen und Geschäftsmodellen im Bereich künstlicher Intelligenz umzugehen. Dies wurde damit begründet, dass die Nutzung neuer und innovativer Technologien wie diejenige der KI nicht in einem rechtsfreien Raum erfolge, sondern vollumfänglich dem geltenden Recht unterstehe und die relevanten Rechtsprinzipien in der Regel technologieneutral formuliert seien, womit sie insbesondere auch auf Systeme mit Methoden künstlicher Intelligenz angewendet werden können.[43]

In der Lehre wird zu Recht darauf hingewiesen, dass die rechtliche Erfassung von KI sektorenspezifisch geprüft und gegebenenfalls vorgenommen werden müsse und dafür plädiert, dass – anders als in der EU – kein spezifisches KI-Gesetz zu schaffen, sondern in den jeweils betroffenen Rechtsbereichen sofern und soweit erforderlich punktuelle Anpassungen der bestehenden Normen vorzunehmen seien.[44] Auch eine bloss punktuelle Anpassung hat unseres Erachtens indes nur dort zu erfolgen, wo bestehende Regelungen durch entsprechende Auslegung nicht angemessen auf KI-Sachverhalte angewendet werden können (wofür gemäss dem erwähnten Bericht des SBFI zumindest im Jahr 2019 keine Anhaltspunkte bestanden). Im Bereich des Finanzmarktrechts steht der FINMA gemäss Art. 7 Abs. 1 lit. b FINMAG insbesondere das Instrument des Rundschreibens zur Verfügung, mit welchem sie zwecks einheitlicher und sachgerechter Praxis offene, unbestimmte Rechtsnormen konkretisieren und Vorgaben für die Ermessensausübung aufstellen kann.[45]

Nachfolgend werden aus der Perspektive verschiedener ausgewählter Rechtsgebiete einige der aktuell diskutierten Herausforderungen und Fragen, die sich in Zusammenhang mit dem Einsatz von Methoden künstlicher Intelligenz ergeben, dargestellt, wobei kein Anspruch auf Vollständigkeit besteht und der Fokus auf den Anwendungsfällen im Bereich des Finanzmarktes bzw. den eingangs dargestellten Einsatzmöglichkeiten liegt.

2. Grundrechte

Ganz grundsätzlich ist im Zusammenhang mit Methoden künstlicher Intelligenz an die Würde des Menschen (Art. 7 BV) zu denken. Die Berücksichtigung der Menschenwürde ist deshalb zentral, weil künstliche Intelligenz nicht dazu führen darf, dass der Mensch als Objekt behandelt wird.[46] Dieses Risiko ist dem Einsatz künstlicher Intelligenz inhärent, weil die entsprechenden Methoden (noch) nicht genügend ausgereift sind, um alle menschlichen Aspekte zu erfassen, zu bewerten und damit zu berücksichtigen.

Weiter kann der Einsatz von Methoden künstlicher Intelligenz das Grundrecht des rechtlichen Gehörs (Art. 29 Abs. 2 BV) tangieren.[47] Wird beispiels-

41 SBFI KI 2019 (Fn. 2), 8.

42 SBFI KI 2019 (Fn. 2), *passim*.

43 SBFI KI 2019 (Fn. 2), 8, 34 f.; *Michal Cichocki,* Guidelines für Künstliche Intelligenz (KI), Besteht aus rechtlicher Sicht Handlungsbedarf?, Jusletter IT 25. Februar 2021, N 27; vgl. demgegenüber aber die kürzlich in Kraft getretene DLT-Gesetzgebung, welche sich zumindest sehr stark an einer Technologie orientiert (Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register, BBl 2020 7801).

44 *Nadja Braun Binder/Thomas Burri/Melinda Florina Lohmann/Monika Simmler/Florent Thouvenin/Kerstin Noëlle Volkinger,* Künstliche Intelligenz, Handlungsbedarf im Schweizer Recht, Jusletter 28. Juni 2021, N 54 f.

45 Vgl. auch die kürzlich von der BaFin veröffentlichten Prinzipien für den Einsatz von Algorithmen in Entscheidungsprozessen: BaFin BDAI 2021 (Fn. 1), *passim*.

46 *Kessler/Oberlin* (Fn. 2), 90; *Werner Pfeil,* Der Mensch steht höher als Technik und Maschine, Benötigen wir ein Grundrecht zum Schutz vor Künstlicher Intelligenz?, Zeitschrift zum Innovations- und Technikrecht 2020, 82 ff., 88; *Rolf H. Weber,* Automatisierte Entscheidungen, Perspektive Grundrechte, SZW 2020, 18 ff., 19.

47 Vgl. dazu auch die Informationspflicht, welche das revidierte Datenschutzgesetz bei einer automatisierten Ein-

weise ein Gerichtsurteil unter Einbezug von Methoden künstlicher Intelligenz gefällt, kann es allenfalls nur beschränkt nachvollziehbar begründet werden, wenn es den Methoden selbst an Transparenz und Nachvollziehbarkeit mangelt.[48] Umgekehrt lässt sich fragen, wie nachvollziehbar die Urteilsbegründung durch einen Menschen ist, zumal viele menschliche Entscheidungen durch Vorurteile *(Bias)* beeinflusst werden.[49]

Auch die Meinungsäusserungsfreiheit und die Medienfreiheit (Art. 16 und 17 BV)[50], das Recht auf Privatsphäre (Art. 13 BV) sowie das Diskriminierungsverbot (Art. 8 Abs. 2 BV) können durch den Einsatz von Methoden künstlicher Intelligenz betroffen sein, wobei gerade die beiden letzten mit Blick auf die eingangs dargelegten Einsatzmöglichkeiten für künstliche Intelligenz im Finanzmarkt[51] besondere Beachtung verdienen.

Das Recht auf *Privatsphäre,* dessen Bedeutung im digitalen Zeitalter von verschiedener Seite in Frage gestellt wird,[52] umfasst mit Art. 13 Abs. 2 BV den Anspruch auf Schutz vor Missbrauch der persönlichen Daten und ist auch als Recht auf informationelle Selbstbestimmung bekannt.[53] Dieses Recht ist in Zusammenhang mit dem Einsatz von KI-Anwendungen regelmässig besonders betroffen, weil künstliche Intelligenz definitionsgemäss eine umfangreiche automatisierte Verarbeitung von (Personen-)Daten voraussetzt. Einen erhöhten Schutz erfuhr das Recht auf informationelle Selbstbestimmung kürzlich durch die Totalrevision des Schweizer Datenschutzgesetzes (DSG), welches insbesondere für automatisierte Einzelentscheidungen neu spezifische Regeln bzw. Informationspflichten vorsieht. Regelmässig dürfte sich beim Einsatz von komplexen KI-Anwendungen auch die Frage stellen, ob bzw. wie die damit verbundenen Datenbearbeitungen mit den datenschutzrechtlichen Bearbeitungsgrundsätzen wie insbesondere demjenigen der Zweckgebundenheit, der Erkennbarkeit und der Verhältnismässigkeit im Einklang stehen bzw. wie sich solche Bearbeitungen andernfalls rechtfertigen lassen.[54]

Das Diskriminierungsverbot gemäss Art. 8 Abs. 2 BV verbietet jegliche Diskriminierung, insbesondere aufgrund von Herkunft, Rasse, Geschlecht, Alter, Sprache, sozialer Stellung, Lebensform, religiöser, weltanschaulicher oder politischer Überzeugung und körperlicher, geistiger oder psychischer Behinderung. Nun können Methoden künstlicher Intelligenz jedoch zu erheblichen Diskriminierungen führen, wenn sie auf diskriminierenden Inhalten basieren und lernende Algorithmen das diskriminierende Verhalten oder diskriminierende Entscheide von Menschen nachahmen bzw. vorwegnehmen.[55] Es besteht also das Risiko, dass künstliche Intelligenz diskriminierende Entscheidungen trifft, weil die Trainingsdaten selbst diskriminierende Elemente enthalten.[56] So könnten beispielsweise bei der Prüfung der Kreditfähigkeit einer Person durch lernende Algorithmen, die auf der Basis von Daten über Kreditgewährungen in der Vergangenheit trainiert wurden, unbeabsichtigt und ohne sachliche Rechtfertigung Merkmale wie Geschlecht oder Herkunft berücksichtigt werden, was nicht nur zu diskriminierenden, sondern auch zu falschen Resultaten führen kann: Weil in der Vergangenheit Frauen angesichts der klassischen Rollenverteilung in einer Familie seltener Kredite aufgenommen haben, stehen den Algorithmen entsprechend weniger Trainingsdaten mit weiblichen Kreditnehmerinnen zur Verfügung, woraus sie den Schluss ziehen könnten, dass Frauen tendenziell weniger kreditfähig seien.[57] Diese Ausgangslage

zelentscheidung vorsehen wird (unten Punkt IV.4) und der «Anspruch auf *menschliches* Gehör», der in der Lehre daraus abgeleitet wird.

48 *Nadja Braun Binder,* Künstliche Intelligenz und automatisierte Entscheidungen in der öffentlichen Verwaltung, SJZ 2019, 467 ff., 472.

49 *Thouvenin/Früh* (Fn. 7), 10.

50 Vgl. dazu weiterführend: *Weber* (Fn. 46), 19.

51 Vgl. Punkt III.

52 Vgl. hierzu die Übersicht in: *Hanspeter Thür,* Die Privatsphäre im Zeitalter von Big Data, Jusletter 21. Mai 2015, N 21 ff., der sogar von einem digitalen Panoptikum spricht.

53 BGE 144 II 91; BSK BV-*Diggelmann,* Art. 13 N 32, in: Bernhard Waldmann/Eva Maria Belser/Astrid Epiney (Hrsg.), Basler Kommentar zur Bundesverfassung, Basel 2015 (zit. BSK BV-*Verfasser*); *Weber* (Fn. 46), 19.

54 Vgl. dazu Punkt IV.4.

55 *Kessler/Oberlin* (Fn. 2), 92; *Weber* (Fn. 46), 19 f.

56 *Braun Binder* (Fn. 48), 473.

57 Vgl. dazu auch den Bericht des Executive Office of the President *[Obama]* zum Thema Big Data, welcher aufzeigt, dass künstliche Intelligenz sich bei ihrer Entscheidung, einen Kredit zu vergeben, auf die Kredithistorie der betreffenden Person, mithin die Vergangenheit und nicht die Gegenwart stützt. Dabei seien 11% der Bevölkerung «credit invisible» und 8,3% «unscorable», weil die Bonitätsprüfungsplattformen zu wenig Daten haben, um deren Kreditfähigkeit zu bewerten. Insgesamt 27–28% der Afroamerikaner und Afroamerikanerinnen und Lateinameri-

führt unmittelbar zur Frage, ob Diskriminierung durch Methoden künstlicher Intelligenz vermieden werden könnte, indem Algorithmen mit möglichst diskriminierungsfreien Daten trainiert werden bzw. der künstlichen Intelligenz signalisiert wird, gewisse Eigenschaften nicht zu berücksichtigen.[58] Studien im FinTech-Bereich zeigen, dass künstliche Intelligenz durchaus so trainiert werden kann, dass sie beispielsweise bei der Kreditvergabe weniger diskriminierende Entscheide fällt als ein Mensch.[59]

Anders begründet, aber nicht minder bedeutsam, ist die Diskriminierungsgefahr in Zusammenhang mit Prämienkalkulationen bzw. Abschlüssen von Versicherungen.[60] *Weber* weist diesbezüglich insbesondere auf die Berücksichtigung körperlicher, geistiger oder psychischer Behinderungen hin.[61] Auch die FINMA hat im Risikomonitor 2020 in Zusammenhang mit den längerfristigen Trends und Risiken den sog. «gläsernen Versicherungsnehmer» und die damit zusammenhängenden Gefahren hervorgehoben. So könnten bestimmte, beispielsweise ethnische, Gruppen mit erhöhten bzw. schlechten Risiken, diese künftig möglicherweise nur zu schlechteren Konditionen versichern lassen als andere Gruppen.[62]

Im Rahmen der Diskussion um KI kommt den Grundrechten eine zentrale Bedeutung zu. Eine untergeordnete Bedeutung kommt ihnen – jedoch immer im Kontext der KI-Anwendung durch Finanzinstitute zu, denn die Grundrechte richten sich grundsätzlich nur an den Staat und nicht an Private. Direkte Drittwirkung kommt gemäss herrschender Lehre und Rechtsprechung weder dem Diskriminierungsverbot nach Art. 8 Abs. 2 BV noch dem Schutz der Privatsphäre zu.[63] Allenfalls könnten die Krankenversicherungsgesellschaften als Unternehmen, die staatliche Aufgaben wahrnehmen, im Sinne von Art. 35 Abs. 2 BV qualifiziert werden, womit diese insbesondere an das Diskriminierungsverbot gebunden wären.[64] Entsprechend wird in der Lehre die Frage diskutiert, ob in Bezug auf das Verhältnis zwischen Privaten gesetzgeberischer Handlungsbedarf bestehen könnte.[65] Dabei wird richtigerweise vorgebracht, dass unter geltendem Recht insbesondere mit Art. 28 Abs. 2 ZGB, bei dessen Auslegung der Zivilrichter aufgrund von Art. 35 Abs. 3 BV auch das Diskriminierungsverbot zu berücksichtigen hat, eine hinreichende Möglichkeit besteht, ungerechtfertigte über der Bagatellschwelle liegende Diskriminierungen infolge Einsatzes von KI als widerrechtliche Persönlichkeitsverletzung rechtlich zu erfassen, weshalb grundsätzlich keine Anpassung der Gesetze notwendig ist.[66] Im Versicherungsbereich hat die FINMA gemäss Art. 46 lit. f VAG i.V.m. Art. 117 Abs. 2 AVO immerhin zu verhindern, dass die Versicherten durch eine «juristisch oder versicherungstechnisch nicht begründbare erhebliche Ungleichbehandlung» benachteiligt werden.[67]

3. Finanzmarktrecht

3.1 Einführung

Das Erbringen von Finanzdienstleistungen ist zur Sicherstellung des Kunden- und Systemschutzes (Art. 4 FINMAG) der Aufsicht der FINMA unterstellt und

kaner und Lateinamerikanerinnen seien «credit invisible» oder «unscorable», wesentlich öfter als weisse Amerikaner und Amerikanerinnen und Asiaten und Asiatinnen. Um diese Ungleichheit zu beheben, werden in diesem Bericht die Kreditinstitute aufgefordert, ihre Informationsquellen zu erweitern. So soll neben Bonitätsprüfungsplattformen und Scoringwerten beispielsweise berücksichtigt werden, ob die Telefonrechnungen regelmässig bezahlt werden oder neben dem Wohnort auch Daten zum Aufenthalt der Person, welche das Mobiltelefon aufzeichnet – vorausgesetzt datenschutzrechtlich zulässig –, berücksichtigt werden (Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights, Executive Office of the President, May 2016, 11 ff.; The Consumer Financial Protection Bureau Office of Research, Data Point: Credit Invisibles, May 2015, 6, abrufbar unter: <*https://files.consumerfinance.gov/f/201505_cfpb_data-point-credit-invisibles.pdf*> [zuletzt besucht: 4. Juni 2021]).

58 Vgl. hierzu *Kessler/Oberlin* (Fn. 2), 90.

59 *Robert Bartlett/Adair Morse/Richard Stanton/Nancy Wallace,* Consumer-Lending Discrimination in the FinTech Era, Cambridge, Juni 2019, Table 6.

60 SBFI KI 2019 (Fn. 2), 81.

61 *Rolf H. Weber,* Big Data, Rechtliche Grenzen von unbegrenzten Möglichkeiten, Jahrestagung vom 7. September 2018, Schwerpunkt: Privatversicherungsrecht, HAVE 2018, 87 ff., 98 f.

62 FINMA-Risikomonitor 2020 (Fn. 36), 17.

63 BGE 138 I 475 E. 3.3.2; BSK BV-*Waldmann* (Fn. 53), Art. 35 N 29. Ein Teil der Lehre will aus Art. 28 ZGB einen Diskriminierungsschutz ableiten, vgl. hierzu *Weber/Henseler* (Fn. 7), 40 m.w.H.

64 *Weber* (Fn. 61), 98.

65 *Braun Binder/Burri/Lohmann/Simmler/Thouvenin/Volkinger* (Fn. 44), N 29.

66 *Braun Binder/Burri/Lohmann/Simmler/Thouvenin/Volkinger* (Fn. 44), N 29 f.

67 Vgl. hinten Punkt IV.3.5.

hat – je nach konkreter Ausgestaltung – nach Massgabe von bestimmten Finanzmarktgesetzen zu erfolgen. Soll eine solche Tätigkeit auf dem Finanzmarkt unter Einsatz von künstlicher Intelligenz erfolgen (z.B. *Robo Advisory*[68] als automatisierte Anlageberatung oder Vermögensverwaltung, Kreditvergabe[69] etc.), stellt sich für den betreffenden Anbieter deshalb immer die Frage, ob bzw. welche finanzmarktrechtlichen Vorgaben aufgrund der fraglichen Tätigkeit zu beachten und wie diese in der Praxis gegebenenfalls umzusetzen sind. Im Nachfolgenden werden diese Fragen aus dem Blickwinkel der relevantesten Finanzmarktgesetze betrachtet.

3.2 Bankengesetz

Das *Bankengesetz*[70] schreibt insbesondere vor, dass die gewerbsmässige Entgegennahme von Publikumseinlagen sowie die öffentliche Empfehlung hierzu einer Bewilligung der FINMA (je nach Geschäftsmodell als Bank- oder Fintech-Lizenz) bedürfen.[71] Weil Geschäftsmodelle, die auf Methoden künstlicher Intelligenz beruhen, soweit ersichtlich aktuell nicht auf die Entgegennahme von Publikumseinlagen,[72] sondern beispielsweise auf die voll- oder teilautomatisierte Anlageberatung bzw. Vermögensberatung fokussieren,[73] fallen sie nicht ohne Weiteres in den Anwendungsbereich des BankG.[74]

Will dagegen eine Bank in einem ihrer Geschäftsbereiche Methoden künstlicher Intelligenz einsetzen, hat sie sich vorab an das BankG und die Bankenverordnung[75] zu halten. Diese technologieneutral ausgestalteten Regeln enthalten keine spezifischen Vorgaben zum Umgang mit künstlicher Intelligenz. Das bedeutet aber nicht, dass die bereits im Rahmen der Grundrechte angesprochenen Herausforderungen, wie beispielsweise die Diskriminierungsgefahr,[76] von Banken nicht einer Beurteilung im Einzelfall unterzogen und ggf. durch entsprechende Massnahmen adressiert werden sollten.

Banken haben neben dem Bankengesetz weitere Finanzmarktgesetze[77] und andere Gesetze, wie beispielsweise das Datenschutzgesetz,[78] aber insbesondere auch die Rundschreiben der FINMA zu beachten. So kann sich in Zusammenhang mit dem Einsatz einer durch einen Dienstleister angebotenen KI-Anwendung beispielsweise die Frage stellen, ob der Einsatz solcher Methoden als Outsourcing wesentlicher Funktionen im Sinne des FINMA-RS 2018/3[79] qualifiziert, womit verschiedene zusätzliche Anforderungen insbesondere zur Auswahl, Instruktion und Kontrolle des Dienstleisters verbunden sind. Die Qualifikation als Outsourcing hängt dabei jedoch nicht von der eingesetzten Technologie, sondern vom Inhalt der betroffenen Dienstleistung bzw. Funktion ab. Weiter haben Banken beispielsweise auch das FINMA-RS 2008/21[80] zu beachten, welches den Umgang mit operationellen Risiken – wozu insbesondere die IT-Infrastruktur gehört – regelt. Auch dieses Rundschreiben ist technologieneutral formuliert und lässt sich entsprechend auf den Umgang mit Risiken anwenden, welche spezifisch aus dem Einsatz von KI-Methoden resultieren können. Schliesslich ist es für Banken aber auch aus Reputationsgründen zentral, die (ethischen) Risiken und Herausforderungen im Zusammenhang mit der Anwendung künstlicher Intelligenz zu identifizieren und adäquat zu adressieren. Die Erarbeitung eines gemeinsamen Verständnisses in Bezug auf die Identifizierung von KI-spezifischen rechtlichen und ethischen Herausforderungen und deren Bewältigung dürfte den Banken in Zukunft die Analyse und Prüfung eines Einsatzes von künstlicher Intelligenz erleichtern.[81]

3.3 Finanzinstituts- und Finanzdienstleistungsgesetz

Das *Finanzinstitutsgesetz*[82] regelt die Anforderungen an die Tätigkeit von Finanzinstituten zum Zweck des Schutzes der Anlegerinnen und Anleger sowie der

68 Zur Definition *Fryzek/Zysset* (Fn. 23), N 3 m.w.H.
69 *Weber* (Fn. 46), 23.
70 BankG (SR 952.0).
71 Art. 1 Abs. 2 und Art. 1*b* Abs. 1 BankG i.V.m. Art. 5 der Bankenverordnung (BankV).
72 Vgl. Einsatzmöglichkeiten in Punkt III.
73 Vgl. Punkt III.
74 Vgl. auch *Fryzek/Zysset* (Fn. 23), N 32.
75 BankV (SR 952.02).
76 Vgl. Punkt IV.2.
77 Vgl. Punkte IV.3.3–IV.3.4.
78 Vgl. Punkt IV.4.
79 FINMA-Rundschreiben 2018/3 «Outsourcing».
80 FINMA-Rundschreiben 2008/21 «Operationelle Risiken – Banken».
81 Vgl. die Initiative von Swiss Banking, abrufbar unter: *<https://www.swissbanking.ch/de/themen/digitalisierung-innovation-cyber-security/kuenstliche-intelligenz-und-daten>* (zuletzt besucht: 9. Juli 2021).
82 FINIG (SR 954.1).

Kundinnen und Kunden und der Gewährleistung der Funktionsfähigkeit des Finanzmarkts.[83] Als bewilligungspflichtige Finanzinstitute gelten unter anderem Vermögensverwalter und Wertpapierhäuser.[84] Das *Finanzdienstleistungsgesetz*[85] legt demgegenüber die Anforderungen für die getreue, sorgfältige und transparente Erbringung von Finanzdienstleistungen fest und regelt das Anbieten von Finanzinstrumenten.[86] Es gilt insbesondere für alle Finanzdienstleister, also alle natürlichen oder juristischen Personen, die gewerbsmässig Finanzdienstleistungen in der Schweiz oder für Kundinnen und Kunden in der Schweiz erbringen.[87]

Anbieter von Geschäftsmodellen, die auf Methoden künstlicher Intelligenz basieren, qualifizieren als Vermögensverwalter im Sinne von Art. 17 Abs. 1 FINIG, wenn die von ihnen verwendete KI-Technologie (z.B. ein *Robo Advisor*[88]) dazu eingesetzt wird, um im Namen und für Rechnung von Kundinnen und Kunden selbstständig Anlageentscheide zu treffen und diese auszuführen. Es ist für die Unterstellungspflicht unter das FINIG mithin unbeachtlich, ob die Tätigkeit der finanzmarktrechtlich relevanten Vermögensverwaltung durch eine natürliche Person oder ein KI-System wie einem *Robo Advisor* erfolgt. Entscheidend ist vielmehr die Verfügungsfähigkeit über Vermögenswerte der Kundinnen und Kunden gestützt auf einen Auftrag. Erteilt ein *Robo Advisor* einer Kundin bzw. einem Kunden lediglich Empfehlungen, so ist der betreffende Anbieter als Erbringer einer Anlageberatung entsprechend nicht dem FINIG unterstellt.[89] Anbieter, die zusätzlich zu einer Tätigkeit als Vermögensverwalter in eigenem Namen für Rechnung ihrer Kundinnen und Kunden Effekten handeln, können schliesslich zudem – unabhängig vom Einsatz von Methoden künstlicher Intelligenz – als Wertpapierhaus (früher: Effektenhändler) qualifizieren, was eine entsprechende Bewilligungspflicht unter dem FINIG mit sich bringt.[90]

Das FIDLEG sieht unter anderem vor, dass sich Kundenberaterinnen und Kundenberater, die nicht für einen beaufsichtigten Schweizer Finanzdienstleister tätig sind, neu in ein sog. «Beraterregister» eintragen lassen müssen.[91] Dies führt zur Frage, ob auch KI-basierte bzw. automatisierte «Berater» wie ein *Robo Advisor,* dessen Anbieter nicht prudenziell durch die FINMA beaufsichtigt wird, in das Register einzutragen ist.[92] Gemäss dem Wortlaut von Art. 3 lit. e FIDLEG qualifizieren als Kundenberaterinnen und Kundenberater ausschliesslich «natürliche Personen», die im Namen eines Finanzdienstleisters oder selbst Finanzdienstleistungen erbringen, was – wie auch der Mindestinhalt des Registers (u.a. Name und Vorname, Ausbildungen etc.) – *gegen* eine Eintragungspflicht spricht. Auch der Zweck des Eintrags, der Kundin bzw. dem Kunden eine Kontrolle über die berufliche Qualifikation ihres bzw. seines Beraters zu ermöglichen,[93] spricht gegen eine Eintragungspflicht für den *Robo Advisor* und auch gegen die Eintragung einer natürlichen Person als dessen «Vertreter», wie dies von einem Teil der Lehre gefordert wird.[94] Unseres Erachtens reicht es mit Blick auf einen effektiven Kundenschutz aus, dass der Finanzdienstleister die Kundinnen und Kunden in Erfüllung seiner (besonderen) Informationspflicht[95] transparent über den Zweck und – in den Grundzügen – über die Funktionsweise und die Risiken des *Robo Advisor* informiert.

Gemäss Art. 8 Abs. 1 FIDLEG hat der Finanzdienstleister seinen Kundinnen und Kunden Informationen über sich selbst (u.a. Name, Adresse und Tätigkeitsfeld) bereitzustellen. Weiter muss der Finanzdienstleister die Kundinnen und Kunden über die Finanzdienstleistung bzw. deren Art, Wesensmerkmale und Funktionsweisen informieren.[96]. Mit Hinweis auf diese Informationspflichten wird in Zusammenhang mit Finanzdienstleistungen, welche auf Methoden künstlicher Intelligenz basieren, von der Lehre[97] gefordert, dass die Kundin bzw. der Kunde insbesondere über die algorithmusbasierte Lösung

83 Art. 1 FINIG.
84 Art. 2 Abs. 1 FINIG.
85 FIDLEG (SR 950.1).
86 Art. 1 Abs. 2 FIDLEG.
87 Art. 2 Abs. 1 i.V.m. Art. 3 lit. d FIDLEG.
88 Vgl. Punkt III.
89 Vgl. aber die Pflichten für Finanzdienstleister unter dem FIDLEG.
90 Art. 2 i.V.m. Art. 41 ff. FINIG.
91 Art. 28 Abs. 1 FIDLEG.
92 Vgl. ausführlich *Fryzek/Zysset* (Fn. 23), N 53 ff.
93 Vgl. Botschaft zum Finanzdienstleistungsgesetz (FIDLEG) und zum Finanzinstitutsgesetz (FINIG) vom 4. November 2021, BBl 2015 8901–9198, 8967.
94 *Fryzek/Zysset* (Fn. 23), N 53 ff.
95 Vgl. dazu sogleich.
96 Art. 8 Abs. 2 FIDLEG i.V.m. Art. 7 Abs. 1 lit. a FIDLEV.
97 *Fryzek/Zysset* (Fn. 23), N 62 m.w.H.

und deren Zweck informiert werden müsse.[98] Dem ist unseres Erachtens zu folgen, weil die Kundin bzw. der Kunde ohne ein grundsätzliches Verständnis der Funktionsweise des entsprechenden Algorithmus keine informierte Entscheidung über den Bezug der fraglichen Dienstleistung treffen kann.

Gemäss Art. 8 Abs. 2 lit. a FIDLEG hat der Finanzdienstleister seine Kundinnen und Kunden sodann über die mit der Finanzdienstleistung verbundenen Risiken zu informieren. Diese Information enthält Angaben über die Finanzinstrumente bzw. eine Darstellung der Risiken, die sich aus der Anlagestrategie ergeben.[99] Die Information zu den allgemeinen Risiken, die mit den Finanzinstrumenten verbunden sind, enthält Angaben zu den Wesensmerkmalen und der Funktionsweise der Finanzinstrumente sowie den sich aus den Finanzinstrumenten ergebenden Verlustrisiken und allfälligen Verpflichtungen für die Kundinnen und Kunden.[100]

Fraglich ist, inwiefern der Finanzdienstleister vor diesem Hintergrund auch potenzielle (technologiespezifische) Risiken, die mit Methoden künstlicher Intelligenz verbunden sind, gegenüber den Kundinnen und Kunden offenlegen muss. Auch wenn das Gesetz bzw. die Verordnung explizit nur von Risiken spricht, welche mit den «Finanzinstrumenten» verbunden sind,[101] halten wir es insbesondere angesichts des kundenseitig (noch) fehlenden Verständnisses für solche neuartigen Methoden bei der Erbringung von Finanzdienstleistungen für angezeigt, dass die Kundinnen und Kunden über diese Risiken aufgeklärt bzw. informiert werden müssen. Diese Pflicht lässt sich unseres Erachtens aus Art. 8 Abs. 1 lit. d FIDLEG i.V.m. Art. 7 Abs. 1 lit. a FIDLEV ableiten, wonach die Kundinnen und Kunden über Art, Wesensmerkmale und Funktionsweisen der Finanzdienstleistung zu informieren sind. Die Information unter dem FIDLEG hat entsprechend gegenüber Finanzdienstleistungen ohne KI-Einsatz zusätzlich in Bezug auf die *algorithmusbasierte Lösung* und deren *Zweck* sowie deren technologie spezifische *Risiken* zu erfolgen.

Beim Einsatz von Methoden künstlicher Intelligenz im Rahmen der Anlageberatung und Vermögensverwaltung ist weiter der Angemessenheits- und Eignungsprüfung gemäss Art. 11 f. FIDLEG besondere Beachtung zu schenken. In deren Rahmen muss sich der Finanzdienstleister über die Kenntnisse und Erfahrungen bzw. finanziellen Verhältnisse und Anlageziele der Kundin bzw. des Kunden erkundigen und gestützt auf diese Angaben ein Risikoprofil erstellen und ggf. eine Anlagestrategie mit der Kundin bzw. dem Kunden vereinbaren.[102] Eine automatisierte Abfrage bzw. Erstellung des Profils hat entsprechend so konzipiert zu sein, dass insbesondere ein fehlendes Verständnis des Geschäfts sowie die Risikoneigung und die Anlageziele der Kundin bzw. des Kunden zuverlässig erkannt und entsprechend berücksichtigt werden.[103] Das setzt voraus, dass die richtigen Fragen bzw. Folgefragen gestellt und gestützt auf die Antworten der Kundin bzw. des Kunden die richtigen Schlüsse gezogen werden.[104]

Wie das Bankengesetz sind auch das FINIG und das FIDLEG technologieneutral ausgestaltet und sehen entsprechend keine spezifischen Vorgaben zum Umgang mit künstlicher Intelligenz vor. Die sich dadurch stellenden Fragen, insbesondere im Zusammenhang mit den Verhaltensregeln und dem Registereintrag,[105] dürften in naher Zukunft durch Praxis und Lehre geklärt werden. Die im Rahmen der Grundrechte dargelegten Herausforderungen, wie beispielsweise die Diskriminierungsgefahr,[106] sollten wiederum einer Beurteilung im Einzelfall unterzogen und ggf. durch entsprechende Massnahmen adressiert werden.

3.4 Geldwäschereigesetzgebung

Das Geldwäschereigesetz[107] gilt vorab für Finanzintermediäre.[108] Dazu gehören sowohl spezialgesetz-

98 Vgl. auch Art. 7 Abs. 1 lit. a FIDLEV, wonach die Information über die Finanzdienstleistung mitunter Angaben zu den *«Funktionsweisen»* der Finanzdienstleistung enthalten muss.

99 Art. 7 Abs. 2 FIDLEV.

100 Art. 7 Abs. 3 FIDLEV.

101 Art. 8 Abs. 2 FIDLEG i.V.m. Art. 7 Abs. 1 und 3 FIDLEV.

102 Art. 17 Abs. 3 FIDLEV.

103 *Rolf H. Weber/Rainer Baisch,* Regulierung von Robo-Advice, Neue Herausforderungen für Finanzintermediäre und Finanzmarktaufsichtsbehörden im Kontext der digitalen Anlageberatung und Vermögensverwaltung, AJP 8/2016, 1065–1078, 1072.

104 Vgl. auch *Fryzek/Zysset* (Fn. 23), N 68.

105 Vgl. Punkt IV.3.3.

106 Vgl. Punkt IV.2.

107 Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung, GwG (SR 955.0).

108 Art. 2 Abs. 1 lit. a GwG.

lich regulierte Unternehmen gemäss Art. 2 Abs. 2 lit. a–f GwG (z.B. Banken) als auch Personen, die berufsmässig fremde Vermögenswerte annehmen oder aufbewahren oder helfen, sie anzulegen oder zu übertragen.[109]

Der Einsatz von Methoden künstlicher Intelligenz im Rahmen einer Dienstleistungserbringung im Finanzbereich führt nicht *per se* zur Anwendbarkeit des GwG. Vielmehr stellt sich die Frage, ob der betreffende Anbieter aufgrund seiner Tätigkeit als Finanzintermediär qualifiziert, was unabhängig davon zu beurteilen ist, ob diese Dienstleistung auf Methoden künstlicher Intelligenz basiert oder nicht. Insofern bedeuten KI-basierte Anwendungen keine besonderen Herausforderungen bei der Beurteilung der Anwendbarkeit der Geldwäschereigesetzgebung.[110]

Die Bedeutung von Methoden künstlicher Intelligenz und deren Herausforderungen sind vielmehr im Bereich der GwG-*Compliance* zu sehen, wo sie immer häufiger z.B. im Rahmen der Transaktionsüberwachung oder bei der Identifizierung von Vertragspartnern etc. eingesetzt werden, was nicht nur zu Kosteneinsparungen, sondern auch zu Qualitätssteigerungen führen kann.[111] Auch die Aufsichtsbehörde hat die Vorteile von IT-Systemen für die Compliance grundsätzlich erkannt und schreibt ebensolche für Banken und Wertpapierhäuser im Rahmen der Transaktionsüberwachung gar explizit in ihrer Verordnung zum Geldwäschereigesetz vor, wobei die Art der verwendeten Technologie, also insbesondere die Frage nach dem Einsatz künstlicher Intelligenz, offengelassen wird.[112] Die FINMA ist grundsätzlich bestrebt, die Geldwäschereigesetzgebung technologieneutral auszulegen, was sie kürzlich im Rahmen der Teilrevision des Rundschreibens 2016/7 «Video- und Online-Identifizierung» bestätigt hat.[113] Es entspricht dem ausdrücklich erklärten Ziel des Regulators, Hürden für die Entwicklung neuer technologischer Lösungen zur Erfüllung regulatorischer Vorgaben abzubauen bzw. keine solchen aufzustellen.[114] Die im Rahmen der Grundrechte dargelegten Herausforderungen, wie beispielsweise die Diskriminierungsgefahr,[115] sind auch im GwG-Bereich einer Beurteilung im Einzelfall zu unterziehen und ggf. durch entsprechende Massnahmen zu adressieren.

3.5 Versicherungsrecht

In der Versicherungsindustrie werden in grossem Umfang Kundendaten gesammelt, weshalb gemeinhin grosse Potenziale im Bereich *Big Data Analytics* gesehen werden.[116] Im Vergleich zu Bankprodukten, die in der Regel zwar individueller ausgestaltet werden können, könnten Versicherungsprodukte daher noch deutlich stärker von Datenanalysen und dem Einsatz künstlicher Intelligenz profitieren, etwa indem die Versicherungsprämien zukünftig abhängig von Daten der betroffenen Person zu ihren Einkäufen, zur Nutzung von Internet oder elektronischen Geräten, ihrem Reiseverhalten oder Mustern ihres Arbeitswegs ausgestaltet werden könnten.[117] Trotzdem kommt auch das Versicherungsrecht bisweilen ohne spezifische Big Data Analytics- bzw. KI-Regelungen aus.

Die FINMA hat in ihrem Risikomonitor 2020 die künstliche Intelligenz zwar nicht als eines der Hauptrisiken, aber – in Kombination mit *Big Data* – immerhin als ein bedeutendes längerfristiges Risiko im Versicherungsbereich identifiziert. Das Risiko sieht sie konkret in den durch Big Data und künstliche Intelli-

109 Art. 2 Abs. 3 GwG.

110 Gl.M. *Thomas Nagel,* Der persönliche und sachliche Geltungsbereich des schweizerischen Geldwäschereigesetzes (GwG), Mit rechtsvergleichenden Hinweisen zu internationalen Standards, dem Recht der Europäischen Union und dem deutschen Recht, Schweizer Schriften zum Finanzmarktrecht (SSFM) 132, Zürich 2020, N 668 f.

111 Vgl. *Markus Winkler,* Credit Scoring, AML Software & Risk, Automatisierte Entscheidungen im Rahmen von Finanzdienstleistungen, SZW 2020, 62 ff., 69, der darauf hinweist, dass verschiedene Anbieter von AML-Software auf den Einsatz von künstlicher Intelligenz verweisen.

112 Art. 20 Abs. 2 GwV-FINMA.

113 Anders bspw. in Österreich, wo das Finanzmarkt-Geldwäschegesetz seit dem 1. März 2021 mit § 7*a* ausdrücklich eine Bestimmung zum *«Transaktionsmonitoring unter Verwendung eines auf künstlicher Intelligenz basierenden Ansatzes»* vorsieht, welche die Anforderungen an die Entwicklung und Umsetzung der entsprechenden Technologien festhält.

114 Vgl. bereits Bericht des Bundesrates in Erfüllung des Postulats 16.3256 *Landolt* vom 18. März 2016, Einsatz innovativer Technologien im Bereich der Finanzmarktaufsicht und -regulierung (RegTech), 15.

115 Vgl. Punkt IV.2.

116 *Puschmann/Weber* (Fn. 39), 91 mit einer Übersicht von Fintech-Innovationen im Versicherungsbereich und den entsprechenden rechtlichen Herausforderungen.

117 SBFI KI 2019 (Fn. 2), 80 m.w.H. und Beispielen.

genz verbesserten Analyseinstrumenten der Versicherungen, welche zwar präzise und korrekte Ergebnisse (insbesondere die Trennung von «guten» und «schlechten» Risiken) ermögliche, diese jedoch nicht mehr einfach nachvollziehbar seien, wodurch wiederum das Risiko von unbeabsichtigter oder intransparenter Diskriminierung und Missbrauch steige.[118]

Aufsichtsrechtlich sind im Bereich der Privatversicherungen[119] individuelle, an jedes Risiko angepasste, sogenannte «risikogerechte» Preise zulässig, solange keine juristisch oder versicherungstechnisch nicht begründbare erhebliche Ungleichbehandlung vorliegt[120] und die entsprechende Ungleichbehandlung demzufolge beabsichtigt und transparent ist.[121] Denn die Prämienindividualisierung beeinträchtigt das Versicherungskonzept des Risikoausgleichs im Kollektiv nicht, welches durch die Unabhängigkeit und Zufälligkeit von Schadenseintritten entsteht.[122] Allerdings weist die FINMA diesbezüglich zu Recht darauf hin, dass ausdifferenziertere, homogenere und kleinere Versicherungskollektive entstehen könnten und so Versicherungsnehmende mit höheren Risiken aufgrund prohibitiver Kosten *de facto* von einer Versicherung ausgeschlossen werden könnten. Dies könnte den Kern der Versicherungsindustrie, das Solidaritätsprinzip, gefährden.[123] Gerade im Bereich der Sozialversicherungen sind vollständig «risikogerechte» Prämien gesellschaftlich nicht erwünscht, weil eine Versicherungsdeckung für alle Personen oder eine staatliche Unterstützung gewisser Tätigkeiten, Regionen oder Bevölkerungsgruppen mit erhöhtem Risiko ermöglicht werden soll.[124]

Auch die Versicherungen sollten daher – und nicht zuletzt aus Reputationsüberlegungen – insbesondere die Risiken von Diskriminierung und Missbrauch durch den Einsatz von KI-basierten Anwendungen einer Beurteilung unterziehen und ggf. durch entsprechende Massnahmen adressieren.

Auf die in diesem Bereich besonders relevanten datenschutzrechtlichen Aspekte dieser Modelle wird unter Punkt 4.4 weiter eingegangen.

3.6 Fazit und Ausblick

Die schweizerische Finanzmarktregulierung definiert aktuell – bis auf eine Ausnahme beim Betrieb des Hochfrequenzhandels[125] – keine spezifischen Anforderungen an den Einsatz von künstlicher Intelligenz.

Das SBFI erachtete die Wahrscheinlichkeit der Notwendigkeit von gesetzlichen Anpassungen aufgrund der starken Regulierung des Finanzmarktrechts gegenüber anderen Branchen zwar als «grösser», weshalb der Einsatz von KI in der Finanzwirtschaft genauer zu verfolgen sei als in anderen Wirtschaftszweigen. Insbesondere könne die fehlende Nachvollziehbarkeit dazu führen, dass Fehlentscheidungen nicht erkannt und Verhaltens-, Verantwortlichkeits-, Informations- oder Rechenschaftspflichten nicht erfüllt werden.[126] Bisher wurden indes keine KI-spezifischen regulatorischen Schritte als nötig erachtet.[127]

Aufgrund der technologieneutralen Ausgestaltung des Finanzmarktrechts besteht unseres Erachtens jedoch kein grundsätzlicher Anpassungsbedarf. Allfällige Auslegungsfragen sind – sobald hinreichend identifiziert – ggf. durch die Lehre und Praxis sowie allenfalls mithilfe von Leitfäden von Branchenverbänden und/oder revidierten bzw. neuen FINMA-Rundschreiben zu klären. Gleichwohl tun Finanz- und Versicherungsinstitute vor dem Einsatz künstlicher Intelligenz gut daran, eine Beurteilung der damit verbundenen Risiken für die Grundrechte der betroffenen Personen durchzuführen und ggf. Vor-

118 FINMA-Risikomonitor 2020 (Fn. 36), 16 f.

119 Ausgenommen die berufliche Vorsorge und die Krankenzusatzversicherung, wo die Prämienbildung durch den Staat beeinflusst wird.

120 Art. 117 Abs. 2 AVO; ausführlich zum engen Anwendungsbereich der Regelung: *Weber* (Fn. 61), 95 f.

121 Vgl. dazu den Hinweis der FINMA auf die Diskriminierungs- und Missbrauchsgefahr durch Intransparenz (FINMA-Risikomonitor 2020 [Fn. 36], 17).

122 SBFI KI 2019 (Fn. 2), 80.

123 FINMA-Risikomonitor 2020 (Fn. 36), 17.

124 SBFI KI 2019 (Fn. 2), 80.

125 Beim Betrieb des Hochfrequenz- bzw. algorithmischen Handels müssen die beaufsichtigten Finanzmarktteilnehmer «durch wirksame Systeme und Risikokontrollen» sicherstellen, dass dadurch keine falschen oder irreführenden Signale für das Angebot, die Nachfrage oder den Kurs für Effekten erfolgen können. Zudem müssen die Beaufsichtigten die wesentlichen Merkmale ihrer algorithmischen Handelsstrategien auf eine auch für Dritte nachvollziehbare Art und Weise dokumentieren. Vgl. FINMA-Rundschreiben 2013/8 «Marktverhaltensregeln», Rz. 62 f.

126 Als «regulatorisch bedeutsam» erachtet das SBFI den Fall, wenn ein Finanzdienstleister den Kunden falsch beriete, die gesetzlichen Eignungs- und Angemessenheitsprüfungen fehlerhaft durchführte oder einen Versicherten ohne juristischen oder versicherungstechnischen Grund benachteiligte.

127 Zum Ganzen: SBFI KI 2019 (Fn. 2), 79 f.

kehrungen zu treffen, um allfälligen identifizierten Risiken vorzubeugen. Die entsprechenden Beurteilungskriterien und Massnahmen könnten branchenspezifisch mithilfe von Leitfäden von Branchenverbänden festgelegt werden.[128]

4. Datenschutzgesetzgebung

Methoden künstlicher Intelligenz und Datenbearbeitung sind untrennbar miteinander verbunden. Künstliche Intelligenz wird mit Daten trainiert, verarbeitet Daten bei ihrer Anwendung und generiert selbst wiederum neue Daten. Sobald dabei *Personen*daten bearbeitet werden, ist der Anwendungsbereich des Schweizer Datenschutzgesetzes (DSG) grundsätzlich eröffnet.[129] Insbesondere im Kreditwesen, aber auch in der Geldwäschereibekämpfung oder bei elektronischen Zahlungssystemen ist die Bearbeitung einer Vielzahl von Personendaten in der Regel unumgänglich.[130] Dies hat diverse datenschutzrechtliche Konsequenzen, von welchen nachfolgend beispielhaft eine Auswahl dargestellt wird.

Insbesondere bei Online-Kreditanträgen ist eine vollständig automatisierte Bearbeitung und damit ein automatisierter Ermessensentscheid möglich.[131] Fällt die Kreditentscheidung negativ aus, so ist es für die betroffene Person wichtig zu wissen, wie diese Entscheidung zustande kam. Andernfalls kann sie weder beurteilen, ob die Entscheidung richtig bzw. nachvollziehbar und nichtdiskriminierend ist noch kann sie allfällige unrichtige bzw. veraltete Daten über ihre Person erkennen und gegebenenfalls berichtigen (lassen).[132] Daher enthält das revidierte Datenschutzgesetz neu die Pflicht des Verantwortlichen, die betroffene Person über eine Entscheidung, die ausschliesslich auf einer automatisierte Datenbearbeitung beruht, zu informieren. Gemäss Art. 21 Abs. 1 revDSG muss die Entscheidung zudem für die betroffene Person mit einer Rechtsfolge verbunden sein (z.B. Abschluss oder Kündigung eines Vertrags[133]) oder sie erheblich beeinträchtigen (z.B. ein verweigerter Vertrag[134] oder die Rückweisung einer Bewerbung). Eine ausschliesslich automatisierte Bearbeitung liegt namentlich dann vor, wenn «[…] keine inhaltliche Bewertung und darauf gestützte Entscheidung durch eine natürliche Person stattgefunden hat.»[135] Gemäss Art. 21 Abs. 2 revDSG muss der Verantwortliche der betroffenen Person auf Antrag weiter die Möglichkeit einräumen, ihren Standpunkt darzulegen (z.B. Hinweis auf falsche oder unvollständige Daten) und die automatisierte Entscheidung von einer natürlichen Person überprüfen zu lassen. Die betroffene Person hat mithin «Anspruch auf menschliches Gehör»[136]. Unter Beachtung der allgemeinen Bearbeitungsgrundsätze (Art. 6 revDSG) und der besonderen Informationspflicht nach Art. 21 revDSG[137] sind automatisierte Einzelentscheidungen aber ohne Weiteres zulässig. Gestützt auf das Auskunftsrecht gemäss Art. 25 Abs. 2 lit. f revDSG ist der betroffenen Person zudem – falls einschlägig – das Vorliegen einer automatisierten Einzelentscheidung als solche sowie die Logik, auf der die Entscheidung beruht, mitzuteilen. Der Algorithmus selbst wird jedoch nicht offengelegt werden müssen,[138] vielmehr sollten – wie unter der DSGVO – relativ allgemeine Angaben genügen.[139] Bei einer automatisierten Kreditbeurteilung müsste bspw. darauf hingewiesen werden, dass diese auf einem Scoring der Kreditwür-

128 Allgemeine Prinzipien für den Einsatz von Algorithmen finden sich auch im bereits erwähnten Prinzipienpapier der BaFin (Fn. 1).

129 Im vorliegenden Beitrag wird auf die Regelungen des totalrevidierten Datenschutzgesetzes (revDSG) Bezug genommen, welches voraussichtlich im Sommer 2022 in Kraft treten wird; Schlussabstimmungstext abrufbar unter: *<https://www.parlament.ch/centers/eparl/curia/2017/20170059/Schlussabstimmungstext%203%20NS%20D.pdf>* (zuletzt besucht: 28. Juni 2021).

130 Vgl. hierzu *Weber* (Fn. 61), 102 f.

131 *Žiga Škorjanc,* Automatisierte Kreditentscheidungen, Compliance Berater CB 2020, 70 ff., 72.

132 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941–7192, 7066.

133 Botschaft DSG 2017 (Fn. 132), 7056.

134 Botschaft DSG 2017 (Fn. 132), 7056.

135 Botschaft DSG 2017 (Fn. 132), 7056.

136 *David Rosenthal,* Der Entwurf für ein neues Datenschutzgesetz, Was uns erwartet und was noch zu korrigieren ist, Jusletter 27. September 2017, N 100.

137 Diese Information kann sowohl im Rahmen der Mitteilung der Entscheidung als auch vorab in der Datenschutzerklärung erfolgen (*David Rosenthal,* Das neue Datenschutzgesetz, Jusletter 16. November 2020, N 112 m.w.H. zu den Modalitäten der Informationspflicht).

138 Botschaft DSG 2017 (Fn. 132), 7067; *Škorjanc* (Fn. 131), 72; *Romy Daedelow,* Wenn Algorithmen (unfair) über Menschen entscheiden…, Welchen Schutz bietet die Datenschutz-Grundverordnung?, Jusletter 26. November 2018, N 31.

139 *Rosenthal* (Fn. 136), N 119.

digkeit der antragstellenden Person basiert und von welcher Quelle dieses stammt (z.B. von einer Kreditauskunftei) oder welche Art von Daten dem Scoring mit welcher Gewichtung zugrunde liegen (z.B. Betreibungsdaten, Zahlungserfahrungen etc.).[140]

Im Zusammenhang mit der Kreditwürdigkeitsprüfung wird schliesslich auch Art. 31 Abs. 2 lit. c revDSG zu beachten sein, wonach der Rechtfertigungsgrund des überwiegenden Interesses nur in Betracht kommt, wenn keine besonders schützenswerten Personendaten bearbeitet und kein Profiling mit hohem Risiko vorgenommen wird. Auch dürfen die betreffenden Personendaten nicht älter als zehn Jahre sein und Dritten nur bekanntgegeben werden, wenn diese die Daten für den Abschluss oder die Abwicklung eines Vertrags mit der betroffenen Person benötigen. Schliesslich muss die betroffene Person volljährig sein. Wird für die Prüfung auf Methoden künstlicher Intelligenz bzw. auf automatisierte Prozesse zurückgegriffen, wird deshalb sehr genau darauf zu achten sein, auf welcher Datenbasis diese arbeiten bzw. trainiert werden.

Der Einsatz von Methoden künstlicher Intelligenz kann weiter eine Datenschutzfolgenabschätzung erforderlich machen. Sofern eine Datenbearbeitung ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen mit sich bringen kann, wird gemäss Art. 22 Abs. 1 revDSG eine vorgängige Risikobeurteilung der Datenbearbeitung durchgeführt werden und allenfalls eine Stellungnahme des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten einzuholen sein (Art. 23 revDSG). Ein hohes Risiko ergibt sich, insbesondere bei Verwendung neuer Technologien, aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung (Art. 22 Abs. 2 revDSG). Der Einsatz von Methoden künstlicher Intelligenz wird somit regelmässig eine Datenschutzfolgenabschätzung erfordern, insbesondere im Krankenversicherungsbereich, in welchem naturgemäss Gesundheitsdaten von Kundinnen und Kunden und damit besonders schützenswerte Personendaten bearbeitet werden.[141] Im Rahmen der Datenschutzfolgenabschätzung wird eine (projektbezogene) «datenschutzrechtliche Selbstbeurteilung» vorgenommen, bei der in einem ersten Schritt die Datenbearbeitungen beschrieben werden, um in einem zweiten Schritt die Risiken für die Persönlichkeit der betroffenen Personen zu analysieren und in einem dritten und letzten Schritt die Massnahmen zur Mitigierung dieser Risiken darzulegen.[142] Beim Einsatz von künstlicher Intelligenz ist demnach stets zu eruieren, welche Personendaten von wem wozu, wie und wo bearbeitet und ggf. weitergegeben werden, ob diese Datenbearbeitungen zu Risiken für die Persönlichkeit der betroffenen Personen führen können und, falls ja, mit welchen technischen und organisatorischen Massnahmen diesen Risiken begegnet werden kann. In der Praxis wird darüber hinaus regelmässig dargelegt, welche «negativen Folgen» die Datenbearbeitungen für die betroffene Person mit einer gewissen Wahrscheinlichkeit haben könnten (z.B. führen fehlerhafte Daten zu einer falschen medizinischen Indikation; eine Person erhält einen Kredit oder einen Job nicht etc.).[143]

5. Produktehaftung

Der Einsatz von KI-Methoden wirft verschiedene Haftungsfragen auf. Entscheidet künstliche Intelligenz beispielsweise, einem Kreditnehmer trotz Anzeichen, die auf seine Zahlungsunfähigkeit schliessen lassen, einen Kredit zu gewähren und wird kurze Zeit nach Kreditvergabe der Konkurs über den Kreditnehmer eröffnet, stellt sich die Frage, ob jemand und falls ja, wer gegenüber dem Kreditgeber für den Kreditausfall einzustehen hat. Im Bereich der Vermögensverwaltung stellt sich die Frage, ob der Vermögensverwalter gegenüber seiner Kundin bzw. seinem Kunden für Verluste haftet, die aufgrund eines Investitionsentscheids entstanden sind, der mit Methoden künstlicher Intelligenz (z.B. «*Robo Advisory*») getroffen wurde oder ob vielmehr der Entwickler dieser Methoden bzw. der Software-Hersteller zur Verantwortung zu ziehen ist. Haften allenfalls beide Personen solidarisch? Oder fehlt es allenfalls gänzlich an einem Haftungssubjekt? Wer haftet, wenn eine Versicherung das sich verwirklichte Risiko aufgrund einer Fehlentscheidung der künstlichen Intelligenz nicht abdeckt? Klar ist, dass ein KI-System selbst (zumindest heute) nicht Haftungssubjekt sein kann, da es nicht rechts-

140 *Rosenthal* (Fn. 136), N 119.
141 *Weber/Henseler* (Fn. 7), 35.
142 *Rosenthal* (Fn. 136), N 148 ff.
143 *Rosenthal* (Fn. 136), N 149.

fähig ist. Die viel diskutierte E-Persönlichkeit bleibt bis heute nur eine Idee der Wissenschaft.[144]

In Frage kommt zunächst eine Haftung nach dem Produkthaftpflichtgesetz (PrHG).[145] Ein Teil der Lehre stellt die Anwendbarkeit des PrHG schon im Grundsatz in Frage, weil das durch Methoden künstlicher Intelligenz gewonnene Ergebnis möglicherweise gar kein Ergebnis menschlicher Tätigkeit sei.[146] Darüber hinaus ist nicht restlos geklärt, ob eine Software als Produkt im Sinne des Produktehaftpflichtgesetzes zu qualifizieren ist. Falls die Software in einem Gerät integriert ist, so stellt das Gerät selbst ein Produkt im Sinne von Art. 3 Abs. 1 lit. a PrHG dar, und dieses kann aufgrund eines Softwarefehlers einen Produktfehler nach Art. 4 PrHG aufweisen.[147] Nicht immer ist die Software jedoch in ein bestimmtes Gerät integriert, sondern wird «nackt» vertrieben. Dies trifft insbesondere auf die meisten der eingangs dargestellten Einsatzmöglichkeiten zu. Die jüngere Lehre will – anders als die ältere Lehre, welche die Produkteigenschaft von Software als immaterielles Rechtsgut verneinte – jede Software, ob Standardsoftware oder Individualsoftware, selbstständig dem PrHG unterstellen.[148] Damit kann tendenziell von der Anwendbarkeit des PrHG auch auf die dargestellten Einsatzmöglichkeiten ausgegangen werden, obwohl aufgrund der fehlenden Rechtsprechung eine gewisse Unsicherheit weiterbesteht. Entsprechend wird in der Lehre zu Recht eine zeitnahe Klärung durch die gesetzliche Verankerung dieser Auslegung gefordert.[149]

Angenommen, die Software allein fällt unter das PrHG, stellt sich die Frage, wann ein Produktfehler im Sinne des PrHG vorliegt. Ausgangspunkt zur Beantwortung dieser Frage ist gemäss *Hänsenberger* allem voran die Unterscheidung, ob ein Schaden aus einem eigentlichen Produktfehler herrührt oder auf dem gewollten selbstständigen Entscheidungsbereich der künstlichen Intelligenz, mithin auf einer Fehlentscheidung beruht.[150] Bei Produktfehlern sei etwa an eine (ursprünglich) fehlerhafte Datenbasis, z.B. aufgrund eines defekten Sensors, zu denken. Zu den Produktionsfehlern zählt *Hänsenberger* auch eine Software, deren Entscheidungsalgorithmus einen Programmierfehler enthält, wodurch die eingespeisten (richtigen) Daten nicht korrekt verarbeitet werden. Unter Letzteres zu subsumieren ist aus seiner Sicht auch eine kompetenzüberschreitende Entscheidung der künstlichen Intelligenz. Demgegenüber liege kein Produktfehler vor, wenn das erlernte Verhalten in der konkreten Situation aufgrund einer (bewusst im Ermessen der Anwendung liegenden) Fehlentscheidung zu einem Schaden führt oder die Entscheidung aus einer Fehlinterpretation der Eingangsdaten, die nicht von einen Programmierfehler herrührt, resultiert.[151] Fehlentscheidungen begründen seines Erachtens keine Haftung, wenn eine Entscheidung innerhalb des der künstlichen Intelligenz bewusst überlassenen Ermessensspielraums ergeht.[152] Daher müsse klar festgelegt werden, welcher Grad an Selbstständigkeit der künstlichen Intelligenz zukomme.[153] Das Überlassen eines Entscheidungsspielraums könnte in der Sache richtig sein, wenn künstliche Intelligenz mit Wahrscheinlichkeiten arbeitet und so nicht antizipieren kann, welche Entscheidung die beste und damit «richtige» sein wird. Andere Autoren ziehen als Massstab zur Bestimmung der Fehlerhaftigkeit einer KI-Anwendung die berechtigten Sicher-

144 Vgl. hierzu *Clara-Ann Gordon/Tanja Lutz,* Haftung für automatisierte Entscheidungen, Herausforderungen in der Praxis, SZW 2020, 53 ff., 56 f.

145 Vgl. zur vertraglichen und ausservertraglichen Haftung z.B. *Gordon/Lutz* (Fn. 144), 57 ff.

146 *Alexia Sidiropoulos,* Haftung für Gerätefehler bei der medizinischen Diagnostik und Behandlung, Sicherheit & Recht 1/2020, 49 ff., 51.

147 BSK PrHG-*Fellmann*, Art. 3 N 10 in: Corinne Widmer Lüchinger/David Oser (Hrsg.), Basler Kommentar zum Schweizerischen Privatrecht, Obligationenrecht I (Art. 1–529), 7. Aufl., Basel 2020 (zit. BSK PrHG-*Verfasser/in*).

148 *Silvio Hänsenberger,* Die Haftung für Produkte mit lernfähigen Algorithmen, Wann haften Hersteller für Schäden durch Produkte mit lernfähigen Algorithmen?, Jusletter 26. November 2018, N 14; s. BSK PrHG-*Fellmann* (Fn. 147), Art. 3 PrHG N 10; *Corinne Widmer Lüchinger,* Apps, Algorithmen und Roboter in der Medizin, Haftungsrechtliche Herausforderungen, HAVE 2019, 3 ff., 7; *Braun Binder/Burri/Lohmann/Simmler/Thouvenin/Volkinger* (Fn. 44), N 43 m.w.H. auf die Lehre.

149 *Braun Binder/Burri/Lohmann/Simmler/Thouvenin/Volkinger* (Fn. 44), N 43.

150 *Hänsenberger* (Fn. 148), N 9 und 50.

151 *Hänsenberger* (Fn. 148), N 11, mit Hinweis auf *Anjali Singhvi/Karl Russell,* Inside the Self-Driving Tesla Fatal Accident, The New York Times, 12. Juli 2016, abrufbar unter: <*www.nytimes.com/interactive/2016/07/01/business/inside-tesla-accident.html*> (zuletzt besucht: 19. Mai 2021).

152 *Hänsenberger* (Fn. 148), N 12.

153 *Hänsenberger* (Fn. 148), N 49.

heitserwartungen heran, die bei «sicherheitskritischen» KI-Anwendungen besonders hoch sein dürften.[154] Ist eine Fehlentscheidung der KI auf eine mangelnde Risikobegrenzung zurückzuführen, so liege bereits zum Zeitpunkt des Inverkehrbringens der KI ein Fehler vor, weil die Herstellerin mit der Programmierung der Algorithmen die Entwicklungsfähigkeit des Systems festgelegt und dadurch die Gefahr einer aus dieser Fähigkeit resultierenden Schädigung geschaffen habe.[155] Die Herstellerin könne dieses Risiko durch sorgfältige Programmierung und Instruktion kontrollieren, weswegen eine Haftung ihrerseits angezeigt sei. Bei lernfähigen KI-Anwendungen verringere sich diese Kontrolle nach dem Inverkehrbringen. Dafür könne nunmehr der Nutzer die KI im Rahmen des «Trainings» beeinflussen. Entsprechend sei es angezeigt, ihn für daraus resultierende Schäden haftbar zu machen. Die Herstellerin hafte nicht für Fehler, die durch «unsachgemässe Änderung» des Produkts nach Inverkehrbringen entstehen,[156] weil das Produkt im Zeitpunkt des Inverkehrbringens ihren Machtbereich verlässt. Auch diesbezüglich fordert die Lehre eine gesetzgeberische Klarstellung.[157]

Eine Beantwortung der hier aufgeworfenen Fragen – sei es auf dem Weg der Rechtsprechung oder Rechtssetzung – wäre zwecks Schaffung von Rechtssicherheit zweifelsohne zu begrüssen. Im Bereich des Finanzmarktrechts werden diese Fragen indes von untergeordneter Bedeutung bleiben, weil es sich bei den Schäden, welche durch den Einsatz von KI entstehen, in aller Regel um (reine) Vermögensschäden handeln dürfte, welche vom PrHG *a priori* nicht erfasst sind.[158] In diesem Zusammenhang ist vielmehr auf die vertraglichen (Art. 398 OR für Dienstleistungen; Art. 197 OR für Produkte) und ausservertraglichen Haftungsbestimmungen (Art. 41 OR) abzustellen.[159]

6. Kartellrecht

Der Einsatz von Methoden künstlicher Intelligenz wie insbesondere Algorithmen kann kartellrechtlich relevant sein, wenn dabei wettbewerbsrelevante Parameter wie bspw. Preise betroffen sind.[160] Dies liegt darin begründet, dass Preisalgorithmen einerseits gezielt so programmiert werden können, dass bspw. zwischen Mitbewerbern abgesprochene Preise bei Online-Angeboten nicht unterschritten werden oder dass sie zur Umsetzung von *Signalling*-Strategien (Versand kollusiver Signale an Mitbewerber) eingesetzt werden.[161] Andererseits fördern Preisalgorithmen aufgrund der Erhöhung der Markttransparenz und der Möglichkeit, häufiger und rascher auf Preisanpassungen zu reagieren, auch die Verhaltensabstimmung zwischen Wettbewerbern.[162] Insgesamt lässt sich festhalten, dass der Einsatz von (Preis-)Algorithmen die Verhaltenskoordination – sei es durch Vereinbarung oder abgestimmte Verhaltensweise – vereinfacht.[163]

Das schweizerische Kartellrecht (KG) ist technologieneutral formuliert und kennt entsprechend keine spezifischen Bestimmungen zum Einsatz von Methoden künstlicher Intelligenz zur Preisbildung etc. Dementsprechend gelangen die allgemeinen Vorschriften – vorab diejenigen über das Kartellverbot – zur Anwendung.[164] Gemäss Art. 5 KG sind «Abreden, die den Wettbewerb auf einem Markt für bestimmte Waren oder Leistungen erheblich beeinträchtigen und sich nicht durch Gründe der wirtschaftlichen Effizienz rechtfertigen lassen, sowie Abreden, die zur Beseitigung wirksamen Wettbewerbs führen, […] unzulässig» und mit direkten Sanktionen[165] bedroht. Als Wettbewerbsabrede gelten rechtlich erzwingbare oder nicht erzwingbare *Vereinbarungen* sowie *aufeinander abgestimmte Verhaltensweisen*.[166] Auch bei Letz-

154 *Braun Binder/Burri/Lohmann/Simmler/Thouvenin/Volkinger* (Fn. 44), N 44.
155 *Braun Binder/Burri/Lohmann/Simmler/Thouvenin/Volkinger* (Fn. 44), N 45.
156 Art. 5 Abs. 1 lit. b PrHG.
157 *Braun Binder/Burri/Lohmann/Simmler/Thouvenin/Volkinger* (Fn. 44), N 46 f.
158 Art. 1 Abs. 1 PrHG *e contrario*.
159 *Gordon/Lutz* (Fn. 144), 57 f.
160 *Oliver Vahrenholt,* Algorithmen und Kartellrecht, Kollusion durch Preisalgorithmen – neue Herausforderungen für das Kartellrecht, Jusletter 26. November 2018, N 1 ff.
161 *Vahrenholt* (Fn. 160), N 24 ff.; *Peter Georg Picht/Benedikt Freund,* Wettbewerbsrecht auf algorithmischen Märkten, sic! 11/2018, 666 ff., 671.
162 *Vahrenholt* (Fn. 160), N 20; *Picht/Freund* (Fn. 161), 670.
163 Vgl. ausführlich etwa: *Peter Georg Picht/Gaspare Tazio Loderer,* Framing algorithms: competition law and (other) regulatory tools, World Compeition 42(3), 2019, 391 ff., 403 f.
164 *Picht/Freund* (Fn. 161), 673.
165 Art. 49*a* Abs. 1 KG.
166 Art. 4 Abs. 1 KG.

teren ist indes ein Mindestmass an Koordination zwingend erforderlich, d.h. es muss auch hier ausdrücklich oder stillschweigend zu einem bewussten und gewollten Zusammenwirken zwischen den Mitbewerbern kommen.[167] Werden Algorithmen koordiniert und mit der Absicht, den Preis als Wettbewerbsparameter zu beeinflussen, eingesetzt, ist ein bewusstes und gewolltes Zusammenwirken ohne Weiteres anzunehmen.[168] Freilich schwierig ist in solchen Fällen die Beweisführung. Mit der Komplexität des Algorithmus und vor allem im Falle von selbstlernenden Algorithmen erhöhen sich auch die Nachweisschwierigkeiten.[169] Als Lösungsansatz wird in der Lehre unter anderem die Einführung einer Vermutung mit der Möglichkeit zur Widerlegung bei Vorliegen starker Indizien diskutiert.[170] Dem Argument, wonach die Widerlegung bei selbstlernenden und intelligenten Algorithmen aufgrund der Eigenständigkeit der algorithmischen Entscheidung oft nicht mehr möglich sei,[171] kann entgegengehalten werden, dass das betreffende Unternehmen – wie bei jedem Einsatz von Methoden künstlicher Intelligenz – die Nachvollziehbarkeit durch angemessene Massnahmen eben gerade sicherstellen sollte.

Preisalgorithmen können nicht nur mit Blick auf Abrede-Sachverhalte, sondern auch im Zusammenhang mit einer marktbeherrschenden Stellung relevant sein. Diese darf gemäss Art. 7 KG nicht dazu missbraucht werden, um andere Unternehmen in der Aufnahme oder Ausübung des Wettbewerbs zu behindern oder die Marktgegenseite zu benachteiligen. Art. 7 Abs. 2 KG führt beispielhaft Verhaltensweisen auf, welche als missbräuchlich gelten. Wird bspw. ein Preisalgorithmus eingesetzt, um unangemessene Preise oder Geschäftsbedingungen zu erzwingen, so wäre dies gemäss Art. 7 Abs. 2 lit. c KG als missbräuchlich zu qualifizieren, sofern dadurch andere Unternehmen in der Aufnahme oder Ausübung des Wettbewerbs behindert oder die Marktgegenseite benachteiligt werden und das betreffende Unternehmen keine Rechtfertigungsgründe geltend machen kann. Das deutsche Bundeskartellamt (BKartA) betonte im Fall «Lufthansa» in Zusammenhang mit KI-Anwendungen, dass der Einsatz eines Algorithmus keine Verantwortungsentlastung mit sich bringe.[172] Das Gleiche gilt auch unter dem Schweizer KG, zumal ein allfälliges Verschulden seitens des marktbeherrschenden Unternehmens für die Frage nach der Missbräuchlichkeit einer Verhaltensweise grundsätzlich keine Rolle spielt.[173]

Der Einsatz von Methoden künstlicher Intelligenz, namentlich von Preisalgorithmen, birgt unter geltendem Kartellgesetz wie gesehen vorab das Risiko von (Preis-)Abreden. Dabei gilt es zu beachten, dass nicht nur Vereinbarungen, sondern auch abgestimmte Verhaltensweisen als unzulässige Abreden qualifizieren können. Dass eine Abrede nicht direkt zwischen Menschen bewirkt wird, ist für deren kartellrechtliche Einordnung irrelevant. Ferner kann der Einsatz von Algorithmen auch in einer einseitigen missbräuchlichen Verhaltensweise resultieren, etwa wenn dadurch unangemessene Preise oder Geschäftsbedingungen erzwungen werden. Vor diesem Hintergrund darf bei der Programmierung der Algorithmen keine Strategie vorgegeben werden, welche sich kartellrechtlich heikel auswirken könnte. Deshalb ist der Programmierung von Preisalgorithmen im Rahmen der Kartellrechts-Compliance hinreichend Rechnung zu tragen.

7. Arbeitsrecht

Künstliche Intelligenz hält auch Einzug in die privatrechtlichen Arbeitsverhältnisse. Unter den Begriff «People Analytics» fällt der Vorgang der Big-Data-Analysen und Überwachungen am Arbeitsplatz. So erheben datenbasierte Formen der Personalsteuerung vom Arbeitnehmer grosse Datenmengen, um diese dann von Algorithmen auszuwerten.[174] Methoden künstlicher Intelligenz können beim Bewer-

167 DIKE Kommentar KG-*Bangerter/Zirlick,* Art. 4 Abs. 1 N 22 m.w.H., in: Roger Zäch/Ruth Arnet/Marino Baldi et al. (Hrsg.), Bundesgesetz über Kartelle und andere Wettbewerbsbeschränkungen (KG), DIKE-Kommentar, Zürich/St. Gallen 2018 (zit. DIKE Kommentar KG-*Verfasser*).

168 DIKE Kommentar KG-*Heizmann/Mayer* (Fn. 167), Art. 2 N 47.

169 *Vahrenholt* (Fn. 161), N 46 m.w.H.

170 *Vahrenholt* (Fn. 161), N 55 m.w.H.; vgl. weitere Lösungsansätze bei *Picht/Loderer* (Fn. 163), 410 ff.

171 *Vahrenholt* (Fn. 160), N 55.

172 Bundeskartellamt, Fallbericht B9-175/17, «Lufthansa», 4.

173 DIKE Kommentar KG-*Stäuble/Schraner* (Fn. 167), Art. 7 N 85 m.w.H.

174 *Gabriel Kasper/Isabelle Wildhaber,* Big Data am Arbeitsplatz, Datenschutz- und arbeitsrechtliche Herausforderungen von People Analytics in Schweizer Unternehmen, in: Ueli Kieser/Kurt Pärli/Ursula Uttinger (Hrsg.), Datenschutztagung 2018, Ein Blick auf aktuelle Rechtsentwicklungen, 189 ff., 190.

bungsprozess (Selektion der Bewerber, Kandidatensuche im Internet, Messung der physiologischen Reaktionen am Bewerbungsgespräch, KI-System führt das Bewerbungsgespräch[175])[176], während des laufenden Arbeitsverhältnisses (Überwachung) und darüber hinaus (Aufbewahrung von Personendaten nach Beendigung des Arbeitsverhältnisses) eingesetzt werden.

Art. 328*b* OR beschränkt die zulässige Datenbearbeitung in gegenständlicher Hinsicht auf Daten zur Eignung der Arbeitnehmerin oder des Arbeitnehmers für das Arbeitsverhältnis und zu dessen Durchführung.[177] Führt ein Roboter das Bewerbungsgespräch (sog. *«Chatbot»*) gelten aufgrund der Technologieneutralität des Gesetzes dieselben Regeln wie bei einem Bewerbungsgespräch mit einem Menschen:[178] Es gilt unter anderem das Frageverbot, welches aus Art. 328*b* OR abgeleitet wird. Die künstliche Intelligenz muss dementsprechend so programmiert werden, dass sie weder nach einer Schwangerschaft, der Gewerkschaftszugehörigkeit noch politischen Ansichten der Bewerberin bzw. des Bewerbers fragt.[179] Sammelt die künstliche Intelligenz vorgängig Informationen zu einer Bewerberin bzw. einem Bewerber im Internet, so darf sie diese Informationen, welche sich im Sinne von Art. 328*b* OR nicht für das Arbeitsverhältnis bzw. dessen Durchführung eignen, nicht ermitteln.[180] Je nach Arbeitgeber ist die KI-Anwendung daher anders zu programmieren, weil dieselben Daten im einen Arbeitsumfeld relevant sein können und daher die Frage danach und Erfassung der Daten gerechtfertigt sind, im anderen hingegen mangels Relevanz nicht.

Im Vordergrund steht während dem Arbeitsverhältnis die Installation einer Videoüberwachungsanlage am Arbeitsplatz. Neben dem Datenschutzgesetz ist auch an dieser Stelle zu beachten, dass der Arbeitgeber nur Daten über die Arbeitnehmerin bzw. den Arbeitnehmer bearbeiten darf, welche die Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind. So kann eine Videoüberwachung aus Sicherheitsgründen oder zu Schulungszwecken gerechtfertigt sein.[181] Videoüberwachungssysteme, welche jedoch gezielt den Arbeitnehmer bzw. die Arbeitnehmerin überwachen sollen, sind verboten (Art. 26 Abs. 1 der Verordnung 3 zum Arbeitsgesetz [ArGV 3]) und können sogar die Gesundheit eines Arbeitnehmers bzw. einer Arbeitnehmerin beeinträchtigen, wenn die Überwachung permanent erfolgt und er/sie sich dadurch einem stetigen Druck ausgesetzt fühlt. Entsprechend erlaubt Art. 26 Abs. 2 ArGV 3 und indirekt auch Art. 328 OR eine erforderliche Videoüberwachung nur, wenn die Gesundheit und Bewegungsfreiheit des Arbeitnehmers bzw. der Arbeitnehmerin nicht eingeschränkt werden. Für zulässig erklärte das Bundesgericht vor einigen Jahren die Überwachung des Kassenraums eines Uhren- und Juwelengeschäfts, da sich erhebliche Bargeldbeträge darin befanden und die Arbeitnehmer bzw. Arbeitnehmerinnen nur sporadisch und kurzeitig erfasst wurden.[182]

V. Rechtsrahmen Ausland

Nachfolgend werden die wichtigsten Anforderungen, welche Finanzmarktaufsichtsbehörden aus anderen Jurisdiktionen an die Verwendung bzw. den Einsatz von Methoden künstlicher Intelligenz durch beaufsichtigte Institute stellen, im Sinne einer Übersicht dargestellt. Dabei sind die meisten Anforderungen in Rahmenwerken erfasst, welche sich in einem frühen Stadium der Entwicklung befinden und aus prinzipienbasierten Corporate Governance Regelungen oder unverbindlichen Leitfäden der Aufsichtsbehörden

175 So der Roboter «Vera» für IKEA, vgl. hierzu: <*https://www.bloomberg.com/news/articles/2018-03-28/this-ai-software-aims-to-do-90-percent-of-hr-s-recruiting-work*> (zuletzt besucht: 24. Juni 2021).

176 Zum Thema Personalentscheidungen des Roboters vgl. *Isabelle Wildhaber,* Robotik am Arbeitsplatz, Robo-Kollegen und Robo-Bosse, AJP 2/2017, 213 ff., 213 ff.

177 BSK OR I-*Portmann/Rudolph* (Fn. 147), Art. 328b OR N 7 ff.

178 *Thomas Söbbing,* Künstliche Intelligenz im HR-Recruiting-Prozess, Rechtliche Rahmenbedingungen und Möglichkeiten, InTeR 2018, 64 ff., 65.

179 CHK-*Emmel*, Art. 328*b* N 4 in: Marc Amstutz/Vito Roberto/Hans Rudolf Trüeb (Hrsg.), Handkommentar zum Schweizer Privatrecht, Wirtschaftliche Nebenerlasse: FusG, UWG, PauRG und KKG, 3. Aufl., Zürich/Basel/Genf 2016.

180 *Kasper/Wildhaber* (Fn. 174), 209.

181 Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), Erläuterungen zur Videoüberwachung am Arbeitsplatz, Rechtliche Rahmenbedingungen, abrufbar unter: <*https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/arbeitsbereich/ueberwachung-am-arbeitsplatz/erlaeuterungen-zur-videoueberwachung-am-arbeitsplatz.html*> (zuletzt besucht: 24. Juni 2021).

182 Urteil des BGer 6B_536/2009 vom 12. November 2009 E. 3.7.

bestehen.[183] Die existierenden Regelungen adressieren fünf gemeinsame Grundsätze – Zuverlässigkeit/Solidität, Rechenschaftspflicht, Transparenz, Fairness und Ethik[184] –, welche nachfolgend am Beispiel ausgesuchter Jurisdiktionen jeweils entsprechend ihrem Aufbau summarisch wiedergegeben werden. Dies ermöglicht einen ersten Einblick in die verschiedenen Anforderungen, welche im Ausland in Zusammenhang mit dem Einsatz künstlicher Intelligenz zu beachten sind.

Zu beachten ist dabei, dass im Ausland teilweise (bereits gegenwärtig oder künftig) allgemeine Anforderungen an KI-Lösungen erfüllt werden müssen, welche sich nicht spezifisch auf Finanzdienstleistungen beziehen. So liegt beispielsweise ein Vorschlag für eine Verordnung des Europäischen Parlaments und Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) vor.[185]

1. Deutschland

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hat sich schon 2018 kritisch geäussert, dass Systeme, die auf Methoden künstlicher Intelligenz basieren, nicht bloss als *Blackbox* zu betrachten sind und festgehalten, dass es in der Verantwortung der beaufsichtigten Unternehmen liegt, die Erklärbarkeit bzw. die Nachvollziehbarkeit von Entscheiden, die auf *Big Data* und Methoden künstlicher Intelligenz basieren, für sachkundige Dritte zu gewährleisten,[186] und dass Maschinen auch bei automatisierten Prozessen nicht die Verantwortung tragen dürfen.[187]

Im Juni 2021 hat die BaFin aufsichtliche Prinzipien für den Einsatz von Algorithmen in Entscheidungsprozessen von Finanzunternehmen publiziert.[188] Das Prinzipienpapier stellt vorläufige Überlegungen zu aufsichtlichen Mindestanforderungen für den Einsatz von künstlicher Intelligenz dar und soll beaufsichtigten Unternehmen als Orientierungshilfe dienen:

Konzeptioneller Rahmen

- **Betrachtung des gesamten Prozesses:** Der aufsichtsrechtliche Fokus richtet sich auf den gesamten algorithmenbasierten Entscheidungsprozess inklusive Einbindung in den Geschäftsprozess.
- **Keine generelle Billigung von Algorithmen:** Algorithmenbasierte Entscheidungsprozesse werden grundsätzlich risikobasiert geprüft, Ausnahmen bestehen bei Modellen, welche regulatorische Kapitalanforderungen ermitteln.
- **Risikoorientiert, proportional und technologieneutral:** Auch bei algorithmischen Entscheidungsprozessen findet ein risikoorientierter, proportionaler und technologieneutraler Ansatz bei der Aufsicht statt.
- **Bestehende Regeln werden ergänzt, präzisiert und weiterentwickelt:** Die nachfolgend aufgeführten Prinzipien stellen vorläufige Überlegungen zu aufsichtsrechtlichen Mindestanforderungen dar.

Übergeordnete Prinzipien

- **Klare Verantwortung der Geschäftsleitung:** Die Geschäftsleitung ist verantwortlich für Strategien und Leitlinien zum Einsatz von algorithmenbasierten Entscheidungsprozessen.
- **Adäquates Risiko- und Auslagerungsmanagement:** Es ist Aufgabe der Geschäftsleitung ein an den Einsatz von algorithmenbasierten Entscheidungsprozessen adaptiertes Risikomanagement zu implementieren.
- **Bias vermeiden:** Ein Bias, also die systematische Verzerrung von Ergebnissen, muss vermieden werden, um eine systematische Benachteiligung einzelner Kundengruppen auszuschliessen.
- **Gesetzlich untersagte Differenzierung ausschliessen:** Bestimmte Differenzierungsmerkmale zur Risiko- und Preiskalkulation dürfen nicht verwendet werden, um mögliche Diskriminierungen auszuschliessen.

183 Financial Stability Institute FSI, Humans keeping AI in the check – emerging regulatory expectations in the financial sector, 2021, 3.

184 Financial Stability Institute (Fn. 183), 6.

185 Siehe Fn. 8.

186 BaFin BDAI 2018 (Fn. 3), 13.

187 Interview mit BaFin-Präsident *Felix Hufeld, Gerold Grasshoff* (Senior Partner, The Boston Consulting Group), Prof. Dr. *Stefan Wrobel* (Leiter, Fraunhofer IAIS) und *Claus Wechselmann* (Geschäftsführer, PD – Berater der öffentlichen Hand) abrufbar unter: <*https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2018/fa_bj_1806_BDAI_Interview.html*> (zuletzt besucht: 28. Juni 2021).

188 BaFin BDAI 2021 (Fn. 1).

Spezifische Prinzipien für die Entwicklungsphase

- **Datenstrategie und Datengovernance:** Daten müssen in ausreichender Quantität und Qualität verwendet werden und es ist ein überprüfbares Verfahren (Datenstrategie) zu verwenden, welches in einer Datengovernance umzusetzen ist.
- **Datenschutzregeln beachten:** Geltende Datenschutzbestimmungen und datenschutzrechtliche Vorgaben sind zu berücksichtigen.
- **Korrekte, robuste und reproduzierbare Ergebnisse sicherstellen:** Es sind korrekte und robuste Ergebnisse sicherzustellen, welche durch einen unabhängigen Dritten reproduzierbar sind.
- **Dokumentation zur internen und externen Nachvollziehbarkeit:** Die Modellauswahl, die Kalibrierung und das Training des Modells sowie die Modellvalidierung sind angemessen zu dokumentieren.
- **Angemessene Validierungsprozesse:** Jeder Algorithmus sollte vor Übernahme in den operativen Betrieb durch eine nicht in die Modellierung eingebundene Person oder Funktion angemessen validiert werden.
- **Verwendung von relevanten Daten zur Kalibrierung und Validierung:** Die verwendeten Daten müssen für den jeweiligen Anwendungsbereich relevant und repräsentativ sein, um ein Bias in der Modellierung zu vermeiden.

Spezifische Prinzipien für die Anwendung

- **Interpretation und Verwertung algorithmischer Ergebnisse für die Entscheidungsfindung:** Ein funktionierender Mechanismus muss eine ausreichende Kontrolle, Feedbackloops und Anpassungsregelungen zur Entwicklungsphase umfassen.
- **«Putting the human in the loop»:** Bei der Interpretation und Verwertung der algorithmischen Ergebnisse sollen Personen risikobasiert eingebunden werden.
- **Intensive Freigabe- und Feedbackprozesse:** Manuelle Freigabe- und Feedbackprozesse sind risikobasiert (z.B. mittels Verwendung von Schwellenwerten) zu implementieren.
- **Etablierung von Notmassnahmen:** Für geschäftskritische Anwendungen sind Business Continuity Massnahmen zu definieren, falls es zu Problemen bei algorithmenbasierten Entscheidungsprozessen kommt.
- **Laufende Validierung, übergeordnete Evaluation und entsprechende Anpassung:** In der praktischen Anwendung müssen Algorithmen laufend validiert werden, um die Funktionalität und Abweichungen anhand von festgelegten Parametern zu überprüfen, um allenfalls notwendige Anpassungen vorzunehmen.

2. Singapur

Die Monetary Authority of Singapore (MAS) publizierte im November 2018 Prinzipien zur Förderung von Fairness, Ethik, Rechenschaftspflicht und Transparenz (Principles to Promote Fairness, Ethics, Accountability and Transparency «FEAT») für die Nutzung von künstlicher Intelligenz und Datenanalyse (artificial intelligence and data analytics «AIDA») im Finanzsektor von Singapur, welche im Februar 2019 mit einem Verweis auf das «Model AI Governance Framework» des nationalen Datenschutzbeauftragten ergänzt wurden:[189]

Fairness

Rechtfertigung

1. Keine ungerechtfertigte systematische Benachteiligung von Einzelpersonen oder Gruppen bei KI-basierten Entscheidungen.
2. Nur gerechtfertigte Verwendung von persönlichen Merkmalen als Eingaben für KI-Entscheidungen.

Genauigkeit und Voreingenommenheit (Bias)

3. Daten und Modelle, die für KI-gesteuerte Entscheidungen verwendet werden, sind regelmässig auf Genauigkeit und Relevanz zu prüfen und zu validieren, um unbeabsichtigte Voreingenommenheit zu minimieren.
4. KI-Entscheidungen sind regelmässig zu überprüfen, damit sich die Modelle bestimmungsgemäss verhalten.

[189] Monetary Authority of Singapore MAS, Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector Update, 7. Februar 2019.

Ethik

5. Die Verwendung von KI hat im Einklang mit den ethischen Standards, Werten und Verhaltensregeln des Unternehmens zu stehen.

6. Für KI-gesteuerte Entscheidungen haben mindestens die gleichen ethischen Standards wie für menschengesteuerte Entscheidungen zu gelten.

Rechenschaftspflicht

Interne Rechenschaftspflicht

7. Die Verwendung von KI bei KI-gesteuerten Entscheidungen ist von einer geeigneten internen Stelle zu genehmigen.

8. Unternehmen, die KI verwenden, sind sowohl für intern entwickelte als auch für extern beschaffte KI-Modelle verantwortlich.

9. Unternehmen, die KI verwenden, sensibilisieren proaktiv das Management und den Verwaltungsrat für ihre Verwendung von KI.

Externe Rechenschaftspflicht

10. Den betroffenen Personen sind Kanäle zur Verfügung zu stellen, um sich über die sie betreffenden KI-gesteuerten Entscheidungen zu erkundigen, Einsprüche einzureichen und Überprüfungen zu beantragen.

11. Verifizierte und relevante Zusatzdaten, die von den betroffenen Personen bereitgestellt werden, sind bei der Überprüfung von KI-gesteuerten Entscheidungen zu berücksichtigen.

Transparenz

12. Um das Vertrauen der Öffentlichkeit zu erhöhen, ist die Verwendung von KI den betroffenen Personen im Rahmen der allgemeinen Kommunikation proaktiv mitzuteilen.

13. Betroffene Personen erhalten auf Anfrage klare Erklärungen darüber, welche Daten verwendet werden, um KI-gesteuerte Entscheidungen über die betroffene Person zu treffen und wie die Daten die Entscheidung beeinflussen.

14. Betroffene Personen erhalten auf Anfrage klare Erklärungen zu den Folgen, die KI-gesteuerte Entscheidungen für sie haben können.

Im November 2019 kündigte die MAS zudem die Schaffung des Veritas-Frameworks zur Förderung der verantwortungsvollen Einführung von künstlicher Intelligenz an.[190] Mit Veritas können Unternehmen im Finanzsektor ihre KI-Anwendungen entlang der FEAT Prinzipien analysieren. Im Januar 2021 wurden in einer ersten Phase Anwendungen im Bereich der Entwicklung von Fairness-Metriken für Kreditrisiko-Scoring und Kundenmarketing abgeschlossen sowie für die zweite Phase mit Anwendungsfällen für Versicherungen im Bereich Underwriting und Betrugserkennung gestartet.[191]

3. Hong Kong

Im November 2019 hat die Hong Kong Monetary Authority (HKMA) die «High-level Principles on Artificial Intelligence» veröffentlicht, um dem Bankensektor Leitlinien für den Einsatz von Anwendungen künstlicher Intelligenz zur Verfügung zu stellen.[192] Die Prinzipien sind dabei allgemein gehalten, um die Entwicklung von KI-Anwendungen nicht einzuschränken:

Governance

1. **Rechenschaftspflicht des Verwaltungsrates und der Unternehmensleitung:** Verwaltungsrat und Unternehmensleitung sind für die Ergebnisse von KI-Anwendungen verantwortlich und sollen sicherstellen, dass ein angemessenes Governance-Rahmenwerk und Risikomanagement-Massnahmen implementiert werden, um den Einsatz von KI-Anwendungen zu überwachen. Ebenso sollen die Rollen und Verantwortlichkeiten der drei Verteidigungslinien («three lines of defence») bei der Entwicklung und Überwachung des Betriebs von KI-Anwendungen klar definiert werden.

Anwendungsdesign und -entwicklung

2. **Ausreichendes Fachwissen:** Da die Konzeption und Entwicklung von KI-Anwendungen spezifisches Fachwissen erfordert, sollten Banken sicherstellen, dass ihre Entwickler über die erfor-

190 Medienmitteilung abrufbar unter: <*https://www.mas.gov.sg/news/media-releases/2019/mas-partners-financial-industry-to-create-framework-for-responsible-use-of-ai*> (zuletzt besucht: 28. Juni 2021).

191 Medienmitteilung abrufbar unter: <*https://www.mas.gov.sg/news/media-releases/2021/veritas-initiative-addresses-implementation-challenges*> (zuletzt besucht: 28. Juni 2021).

192 Hong Kong Monetary Authority HKMA, High-level Principles on Artificial Intelligence, 1. November 2019.

derliche Kompetenz und Erfahrung verfügen und die Geschäftsleitungen sicherstellen, dass eingesetzte Mitarbeiter angemessen ausgewählt, ausgebildet und überwacht werden.

3. **Sicherstellung eines angemessenen Niveaus der Erklärbarkeit von KI-Anwendungen:** Vertrauenswürdige und robuste KI-Anwendungen sollten für alle relevanten Parteien erklärbar sein (keine «Blackbox-Ausrede»). Banken sollten während der Entwicklungsphase angemessene Massnahmen ergreifen, um ein ihrer KI-Anwendungen entsprechendes Mass an Erklärbarkeit sicherzustellen.
4. **Verwendung von Daten in guter Qualität:** Da die Genauigkeit und Leistung von KI-Anwendungen stark von den Daten abhängen, die zum Trainieren der KI-Modelle verwendet werden, sollten Banken ein effektives Data-Governance-Rahmenwerk einführen, um sicherzustellen, dass die verwendeten Daten von guter Qualität und Relevanz sind.
5. **Durchführen einer strengen Modellvalidierung:** Eine strenge Validierung bzw. Prüfung der trainierten KI-Modelle sollte durchgeführt werden, um die Genauigkeit und Angemessenheit der KI-Modelle zu bestätigen, bevor sie für den produktiven Einsatz eingesetzt werden. Es ist vorzuziehen, eine unabhängige Partei (z.B. die zweite oder dritte Verteidigungslinie oder einen externen Berater) in den Modellvalidierungsprozess einzubeziehen.
6. **Sicherstellung der Überprüfbarkeit von KI-Anwendungen:** Die Ergebnisse von KI-Anwendungen sind kontinuierlich zu verfolgen und Evidenzen zu sammeln, um bei Vorfällen Abklärungen treffen zu können. Es sind genügend Audit-Protokolle und eine ausreichende Dokumentation während der Designphase zu erstellen.
7. **Implementierung einer wirksamen Managementüberwachung von Drittanbietern:** Wenn Banken bei der Entwicklung von KI-Anwendungen auf Drittanbieter zurückgreifen, sollten diese einer angemessenen Prüfung unterzogen werden, bei welcher die anwendbaren Prinzipien zu berücksichtigen sind. Weiter ist eine regelmässige Prüfung von Drittanbietern und der erbrachten Dienstleistungen notwendig.
8. **Ethisch, fair und transparent sein:** KI-gesteuerte Entscheidungen sollen keine Verbrauchergruppen diskriminieren oder ungewollt vorein-

genommen sein. Der Einsatz von KI-Anwendungen sollte mit den Unternehmenswerten und ethischen Standards der Banken übereinstimmen und die Grundsätze des Verbraucherschutzes wahren. KI-gestützte Dienstleistungen müssen für den Verbraucher transparent sein und die damit verbundenen Risiken müssen klar sein.

Laufende Überwachung und Wartung

9. **Durchführung regelmässiger Überprüfungen und fortlaufende Überwachung:** Da KI-Anwendungen aus Live-Daten lernen und sich die Modelle so anders verhalten können, sind regelmässige Überprüfungen durchzuführen und eine fortlaufende Überwachung sicherzustellen.
10. **Einhaltung von Datenschutzanforderungen:** Es sind effektive Datenschutzmassnahmen zu implementieren und wenn möglich Personendaten zu anonymisieren.
11. **Implementierung effektiver Cybersicherheitsmassnahmen:** Die Verwendung von KI-Anwendungen kann zu neuen Cyber-Bedrohungen führen. Banken haben sicherzustellen, dass Sicherheitskontrollen solche Bedrohungen angemessen mitigieren.
12. **Risikominderung und Notfallplan:** Zusätzlich zu risikomitigierenden Massnahmen (z.B. Einbezug von Menschen oder Risikolimiten) ist ein Notfallplan zu erstellen, um KI-Anwendungen mit konventionellen Prozessen weiterzuführen.

Ebenfalls im November 2019 hat die HKMA Prinzipien zum Verbraucherschutz in Bezug auf die Verwendung der Analyse von grossen Datenmengen und KI durch beaufsichtigte Unternehmen herausgegeben.[193] Die Prinzipien adressieren Themen zur Governance und Rechenschaftspflicht, Fairness, Transparenz und Offenlegung sowie zu Datenschutz und Datensicherheit.

4. Frankreich

Die Autorité de contrôle prudentiel et de résolution (ACPR) hat im Dezember 2018 ein Diskussionspapier über Herausforderungen von künstlicher Intelligenz im Finanzsektor herausgegeben und dabei verschie-

[193] Hong Kong Monetary Authority HKMA, Consumer Protection in respect of Use of Big Data Analytics and Artificial Intelligence by Authorized Institutions, 5. November 2019.

dene Anwendungsfälle und Risiken aufgezeigt.[194] Ein weiteres Diskussionspapier wurde im Juni 2020 herausgegeben, mit welchem ein Konsultationsverfahren gestartet wurde und neben Governance und anderen Anforderungen vier unabhängige Kriterien für die Evaluierung von auf künstlicher Intelligenz basierenden Algorithmen und Lösungen vorgestellt wurden:[195]

- **Angemessene Datenverwaltung:** Ist eine grundlegende Anforderung für jeden Algorithmus in Bezug auf Leistung und Einhaltung regulatorischer Vorschriften und muss ethische Überlegungen wie Fairness sicherstellen und Diskriminierung verhindern.
- **Leistung eines KI-Algorithmus:** Die Genauigkeit kann anhand einer Vielzahl von Metriken unter technischen und funktionalen Kriterien untersucht werden, die ausgewählten Kriterien sind jedoch mit Anforderungen an die Erklärbarkeit abzuwägen.
- **Stabilität:** Beschreibt wie robust und belastbar sich das Verhalten eines KI-Algorithmus über seinen Lebenszyklus hinweg erweist.
- **Erklärbarkeit:** Transparenz und Interpretierbarkeit müssen im Kontext gewährleisten, dass die Erklärbarkeit gegenüber Kunden oder anderen Anspruchsgruppen gegeben ist. Dabei sind vier Ebenen von Erklärbarkeit vorgesehen:
  1. **Beobachtung:** Wie arbeitet der Algorithmus (technisch)? Was ist der Zweck des Algorithmus (funktional)?
  2. **Rechtfertigung:** Warum hat der Algorithmus dieses Resultat produziert?
  3. **Annährung:** Wie arbeitet der Algorithmus?
  4. **Replizierung:** Wie kann man beweisen, dass der Algorithmus korrekt arbeitet?

Im Dezember 2020 wurden die Rückmeldungen aus dem Konsultationsverfahren der Öffentlichkeit zugänglich gemacht.[196]

5. Niederlande

Im Juli 2019 hat De Nederlandsche Bank DNB allgemeine Grundsätze für den Einsatz von KI im Finanzsektor herausgegeben («SAFEST»), welche in sechs Kernpunkte des verantwortungsvollen Umgangs mit KI unterteilt sind:[197]

Zuverlässigkeit

1. Sicherstellung der generellen Einhaltung der regulatorischen Verpflichtungen in Bezug auf KI-Anwendungen.
2. Minderung von finanziellen (und anderen relevanten aufsichtsrechtlichen) Risiken bei der Entwicklung und Nutzung von KI-Anwendungen.
3. Fokussierung auf die Mitigierung von Modellrisiken für wesentliche KI-Anwendungen.
4. Sicherstellung und Verbesserung der Qualität der Daten die von KI-Anwendungen verwendet werden.
5. Kontrolle über (das korrekte Funktionieren von) beschafften und/oder ausgelagerten KI-Anwendungen.

Verantwortlichkeit

6. Zuweisung der endgültigen Verantwortung für KI-Anwendungen und das Management der damit verbundenen Risiken auf Verwaltungsratsebene.
7. Integration der Verantwortung in das Risikomanagement-Rahmenwerk der Organisation.
8. Implementierung der Verantwortung in Bezug auf externe Stakeholder.

Fairness

9. Definition und Implementierung des Konzepts der Fairness in Bezug auf KI-Anwendungen.
10. Überprüfung (der Ergebnisse) von KI-Anwendungen auf unbeabsichtigte Diskriminierung.

Ethik

11. Spezifikation von Zielen, Standards und Anforderungen in einem ethischen Kodex für die Einführung und Anwendung von KI.
12. Ausrichtung der (Ergebnisse von) KI-Anwendungen in Einklang mit den rechtlichen Verpflichtungen, Werten und Prinzipien der Organisation.

194 *Olivier Fliche/Su Yang,* Artificial intelligence: challenges for the financial sector, ACPR discussion paper, Dezember 2018.

195 *Laurent Dupont/Olivier Fliche/Su Yang,* Governance of Artificial Intelligence in Finance, ACPR discussion document, Juni 2020.

196 *Laurent Dupont,* Governance of artificial intelligence in finance, ACPR Summary of consultation responses, Dezember 2020.

197 De Nederlandsche Bank DNB, General principles for the use of Artificial Intelligence in the financial sector, 2019.

Kenntnisse

13. Sicherstellen, dass das Senior Management ein angemessenes Verständnis von KI hat (in Bezug auf ihre Rollen und Verantwortlichkeiten).
14. Schulung von Risikomanagement- und Compliance Personal in KI.
15. Entwicklung von Bewusstsein und Verständnis für KI innerhalb der Organisation.

Transparenz

16. Transparente Strategie und Entscheidungen bezüglich der internen Einführung und Nutzung von KI.
17. Förderung der Nachvollziehbarkeit und Erklärbarkeit von KI-gesteuerten Entscheidungen und Modellergebnissen.

6. Vereinigtes Königreich

Im Oktober 2019 haben die Bank of England (BoE) und die Financial Conduct Authority (FCA) eine Umfrage zum maschinellen Lernen im britischen Finanzsektor durchgeführt, um den Umfang der Verwendung sowie Anwendungsfälle, Vorteile und Risiken festzustellen.[198] Bei der Auswertung wurde festgehalten, dass die Unternehmen die Risiken im Zusammenhang mit dem Einsatz neuer Technologien identifizieren, verstehen und managen sollen und dass eine Arbeitsgruppe zu künstlicher Intelligenz mit dem öffentlichen und privaten Sektor geschaffen werden soll. Die Arbeitsgruppe hat im Oktober 2020 das erste Mal getagt.[199]

7. Österreich

Das Finanzmarkt-Geldwäschegesetz enthält seit dem 1. März 2021 mit § 7*a («Transaktionsmonitoring unter Verwendung eines auf künstlicher Intelligenz basierenden Ansatzes»)* eine ausdrückliche gesetzliche Grundlage zur Verwendung von künstlicher Intelligenz oder «anderen fortschrittlichen Technologien». Die Entwicklung und die Umsetzung der Funktionsweise des Transaktionsmonitoringsystems ist dabei hinreichend zu dokumentieren damit die Funktionsweise nachvollziehbar ist und der Finanzmarktaufsicht aufgezeigt werden kann.[200]

V. Fazit

Anders als in der EU ist in der Schweiz die Einführung von KI-spezifischen Regelungen derzeit nicht vorgesehen. Eine interdepartementale Arbeitsgruppe der Bundesverwaltung ist im Jahr 2019 zum Ergebnis gelangt, dass die bestehenden rechtlichen Regelungen, insbesondere auch im Finanzmarkt, aufgrund ihrer technologieneutralen Ausgestaltung genügen, um Sachverhalte mit KI-Anwendungen gleichermassen rechtlich zu erfassen wie solche ohne KI-Einsatz.

Selbstredend ist die Notwendigkeit gesetzgeberischen Tätigwerdens aufgrund der Weiterentwicklungen im Bereich künstlicher Intelligenz und deren Einsatzpotenzial laufend neu zu beurteilen. Im Falle von allfälligen Rechtsunklarheiten sollte indes zunächst geprüft werden, ob diese durch praktische Auslegungshilfen, im Finanzmarkt bspw. in Form von FINMA-Rundschreiben, ausgeräumt werden können.

Zudem lassen sich mit branchenspezifischen Leitlinien Prinzipien für die Anwendung von KI-Methoden formulieren, um eine einheitliche Auslegung der einschlägigen Rechtsnormen zu gewährleisten und gegebenenfalls darüber hinaus ethische Grundsätze aufzustellen. Bei der Ausarbeitung solcher Richtlinien könnten bspw. das bereits erwähnte Prinzipienpapier der BaFin[201] als Vorlage dienen.

In der Zwischenzeit können sich beaufsichtigte Institute, die am Einsatz von Methoden künstlicher Intelligenz interessiert sind, insbesondere an den Vorgaben und Prinzipienpapieren ausländischer Finanzmarktaufsichtsbehörden orientieren, die eine gute Grundlage und Vergleichsmöglichkeiten für die Festlegung von Anforderungen an KI-Methoden bieten.

198 Bank of England BoE/Financial Conduct Authority FCA, Machine learning in UK financial services, Oktober 2019.

199 Medienmitteilung abrufbar unter: *<https://www.bankofengland.co.uk/Events/2020/October/fintech-ai-public-private-forum>* (zuletzt besucht: 28. Juni 2021).

200 *<https://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40230848/NOR40230848.html>* (zuletzt besucht: 9. Juni 2021).

201 Siehe Fn. 1.