



universität
wien

MASTER THESIS

Titel der Master Thesis / Title of the Master's Thesis

„Der Rechtsrahmen für die Anwendung der künstlichen
Intelligenz in der Geschäftstätigkeit von Unternehmen:
eine vergleichende Analyse der Initiativen in der
Europäischen Union und den USA“

verfasst von / submitted by

Vladyslav Hlavatskyi

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of
Master of Laws (LL.M.)

Wien, 2020 / Vienna 2020

Studienkennzahl lt. Studienblatt /
Postgraduate programme code as it appears on
the student record sheet:

UA 992 548

Universitätslehrgang lt. Studienblatt /
Postgraduate programme as it appears on
the student record sheet:

Europäisches und Internationales Wirtschaftsrecht /
European and International Business Law

Betreut von / Supervisor:

ao. Univ.-Prof. Dr. Siegfried Fina

Abstract

(English version below)

Künstliche Intelligenz und andere aufkommende Technologien sind bereits der Alltag in der modernen Welt. Die Führungsrolle auf dem Gebiet der künstlichen Intelligenz und die Ausarbeitung eines Rechtsrahmens für deren effektive und sichere Anwendung stellt sowohl für die EU als auch für die USA eine strategische Priorität dar.

Diese Master Thesis enthält eine vergleichende Analyse bestehender Initiativen zur gesetzlichen Regelung der Anwendung künstlicher Intelligenz in der Geschäftstätigkeit von Unternehmen in der EU und in den USA. Außerdem behandelt sie die Frage zur Notwendigkeit und Zulässigkeit der rechtlichen Regulierung künstlicher Intelligenz, sowie Aspekte der unternehmerischen Anwendung künstlicher Intelligenz, die besonders regulierungsbedürftig sein können.

Die vorliegende vergleichende Analyse betrifft insbesondere die Initiativen zu Anpassung des Binnenmarktrechts für den freien grenzüberschreitenden Verkehr der auf künstlicher Intelligenz gestützten Produkte und Dienstleistungen in der EU, Schutz der grundlegenden Menschenrechte bei der Anwendung künstlicher Intelligenz (insbesondere Schutz der personenbezogenen Daten und Verhütung der Diskriminierung), Haftungsmodelle für den durch künstliche Intelligenz verursachten Schaden (insbesondere Regulierung automatisierter Fahrzeuge), Produktsicherheitsvorschriften und Marktüberwachung der Technologien künstlicher Intelligenz.

Als Ergebnis der durchgeführten Analyse sind eigene Empfehlungen bzw. Vorschläge zur Verbesserung der untersuchten Initiativen bzw. Regelungen in der EU und den USA dargestellt.

Abstract

Artificial intelligence and other emerging technologies are already part of everyday life in the modern world. Leadership in the field of artificial intelligence and establishment of a legal framework for its effective and safe application is a strategic priority for both the EU and the United States.

This Master Thesis contains a comparative analysis of existing initiatives for regulation of the artificial intelligence application in the business activity of companies in the EU and in the USA. In addition, it deals with the question of the necessity and admissibility of legal regulation of artificial intelligence, as well as aspects of the entrepreneurial application of artificial intelligence, which can be particularly in need of regulation.

This comparative analysis particularly concerns the initiatives to adaption of the internal market law for the free cross-border movement of products and services based on artificial intelligence in the EU, protection of fundamental human rights when using artificial intelligence (in particular protection of personal data and prevention of discrimination), liability models for the damage caused by artificial intelligence (in particular by autonomous vehicles), product safety regulations and market supervision of artificial intelligence technologies.

As a result of the analysis carried out, own recommendations and suggestions for improving the investigated initiatives and regulations in the EU and the USA are presented.

Inhaltsverzeichnis

Einleitung	8
Kapitel 1: Rechtliche Gesichtspunkte der KI in der Geschäftstätigkeit	12
1.1. Definition der KI	12
1.1.1. <i>Technische Definition und wesentliche Technikeigenschaften der KI</i>	12
1.1.2. <i>Definitionsversuche durch die internationalen Organisationen</i>	14
1.2. Anwendung der KI in der Geschäftstätigkeit von Unternehmen	16
1.3. KI und Regulierung	18
1.4. Rechtliche Herausforderungen der KI-Anwendung in der Geschäftstätigkeit	21
Kapitel 2: Initiativen in der EU	24
2.1. Überblick der bestehenden Initiativen zur Regulierung der KI in der EU	24
2.2. Initiativen zur Schaffung des Binnenmarktes für KI.....	28
2.3. Initiativen zum Schutz der grundlegenden Menschenrechte	31
2.3.1. <i>Schutz personenbezogener Daten und des Privatlebens</i>	32
2.3.2. <i>Verhütung der Diskriminierung</i>	36
2.4. Initiativen zur Haftung.....	38
2.4.1. <i>Bestehende Haftungsmodelle in dem Nationalrecht</i>	41
2.4.2. <i>Bericht über die Haftung für künstliche Intelligenz und andere aufkommende Technologien (Expertengruppe für Haftung und neue Technologien)</i>	45
2.4.3. <i>Bericht über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung COM (2020) 64 endgültig (Europäische Kommission)</i>	47
2.5. Initiativen zur Produktsicherheit und zum Marktaufsicht	48
2.5.1. <i>Bericht über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung COM (2020) 64 endgültig (Europäische Kommission)</i>	52
2.5.1. <i>Produktsicherheit für automatisierte Fahrzeuge</i>	53
2.5.2. <i>Initiativen zur Marktüberwachung</i>	55

Kapitel 3: Initiativen in den USA	58
3.1. Überblick der bestehenden Initiativen zur Regulierung der KI in den USA	58
3.1.1. <i>Jüngste Initiativen auf Bundesebene</i>	58
3.1.2. <i>Gesetzliche Definition</i>	61
3.1.3. <i>Rolle einzelner Bundesstaaten</i>	61
3.2. Initiativen zum Schutz der grundlegenden Menschenrechte	62
3.3. Initiativen zur Haftung.....	67
3.4. Initiativen zur Produktsicherheit	69
Kapitel 4: Abschließender Vergleich der Initiativen in der EU und den USA	76
4.1. Vergleich der Initiativen der EU und USA.....	76
a) <i>Vergleich der Ansätze zur Schaffung des Rechtsrahmens für KI</i>	76
b) <i>Vergleich der Initiativen zum Schutz der grundlegenden Menschenrechte</i>	77
c) <i>Vergleich der Initiativen zur Haftung</i>	77
d) <i>Vergleich der Initiativen zu Produktsicherheit und Marktaufsicht</i>	78
4.2. Empfehlungen zur Verbesserung der untersuchten Initiativen	78
Fazit	81
Literaturverzeichnis	84
Eidesstattliche Erklärung	94

Abkürzungsverzeichnis

ABGB	Allgemeines bürgerliches Gesetzbuch
Abs.	Absatz
ADM-Systeme	Algorithmische Entscheidungssysteme
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AI HGL	Hochrangige Expertengruppe für künstliche Intelligenz
Art.	Artikel
bzw.	beziehungsweise
ca.	circa, ungefähr
dh.	das heißt
DoT	US-Verkehrsministerium (Department of Transport)
DSVGO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
EG	Europäische Gemeinschaft
EKHG	Eisenbahn- und Kraftfahrzeughaftpflichtgesetz
ESAs	European Supervision Authorities (Europäische Aufsichtsbehörde)
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EUV	Vertrag über die Europäische Union
EWG	Europäische Wirtschaftsgemeinschaft
FTC	Bundeshandelskommission (Federal Trade Commission)
ggf.	gegebenenfalls
inkl.	inklusive
insb.	insbesondere
IoT	Internet der Dinge
iSd	im Sinn des, - der
KI	Künstliche Intelligenz
NHTSA	National Highway Traffic Safety Administration

NIST	National Institute of Standards and Technology, Nationales Institut für Standards und Technologie
Nr.	Nummer
NTF	New Technologies Formation (Formation für neue Technologien)
OECD	Organisation for Economic Cooperation and Development
PwC	PricewaterhouseCoopers
S.	Seite
s.	siehe
SAE	Society of Automotive Engineers International (Verband der Automobilingenieure)
sog.	sogenannt
US bzw. USA	Vereinigte Staaten von Amerika
usw.	und so weiter
vgl.	vergleiche
z.B.	zum Beispiel

Einleitung

„Artificial intelligence is a rare case where we need to be proactive about regulation instead of reactive. Because I think by the time we are reactive in artificial intelligence regulation, it's too late. Normally the way regulations are set up is a while bunch of bad things happen, there's a public outcry, and after many years a regulatory agency is set up to regulate that industry. It takes forever. That, in the past, has been bad but not something which represented a fundamental risk to the existence of civilization. Artificial intelligence is a fundamental risk to the existence of human civilization.“
(Elon Musk)¹

Man kann die moderne Welt ohne die rasche Entwicklung der Technologien und die intensive Digitalisierung aller Lebensbereiche kaum vorstellen. In vielen Ländern sind die Digitalisierung und die Automatisierung schon der Alltag der staatlichen Verwaltung und der Geschäftstätigkeit von Unternehmen. Der Begriff der KI ist heutzutage in aller Munde. Er umfasst eine breite Reihe der Technologien, wie etwa maschinelles Lernen, Robotik, künstliche neuronale Netze, Computerlinguistik usw.

Problemstellung

KI ermöglicht es den Unternehmen, intelligenter und schneller zu wirtschaften und mit deutlich weniger mehr zu leisten. Laut Expertenaussagen von PwC könnte KI bis 2030 bis zu 15,7 Billionen US-Dollar zur Weltwirtschaft beitragen, mehr als die derzeitigen Erträge Chinas und Indiens zusammen. Davon können 6,6 Billionen US-Dollar wegen höherer Produktivität zufließen.²

Zu gleicher Zeit bringt die Anwendung von KI zahlreiche rechtliche Herausforderungen mit. Darunter sind zunächst folgende zu nennen: Schutz der personenbezogenen Daten bei der Bearbeitung der Daten durch KI und der Automatisierung der Entscheidungsfindungsprozesse, Haftung für die durch KI verursachten Schäden, Frage zur Notwendigkeit der Produktsicherheitskontrolle von sog. intelligenten Waren (z.B. Roboter, Robotersysteme, automatisierte Fahrzeuge) durch die Marktüberwachungsbehörden. Vor diesem Hintergrund ist

¹Kurt Wagner, Interview with Elon Musk (15 July 2017), abrufbar unter <https://www.vox.com/2017/7/15/15976744/elon-musk-artificial-intelligence-regulations-ai>, letzter Zugriff: 20.03.2020

²PwC, *Sizing the prize: What's the real value of AI for your business and how can you capitalise?* (2017), abrufbar unter <https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf>, letzter Zugriff: 25.03.2020, S. 3

es auch fraglich, ob das bestehende Konzept des Binnenmarktrechts in der EU ausreichend geeignet ist, den freien grenzüberschreitenden Verkehr der sog. KI-Waren und Dienstleistungen zu ermöglichen.

Die Bedeutung der KI in der modernen Welt kann am besten durch die Angabe der Statistik zu den Investitionsvolumen in KI-Industrie zum Ausdruck gebracht, die Europäische Kommission in Weissbuch „Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen“ angeführt hat. Nach deren Angaben wurden 2016 in Europa ca. 3,2 Milliarden Euro in KI investiert, in Nordamerika - 12,1 Milliarden Euro und in Asien 6,5 Milliarden Euro.³ Wie es sich aus diesen Daten ergibt, sind die EU und die USA einige der führenden Akteure in KI-Zweig.

Vor diesem Grund werden in dieser Master Thesis die bestehenden Rechtsvorschriften bzw. die Schlüsselinitiativen zur Regulierung der KI in der EU und den USA analysiert bzw. verglichen. Unter Initiativen sollte man nicht nur Entwürfe der ausgearbeiteten Rechtsakte, sondern auch die bereits umgesetzte Gesetzgebung verstehen. Die Untersuchung der bestehenden Rechtsvorschriften ist deshalb auch von großer Bedeutung im Kontext dieses Themas, weil die EU bereits einige Initiativen, insb. auf dem Gebiet des Datenschutzes⁴, in ihrem Rechtssystem implementierte.

Zielsetzung und Forschungsfragen

Die oben genannten rechtlichen Herausforderungen der KI-Anwendung und deren Potenzial des wirtschaftlichen Wachstums ermutigen die Staaten, ihre eigenen Ansätze und Initiativen zur Regulierung dieses Phänomens zu entwickeln. In diesem Zusammenhang besteht das Ziel dieser Arbeit grundsätzlich in Analyse und Vergleichung der Initiativen zur Regulierung der KI-Anwendung in der Geschäftstätigkeit in der EU und USA. Überblicksmäßig sollen so die Vorteile und die Nachteile der entsprechenden Initiativen zur Regulierung der KI festgestellt werden. Daher ist das hauptsächliche Ergebnis der Analyse in der vorliegenden Master Thesis die Erarbeitung und die Darstellung der eigenen Verbesserungsvorschläge bzw. Empfehlungen in Bezug auf Regulierung der KI in der Geschäftstätigkeit.

³ Europäische Kommission, Weissbuch „Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen“ COM (2020) 65 endgültig, abrufbar unter https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_de.pdf, letzter Zugriff am 30.05.2020 S. 4

⁴ z.B. verfügt die EU bereits über ein in DSGVO verankertes Datenschutzrecht, das unter anderem KI-Anwendung berücksichtigt

Die zentrale wissenschaftliche Fragestellung dieser Arbeit ist wie folgt:

- Soll die Anwendung der KI in der Geschäftstätigkeit von Unternehmen der Regulierung unterliegen?
- Falls diese Frage zu bejahend ist, welche Aspekte des KI-Einsatzes sind besonders regulierungsbedürftig?
- Ist das Vorliegen der ethischen Leitlinien zur Ausarbeitung der Regelungen für KI erforderlich?
- Sind die bestehenden Rechtsvorschriften in der EU und in den USA gut geeignet, die Herausforderungen bzw. Risiken der KI-Anwendung in der Geschäftstätigkeit von Unternehmen zu meistern?
- Welche Initiativen zur Regulierung von KI in der Geschäftstätigkeit bestehen zu dieser Zeit in der EU und in den USA?
- Welche Vorteile und Nachteile bzw. Lücken haben die bestehenden Rechtsvorschriften bzw. Initiativen der EU und USA?
- Welche Empfehlungen zur Verbesserung der untersuchten Initiativen bzw. Regelungen als Ergebnis der durchgeführten Analyse vorgeschlagen werden können?

Vorgehensweise, Methode, Quellen

Die wissenschaftliche Grundlage dieser Master Thesis stellt eine vergleichende Rechtsquellenanalyse dar. Die europäischen Rechtsgrundlagen werden über die Informationssysteme der EU recherchiert. Einige Rechtsvorschriften in den USA und die Unterlagen der internationalen Organisationen (z.B. EU und OECD), die nur in englischer Sprache verfügbar sind, werden in ihrer englischen Fassung zitiert.

Aufbau der Arbeit

Zunächst wird es in einem ersten Kapitel auf den Begriff „KI“ näher eingegangen. Hierbei werden unterschiedliche Definitionen von KI vorgestellt und die dieser Erscheinung zugrunde liegenden Technologien dargelegt werden. Überdies werden die KI-Anwendungsbereiche in der Geschäftstätigkeit von Unternehmen, sowie die Notwendigkeit zur Erarbeitung des Rechtsrahmens für KI-Anwendung und deren besonders regulierungsbedürftigen Aspekte behandelt.

Darauf aufbauend wird im zweiten Kapitel dargestellt, welche Rechtsvorschriften und Initiativen zur Regulierung der KI zurzeit in der EU bestehen. Bei der vorliegenden Untersuchung kommen insb. folgende Rechtsaspekte des KI-Einsatzes in der Geschäftstätigkeit verschiedener Unternehmen in Betracht: Anpassung des Binnenmarkts in der EU, Schutz der grundlegenden Menschenrechte (insb. Schutz der personenbezogenen Daten und der Privatsphäre, Verhütung der Diskriminierung), Haftung für KI-Schaden, Produktsicherheit und Marktaufsicht. Die relevanten Initiativen und bestehender Rechtsrahmen in den USA in Bezug auf KI-Regulierung unter Einbeziehung der oben genannten Rechtsaspekte werden im dritten Kapitel dieser Master Thesis behandelt.

Zum Schluss im vierten Kapitel erfolgt der abschließende vergleichende Überblick der bestehenden Vorschriften bzw. Initiativen zur Schaffung des Rechtsrahmens für die KI-Anwendung in der Geschäftstätigkeit in der EU und den USA, sowie deren Vorteile und Nachteile bzw. Lücken festgestellt und wird die abschließende Zusammenfassung dargelegt. Als Ergebnis der durchgeführten Untersuchung werden eigene Empfehlungen zur Verbesserung der untersuchten Initiativen und Regelungen dargestellt.

Kapitel 1: Rechtliche Gesichtspunkte der KI in der Geschäftstätigkeit

1.1. Definition der KI

Vor der Untersuchung des bestehenden Rechtsrahmens für KI in der Geschäftstätigkeit von Unternehmen ist zunächst dieser Begriff in Hinblick auf die Technikeigenschaften der KI-Systeme und die Praxis der internationalen Organisationen zu definieren. Allerdings gibt es noch keine weithin akzeptierte Definition von KI auch unter Experten auf diesem Gebiet.⁵ In der Definierung dieses Begriffs besteht auch keine Einstimmigkeit unter den Staaten und internationalen Organisationen. Das Fehlen eines klar definierten Anwendungsbereichs würde die Industriebranchen unsicher machen, ob ihre Aktivitäten der Regulierung unterliegen, und die Definition von KI den Gerichten überlassen.⁶ Für die Zwecke der weiteren Analyse werden grundsätzlich die bestehenden technischen und juristischen Definitionen erörtert, sowie die grundlegenden Subbereiche bzw. Technologieart der KI kurz dargestellt.

1.1.1. Technische Definition und wesentliche Technikeigenschaften der KI

Das Oxford Wörterbuch definiert KI als „*die Theorie und die Entwicklung von Computersystemen, die Aufgaben ausführen können, die normalerweise menschliche Intelligenz erfordern, wie visuelle Wahrnehmung, Spracherkennung, Entscheidungsfindung und Übersetzung zwischen Sprachen*“.⁷ Dieser Definition kann man hauptsächlich entnehmen, dass KI gut geeignet ist, die für den Menschen kennzeichnenden Denken bzw. Tätigkeit zu übernehmen.

Aus technischer Sicht unterscheidet man grundsätzlich allgemeine (oder auch starke) und angewandte (oder auch schwache) KI. Ein allgemeines (starkes) KI-System soll imstande sein, die meisten Aufgaben zu erfüllen, zu denen auch der Mensch in der Lage ist.⁸ Die angewandte (schwache) KI ist umgekehrt gut geeignet, einzelne Anwendungsprobleme zu lösen, wobei die

⁵ vgl. Miriam C Buiten, ‘Towards Intelligent Regulation of Artificial Intelligence’ (2019) 10(1) European Journal of Risk Regulation, abrufbar unter <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/towards-intelligent-regulation-of-artificial-intelligence/AF1AD1940B70DB88D2B24202EE933F1B/core-reader>, letzter Zugriff am 30.04.2020

⁶ Ebenda

⁷ The Oxford English Dictionary, Definition of “artificial intelligence” (*Lexico*), abrufbar unter https://en.oxforddictionaries.com/definition/artificial_intelligence, letzter Zugriff am 01.05.2020

⁸ vgl. Hochrangige Expertengruppe für künstliche Intelligenz, Eine Definition der KI: Wichtigste Fähigkeiten und Wissenschaftsgebiete (April 2019), abrufbar unter https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60664, letzter Zugriff am 01.05.2020, S. 5

KI-Systeme zur Selbstoptimierung bzw. zum Lernen fähig sind. Außerdem versuchen die KI-Systeme menschliche Intelligenz zu simulieren.⁹ Bei der Mehrheit der gegenwärtig angewandten KI-Systeme handelt es sich um die schwache KI¹⁰, z.B.: Texten- und Sprachverarbeitung, automatisierte Fahrzeuge usw.

Laut Ansicht der Europäischen Kommission können die KI-basierte Systeme rein softwaregestützt in einer virtuellen Umgebung ihre Aufgaben erfüllen (z. B. Suchmaschinen, Sprachassistenten, Gesichts- und Spracherkennungssysteme), aber auch in jeweiligen Hardware-Systemen eingebettet sein (z.B. moderne Roboter, automatisierte Fahrzeuge, Drohnen oder Anwendungen aus IoT).¹¹

In Hinblick auf die Untersuchung der praktischen Anwendung und deren Rechtsrahmens ist es auch von Bedeutung, verschiedene KI-Technologien abzugrenzen. Alle Unterfelder sind je nach den Arten der anzuwenden bzw. zugrunde legenden Technologien zu unterscheiden. Unten sind folgende größte Unterfelder mit kurzer Beschreibung angeführt:

- **Maschinelles Lernen (Machine Learning)** bedeutet, Algorithmen so zu programmieren, „dass sie auf der Grundlage eines Datensatzes bestimmte Muster ableiten können, um zu ermitteln, welche Handlungsschritte zur Erreichung eines bestimmten Ziels erforderlich sind“. ¹² Anwendungsbereich des maschinellen Lernens umfassen typischerweise das Zuführen (relativ) automatisierter Programme mit einem großen Datensatz von Eingaben und das Lösen von Problemen bzw. das Identifizieren von Problemen unter Verwendung ergebnisorientierter Entscheidungen basierend auf dem Datensatz,¹³
- **Tiefes Lernen (Deep Learning)** ist eine Unterart neuronaler Netze. Es umfasst bestimmte Arten von neuronalen Netzen, die mit sehr „rohen“ Eingabedaten arbeiten und die Daten durch viele Schichten nichtlinearer Transformationen verarbeiten, um

⁹ Was ist künstliche Intelligenz? (Retresco), abrufbar unter <https://www.retresco.de/lexikon/kuenstliche-intelligenz/#was-ist-k%C3%BCnstliche-intelligenz>, letzter Zugriff am 01.05.2020

¹⁰ vgl. Hochrangige Expertengruppe für künstliche Intelligenz, Eine Definition der KI: Wichtigste Fähigkeiten und Wissenschaftsgebiete (April 2019), abrufbar unter https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60664, letzter Zugriff am 01.05.2020, S. 5

¹¹ vgl. Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Künstliche Intelligenz für Europa“ COM (2018) 237 endgültig, abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52018DC0237&from=DE>, letzter Zugriff am 20.04.2020 S. 1

¹² COM (2020) 65 endgültig, S. 20

¹³ Rachel Wilka, Rachel Landy, Scott A. McKinney, 'How Machines Learn: Where Do Companies Get Data for Machine Learning and What Licenses Do They Need?' (2018) 13(3) Washington Journal of Law, Technology & Arts, abrufbar unter <https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=1274&context=wjlta>, letzter Zugriff am 01.05.2020, S. 5

eine Zielausgabe zu erreichen.¹⁴ Künstliche neuronale Netze sind nach der Vorlage der biologischen Netze aufgebaut, aus denen das Gehirn von Menschen bzw. Tieren besteht. Der Hauptunterschied zwischen maschinellern Lernen und tiefem Lernen ergibt sich allerdings aus der Art und Weise, wie Daten in einem System dargestellt sind. Algorithmen für maschinelles Lernen erfordern fast immer strukturierte Daten, während Netzwerke beim tiefen Lernen auf Schichten der künstlichen neuronalen Netze gestützt sind;

- **Roboter** stellt ein physisches System dar, das KI verwendet. Dieses Wort wird häufig verwendet, um jede Art der Automatisierung eines Prozesses durch eine jeweilige Maschine zu beschreiben, wobei ein derartiges System KI für Ausführung einer Ausgabe braucht.¹⁵ Man unterscheidet je nach Anwendungszweck verschiedene Arten der Roboter (z.B. Industrieroboter, die in verschiedenen Branchen der Industrie Anwendung finden)¹⁶;
- **Expertensysteme (wissensbasierte Systeme)** stellt ein Computersystem dar, das den Entscheidungsprozess eines menschlichen Experten simuliert. Sie „können als Vermittler zwischen menschlichen Experten angesehen werden, die im Wissenserwerbsmodus mit den Systemen interagieren, und menschlichen Benutzern, die im Konsultationsmodus mit den Systemen interagieren“¹⁷;
- **Computerlinguistik (Natural Language Processing)** bezeichnet Algorithmen, die Eingaben in die menschliche Sprache verarbeiten und in verständliche Darstellungen umwandeln.¹⁸

1.1.2. Definitionsversuche durch die internationalen Organisationen

Die internationalen Organisationen sind bei der Ausarbeitung der legalen Definitionen der KI für künftigen Rechtsrahmen überaus aktiv. Bis jetzt gibt es auch einige Versuche zur Ausarbeitung des offiziellen Begriffes in der EU für die zukünftige Gesetzgebungstätigkeit. Die

¹⁴ Future of Privacy Forum, *The Privacy Expert's Guide to Artificial Intelligence and Machine Learning* (2018), abrufbar unter https://fpf.org/wp-content/uploads/2018/10/FPF_Artificial-Intelligence_Digital.pdf, letzter Zugriff am 30.05.2020, S. 20

¹⁵ vgl. Jacob Turner, *Robot Rules: Regulating Artificial Intelligence* (Fountain Court Chamber: London 2019), S. 16

¹⁶ vgl. Martin Schnetter, *Robotik und ihre Regulierung: Tendenzen in Technik, Recht und Ethik* (Berliner Wissenschafts-Verlag 2016), S. 22-23

¹⁷ Avron Barr, Edward A. Feigenbaum, *The Handbook of Artificial Intelligence: Volume 1*, (Butterworth-Heinemann 1981), S. 9

¹⁸ PwC, *Sizing the prize: What's the real value of AI for your business and how can you capitalise?* (2017), abrufbar unter <https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf>, letzter Zugriff: 25.03.2020, S. 26

Europäische Kommission hat den Begriff der KI in ihrer Mitteilung „Künstliche Intelligenz für Europa“ folgendermaßen definiert:

„KI bezeichnet Systeme mit einem „intelligenten“ Verhalten, die ihre Umgebung analysieren und mit einem gewissen Grad an Autonomie handeln, um bestimmte Ziele zu erreichen. KI-basierte Systeme können rein softwaregestützt in einer virtuellen Umgebung arbeiten (z.B. Sprachassistenten, Bildanalysesoftware, Suchmaschinen, Sprach- und Gesichtserkennungssysteme), aber auch in Hardware-Systeme eingebettet sein (z.B. moderne Roboter, autonome Pkw, Drohnen oder Anwendungen des „Internet der Dinge“).“¹⁹

Im Juni 2018 setzte die Europäische Kommission die Hochrangige Expertengruppe für künstliche Intelligenz (in folgendem als „AI HGL“ genannt) aus 52 Mitglieder ein, darunter Vertretern der Wissenschaft, der Zivilgesellschaft und der Industrie. Die AI HGL hat in ihrem Dokument „Eine Definition der KI: Wichtigste Fähigkeiten und Wissenschaftsgebiete“ eine von der Europäischen Kommission angegebene Definition der KI etwas erweitert. Das Ziel solcher Neufassung der Definition besteht in der Vorbeugung der *„Missverständnisse und Schaffung einer gemeinsamen Wissensbasis über KI, die auch von Nichtfachleuten sinnvoll genutzt werden kann“*.²⁰ Die neue Definition dient auch der Ausarbeitung und Vereinheitlichung der weiteren Vorschriften zur Regulierung der KI und lautet wie folgt:

„Systeme der KI sind vom Menschen entwickelte Softwaresysteme (und ggf. auch Hardwaresysteme), die in Bezug auf ein komplexes Ziel auf physischer oder digitaler Ebene handeln, indem sie ihre Umgebung durch Datenerfassung wahrnehmen, die gesammelten strukturierten oder unstrukturierten Daten interpretieren, Schlussfolgerungen daraus ziehen oder die aus diesen Daten abgeleiteten Informationen verarbeiten, und über das bestmögliche Handeln zur Erreichung des vorgegebenen Ziels entscheiden. KI-Systeme können entweder symbolische Regeln verwenden oder ein numerisches Modell erlernen, und sind auch in der Lage, die Auswirkungen ihrer früheren Handlungen auf die Umgebung zu analysieren und ihr Verhalten entsprechend anzupassen.“²¹

Rat der OECD führte in seinem Dokument „Recommendation of the Council on OECD Legal Instruments Artificial Intelligence“ folgende Definition der KI an:

¹⁹ COM (2018) 237 endgültig, S. 1.

²⁰ Hochrangige Expertengruppe für künstliche Intelligenz, Eine Definition der KI: Wichtigste Fähigkeiten und Wissenschaftsgebiete (April 2019), abrufbar unter https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60664, letzter Zugriff am 01.05.2020, S. 1

²¹ Ebenda, S. 6

„Artificial Intelligence (AI) is a general-purpose technology that has the potential to improve the welfare and well-being of people, to contribute to positive sustainable global economic activity, to increase innovation and productivity, and to help respond to key global challenges. It is deployed in many sectors ranging from production, finance and transport to healthcare and security“²²

Außerdem kann man dem Text dieses Dokumentes weitere Definition der KI-Systeme entnehmen:

„An AI system is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy“²³

Zusammenfassend kann man sagen, dass es zurzeit gar keine einheitliche rechtliche Definition der KI gibt, die von der EU und von anderen internationalen Organisationen als geeignet anerkannt wird. Aufgrund der oben angeführten Definitionsversuche ist KI als eine spezifische Technologie zu betrachten, die geeignet ist, selbstständig Funktionen auszuführen bzw. Probleme zu lösen, von denen sonst angenommen wird, dass sie menschliche Intelligenz erfordern. Ein Fehlen der klar festgestellten juristischen Definition kann im Weiteren die Ausarbeitung des einheitlichen Rechtsrahmens für KI erschweren.

Den oben angeführten Definitionen der KI ist zu entnehmen, dass die wesentlichsten Merkmale der KI-Technologien sind: 1) Autonomie – KI-Systeme benötigen das menschliche Eingreifen grundsätzlich nur bei ihrer Ausarbeitung, sonst können sie ohne Menschen ihre Aufgaben ausführen; 2) Opazität – KI-Systeme können selbst ihre Leistung aus der bisherigen Erfahrung verbessern; 3) Komplexität – bei den KI-Systemen handelt es sich normalerweise um eine große Anzahl von Bestandteilen und betroffenen Personen; 4) Datenabhängigkeit – Funktionsweise der KI-Technologien berührt sich normalerweise auf der Verarbeitung der großen Datenumfänge, insb. bei maschinellem Lernen.

1.2. Anwendung der KI in der Geschäftstätigkeit von Unternehmen

KI ist in der Geschäftstätigkeit von Unternehmen bereits weit verbreitet. Sie gibt den Unternehmen die Möglichkeit, ihre Geschäftsprozesse intelligenter, sparsamer und schneller zu

²² OECD, Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449), abrufbar unter <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>, letzter Zugriff am 15.04.2020

²³ Ebenda, Punkt 1, Abs. 1

gestalten. Nach der Studie von PwC „Künstliche Intelligenz als Innovationsbeschleuniger im Unternehmen“ glauben 72 Prozent der befragten Geschäftsführer in Deutschland, dass KI der ausschlaggebende Geschäftsvorteil der Zukunft sein wird.²⁴

In Bezug auf die Anwendung der KI in der Geschäftstätigkeit kommen in erster Linie folgende Fälle bzw. Anwendungsbereiche in Betracht:

a. Geschäftsprozessoptimierung und -automatisierung

In der Geschäftstätigkeit jedes Unternehmens gibt es solche alltäglichen Aufgaben bzw. Probleme, deren Lösung immer viel Zeit in Anspruch nimmt und die Betätigung der Menschen nicht benötigt bzw. nur in geringerem Ausmaß fordert. Gefährliche Tätigkeiten, die einen unmittelbaren Einfluss auf die Gesundheit des Menschen ausüben, werden auch von Robotern übernommen. Solche Aufgaben wie das Schweißen oder Lackieren lassen sich auch automatisieren.²⁵ Automatisierte Fahrzeuge sind auch ein Beispiel für die Anwendung der KI-Systeme in dem gegenwärtigen Alltag;

b. Automatisierung der Entscheidungsfindungsprozesse

Profiling und automatisierte Entscheidungen dienen grundsätzlich der besseren Vermarktung von Dienstleistungen und Produkten auf individuelle Bedürfnisse, wobei die Steigerung der Effizienz und Einsparung von Vermögen ermöglicht werden können, sowie der Erleichterung der Entscheidungsfindungsprozesse in großen Unternehmen. Das Finanz- und Versicherungswesen sowie die Marketing- und Werbebranche sind nur wenige Bereiche dar, in denen Profiling zur Unterstützung der Entscheidungsfindung angewandt wird.²⁶ Automatisierte Entscheidung können das Unternehmen z.B. bei der Feststellung von individuellen Preisen während der Berechnung der Angebote, sowie bei Begründung oder Kündigung eines Arbeitsverhältnisses unterstützen;

²⁴ PwC, *Künstliche Intelligenz als Innovationsbeschleuniger im Unternehmen: Zuversicht und Vertrauen in Künstliche Intelligenz* (2018), abrufbar unter <https://www.pwc.de/de/digitale-transformation/ki-als-innovationsbeschleuniger-in-unternehmen-whitepaper.pdf>, letzter Zugriff am 20.04.2020, S. 5

²⁵ Milad Safar, Einfach erklärt: Was ist Künstliche Intelligenz? (Weissenberg Solutions), abrufbar unter <https://weissenberg-solutions.de/was-ist-kuenstliche-intelligenz/>, letzter Zugriff am 20.04.2020

²⁶ Artikel-29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679 WP251rev.01, abrufbar unter <https://www.dsb.gv.at/dam/jcr:768b9c7f-f0f6-45d7-b2aa-d113d121ea69/Leitlinien%20zu%20automatisierten%20Entscheidungen%20im%20Einzelfall%20einschlie%C3%9Flich%20Profiling%20f%C3%BCr%20die%20Zwecke%20der%20Verordnung%202016-679.pdf>, letzter Zugriff am 21.12.2020, S. 5

c. Sprach- und Textverarbeitung

Außerdem erfüllen die KI-Technologien die folgenden Aufgaben: Recherche von Informationen in großen Datenmengen, automatische Übersetzung, Korrektur von Rechtschreibfehlern, Prüfung auf grammatische Richtigkeit bzw. Feststellung grammatischer Fehler, Erkennung und Generierung der natürlichen Sprache usw.;

d. Personalisierte Werbung und Marketingnachrichten

KI und insb. Technologie von Profiling ermöglichen die Verarbeitung des großen Umfanges der personenbezogenen Daten zur Erstellung der personalisierten Werbungen, die sich an Zielgruppen der potenziellen Verbraucher mit bestimmten Merkmalen richtet, aufgrund der Eigenschaften des Produkts bzw. der Dienstleistung oder der Person, an die solche Werbung gerichtet ist. Solche Merkmale sind sehr divers und können wie folgt sein: rassische oder ethnische Herkunft, Alter, Geschlecht, Einkommensniveau, persönliche bzw. fachliche Interesse, Gesundheitszustand, Familienstand, Ausbildungsniveau, alltägliche Gewohnheiten, politische Einstellung usw.;

e. Kundenberatung per Telefon und Chatbots

Unter Bezeichnung *Chatbot* versteht man „*ein technisches Dialogsystem, mit dem per Texteingabe oder Sprache kommuniziert werden kann*“.²⁷ Sie kommen zur Anwendung, um die große Menge der Anfragen der Kunden ohne den direkten Angriff des Mitarbeiters zu beantworten bzw. bearbeiten.

1.3. KI und Regulierung

Der ethische Rahmen und die rechtliche Regulierung für KI in der Wirtschaft, sowie im alltäglichen Leben ist heutzutage ein aufkommendes Problem in vielen Ländern weltweit, insb. in der EU. Die Europäische Kommission vertritt in ihrem „Koordiniertem Plan für KI“ die Ansicht, dass „*ein Rechtsrahmen für die weitere Entwicklung der KI erforderlich ist, der ausreichend flexibel ist, um Innovation zu fördern, und gleichzeitig ein hohes Maß an Schutz und Sicherheit gewährleistet wird*“.²⁸

²⁷ Stefan Luber, Nico Litzel, Was ist ein Chatbot? (*Bigdata Insider*, 28. Februar 2018), abrufbar unter <https://www.bigdata-insider.de/was-ist-ein-chatbot-a-690591/>, letzter Zugriff am 30.04.2020

²⁸ Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Koordinierter Plan für künstliche Intelligenz“ COM (2018) 795 endgültig, abrufbar unter <https://eur->

In erster Linie muss man der Inhalt des Begriffs „Regulierung“ untersuchen. Regulierung wird von Philip Selznick und Julia Black als „*die absichtliche Nutzung von Autorität, um das Verhalten einer anderen Partei gemäß festgelegten Standards zu beeinflussen, einschließlich Instrumenten zur Informationserfassung und Verhaltensänderung*“²⁹ definiert. Wenn man über die Regulierung der KI spricht, sollte beachtet werden, dass KI solche Funktionen ausführen kann, von denen sonst angenommen wird, dass sie menschliche Intelligenz erfordern. Diese Eigenschaft der KI-Technologie macht ihre Vorgänge für den Benutzer oder eine andere interessierte Person nicht immer nachvollziehbar, sowie führt zu den unvorhersehbaren Folgen ihrer Anwendung, was auch als sog. Black-Box-Effekt der KI genannt.³⁰

Neue Technologien geben häufig Anlass zu Sorge und Fragen bezüglich der Folgen ihres Einsatzes. Wie bereits erwähnt, können zahlreiche Wege zur KI-Anwendung dem Unternehmen und der Wirtschaft des gesamten Landes zugutekommen. Gleichzeitig können sie einem Menschen zahlreiche Schäden verursachen. Diese Schäden können sowohl materiell (wie Verlust von Menschenleben, Sachschäden usw.) als auch immateriell (wie Beeinträchtigung der Privatsphäre, Einschränkung freier Meinungsäußerung, Verachtung der Menschenwürde und Diskriminierung z.B. beim Zugang zu Beschäftigung und zu Produkten und Dienstleistungen usw.) sein und sich in einer Vielzahl von Risiken resultieren.³¹

Nach der Ansicht der Europäischen Kommission sollte der neue Rechtsrahmen für KI „*zielführend und nicht übermäßig präskriptiv*“ sein.³² Der Gesetzgeber muss jedenfalls beachten, dass Anwendung der KI nicht nur Risiken für menschliches Leben, Gesundheit, Menschenrechte mitbringt, sondern auch beim Vorliegen der wirksamen gesetzlichen Garantien bzw. Rechtsbehelfe durch Wertschöpfungspotenziale auch der gesamten Gesellschaft zugutekommt.³³

[lex.europa.eu/resource.html?uri=cellar:22ee84bb-fa04-11e8-a96d-01aa75ed71a1.0003.02/DOC_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:22ee84bb-fa04-11e8-a96d-01aa75ed71a1.0003.02/DOC_1&format=PDF), letzter Zugriff am 15.04.2020, S. 9

²⁹ Roger Brownsword, Eloise Scotford, Karen Yeung, *The Oxford Handbook of Law, Regulation and Technology* (Oxford University Press, Auflage:1 2017), S. 6

³⁰ vgl. Miriam C Buiten, ‘Towards Intelligent Regulation of Artificial Intelligence’ (2019) 10(1) European Journal of Risk Regulation, abrufbar unter <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/towards-intelligent-regulation-of-artificial-intelligence/AF1AD1940B70DB88D2B24202EE933F1B/core-reader>, letzter Zugriff am 30.04.2020

³¹ vgl. COM (2020) 65 endgültig, S. 12

³² Ebenba, S. 20

³³ vgl. Mario Martini, *Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz* (Springer-Verlag 2019), S. 109-110

Zur Erreichung dieser Zielsetzung soll sog. ein risikobasierter Ansatz angewandt werden. Daher sollte das regulatorische Eingreifen zu den bestehenden Risiken aus der KI-Anwendung verhältnismäßig sein, um die nicht gerechtfertigten Hemmnisse für eine unternehmerische Tätigkeit nicht zu schaffen und dadurch unternehmerische Freiheit nicht zu beeinträchtigen. Die Regulierungsbehörden müssen die „Black Box“ der KI öffnen und sich fragen, welche Aspekte der KI-Technologie die Risiken mitbringen und woher diese Risiken stammen.³⁴ In diesem Kapitel wird es weiter erläutert, welche Risiken für den Menschen bei der Anwendung der KI-Systeme in der Geschäftstätigkeit des Unternehmens entstehen können.

Andererseits verfügen die meisten bestehenden Rechtsordnungen bereits über die Vorschriften, die gut geeignet sind, die Herausforderungen der neuen digitalen Technologien, insbesondere Herausforderung der KI zu meistern. Darunter sind insbesondere folgende Beispiele zu listen: Produkthaftungsvorschriften und DSGVO³⁵ in der EU, Vorschriften über Gefährdungshaftung für gefährliche Technologien in den nationalen Rechtsordnungen usw. Allerdings muss man in jedem einzelnen Fall betrachten, ob eine spezifische Norm gut geeignet ist, alle technische Eigenschaften der KI-Technologie zu berücksichtigen und die entsprechenden Risiken zu mindern bzw. vollständig zu verhüten (sog. „case-by-case approach“).

In Ermangelung angemessener gesetzlicher Vorschriften zur Regulierung der KI kann die sogenannte Selbstregulierung eine geeignete Alternative zur Minderung der Risiken werden, wenn die Regeln ohne Beteiligung von den staatlichen Behörden zu erstellen sind. Dies hat mit Verhaltenskodizes zu tun, die von Handelsgruppen genehmigt wurden, praktisch solchen, die von Verbänden entwickelt wurden, deren Statuten die Mitglieder zur Einhaltung verpflichten.³⁶ Die auf solche Weise ausgearbeiteten Regeln können gut geeignet sein, Unternehmen in einer bestimmten Branche zu verpflichten, technische Standards für Produktsicherheit und Verarbeitung personenbezogener Daten einzuhalten. Aber was Fragen der Deliktshaftung angeht, können derartige Regeln kaum angewandt werden, weil der Vollzug der Ansprüche auf den Schadenersatz in erster Linie auf das Vorliegen der gesetzlichen Vorschriften ankommt (insb. im Strafrecht). Vor diesem Hintergrund kann die sogenannte Selbstregulierung die

³⁴ vgl. Miriam C Buiten, ‘Towards Intelligent Regulation of Artificial Intelligence’ (2019) 10(1) European Journal of Risk Regulation, abrufbar unter <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/towards-intelligent-regulation-of-artificial-intelligence/AF1AD1940B70DB88D2B24202EE933F1B/core-reader>, letzter Zugriff am 30.04.2020

³⁵ s. Art. 22 DSGVO

³⁶ Wolfgang Hoffmann-Riem, *Artificial Intelligence as a Challenge for Law and Regulation*, Regulating Artificial Intelligence (Springer International Publishing 2020), S. 20

gesetzlichen Vorschriften bei der Verhütung bzw. Minimierung der Risiken aus der KI-Anwendung für das Leben und Gesundheit des Menschen kaum ersetzen.

Erster Schritt im Aufbau des Rechtsrahmens für KI-Systeme ist eine Ausarbeitung der ethischen Leitlinien. Solche ethischen Leitlinien sollten alle wesentlichen technischen Eigenschaften der KI-Technologie berücksichtigen, sowie Basis für künftige Rechtsvorschriften bzw. eine Anpassung der geeigneten bestehenden Gesetzbestimmungen darstellen. Sie dienen einer Systematisierung der Rechtsvorschriften und der Vermeidung der Fehler bei deren Ausarbeitung.

Zusammenfassend kann gesagt werden, dass KI-Anwendung in der modernen Wirtschaft tatsächlich der wirksamen Regulierung bedarf, die alle wesentlichen technischen Eigenschaften dieser Technologien und deren Risiken berücksichtigt. Die Regulierung der KI-Anwendung ist aber inwiefern zulässig, wenn die Menschenrechte und Sicherheit des Menschen dadurch gefährdet sind.

1.4. Rechtliche Herausforderungen der KI-Anwendung in der Geschäftstätigkeit

In Bezug auf die Ermöglichung des vollständigen Einsatzes der KI und die Minderung bestehenden Risiken deren Anwendung in der Geschäftstätigkeit sind folgende Bereiche bzw. Aspekte der Geschäftstätigkeit besonders regulierungsbedürftig:

- a. Anpassung des EU-Binnenmarktrechts zur Ermöglichung des freien grenzüberschreitenden Verkehrs der KI-Waren und Dienstleistungen

Ein Kernstück des EU-Binnenmarkts ist der freie Verkehr von Waren, Personen, Dienstleistungen und Kapital. Unterschiedliche Systeme von Zertifizierung und Tests, Produktsicherheitsvorschriften in Bezug auf die KI-Waren, sowie unterschiedliche Systeme der beruflichen Aus- und Weiterbildung in verschiedenen Mitgliedstaaten machen die Erfüllung solcher Zielsetzung unmöglich. In seiner EntschlieÙung vom 12. Februar 2019 zur umfassenden europäischen Industriepolitik in Bezug auf künstliche Intelligenz und Robotik hebt das Europäische Parlament hervor, „*wie wichtig der Grundsatz der gegenseitigen Anerkennung bei der grenzüberschreitenden Nutzung intelligenter Waren, darunter Roboter und Robotersysteme*“, ist.³⁷ In diesem Zusammenhang muss man die

³⁷ EntschlieÙung des Europäischen Parlaments vom 12. Februar 2019 zur umfassenden europäischen Industriepolitik in Bezug auf künstliche Intelligenz und Robotik (2018/2088(INI)), Punkt 118

bestehenden Initiativen der EU zur Harmonisierung der nationalen Rechtsvorschriften über die Normung der sog. KI-Waren, sowie die Feststellung der Qualifikation zur Erbringung der sog. KI-gestützten Dienstleistungen auf EU-Ebene untersuchen.

- b. Schutz der grundlegenden Menschenrechte, inkl. der personenbezogenen Daten und der Privatsphäre, sowie Nichtdiskriminierung bei der Datenverarbeitung durch KI-Systeme sowie bei der Anwendung der ADM-Systeme

Nach der Auffassung der Europäischen Kommission „werden die Menschen zunehmend von Maßnahmen und Entscheidungen betroffen, die von oder mithilfe von KI-Systemen gefällt werden und zuweilen schwer nachvollziehbar sind oder kaum wirksam angefochten werden könnten“.³⁸ Durch Profiling können die großen Unternehmen unter anderem die alltäglichen Gewohnheiten der Nutzer analysieren, wobei der Schutz der personenbezogenen Daten und des Privatlebens gefährdet wird. Nach der Auffassung der Europäischen Datenschutzexperten können „sich auch bestehende Klischeevorstellungen verfestigen und die soziale Kluft zunehmen“. Außerdem können Personen auf eine bestimmte Kategorie festgelegt und auf ihre vorgeschlagenen Präferenzen beschränkt werden.³⁹ Außerdem bei der Bearbeitung der Bewerbungen durch die ADM-Systeme können die Bewerber (insbesondere mit der Behinderung) nicht gerechtfertigt diskriminiert werden.

- c. Haftungsmodelle für KI

Die Menschen sind geeignet, die Fehler fahrlässig bzw. vorsätzlich zu machen, die gravierenden Schäden für Leben und Gesundheit der Menschen nach sich ziehen. Aber es kommt eben manchmal beim Einsatz der Algorithmen bzw. Roboter in der Industrie und im Alltag vor. Die absolute Mehrheit der modernen Rechtsordnungen verfügt über geeignete Rechtsvorschriften zur Haftung für die durch das menschliche Tun bzw. Unterlassung verursachten Schaden. Beim Einsatz der komplexen KI-Systeme ist es aber

³⁸ COM (2020) 65 endgültig, S. 13

³⁹ Artikel-29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679 WP251rev.01, abrufbar unter <https://www.dsb.gv.at/dam/jcr:768b9c7f-f0f6-45d7-b2aa-d113d121ea69/Leitlinien%20zu%20automatisierten%20Entscheidungen%20im%20Einzelfall%20einschlie%C3%9Flich%20Profiling%20f%C3%BCr%20die%20Zwecke%20der%20Verordnung%202016-679.pdf>, letzter Zugriff am 21.12.2020, S. 6.

schwierig festzustellen, wer für die dadurch verursachten Schaden haften muss – ggf. Betreiber bzw. Hersteller des KI-Systems.

d. Produktsicherheitsvorschriften und Marktaufsicht in Bezug auf die Produkte unter Einbeziehung der KI

Zur Förderung der vollständigen Entwicklung und Einsatzes von KI in der Gesellschaft und Unternehmen muss man das Vertrauen der Verbraucher in Bezug auf die Qualität und Sicherheit der KI-Waren und Dienstleistungen wahren. Die Verbraucher sollen über die Funktionsweise der KI und deren Gefahren informiert werden, um imstande sein zu können, Schaden für Leben und Gesundheit zu verhüten. In diesem Zusammenhang scheint die staatliche Einmischung in die neuen Technologiegebieten durch Marktaufsicht unvermeidbar zu sein. Jedoch ist die Frage zum Grad solcher Einmischung offen.

Weiterhin in den nächsten Kapiteln werden der bestehende Rechtsrahmen und die Gesetzgebungsinitiativen in der EU und in den USA in Bezug auf die Regulierung der oben angeführten Aspekte bzw. Probleme der KI in der Geschäftstätigkeit der Unternehmen untersucht und abschließend verglichen.

Kapitel 2: Initiativen in der EU

2.1. Überblick der bestehenden Initiativen zur Regulierung der KI in der EU

In einem Zwischenbericht zu digitalem Binnenmarkt stelle die Europäische Kommission eine Notwendigkeit fest, eine Prüfung durchzuführen, „*ob es möglicherweise nötig ist, den gegenwärtigen Rechtsrahmen an neue technische Entwicklungen (z.B. Robotik, künstliche Intelligenz und 3D-Druck) anzupassen*“.⁴⁰ Sie erklärte weiter in Weissbuch „Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen“ von 2020 zu ihren Zielen, „*wissenschaftliche Durchbrüche zu ermöglichen, die Technologieführerschaft der EU zu wahren und sicherzustellen, dass neue Technologien im Dienst aller Europäerinnen und Europäer stehen – sie sollen Verbesserungen im Alltag bewirken, und gleichzeitig die Rechte der Bürgerinnen und Bürger achten*“.⁴¹

Am 25. April 2018 hat die Europäische Kommission in ihrer Mitteilung zum Thema „KI für Europa“⁴² verabschiedet, in der die KI-Initiative der EU dargelegt wird, um die Chancen der KI auszunutzen und die neuen Herausforderungen der KI zu minimisieren bzw. verhindern. Diese KI-Initiative sieht die Durchführung der Maßnahmen vor, die in drei Teilen gegliedert sind⁴³:

- 1) Förderung der technologischen und industriellen Leistungsfähigkeit der EU sowie der weiteren Verbreitung von KI in der gesamten Wirtschaft durch öffentliche und private Investitionen;
- 2) Vorbereitung auf sozioökonomische Veränderungen;
- 3) Gewährleistung eines geeigneten ethischen und rechtlichen Rahmens.

Im Dezember 2018 veröffentlichte AI HGL den Entwurf der Ethik-Leitlinien für eine vertrauenswürdige KI.⁴⁴ Nach weiteren Beratungen von AI HGL in Hinblick auf die

⁴⁰ Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über die Halbzeitüberprüfung der Strategie für einen digitalen Binnenmarkt „Ein vernetzter digitaler Binnenmarkt für alle“ COM (2017) 228 endgültig, abrufbar unter https://eur-lex.europa.eu/resource.html?uri=cellar:a4215207-362b-11e7-a08e-01aa75ed71a1.0003.02/DOC_1&format=PDF, letzter Zugriff am 15.04.2020, S. 14

⁴¹ COM (2020) 65 endgültig, S. 2

⁴² COM (2018) 237 endgültig

⁴³ s. COM (2018) 237 endgültig, S. 7-22

⁴⁴ Hochrangige Expertengruppe für künstliche Intelligenz, Ethik-Leitlinien für eine vertrauenswürdige KI (April 2019), abrufbar unter <https://op.europa.eu/de/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1>, letzter Zugriff am 01.05.2020

Diskussionen über die Europäische KI-Allianz, die Konsultationen der Interessengruppen und die Treffen mit Vertretern der Mitgliedstaaten wurden die Leitlinien in April 2019 überarbeitet und neu veröffentlicht. Diesen Leitlinien kommt kein verbindlicher Charakter zu, daher begründen sie keine rechtlichen Verpflichtungen für Mitgliedstaaten.

Auf Grundlage dieses Dokuments stellte die Europäische Kommission ihren eigenen Ansatz zu den ethischen Aspekten der KI-Anwendung in ihrer Mitteilung „Schaffung von Vertrauen in eine auf den Menschen ausgerichtete künstliche Intelligenz“⁴⁵ dar. Ihrer Auffassung nach ist KI *„kein Selbstzweck, sondern ein Instrument, das den Menschen dienen muss und letztlich das Wohlergehen der Menschen steigern soll“* (menschenzentrierter Ansatz). Das Vertrauen ist eine Grundvoraussetzung für die Verfolgung eines auf den Menschen ausgerichteten Ansatzes für die KI (Vertrauenswürdigkeit der KI).⁴⁶ Das Kernprinzip der EU-Leitlinien besteht darin, dass die EU einen „menschenzentrierten“ Ansatz für KI beibehalten muss, der die europäischen Werte respektiert. Die Kernanforderungen an KI-Anwendungen sind wie folgt:

- Vorrang menschlichen Handelns und menschlicher Aufsicht;
- Technische Robustheit und Sicherheit;
- Privatsphäre und Datenqualitätsmanagement;
- Transparenz;
- Vielfalt, Nichtdiskriminierung und Fairness;
- Gesellschaftliches und ökologisches Wohlergehen;
- Rechenschaftspflicht.⁴⁷

Das Europäische Parlament ist auch an der Ausarbeitung von Rechtsvorschriften für KI beteiligt, indem es am 19. Februar 2019 eine Entschließung zur umfassenden europäischen Industriepolitik in Bezug auf KI und Robotik⁴⁸ verabschiedete. In dieser Entschließung forderte es die Europäische Kommission auf, *„die geltenden Vorschriften mit Blick auf die Förderung eines rechtlichen Umfelds, das für die Entwicklung der KI vorteilhaft und mit dem Grundsatz der besseren Rechtsetzung zu vereinbaren ist, regelmäßig neu zu bewerten, um sicherzustellen,*

⁴⁵ Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Schaffung von Vertrauen in eine auf den Menschen ausgerichtete künstliche Intelligenz“ COM (2019) 168 endgültig, abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52019DC0168&from=DE>, letzter Zugriff am 01.06.2020

⁴⁶ Ebenda, S. 2

⁴⁷ Ebenda, S. 4

⁴⁸ Entschließung des Europäischen Parlaments vom 12. Februar 2019 zur umfassenden europäischen Industriepolitik in Bezug auf künstliche Intelligenz und Robotik (2018/2088(INI))

*dass sie in Bezug auf KI ihren Zweck erfüllt, wobei auch die Grundwerte der EU zu achten sind, sowie neue Vorschläge möglichst zu ändern oder zu ersetzen, wenn dies nachweislich nicht der Fall ist“.*⁴⁹ Außerdem beinhaltet dieses Dokument unter anderem im Abschnitt 4 auch die Hinweise bzw. die Ansätze zur Schaffung des künftigen Rechtsrahmens für KI, insbesondere in Bezug auf die folgenden Aspekte der KI-Anwendung:⁵⁰

- Anpassung des EU-Binnenmarkts in Bezug auf den grenzüberschreitenden Verkehr der sog. intelligenten Waren (Punkt 4.1. „ein Binnenmarkt für KI“);
- Schutz personenbezogener Daten;
- Haftungsfragen;
- Verbraucherschutz und Stärkung der Verbraucher;
- Rechte des geistigen Eigentums (die Einhaltung des horizontalen und technologisch neutralen Ansatzes in Bezug auf die Rechte des geistigen Eigentums für die Produkte und Technologien, bei denen KI zum Einsatz kommt).

Am 19. Februar 2020 wurde Weissbuch „Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen“⁵¹ durch die Europäische Kommission veröffentlicht. In diesem Weissbuch stellte die Europäische Kommission ein Konzept für die EU-Länder dar, wie man einerseits die Vorteile der KI-Anwendung für Wissenschaft, Wirtschaft und Gesellschaft insgesamt nutzbar machen kann und andererseits auch den damit verbunden Herausforderungen meistern kann.

Das Weissbuch enthält auch die Modalitäten des künftigen KI-Regulierungsrahmens, die für die Schaffung des „Ökosystems für Vertrauen“ in Bezug auf den KI-Einsatz notwendig sind⁵², sowie die Ausführungen zur möglichen Anpassung der bestehenden EU-Vorschriften unter Berücksichtigung von KI (grundsätzlich auf dem Gebiet der Produktsicherheit). Nach der Auffassung der Europäischen Kommission sind vor allem die Risiken für die Beeinträchtigung der Grundrechte, die Sicherheit und das wirksame Funktionieren der Haftungsregelung zu berücksichtigen.⁵³

Zusammen mit dem Weissbuch veröffentlichte Europäische Kommission am selben Tag eine Reihe von Begleitdokumenten, darunter einen „Bericht über die Auswirkungen künstlicher

⁴⁹ Ebenda, Punkt 114

⁵⁰ s. 2018/2088(INI), Punkte 114-137

⁵¹ COM (2020) 65 endgültig

⁵² vgl. Ebenda, S. 3

⁵³ vgl. Ebenda, S. 12

Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung“⁵⁴ und „Eine europäische Datenstrategie“⁵⁵. Dieser Bericht enthält die Empfehlungen der Europäischen Kommission zur Anpassung der bestehenden Produktsicherheits- und Produkthaftungsvorschriften der EU unter Berücksichtigung der technischen Eigenschaften bzw. Risiken der KI-Systeme. Diese Dokumente samt Weissbuch sollten als eine Basis für die Ausarbeitung der künftigen Vorschriften zur Regulierung der KI dienen, insb. auf den Gebieten der Produktsicherheit und Produkthaftung. Auf diese Empfehlungen ist es weiter in dieser Master Thesis näher eingegangen.

Eine europäische Datenstrategie stellt politische Maßnahmen vor, die darauf abzielen, eine europäische „Datenwirtschaft“ innerhalb der nächsten fünf Jahre zu schaffen⁵⁶, sowie behandelt relevante Aspekte für die Entfaltung der KI-Technologien in der EU, wie etwa eine Datenverfügbarkeit und Verhinderung einer Fragmentierung der rechtlichen Rahmenbedingungen zwischen den EU-Mitgliedstaaten⁵⁷. Sie ist auf vier sog. Säulen gestützt, die konkrete Vorschläge für Regulierungsmaßnahmen enthalten:⁵⁸

- 1) Ein sektorübergreifender Rahmen für Datenzugang und Datennutzung;
- 2) Investitionen in Daten und Infrastrukturen für das Hosting, die Verarbeitung und die Nutzung von Daten sowie der Interoperabilität;
- 3) Stärkung der Handlungskompetenz des Einzelnen, insbesondere deren Rechte in Bezug auf seine Daten;
- 4) Erstellung gemeinsamer europäischer Datenräume in strategischen Sektoren und Bereichen von öffentlichem Interesse.

Am 20. Oktober 2020 verabschiedete Europäisches Parlament weitere Entschlüsse zu folgenden Themen: Rahmen für die ethischen Aspekte von künstlicher Intelligenz, Robotik und

⁵⁴ Europäische Kommission, Bericht über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung COM (2020) 64 endgültig, abrufbar unter https://ec.europa.eu/info/sites/info/files/report-safety-liability-artificial-intelligence-feb2020_de.pdf, letzter Zugriff am 15.04.2020

⁵⁵ Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Eine europäische Datenstrategie“ COM (2020) 66 endgültig, abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020DC0066&from=DE>, letzter Zugriff am 30.04.2020

⁵⁶ Ebenda, S. 2

⁵⁷ vgl. Ebenda, S. 7

⁵⁸ s. COM (2020) 66 endgültig, S. 14-27

damit zusammenhängenden Technologien⁵⁹, Regelung der zivilrechtlichen Haftung beim Einsatz künstlicher Intelligenz⁶⁰ und Rechte des geistigen Eigentums bei der Entwicklung von KI-Technologien.⁶¹ Erste zwei Entschlüsse fassen die bisherigen Initiativen in Bezug auf die Schaffung der auf den Menschen ausgerichteten KI, risikoorientierten Ansatz, Verhütung der Diskriminierung und die Notwendigkeit der Anpassung der bestehenden Haftungsvorschriften. Allerdings betont das Europäische Parlament in seiner dritten Entschlüsselung, „dass der geltende Rahmen für geistiges Eigentum in Fällen, in denen KI nur als Hilfsmittel zur Unterstützung eines Autors im Schaffensprozess verwendet wird, weiterhin Anwendung findet“.⁶² Nach seiner Auffassung müssen die durch KI-Systeme erzeugte Schöpfungen gemäß dem Rechtsrahmen für Rechte des geistigen Eigentum geschützt werden.⁶³

Zu gleicher Zeit muss man auch beachten, dass die EU schon über die einschlägigen Rechtsvorschriften verfügt, die dazu geeignet sind, die KI-Anwendung in der Wirtschaftstätigkeit zu regulieren und die damit verbunden Herausforderungen zu meistern. Im Mai 2018 wurden die ersten Vorschriften der EU über die Sicherheit von Netzen und Informationssystemen, sowie strengere Regeln von DSGVO für den Schutz personenbezogener Daten verabschiedet.⁶⁴ Daher werden diese bestehenden Rechtsvorschriften neben der Initiativen zur künftigen Gesetzgebung im Rahmen dieser Master Thesis behandelt.

2.2. Initiativen zur Schaffung des Binnenmarktes für KI

Gemäß Art. 26 Abs. 2 AEUV umfasst der Binnenmarkt „einen Raum ohne Binnengrenzen, in dem der freie Verkehr von Waren, Personen, Dienstleistungen und Kapital gemäß den Bestimmungen der Verträge gewährleistet ist“.⁶⁵ In der Mitteilung der Europäischen Kommission „Koordinierter Plan für künstliche Intelligenz“ wurde ferner hervorgehoben, dass ein echter Binnenmarkt mit einer festen digitalen Dimension es den Unternehmen erleichtert,

⁵⁹ Legislative Entschlüsselung des Europäischen Parlaments vom 20. Oktober 2020 mit Empfehlungen an die Kommission zu dem Rahmen für die ethischen Aspekte von künstlicher Intelligenz, Robotik und damit zusammenhängenden Technologien (2020/2012(INL))

⁶⁰ Entschlüsselung des Europäischen Parlaments vom 20. Oktober 2020 mit Empfehlungen an die Kommission für eine Regelung der zivilrechtlichen Haftung beim Einsatz künstlicher Intelligenz (2020/2014(INL))

⁶¹ Entschlüsselung des Europäischen Parlaments vom 20. Oktober 2020 zu den Rechten des geistigen Eigentums bei der Entwicklung von KI-Technologien (2020/2015(INI))

⁶² Ebenda, Punkt 14

⁶³ Ebenda, Punkt 15

⁶⁴ COM (2018) 237 endgültig, S. 18

⁶⁵ Vertrag über die Arbeitsweise der Europäischen Union (konsolidierte Fassung) [2012] ABl L 326/47, Art. 26 Abs. 2

„grenzüberschreitend zu expandieren und Handel zu treiben, und so weitere Impulse für Investitionen geben“.⁶⁶ Die EU ist schon im Besitz einiger Initiativen zur Anpassung dessen Binnenmarktrechts zur Ermöglichung des freien grenzüberschreitenden Verkehrs der Daten, sowie der KI-Produkte bzw. Dienstleistungen.

2015 wurde Strategie für einen digitalen Binnenmarkt⁶⁷ durch Europäische Kommission veröffentlicht. Sie dient grundsätzlich der Erleichterung des Zugangs der Verbraucher zu digitalen Gütern und Dienstleistungen in ganz Europa, sowie stellt rechtliche Bedingungen für Funktionieren digitaler Netze. Dieses Dokument enthält keine expliziten Verweise auf KI. Europäische Kommission beschreibt ihr Konzept des digitalen Binnenmarkts wie folgt:

*„In einem digitalen Binnenmarkt ist der freie Verkehr von Waren, Personen, Dienstleistungen und Kapital gewährleistet und können Privatpersonen und Unternehmen unter fairen Wettbewerbsbedingungen und auf der Grundlage hoher Verbraucher- und Datenschutzstandards ungeachtet ihrer Staatsangehörigkeit bzw. ihres Wohn- oder Geschäftssitzes nahtlos Online-Aktivitäten nachgehen und Internetanwendungen nutzen.“*⁶⁸

Eine vollständige Entwicklung und Funktion der KI-Systeme wie maschinelles Lernen und künstliche neuronale Netzwerke benötigen den großen Umfang der zu verarbeiten Daten. In der obenerwähnten europäischen Datenstrategie der Europäischen Kommission von Februar 2020 ist hervorgehoben, dass ein für die weitere Entwicklung der KI genügendes Ausmaß der Daten in der EU noch nicht verfügbar.⁶⁹ Zur Lösung dieses Problems soll ein Binnenmarkt für den freien Verkehr der Daten eingerichtet werden, wobei europäische Vorschriften und wirksame Durchsetzungsmechanismen gewährleistet werden sollten.⁷⁰ Diese Bestimmungen sollten vor allem dem Schutz personenbezogener Daten und dem Verbraucherschutz dienen.

Allerdings wurde die Konzeption des Binnenmarkts für KI erst durch das Europäische Parlament dargestellt. Wie im vorherigen Abschnitt erwähnt, forderte das Europäische Parlament in seiner Entschließung vom 12. Februar 2019 die Europäische Kommission auf, der schnellen technologischen Entwicklung der KI-Technologien die Rechnung zu tragen, sowie

⁶⁶ COM (2018) 795 endgültig, S. 4.

⁶⁷ Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Strategie für einen digitalen Binnenmarkt für Europa“ COM (2015) 192 endgültig, abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52015DC0192&from=DE>, letzter Zugriff am 20.06.2020

⁶⁸ Ebenda, S. 3

⁶⁹ vgl. COM (2020) 66 endgültig, S. 7

⁷⁰ Ebenda

legte eine Reihe der Anweisungen bzw. Vorschläge zur Schaffung des Binnenmarktes für KI vor, die bei der Anpassung des Unionsrechts zu berücksichtigen sind. Darunter sind folgende zu nennen⁷¹:

- Berücksichtigung der mit KI verbundenen ethischen Aspekte bei der Ausarbeitung der Tests und Zertifizierungen, sowie Produktsicherheitsvorschriften für KI⁷²;
- Auswertung zur Notwendigkeit der Aktualisierung des politischen Rahmens und des Regelungsrahmens in Bezug auf den Einsatz der KI⁷³;
- Schaffung des einheitlichen Regelwerks in allen EU-Ländern für automatisierte Fahrzeuge (z.B. zivile Drohne), „mit dem das richtige Gleichgewicht zwischen den Interessen und potenziellen Gefahren für Nutzer, Unternehmen und andere betroffene Parteien hergestellt und gleichzeitig eine Überregulierung der Robotik- und der KI-Systeme vermieden wird“⁷⁴;
- Modernisierung der Systeme der beruflichen Aus- und Weiterbildung, insbesondere Richtlinie über eine Verhältnismäßigkeitsprüfung⁷⁵, Richtlinie über die Anerkennung von Berufsqualifikationen⁷⁶;
- Schaffung der europaweiten Normung im Bereich der KI in Zusammenarbeit mit den europäischen bzw. internationalen Normungsgremien, insbesondere in der intelligenten Fertigung, bei Robotern, fahrerlosen Fahrzeugen, im Bereich der virtuellen Realität, bei der Gesundheitsversorgung und Datenanalyse⁷⁷;
- Unzulässigkeit der letztendlichen Entscheidung durch KI-Systeme ohne Eingriff des Menschen in solchen Gebieten, wie Medizin, Justiz und Buchhaltung.

Ferner beinhaltet dieses Dokument die Hinweise zur Verabschiedung der Ethik-Charta für KI und Ausarbeitung bzw. Anpassung der Unionsvorschriften auf solchen Gebieten, wie Schutz personenbezogener Daten, Haftungsfragen, Verbraucherschutz (insbesondere

⁷¹ Entschließung des Europäischen Parlaments vom 12. Februar 2019 zur umfassenden europäischen Industriepolitik in Bezug auf künstliche Intelligenz und Robotik (2018/2088(INI)), Punkte 118-124

⁷² vgl. Ebenda, Punkt 118

⁷³ s. Ebenda, Punkt 119

⁷⁴ Ebenda, Punkt 120

⁷⁵ Richtlinie (EU) 2018/958 des Europäischen Parlaments und des Rates vom 28. Juni 2018 über eine Verhältnismäßigkeitsprüfung vor Erlass neuer Berufsreglementierungen [2018] ABl L 173/25

⁷⁶ Richtlinie 2013/55/EU des Europäischen Parlaments und des Rates vom 20. November 2013 zur Änderung der Richtlinie 2005/36/EG über die Anerkennung von Berufsqualifikationen und der Verordnung (EU) Nr. 1024/2012 über die Verwaltungszusammenarbeit mit Hilfe des Binnenmarkt-Informationssystems („IMI-Verordnung“) [2013] ABl L 354/132

⁷⁷ Ebenda, Punkt 122

Produktsicherheit) und Marktüberwachung.⁷⁸ Da sich diese Aspekte in der Praxis sehr vielfältig bzw. komplex aufweisen können und zum Gegenstand der zahlreichen Gesetzgebungsinitiativen in der EU geworden sind, ist es auf sie in folgenden Abschnitten näher einzugehen.

Nach Meinung des Europäischen Parlaments sind die Rechte des geistigen Eigentums auch von Bedeutung für die Entfaltung und Förderung der KI-Technologien in der EU. In seiner Entschließung fordert es ferner die Europäische Kommission auf, *„einen horizontalen und technologisch neutralen Ansatz in Bezug auf die Rechte des geistigen Eigentums zu unterstützen, die auf die verschiedenen Branchen anwendbar sind, in denen die Robotik zum Einsatz kommen könnte“*.⁷⁹

In dem obenerwähnten Weissbuch „Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen“ hob die Europäische Kommission ebenfalls eine Notwendigkeit des einheitlichen europäischen KI-Konzepts hervor, *„um die Fragmentierung des Binnenmarkts zu vermeiden“*.⁸⁰ Dieses Dokument beinhaltet ebenfalls die Hinweise zur Schaffung der obligatorischen Konformitätsbewertungen für KI-Anwendungen mit hohem Risiko, *„die ein Teil der Konformitätsbewertungsmechanismen sein sollte, die es bereits für eine große Zahl von Produkten gibt, die auf dem EU-Binnenmarkt in Verkehr gebracht werden“*.⁸¹

2.3. Initiativen zum Schutz der grundlegenden Menschenrechte

Nach Art. 2 EUV sind die Werte, auf die sich die EU gründet, *„die Achtung der Menschenwürde, Freiheit, Demokratie, Gleichheit, Rechtsstaatlichkeit und die Wahrung der Menschenrechte einschließlich der Rechte der Personen, die Minderheiten angehören“*.⁸² Infolge der KI-Anwendung besteht die Gefahr der Beeinträchtigung dieser Werte und der Menschenrechte. Nach Auffassung der Europäischen Kommission gilt dies für *„das Recht auf freie Meinungsäußerung, die Versammlungsfreiheit, die Achtung der Menschenwürde, die Nichtdiskriminierung ungeachtet des Geschlechts, der Rasse oder der ethnischen Herkunft, der religiösen Überzeugung oder Weltanschauung, einer Behinderung, des Alters oder der sexuellen Ausrichtung, den Schutz personenbezogener Daten und des Privatlebens“*.⁸³

⁷⁸ s. Ebenda, Punkte 138-142

⁷⁹ Ebenda, Punkt 136

⁸⁰ COM (2020) 65 endgültig, S. 3

⁸¹ Ebenda, S. 27

⁸² Vertrag über die Europäische Union (konsolidierte Fassung) [2012] ABL L 326/13, Art. 2

⁸³ COM (2020) 65 endgültig, S. 12

2.3.1. Schutz personenbezogener Daten und des Privatlebens

Das moderne System des Datenschutzes in der EU ist auf Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DSGVO)⁸⁴ gestützt. DSGVO beinhaltet die europaweit einheitlichen Vorschriften, die den Umgang mit den personenbezogenen Daten natürlicher Personen in der ganzen EU regeln.

DSGVO beinhaltet auch unter anderem die Vorschriften, die speziell geeignet sind, die Gefahren für personenbezogene Daten in Hinblick auf KI-Anwendung, wie etwa Profiling und automatisierte Entscheidungen zu behandeln. Daher sind die Initiativen der EU auf dem Gebiet des Datenschutzes bei der KI-Anwendung schon in dem Unionsrecht in Form der geltenden Rechtsvorschriften verankert. Gemäß Art. 22 Abs. 1 DSGVO „*hat die betroffene Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt*“.⁸⁵

Zunächst sind Profiling und ausschließlich automatisierte Entscheidungen unter Einbeziehung der Vorschriften von DSGVO zu definieren. In Art. 4 Abs. 4 DSGVO ist Profiling wie folgt definiert:

*„jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen“*⁸⁶

Profiling wird oft verwendet, um Prognosen über Verhalten der Verbraucher zu treffen, um anhand der Eigenschaften einer Person die Angaben über eine Person und ihre Interessen,

⁸⁴ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) [2016] ABl L 119/1

⁸⁵ Ebenda, Art. 22 Abs. 1

⁸⁶ Ebenda, Art. 4 Abs. 4

Vorlieben bzw. Gewohnheiten abzuleiten.⁸⁷ Ausschließlich automatisierte Entscheidungsfindungen sind auf der Fähigkeit der KI-Systeme (unter anderem auch der ADM-Systeme) gestützt, Entscheidungen ohne direkte Beteiligung einer Person mithilfe technischer Mittel zu treffen.⁸⁸ Die ADM-Systeme ziehen häufig Profiling hinein, allerdings können sie ohne dies funktionieren.

Sowohl Profiling als auch automatisierte Entscheidungen (aber nicht ausschließlich automatisierte) stellen eine Verarbeitung personenbezogener Daten dar und dies eröffnet den Anwendungsbereich der DSGVO in Bezug auf die Verarbeitung solcher personenbezogenen Daten durch KI-Systeme.⁸⁹ Deshalb muss man Definition personenbezogener Daten angeben bzw. erläutern. Unter personenbezogenen Daten muss man iSd DSGVO alle Informationen verstehen, „die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“.⁹⁰ In Fall einer identifizierten Person geht es logischerweise um eine konkrete festgestellte Person, dh. zumindest der Name einer Person ist bekannt. Allerdings ist als identifizierbar eine natürliche Person anzusehen, „die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“.⁹¹

Art. 22 Abs. 2 DSGVO beinhaltet drei Ausnahmefälle, wenn eine solche automatisierte bzw. eine Wirkung entfaltende Entscheidung zulässig ist:

- eine solche Entscheidung ist für den Abschluss oder die Erfüllung eines Vertrages zwischen dem Betroffenen und dem Verantwortlichen erforderlich;

⁸⁷ vgl. Artikel-29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679 WP251rev.01, abrufbar unter <https://www.dsb.gv.at/dam/jcr:768b9c7f-f0f6-45d7-b2aa-d113d121ea69/Leitlinien%20zu%20automatisierten%20Entscheidungen%20im%20Einzelfall%20einschlie%C3%9Flich%20Profiling%20f%C3%BCr%20die%20Zwecke%20der%20Verordnung%202016-679.pdf>, letzter Zugriff am 21.12.2020, S. 7

⁸⁸ Ebenda, S. 8

⁸⁹ vgl. Conrad Sebastian Conrad, ‘Kann die Künstliche Intelligenz den Menschen entschlüsseln? — Neue Forderungen zum Datenschutz’ (2018) 42(9), DuD, 541, abrufbar unter <https://link.springer.com.uaccess.univie.ac.at/content/pdf/10.1007/s11623-018-0996-z.pdf>, letzter Zugriff am 01.06.2020, S. 542-543

⁹⁰ Verordnung (EU) 2016/679, Art. 4 Abs. 1

⁹¹ Ebenda, Art. 4, Abs. 1

- eine Rechtsvorschrift der EU oder des Mitgliedstaates (der Verantwortliche unterliegt) liegt dafür vor, wenn sie angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthält;
- eine betroffene Person hat das ausdrücklich einwilligt.⁹²

Wenn die erste Ausnahme oder die dritte Ausnahme die Anwendung finden, muss der Verantwortliche *„angemessene Maßnahmen treffen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört“*.⁹³

Profiling und automatisierte Entscheidungen als die Arten der Verarbeitung personenbezogener Daten unterliegen den Vorschriften der DSGVO und bedürfen daher mindestens einer der folgenden Rechtsgrundlagen nach Art. 6 Abs. 1 DSGVO⁹⁴, wie:

- a) das Vorliegen einer Einwilligung der betroffenen Person zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke;
- b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
- c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
- d) die Verarbeitung ist für den Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich;
- e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, erforderlich;
- f) die Verarbeitung ist für Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich.⁹⁵

In Art. 5 Abs. 1 DSGVO sind folgende Grundsätze bzw. Prinzipien für die Verarbeitung der personenbezogenen Daten verankert, die auch für Profiling und automatisierte Entscheidungen maßgeblich sind:

⁹² Ebenda, Art. 22 Abs. 2

⁹³ Ebenda, Art. 22 Abs. 3

⁹⁴ vgl. Lukas Feiler, Nikolas Forgó, *EU-DSGVO: EU-Datenschutz-Grundverordnung: Kurzkommentar* (Verlag Österreich 2017), S. 165

⁹⁵ Verordnung (EU) 2016/679, Art. 6 Abs. 1

- Rechtmäßigkeit – die Verarbeitung ist nur beim Vorliegen einer der in Art. 6 Abs. 1 DSGVO verankerten Grundlagen rechtmäßig;
- Verarbeitung nach Treu und Glauben;
- Transparenz – nach Art. 12 Abs. 1 DSGVO trifft der Verantwortliche geeignete Maßnahmen, um der betroffenen Person alle Informationen, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln⁹⁶;
- Zweckbindung – personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;
- Datenminimierung – personenbezogene Daten sind dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt zu werden;
- Richtigkeit – der Verantwortliche hat alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;
- Speicherbegrenzung – Speicherung der personenbezogenen Daten ermöglicht die Identifizierung der betroffenen Personen nur so lange, wie das für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von DSGVO zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke verarbeitet werden;
- Integrität und Vertraulichkeit – Gewährleistung einer angemessenen Sicherheit, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.⁹⁷

Gemäß Art. 9 Abs. 1 DSGVO ist die Verarbeitung der besonderen Kategorien der personenbezogenen Daten untersagt, *„aus denen die rassische und ethnische Herkunft,*

⁹⁶ Ebenda, Art. 12 Abs. 1

⁹⁷ Ebenda, Art. 6 Abs. 1

*politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person“.*⁹⁸ Diese besonderen Kategorien von Daten können auch aus Profiling abgeleitet bzw. hergeleitet werden. Das Funktionieren von ADM-Systemen darf grundsätzlich auf diesen Kategorien der Daten nicht gestützt werden, außer die betroffene Person ihre Einwilligung gab oder die Verarbeitung auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats durchzuführen ist.⁹⁹ In diesem Fall sollte der Verantwortliche sicherstellen, dass:

- die Verarbeitung mit dem ursprünglichen Zweck vereinbar ist;
- eine Rechtsgrundlage für die Verarbeitung der besonderen Datenkategorie (Einwilligung betroffener Person) ermittelt wurde;
- die betroffene Person über die Verarbeitung unterrichtet wird.¹⁰⁰

Gemäß DSGVO trägt der Verantwortliche die zusätzlichen Pflichten in Bezug auf die Verarbeitung der personenbezogenen Daten der Kinder. Artikel 22 DSGVO beinhaltet selbst keine Vorschriften diesbezüglich. In Erwägungsgrund 71 der DSGVO heißt es jedoch, dass Kind nicht von einer automatisierten Entscheidungsfindung und Profiling betroffen sein sollte.¹⁰¹

2.3.2. Verhütung der Diskriminierung

Anderer Aspekt des Menschenrechtsschutzes bei der KI-Anwendung ist Verhütung der Diskriminierung bei der Einbeziehung der KI-Systeme in die automatisierten Entscheidungsprozesse. Gemäß Art. 21 Abs. 1 Charta der Grundrechte der EU ist die Diskriminierung insb. *„wegen des Geschlechts, der Rasse, der Hautfarbe, der ethnischen oder sozialen Herkunft, der genetischen Merkmale, der Sprache, der Religion oder der Weltanschauung, der politischen oder sonstigen Anschauung, der Zugehörigkeit zu einer*

⁹⁸ Ebenda, Art. 9 Abs. 1

⁹⁹ vgl. Ebenda, Art. 22 Abs. 4

¹⁰⁰ Artikel-29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679 WP251rev.01, abrufbar unter <https://www.dsb.gv.at/dam/jcr:768b9c7f-f0f6-45d7-b2aa-d113d121ea69/Leitlinien%20zu%20automatisierten%20Entscheidungen%20im%20Einzelfall%20einschlie%C3%9Flich%20Profiling%20f%C3%BCr%20die%20Zwecke%20der%20Verordnung%202016-679.pdf>, letzter Zugriff am 21.12.2020, S. 17

¹⁰¹ Ebenda, Erwägungsgrund 71

*nationalen Minderheit, des Vermögens, der Geburt, einer Behinderung, des Alters oder der sexuellen Ausrichtung verboten“.*¹⁰²

Grundsätzlich unterscheidet man unmittelbare (auch als „direkt“ genannt) Diskriminierung und mittelbare (auch als „indirekt“ genannt) Diskriminierung, deren Abgrenzung in dem Unionsrecht festgestellt ist. Eine derartige Abgrenzung kann am besten anhand von Richtlinie 2010/41/EG des Europäischen Parlaments und des Rates vom 7. Juli 2010 zur Verwirklichung des Grundsatzes der Gleichbehandlung von Männern und Frauen, die eine selbständige Erwerbstätigkeit ausüben, und zur Aufhebung der Richtlinie 86/613/EWG des Rates dargestellt werden. So spricht man über direkte Diskriminierung, wenn eine Person *„aufgrund ihres Geschlechtes in einer vergleichbaren Situation eine weniger günstige Behandlung als eine andere Person erfährt, erfahren hat oder erfahren würde“* (oder aufgrund jeweiliger sonstigen Merkmale).¹⁰³ Indirekte Diskriminierung ist hingegen *„eine Situation, in der dem Anschein nach neutrale Vorschriften, Kriterien oder Verfahren Personen des einen Geschlechts in besonderer Weise gegenüber Personen des anderen Geschlechts benachteiligen können, es sei denn, die betreffenden Vorschriften, Kriterien oder Verfahren sind durch ein rechtmäßiges Ziel sachlich gerechtfertigt und die Mittel sind zur Erreichung dieses Ziels angemessen und erforderlich“*.¹⁰⁴

Eine Anwendung der ADM-Systeme und sonstiger auf KI gestützten Algorithmen kann in folgenden Bereichen bzw. Aspekten der Geschäftstätigkeit des Unternehmens zur Diskriminierung führen: automatisierte Verarbeitung der Bewerbungen beim Beschäftigungsprozess, Erstellung der Preise für die Leistungen (sog. Preisdiskriminierung), Erstellung der Werbung auf Online-Suchmaschinen, Kundenberatung durch Chatbots usw. Eine solche Diskriminierung kann sowohl auf absichtliche Handlungen des Entwicklers von KI-Systemen herbeigeführt (unmittelbare Diskriminierung) als auch in Folge des autonomen Betriebs von Algorithmen ohne menschliches Eingreifen entstehen (mittelbare oder indirekte Diskriminierung).

Die EU verfügte bereits über die umfassenden Vorschriften zur Verhütung der Diskriminierung im primären und sekundären Recht, darunter kann man insb. die folgenden Rechtsquellen

¹⁰² Charta der Grundrechte der Europäischen Union [2012] ABl C 326/391, Art. 21 Abs. 1

¹⁰³ Richtlinie 2010/41/EU des Europäischen Parlaments und des Rates vom 7. Juli 2010 zur Verwirklichung des Grundsatzes der Gleichbehandlung von Männern und Frauen, die eine selbständige Erwerbstätigkeit ausüben, und zur Aufhebung der Richtlinie 86/613/EWG des Rates [2010] ABl L 180/1, Art. 3 Punkt a)

¹⁰⁴ Ebenda, Art. 3 Punkt b)

nennen: Art. 157 AEUV, Richtlinie 2006/54/EG zur Verwirklichung des Grundsatzes der Chancengleichheit und Gleichbehandlung von Männern und Frauen in Arbeits- und Beschäftigungsfragen (Frauen und Männer sollen bei gleicher bzw. gleichwertiger Arbeit gleich verdienen), Rassengleichstellungsrichtlinie 2000/43/EG¹⁰⁵, Richtlinie 2004/113/EG des Rates vom 13. Dezember 2004 zur Verwirklichung des Grundsatzes der Gleichbehandlung von Männern und Frauen beim Zugang zu und bei der Versorgung mit Gütern und Dienstleistungen, Richtlinie 2000/78/EG des Rates vom 27. November 2000 zur Festlegung eines allgemeinen Rahmens für die Verwirklichung der Gleichbehandlung in Beschäftigung und Beruf usw. Der EuGH ist auch auf dem Gebiet der Diskriminierungsbekämpfung überaus aktiv. Unter den prominentesten Judikaten von EuGH sind insb. die folgenden Fälle zu nennen: *Bougnaoui*¹⁰⁶, *Coleman*¹⁰⁷, *CHEZ*¹⁰⁸, *Egenberger*¹⁰⁹, *Test-Achats*.¹¹⁰

Der oben erläuterte Artikel 22 DSGVO ist die einzige Rechtsvorschrift des EU-Rechts, die mögliche Diskriminierung beim Einsatz der ADM-Systeme regelt, die schon im Abschnitt 2.3.1. behandelt wurde. Allerdings gibt es mittlerweile keine weiteren EU-Vorschriften zur Behandlung der Diskriminierung beim Einsatz der KI-Algorithmen in der Geschäftstätigkeit. Das Nichtdiskriminierungsrecht könnte jedoch dazu beitragen, Menschen vor algorithmischer Diskriminierung zu schützen. Es weist mehrere Schwächen auf, wenn es auf algorithmische Diskriminierung Anwendung findet¹¹¹, z.B. ist dem Opfer manchmal schwierig zu beweisen, dass eine durch ADM-System getroffene Entscheidung eine geschützte Klasse bzw. Gruppe der Personen überproportional beeinflusst und somit diskriminierend ist.

2.4. Initiativen zur Haftung

Die sichere und vertrauensvolle Anwendung der KI in der Geschäftstätigkeit benötigt die geeigneten Rechtsvorschriften zur Haftung der Hersteller und der Betreiber der KI-Produktion. Dabei ist es zu betonen, dass EU bereit über den gewiesenen Rechtsrahmen verfügt, der auch

¹⁰⁵ Richtlinie 2000/43/EG des Rates vom 29. Juni 2000 zur Anwendung des Gleichbehandlungsgrundsatzes ohne Unterschied der Rasse oder der ethnischen Herkunft [2016] ABL L 180/22

¹⁰⁶ s. C-188/15 Asma Bougnaoui und Association de défense des droits de l'homme (ADDH) gegen Micropole SA [2017] EU:C:2017:204

¹⁰⁷ s. C-303/06 S. Coleman v Attridge Law and Steve Law [2008] EU:C:2008:415

¹⁰⁸ s. C-83/14 CHEZ Razpredelenie Bulgaria AD v Komisia za zashtita ot diskriminatsia [2015] EU:C:2015:480

¹⁰⁹ s. C-414/16 Vera Egenberger v Evangelisches Werk für Diakonie und Entwicklung e.V. [2018] EU:C:2018:257

¹¹⁰ s. C-236/09 Association Belge des Consommateurs Test-Achats ASBL and Others v Conseil des ministres [2011] EU:C:2011:100

¹¹¹ Frederik J. Zuiderveen Borgesius, 'Strengthening legal protection against discrimination by algorithms and artificial intelligence' (2020) 22(7) The International Journal of Human Rights, abrufbar unter <https://www.tandfonline.com/doi/full/10.1080/13642987.2020.1743976>, letzter Zugriff am 20.06.2020

geeignet ist, die Haftungsfragen in Bezug auf die KI-Anwendung zu behandeln. Der Einsatz von KI in Produkten und Dienstleistungen in der Geschäftstätigkeit kann zu Schaden für menschliches Leben und Gesundheit führen, wobei derzeitige Haftungs Vorschriften des EU-Rechts sie nicht explizit erfassen.¹¹²

Das bestehende Deliktsrecht in der EU umfasst folgende wichtigste Rechtsquellen: Produkthaftungsrichtlinie¹¹³, Artikel 82 DSGVO - Haftung für datenschutzrechtliche Verstöße, Richtlinie über die Kraftfahrzeug-Haftpflichtversicherung¹¹⁴, Richtlinie zur Haftung für Verstoß gegen das Wettbewerbsrecht.¹¹⁵ Die Kollisionsnormen für das Deliktsrecht sind grundsätzlich in der Verordnung Rom II verankert.¹¹⁶ Dabei zu beachten ist, dass die Gesetzgebung einzelner Mitgliedstaaten auch die Vorschriften zum Deliktsrecht beinhalten, die je nach dem Land unterscheiden können. Vor diesem Hintergrund werden die einschlägigen Vorschriften verschiedener Mitgliedstaaten weiter behandelt, insb. Regelungen aus österreichischem Recht.

In der EU wurde bereits die Ausarbeitung der Rechtsvorschriften zur deliktischen Haftung beim Einsatz der KI-Systeme und anderer neuen Technologien begonnen. Am 16. Februar 2017 verabschiedete das Europäische Parlament eine Entschließung¹¹⁷ mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik, in der es der Europäischen Kommission eine Reihe von Regulierungsinitiativen im Bereich für KI empfohlen hat. Unter anderem forderte es die Kommission auf, ihm *„einen Vorschlag für ein Rechtsinstrument über rechtliche Fragen im Zusammenhang mit der Entwicklung und Verwendung von Robotik und KI, wie sie in den nächsten 10 bis 15 Jahren vorhersehbar ist, zu unterbreiten, und zwar kombiniert mit nicht-rechtlichen Instrumenten wie Leitlinien und Verhaltenskodizes gemäß den als Anlage beigefügten Empfehlungen“*.¹¹⁸

¹¹² vgl. COM (2020) 65 endgültig, S. 16

¹¹³ Richtlinie 85/374/EWG des Rates vom 25. Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte [1985] ABl L 210/29

¹¹⁴ Richtlinie 2009/103/EG des Europäischen Parlaments und des Rates vom 16. September 2009 über die Kraftfahrzeug-Haftpflichtversicherung und die Kontrolle der entsprechenden Versicherungspflicht [2009] ABl L 263/11

¹¹⁵ Richtlinie 2014/104/EU des Europäischen Parlaments und des Rates vom 26. November 2014 über bestimmte Vorschriften für Schadensersatzklagen nach nationalem Recht wegen Zuwiderhandlungen gegen wettbewerbsrechtliche Bestimmungen der Mitgliedstaaten und der Europäischen Union [2014] ABl L 349/1

¹¹⁶ Verordnung (EG) Nr. 864/2007 des Europäischen Parlaments und des Rates vom 11. Juli 2007 über das auf außervertragliche Schuldverhältnisse anzuwendende Recht („Rom II“) [2007] ABl L 199/40

¹¹⁷ Entschließung des Europäischen Parlaments vom 16. Februar 2017 mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103(INL))

¹¹⁸ Ebenda, Punkt 51

Am 25. April 2018 veröffentlichte die Europäische Kommission ein Arbeitsdokument „Haftung für aufkommende digitale Technologien“, das am selben Tag eine Mitteilung der Europäischen Kommission an die anderen Institutionen unter Bezeichnung „Künstliche Intelligenz für Europa“¹¹⁹ begleitete. In dieser Mitteilung zur KI für Europa wurde es unter anderem über die Prüfung des Sicherheitsrahmens und die Haftungsvorschriften auf nationaler bzw. europäischen Ebene erklärt, um festzustellen, ob sie *„vor dem Hintergrund dieser neuen Herausforderungen ihren Zweck erfüllen oder ob es etwaige Lücken zu schließen gilt“*.¹²⁰

Außerdem setzte die Europäische Kommission im März 2018 eine Expertengruppe für Haftung und neue Technologien ein. Sie arbeitet in zwei verschiedenen Formationen: in der Formation der Produkthaftungsrichtlinie und der Formation für neue Technologien (New Technologies Formation - NTF).¹²¹ Die Experten von NTF wurden gebeten zu prüfen, ob die derzeitigen Haftungsregelungen noch ausreichen, um die Einführung neuer Technologien wie KI durch Förderung der Investitionsstabilität und des Vertrauens der Nutzer zu erleichtern. Bei Mängeln sollte der NTF Änderungsempfehlungen angeben, ohne sich auf bestehende nationale und EU-Rechtsinstrumente zu beschränken.¹²²

Die Ergebnisse dieser Arbeit kamen bald. Am 21. November 2019 wurde ein Bericht über die Haftung für KI und die anderen entstehenden Technologien¹²³ durch die Europäische Kommission veröffentlicht, der durch die NTF-Expertengruppe erstellt wurde. In diesem Dokument wurden die bestehenden Sicherheits- und Haftungsvorschriften in Bezug der verschiedenen KI-Anwendung bewertet, sowie die einschlägigen Befunde für die Schaffung des künftigen Rechtsrahmens vorgeschlagen, die weiter in diesem Abschnitt dargestellt bzw. erläutert werden.

Bei der Erstellung des Berichts über die Haftung für KI und die anderen aufkommenden Technologien von 2019 wurde es festgestellt, dass die Gesetze der EU-Mitgliedstaaten grundsätzlich keine spezifische Haftungsregelungen beinhalten, die speziell für Schäden gelten, die durch den Einsatz neuer digitalen Technologien, wie KI entstehen.¹²⁴ Vor diesem

¹¹⁹ COM (2018) 237 endgültig

¹²⁰ Ebenda, S. 19

¹²¹ Expert Group on Liability and New Technologies, Report on Liability for Artificial Intelligence and other emerging technologies (2019), abrufbar unter <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608>, letzter Zugriff am 23.05.2020, S. 12

¹²² Ebenda, S. 13

¹²³ Ebenda

¹²⁴ Ebenda, S. 15

Hintergrund verfasste die Europäische Kommission einen oben erwähnten Bericht über die Auswirkungen der KI in Hinblick auf Sicherheit und Haftung, der zusammen mit Weissbuch zur KI im Februar 2020 veröffentlicht wurde. Er beinhaltet unter anderem ebenfalls die Empfehlung zu den Modalitäten des künftigen KI-Haftungsrahmens.

Gemäß nationalem Recht sind allerdings mehrere voneinander unabhängige Schadenersatzansprüche aufgrund einer verschuldensabhängigen bzw. einer verschuldensunabhängigen Haftung zugänglich, falls die Schäden durch Produkte und Dienstleistungen verursacht wurden.¹²⁵ Daher werden sie jetzt in Hinblick auf technische Spezifität der KI-Systeme sowie unter Einbeziehung der Befunde aus dem Bericht der NTF-Expertengruppe über die Haftung für KI und dem Bericht Europäischer Kommission über die Auswirkungen der KI in Hinblick auf Sicherheit und Haftung untersucht.

2.4.1. Bestehende Haftungsmodelle in dem Nationalrecht

Allgemeine Regel für Schadenersatz im Deliktrecht

Gemäß dem österreichischen ABGB kommt die Geltendmachung des Schadenersatzanspruches auf kumulative Erfüllung der folgenden Voraussetzungen an: 1) das Vorliegen des Schadens; 2) Rechtswidriges Verhalten und Verschulden; 3) Kausalität zwischen zwei ersten Voraussetzungen.¹²⁶ Die Mehrheit der modernen Rechtsordnungen kennt dieses Haftungsmodell. Allerdings kann dieser klassische Schadenersatz in Bezug auf KI-Technologien in der Praxis problematisch sein. In der Regel muss das Opfer nachweisen, dass sein Schaden auf ein Verhalten oder ein Risiko zurückzuführen ist, das dem Beklagten zuzurechnen ist. Ein Opfer sollte dann Beweise dafür vorlegen, was ziemlich schwierig und lästig im Fall der KI-Systeme ist. Das ist immer noch schwieriger, wenn der Algorithmus von einem KI-System entwickelt oder modifiziert wurde, das durch maschinelles Lernen und Deep-Learning-Techniken auf der Grundlage mehrerer externer Daten betrieben wird, die seit Beginn seines Betriebs gesammelt wurden. Die eingebetteten Kriterien für die Erfassung und Analyse von Daten und den Entscheidungsprozess können möglicherweise nicht erklärbar sein und häufig teure Analysen durch Experten erfordern.¹²⁷

¹²⁵ vgl. COM (2020) 64 endgültig, S. 15

¹²⁶ s. § 1293 bis 1341 ABGB

¹²⁷ Expert Group on Liability and New Technologies, Report on Liability for Artificial Intelligence and other emerging technologies (2019), abrufbar unter <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608>, letzter Zugriff am 23.05.2020, S. 20

Was Schuld bzw. rechtswidriges Verhalten angeht, erschwert KI die Anwendung fehlerbasierter Haftungsregeln, da es keine gut etablierten Modelle für das ordnungsgemäße Funktionieren dieser Technologien gibt und die Möglichkeit besteht, dass sie sich als Ergebnis des Lernens ohne direkte menschliche Kontrolle entwickeln. Die Funktionsweise der KI-Systeme können an Sorgfaltspflichten ihrer Ersteller nicht gemessen werden, die auf menschliches Verhalten ausgelegt sind. Ein Verstoß gegen die gesetzlichen oder behördlichen Anforderungen an KI-Produkte kann auch ein leichteres Haftungsmodell für das Opfer auslösen, indem beispielsweise die Beweislast für Fehler in vielen Systemen verlagert wird. Allerdings sollten solche Anforderungen von Anfang an vorhanden sein, was noch nicht der Fall ist.¹²⁸ Außerdem fällt es dem Opfer meistens schwierig, die Schuld des Beklagten zu beweisen. Je komplexer die Umstände sind, die zum Schaden des Opfers führen, desto schwieriger ist es, relevante Beweise für ein Verschulden zu identifizieren.¹²⁹ Vor diesem Hintergrund sind die verschuldensabhängigen Haftungsmodelle für den Umgang mit den durch KI verursachten Schaden nicht geeignet.

Haftung für fremdes Verschulden (Verhalten)

Bei einer Haftung für fremdes Verschulden haftet der Beklagte für die unerlaubten Handlungen eines anderen, wobei ein Normverstoß durch denjenigen vorliegt, für den der Beklagte (mit)haftet.¹³⁰ Nach diesem Konzept sollte der Betreiber von KI-Systemen für die durch diese Systeme verursachten Schäden haften. Die Verwendung einer selbstlernenden und autonomen Maschine bzw. Systeme zur Unterstützung sollte nicht anders behandelt werden als die Verwendung eines Menschen, wenn diese Unterstützung zum Schaden eines Dritten führt (sog. „Prinzip der funktionalen Äquivalenz“).¹³¹ Zumindest in den Rechtsordnungen, in denen die Haftung für fremdes Verschulden als eine Variante der Verschuldenshaftung betrachtet wird und der Auftraggeber für das Fehlverhalten eines anderen haftbar gemacht wird, kann es jedoch schwierig sein, den Maßstab zu ermitteln, anhand dessen die Tätigkeiten nichtmenschlicher

¹²⁸ Ebenda, S. 23

¹²⁹ Ebenda, S. 24

¹³⁰ Eoin Quill, *Irland*, Staatshaftung in Europa: Nationales und Unionsrecht (De Gruyter; Auflage: 1 2013), S. 293

¹³¹ Expert Group on Liability and New Technologies, Report on Liability for Artificial Intelligence and other emerging technologies (2019), abrufbar unter <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608>, letzter Zugriff am 23.05.2020, S. 25

Helfer bewertet werden, um das Fehlverhaltenselement menschlicher Helfer widerzuspiegeln.¹³²

Gefährdungshaftung

Die gesetzlichen Tatbestände in dieser Hinsicht sind meistens entweder an ein gefährliches Verhalten oder an eine Herrschaft über eine Gefahrenquelle angeknüpft. Normalerweise richtet sich diese Haftungsart gegen diejenige Person, dem die Verantwortung für die Gefahr zugewiesen ist.¹³³ Ein Beispiel für Gefährdungshaftung in dem österreichischen Recht ist EKHG, wonach der Betriebsunternehmer der Eisenbahn bzw. der Halter des Kraftfahrzeuges haftet¹³⁴, falls ein Mensch „*durch einen Unfall beim Betrieb einer Eisenbahn oder beim Betrieb eines Kraftfahrzeugs getötet, an seinem Körper oder an seiner Gesundheit verletzt oder eine Sache beschädigt*“ wird.¹³⁵ In Gegenteil zu den oben erwähnten Haftungsarten ist das Vorliegen des Verschuldens in diesem Fall nicht erforderlich, um die Schadenersatzansprüche geltend zu machen. Seit 19. Jahrhundert wurde die Gefährdungshaftung in die Gesetzgebung einiger europäischer Länder übernommen, um die Herausforderungen der neuen Technologien zu meistern, die potenziell gefährlich sein können.¹³⁶

Eine Gefährdungshaftung für den Betrieb von Computern oder Software ist in Europa bislang weitgehend unbekannt, obwohl es einige begrenzte Beispiele gibt, in denen Länder die Haftung des Betreibers eines Computersystems vorsehen, beispielsweise bei den von dem Staat betriebenen Datenbanken¹³⁷. Der Vorteil einer Gefährdungshaftung für das Opfer liegt auf der Hand, weil es die Schuld und das Fehlverhalten des Beklagten, sowie den Kausalzusammenhang zwischen einem solchen Fehlverhalten und dem Verlust des Opfers nachzuweisen hat.¹³⁸ Allerdings soll der Gesetzgeber die potenziellen negativen Auswirkungen einer Gefährdungshaftung (wie überflüssige Abschreckung des Betreibers) auf weitere Entwicklung und Förderung der KI-Technologie nicht außer Acht lassen.¹³⁹

¹³² Ebenda

¹³³ vgl. Anne Röthel, ‘Gefährdungshaftung’ (2012) 34(6) JURA – Juristische Ausbildung, abrufbar unter <https://doi-org.uaccess.univie.ac.at/10.1515/jura-2012-0095>, letzter Zugriff am 20.06.2020, S. 445

¹³⁴ Eisenbahn- und Kraftfahrzeughaftpflichtgesetz, BGBl. Nr. 48/1959, § 5, Abs. 1

¹³⁵ Ebenda, § 1

¹³⁶ Expert Group on Liability and New Technologies, Report on Liability for Artificial Intelligence and other emerging technologies (2019), abrufbar unter <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608>, letzter Zugriff am 23.05.2020, S. 25

¹³⁷ Ebenda, S. 26

¹³⁸ Ebenda

¹³⁹ vgl. Ebenda, S. 27

Produkthaftung

Der bestehende Haftungsrahmen auf dem Gebiet der Produkthaftung in der EU wird grundsätzlich durch Produkthaftungsrichtlinie¹⁴⁰ auf dem Unionseben aufgebaut. Grundsätzlich dient die Produktsicherheitsrichtlinie einer *„Angleichung der einzelstaatlichen Rechtsvorschriften über die Haftung des Herstellers für Schäden, die durch die Fehlerhaftigkeit seiner Produkte verursacht worden sind“*.¹⁴¹ Die Produkthaftungsrichtlinie betrifft Schäden, die entweder durch den Tod bzw. Körperverletzungen an Menschen oder an Privateigentum verursacht wurden. Allerdings hat sie selbst zum Ziel keine Harmonisierung, sondern sie öffnet *„den Weg für eine umfassendere Harmonisierung“*.¹⁴² Deshalb ist bis jetzt eine Produktsicherheitshaftung in der EU noch nicht harmonisiert. Sondern schafft sie den Schutzniveau auf EU-Ebene, *„die von der nationalen verschuldensabhängigen Haftung allein nicht abgedeckt ist“*.¹⁴³

Der Hersteller haftet aufgrund der Produktsicherheitsrichtlinie für fehlerhafte Produkte nur dann, wenn er diese in Verkehr gesetzt hat. Gemäß Art. 4 Produkthaftungsrichtlinie hat der Geschädigte den Schaden, den Fehler und den ursächlichen Zusammenhang zwischen Fehler und Schaden zu beweisen.¹⁴⁴ Die Europäische Kommission ist besorgt, dass es jedoch bei automatisierten Fahrzeugen überaus schwierig sein kann, *„einen Produktfehler, den entstandenen Schaden und den Kausalzusammenhang zwischen diesen beiden nachzuweisen“*.¹⁴⁵ Dies ermutigt die EU und deren Mitgliedstaaten, neue Einsätze zur Haftung für die durch die fehlerhaften KI-Produkte verursachten Schäden auszuarbeiten.

Bei der Feststellung des Anwendungsbereichs der Produktsicherheitsrichtlinie versteht man unter dem Begriff „Produkt“ *„jede bewegliche Sache, ausgenommen landwirtschaftliche Naturprodukte und Jagderzeugnisse, auch wenn sie einen Teil einer anderen beweglichen Sache oder einer unbeweglichen Sache bildet“*.¹⁴⁶ Vor dem Hintergrund dieser Definition ist die Abgrenzung zwischen den Produkten und den Dienstleistungen klar. In KI-Systemen interagieren Produkte und Dienstleistungen allerdings permanent und eine derartige klare

¹⁴⁰ Richtlinie 85/374/EWG

¹⁴¹ Ebenda, Erwägungsgrund 1

¹⁴² Ebenda, Erwägungsgrund 18

¹⁴³ COM (2020) 64 endgültig, S. 15

¹⁴⁴ Richtlinie 85/374/EWG, Art. 4

¹⁴⁵ COM (2020) 65 endgültig, S. 14

¹⁴⁶ Richtlinie 85/374/EWG, Art. 2

Abgrenzung zwischen ihnen ist nicht möglich. Es ist auch aus diesem Grund fraglich, ob Software unter das rechtliche Konzept des Produkts oder der Produktkomponente fällt.¹⁴⁷

Anderer wichtiger und problematischer Tatbestand in Hinblick auf Produkthaftung ist eine Feststellung des Fehlers an einem Produkt. Dies wird auf der Grundlage der Sicherheitserwartungen eines Durchschnittsverbrauchers unter Berücksichtigung aller relevanten Umstände bewertet.¹⁴⁸ Die Interkonnektivität von KI-Produkten macht es überaus schwierig, ein Fehler an Produkt zu identifizieren. Komplexe autonome KI-Systeme mit Selbstlernfähigkeiten werfen auch die Frage auf, ob unvorhersehbare Abweichungen im Entscheidungspfad als Fehler (wie etwa bei ADM-Systemen) behandelt werden können.¹⁴⁹ Also die Anwendung der Produkthaftungsvorschriften in Bezug auf die KI-Systeme erfordert ebenfalls einer Anpassung.

2.4.2. Bericht über die Haftung für künstliche Intelligenz und andere aufkommende Technologien (Expertengruppe für Haftung und neue Technologien)

In Anbetracht der oben angeführten Ausführungen der NTF-Expertengruppe und der Europäischen Kommission sind die bestehenden Haftungsmodelle für den Umgang mit neuen digitalen Technologien wie KI kaum geeignet. Weiter werden die Vorschläge der NTF-Expertengruppe und der Europäischen Kommission zur Anpassung der bestehenden Haftungsmodelle dargestellt. Die wichtigsten Ergebnisse der Analyse aus dem Bericht der Europäischen Kommission über die Haftung für KI und die anderen aufkommenden Technologien, die auf den Ausarbeitungen der NTF-Expertengruppe gestützt sind, können wie folgt kurz dargestellt bzw. zusammengefasst werden:

- 1) Folgende technische Eigenschaften der aufkommenden digitalen Technologien sollten bei der Anpassung des bestehenden Deliktrechts berücksichtigt werden: Komplexität, Opazität, Offenheit, Autonomie, Vorhersehbarkeit, Datenabhängigkeit und Verletzbarkeit;¹⁵⁰

¹⁴⁷ Expert Group on Liability and New Technologies, Report on Liability for Artificial Intelligence and other emerging technologies (2019), abrufbar unter <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608>, letzter Zugriff am 23.05.2020, S. 28

¹⁴⁸ Richtlinie 85/374/EWG, Art. 6 Abs. 1

¹⁴⁹ Expert Group on Liability and New Technologies, Report on Liability for Artificial Intelligence and other emerging technologies (2019), abrufbar unter <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608>, letzter Zugriff am 23.05.2020, S. 28

¹⁵⁰ vgl. Ebenda, S. 32-33

- 2) In Anbetracht der großen Vielfalt der mit KI entstandenen Risiken ist es fast unmöglich, einen einheitlichen Rechtsrahmen für alle mögliche derartige Risiken auszuarbeiten;¹⁵¹
- 3) Verschuldensabhängige und verschuldensunabhängige Haftungsregime (wie Gefährdungshaftung und Produkthaftungshaftung) sollten weiterhin koexistieren. In einigen Fällen gilt die vertragliche Haftung oder andere Entschädigungsregelungen neben oder anstelle des Deliktrechts;¹⁵²
- 4) Es ist nicht erforderlich, KI oder andere neue Technologien eine Rechtspersönlichkeit zu verleihen, da der Schaden, den diese verursachen können, den natürlichen Personen oder den bestehenden Kategorien der juristischen Personen zugerechnet werden können;¹⁵³
- 5) Eine Gefährdungshaftung sollte in Bezug auf den Betreiber der KI-Systeme angewandt werden, um die bestehenden Risiken entsprechend zu meistern.¹⁵⁴ Der Betreiber heißt *„eine Person, die die Kontrolle über das mit dem Betrieb neuer digitaler Technologien verbundene Risiko hat und von einem solchen Betrieb profitiert“*;¹⁵⁵
- 6) Ein Hersteller von Produkten, die aufkommende digitale Technologien enthalten, sollten für Schäden haftbar gemacht werden, die durch Fehler an ihren Produkten verursacht werden, selbst wenn solcher Fehler durch Änderungen am Produkt verursacht wurde, die nach dem Inverkehrbringen unter der Kontrolle des Herstellers vorgenommen wurden;¹⁵⁶
- 7) Eine Person, die eine Technologie verwendet, die ein gewisses Maß an Autonomie besitzt, sollte nicht weniger für den daraus resultierenden Schaden verantwortlich sein, als wenn dieser Schaden durch eine menschliche Hilfskraft verursacht worden wäre (dh. bei Schaden durch autonome KI-Systeme, wie automatisierte Fahrzeuge, sollte eine Haftung für fremdes Verschulden gelten);¹⁵⁷
- 8) KI sollten ggf. mit Protokollierungsfunktionen ausgestattet sein („logging by design“). Wenn keine Protokollierung durchgeführt wird oder kein angemessener Zugriff auf protokollierte Daten gewährt wird, sollte sich die Beweislast umkehren, um das Opfer nicht zu schädigen. In solchen Fällen sollte eine widerlegbare Vermutung angewandt

¹⁵¹ vgl. Ebenda, S. 34

¹⁵² vgl. Ebenda, S. 36

¹⁵³ vgl. Ebenda, S. 38

¹⁵⁴ vgl. Ebenda, S. 39

¹⁵⁵ Ebenda, S. 41

¹⁵⁶ vgl. Ebenda, S. 42-43

¹⁵⁷ vgl. Ebenda, S. 45

werden, dass die durch die fehlenden Angaben nachzuweisende Haftungsbedingung erfüllt ist;¹⁵⁸

- 9) Wenn der Schaden von einer Art ist, die durch Sicherheitsvorschriften vermieden werden sollte, sollte die Nichteinhaltung dieser Sicherheitsvorschriften zu einer Umkehrung der Beweislast zu Gunsten des Opfers führen;¹⁵⁹
- 10) Normalerweise sollte das Opfer weiterhin nachweisen, was genau seinen Schaden verursacht hat. Wenn nachgewiesen wird, dass Schaden durch KI bzw. KI-Systeme und Produkte verursacht wurde und die Haftung dafür von der Absicht oder Fahrlässigkeit einer Person abhängig gemacht wird, sollte die Beweislast für ein Verschulden umgekehrt werden, wenn unverhältnismäßige Schwierigkeiten und Kosten für die Festlegung des entsprechenden Pflegestandards und den Nachweis ihrer Verletzung notwendig sind;¹⁶⁰
- 11) Die Zerstörung der Daten des Opfers sollte als Schaden angesehen werden, der unter bestimmten Bedingungen entschädigt werden muss (wie etwa Vorliegen der Absicht, die Haftung ergibt sich aus dem Vertrag);¹⁶¹
- 12) Wenn ein Dritter einem erhöhten Schadensrisiko ausgesetzt ist, könnte die obligatorische Versicherung den Opfern einen besseren Zugang zu Entschädigungen ermöglichen und potenzielle Täter vor dem Haftungsrisiko schützen.¹⁶²

2.4.3. Bericht über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung COM (2020) 64 endgültig (Europäische Kommission)

In dem oben erwähnten Bericht der Europäischen Kommission über die Auswirkungen der KI in Hinblick auf Sicherheit und Haftung wurden folgende Aspekte dargestellt bzw. erläutert, die bei der Ausarbeitung der künftigen Haftungsvorschriften in Bezug auf den durch KI-Systeme verursachten Schaden zu berücksichtigen sind:

- 1) Komplexität von Produkten, Dienstleistungen und der Wertschöpfungskette: Der Begriff „Produkt“ hat in der Produkthaftungsrichtlinie einen breiten Umfang. Allerdings sollte er weiter präzisiert werden, *„um der Komplexität neuer Technologien besser Rechnung zu tragen und sicherzustellen, dass für durch fehlerhafte Produkte*

¹⁵⁸ vgl. Ebenda, S. 47

¹⁵⁹ vgl. Ebenda, S. 48

¹⁶⁰ vgl. Ebenda, S. 52

¹⁶¹ vgl. Ebenda, S. 59

¹⁶² vgl. Ebenda, S. 61

*verursachte Schäden, die auf Software oder andere digitale Merkmale zurückzuführen sind, stets Schadenersatz gewährt wird“;*¹⁶³

- 2) Konnektivität und Offenheit: Diese Eigenschaften der KI-Produkte können die Sicherheitserwartungen in Bezug auf Schäden beeinflussen, die sich aus Cybersicherheitsverletzungen ergeben. Darüber hinaus können verbundene Produkte auch für Zwecke verwendet werden, die über die vom Hersteller vernünftigerweise erwarteten hinausgehen.¹⁶⁴ Daher ist es notwendig, die Rechtsvorschriften zum Ersatz von Schäden, die den Nutzern entstanden sind, zu präzisieren und zu erleichtern, insb. in Situationen, in denen eine vernünftige Verwendung vorhersehbar ist;
- 3) Autonomie und Opazität: KI-Systeme können ihre Leistung durch Lernen aus der bisherigen Erfahrung verbessern, was als Opazität zu bezeichnen ist. Autonome KI-Systeme erfüllen ihre Funktionen, *„ohne dass jeder Schritt im Voraus festgelegt wird, und werden in geringerem Maße oder schließlich gar nicht mehr unmittelbar durch den Menschen gesteuert oder beaufsichtigt“*.¹⁶⁵ Daher ist es für Europäische Kommission fraglich, *„unter welchen Bedingungen sich die Haftung des Herstellers durch die Selbstlerneigenschaften verlängert und in welchem Umfang der Hersteller bestimmte Änderungen hätte voraussehen müssen“*.¹⁶⁶ Vor diesem Hintergrund könnte der in der Produkthaftungsrichtlinie verankerte Begriff des „Inverkehrbringens“ *„in enger Abstimmung hinsichtlich entsprechender Änderungen im Produktsicherheitsrahmen der Union überarbeitet werden“*.¹⁶⁷
- 4) Erleichterung der Beweislastregel in den komplexen IoT-Umgebungen: Um die Folgen der Komplexität der IoT-Umgebungen zu mildern, ist es erforderlich, die Anpassungen der nationalen Gesetzgebung in dieser Hinsicht durchzuführen, *„um den Opfern von Schäden im Zusammenhang mit KI die Beweislast zu erleichtern“*.¹⁶⁸

2.5. Initiativen zur Produktsicherheit und zum Marktaufsicht

Die europäischen Institutionen sind auch auf dem Gebiet der Sicherstellung der KI-Produkte bzw. -Systeme überaus aktiv. In der Mitteilung der Europäischen Kommission „Schaffung von Vertrauen in eine auf den Menschen ausgerichtete künstliche Intelligenz“ ist es

¹⁶³ COM (2020) 64 endgültig, S. 17

¹⁶⁴ vgl. Ebenda, S. 18

¹⁶⁵ Ebenda

¹⁶⁶ Ebenda, S. 19

¹⁶⁷ Ebenda

¹⁶⁸ Ebenda, S. 17

festgestellt, dass KI-Systeme konzeptuell integrierte Schutz- und Sicherheitsvorkehrungen aufweisen sollten, um in jeder Phase nachprüfbar sicher zu sein, wobei es auf die körperliche und geistige Sicherheit aller Beteiligten ankommt.¹⁶⁹ Daher benötigt eine derartige sichere Anwendung der KI-Systeme den geeigneten Rechtsrahmen – nämlich die Regeln zu Verbraucherschutz und Produktsicherheit, die technischen Eigenschaften der KI-Systeme vollständig berücksichtigen.

Das Verbraucherschutzrecht beinhaltet spezifische Rechtsvorschriften, die für die Rechtsgeschäfte gelten, an denen einerseits ein Unternehmer teilnimmt, andererseits – eine Person, die kein Unternehmer ist (sog. „business-to-consumer“ Geschäfte). In der EU sind die Verbraucherschutz- bzw. Produktsicherheitsregeln auch ein wesentlicher Bestandteil des Binnenmarktrechts, da sie den grenzüberschreitenden Verkehr der KI-Waren und Dienstleistungen ermöglichen.

In der Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2011 über die Rechte der Verbraucher, zur Abänderung der Richtlinie 93/13/EWG des Rates und der Richtlinie 1999/44/EG des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 85/577/EWG des Rates und der Richtlinie 97/7/EG des Europäischen Parlaments und des Rates ist Verbraucher als jede natürliche Person definiert, „*die bei von dieser Richtlinie erfassten Verträgen zu Zwecken handelt, die außerhalb ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit liegen*“.¹⁷⁰

Die folgenden Prinzipien gelten für den Bereich von dem Verbraucherschutz in der EU:

- **Schutz der schwächeren Partei:** Ein Verbraucher ist als eine schwächere Partei in Verhältnissen mit den Unternehmern anzusehen.¹⁷¹ Daher erfordert der Verbraucher einen besonderen Schutz seiner Rechte. Einige Unternehmer nutzen die Unwissenheit und Unsicherheit des Verbrauchers. Daher ahnen viele Verbraucher meistens oft gar nicht, dass ihre Rechte verletzt werden, und selbst wenn sie eine Verletzung ihrer

¹⁶⁹ COM (2019) 168 endgültig, S. 5

¹⁷⁰ Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2011 über die Rechte der Verbraucher, zur Abänderung der Richtlinie 93/13/EWG des Rates und der Richtlinie 1999/44/EG des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 85/577/EWG des Rates und der Richtlinie 97/7/EG des Europäischen Parlaments und des Rates [2011] ABL L 304/64, Art. 2 Abs. 1

¹⁷¹ vgl. European University Institute, *Department of law Consumer law and artificial intelligence Challenges to the EU consumer law and policy stemming from the business' use of artificial intelligence* (EUI working papers 2018), https://pdfs.semanticscholar.org/d15a/13a15d74ce0168293c6477d1eb37c5692744.pdf?_ga=2.75614742.280107500.1590079789-947451715.1590079789, letzter Zugriff am 21.05.2020, S. 10

eigenen Rechte feststellen, wissen sie oft nicht, auf welche Weise sie sich schützen und die verletzten Rechte wiederherstellen können;

- **Geregelte Autonomie:** Grundsätzlich sind die Unternehmer frei zu entscheiden, ob und unter welchen Bedingungen sie in Märkte eintreten möchten, ebenso wie die Freiheit der Kunden besteht, die Produkte und Dienstleistungen zu wählen und die Bedingungen, unter denen sie bereit sind, Rechtsbeziehungen einzugehen.¹⁷² Allerdings ist eine derartige Freiheit nicht unbegrenzt. Die Unternehmer bzw. die Lieferanten sollen die unlauteren Geschäftspraktiken vermeiden (wie vergleichende Werbung und unlautere Geschäftsbedingungen in Verträgen mit Verbrauchern);
- **Nichtdiskriminierung:** Dem EU-Gesetzgeber ist es bis jetzt nicht gelungen, das Nichtdiskriminierungsprinzip vollständig auf den Verbrauchsbereich auszudehnen. Verbraucher können diskriminiert werden, wenn der Unternehmer sie aus diskriminierenden Gründen für wirtschaftliche Transaktionen auswählt und somit den Zugang zum Markt verweigert.¹⁷³ KI ermöglicht noch die ausgefeilteren Formen der Anzeigen und Angebote, die einen erneuten Fokus und möglicherweise eine völlig neue Perspektive auf das Prinzip der Nichtdiskriminierung in privatrechtlichen Beziehungen einladen¹⁷⁴;
- **Schutz der Konsumentenprivatsphäre** ist im Wesentlichen durch die Vorschriften von DSGVO gewährleistet. Sie regeln nicht nur die Verhältnisse zwischen den Bürgern und Staat, sondern auch zwischen den Bürger (und Verbrauchers) und Wirtschaftsteilnehmern. Infolgedessen rücken Datenschutz und Verbraucherschutz näher zusammen.¹⁷⁵

Die Produktsicherheitsvorschriften bilden ein Herzstück des EU-Verbraucherrechts. Mit diesen Vorschriften soll es sichergestellt werden, dass die EU einen Beitrag zum Schutz der Gesundheit und der Sicherheit der Verbraucher leistet.¹⁷⁶ Durch eine Vereinheitlichung bzw. Harmonisierung der Produktsicherheitsvorschriften in den Mitgliedstaaten wird hauptsächlich der freie grenzüberschreitende Verkehr der Waren innerhalb EU (insb. der sog. intelligenten

¹⁷² vgl. Ebenda, S. 12

¹⁷³ vgl. Ebenda, S. 17

¹⁷⁴ vgl. Ebenda, S. 18

¹⁷⁵ Ebenda

¹⁷⁶ Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates vom 3. Dezember 2001 über die allgemeine Produktsicherheit [2001] ABl L 11/4, Erwägungsgrund 4

KI-Waren) ermöglicht. Daher stellen die Produktsicherheitsvorschriften einen wesentlichen Teil des Binnenmarktrechts der EU dar.

Die grundlegende Rechtsquelle zur Produktsicherheit in der EU ist die Richtlinie über die allgemeine Produktsicherheit.¹⁷⁷ In den Erwägungsgründen dieser Produktsicherheitsrichtlinie heißt es, dass eine horizontale Harmonisierung der EU-Vorschriften *„zur Festlegung einer allgemeinen Produktsicherheitsanforderung mit Bestimmungen über die allgemeinen Verpflichtungen der Hersteller und Händler“* für die Gewährleistung eines hohen Verbraucherschutzstandards erforderlich ist.¹⁷⁸ Daher dienen die Bestimmungen der Produktsicherheitsrichtlinie ebenfalls dem Verbraucherschutz. Neben den Produktsicherheitsvorschriften gelten in der EU auch ergänzende sektorspezifische Vorschriften, insb. in Bezug auf die Kraftfahrzeuge und Luftfahrzeuge.

Die Produktsicherheitsrichtlinie enthält die Sicherheitsanforderungen an alle Produkte, die sicherstellen sollen, dass alle *„in den Verkehr gebrachten Produkte sicher sind“*¹⁷⁹. Unter diesem Begriff iSd Produktsicherheitsrichtlinie versteht man *„jedes Produkt, das - auch im Rahmen der Erbringung einer Dienstleistung - für Verbraucher bestimmt ist oder unter vernünftigerweise vorhersehbaren Bedingungen von Verbrauchern benutzt werden könnte, selbst wenn es nicht für diese bestimmt ist, und entgeltlich oder unentgeltlich im Rahmen einer Geschäftstätigkeit geliefert oder zur Verfügung gestellt wird, unabhängig davon, ob es neu, gebraucht oder wiederaufgearbeitet ist“*¹⁸⁰ (allerdings mit Ausnahme gebrauchter Produkte). Die Produktsicherheitsrichtlinie findet allerdings auf Dienstleistungen keine Anwendung, *„aber zur Erreichung der angestrebten Schutzziele sollte sie auch für Produkte gelten, die den Verbrauchern im Rahmen einer Dienstleistung geliefert oder zur Verfügung gestellt werden, um von ihnen benutzt zu werden“*.¹⁸¹

Die Produktsicherheitsvorschriften finden gleichfalls eine Anwendung auf Produkte, die KI bzw. KI-Systeme enthalten. Nach Auffassung der Europäischen Kommission *„sollten KI-Systeme konzeptuell integrierte Schutz- und Sicherheitsvorkehrungen aufweisen, damit sie in jeder Phase nachprüfbar sicher sind, wobei es auf die körperliche und geistige Sicherheit aller Beteiligten ankommt“*.¹⁸² Allerdings in Anbetracht der oben erwähnten technischen

¹⁷⁷ Ebenda

¹⁷⁸ Ebenda, Erwägungsgrund 4

¹⁷⁹ Ebenda, Art. 1 Abs. 1

¹⁸⁰ Ebenda, Art. 2, Punkt a)

¹⁸¹ Ebenda, Erwägungsgrund 9

¹⁸² COM (2019) 168 endgültig, S. 5-6

Eigenschaften sind die bestehenden Produktsicherheitsvorschriften meistens nicht geeignet, die KI-Systeme zu behandeln. Vor diesem Hintergrund hat der EU-Gesetzgeber mehrere Versuche unternommen, die Sicherheitsanforderungen an KI-Produkten und deren Marktaufsicht zu regeln.

2.5.1. Bericht über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung COM (2020) 64 endgültig (Europäische Kommission)

In dem schon erwähnten „Bericht über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung“ stellte die Europäische Kommission ihre Empfehlung zu den Modalitäten der Anpassung der bestehenden Produktsicherheitsvorschriften der EU dar, wobei die Herausforderungen bzw. Risiken des KI-Einsatzes berücksichtigt sind:

- 1) Konnektivität: Diese Eigenschaft stellt eine große Herausforderung für die traditionelle Haftungsmodelle dar, *„da sie die Sicherheit des Produkts direkt beeinträchtigen und, sofern das Produkt gehackt werden kann, indirekt zu Sicherheitsbedrohungen führen und sich auf die Sicherheit der Nutzer auswirken kann“*.¹⁸³ Daher empfiehlt die Europäische Kommission explizite Vorschriften wie einer expliziten Bewertung der Risiken anzunehmen, die sich aus der Interkonnektivität ergeben, um einen besseren Schutz der Nutzer und mehr Rechtssicherheit zu gewährleisten;
- 2) Autonomie: Unbeabsichtigte Ergebnisse der Anwendung der KI-Systeme können Benutzern und anderen betroffenen Personen Schaden zufügen. Daher *„könnte ein neues Risikobewertungsverfahren für Produkte eingeführt werden, bei denen es während ihrer Lebensdauer zu erheblichen Änderungen kommt“*.¹⁸⁴ Darüber hinaus sollten spezifische Anforderungen festgelegt werden, um die menschliche Kontrolle über KI-Systeme zu gewährleisten, beginnend mit ihrer Gestaltung während ihres gesamten Lebenszyklus;
- 3) Psychische Gesundheitsrisiken: Der Begriff „Gesundheit“ umfasst auch das geistige Wohlbefinden. Der Hersteller der KI-gestützten Systeme sollte daher verpflichtet werden, insb. *„den immateriellen Schaden zu berücksichtigen, den ihre Produkte vor*

¹⁸³ COM (2020) 64 endgültig, S. 6

¹⁸⁴ Ebenda, S. 9

allem bei schutzbedürftigen Nutzern wie älteren, in Pflege befindlichen Menschen verursachen könnten“¹⁸⁵;

- 4) Datenabhängigkeit: Sicherheitsrisiken können sich aus der fehlerhaften Verarbeitung von Daten eines Produkts ergeben, einschließlich mangelnder Genauigkeit oder Relevanz. Da die bestehenden Produktsicherheitsvorschriften der EU nicht ausdrücklich auf die Sicherheitsrisiken eingegangen sind, die sich aus fehlerhaften Daten ergeben¹⁸⁶, sollten sie entsprechend ergänzt bzw. angepasst werden, um die derartigen Risiken zu berücksichtigen;
- 5) Opazität: In Bezug auf den „Black-Box-Effekt“ der KI-Systeme stellte die Europäische Kommission eine mögliche neue Herausforderung für Ex-post-Durchsetzungsmechanismen für die Produktsicherheit fest, die nicht durch bestehende Rechtsvorschriften abgedeckt ist. Daher sollen die Transparenzanforderungen für die KI-Systeme an Rechenschaftspflicht und menschliche Kontrolle der ADM-Systeme zu berücksichtigen.¹⁸⁷ Nach der Auffassung der Europäischen Kommission könnte eine Möglichkeit zur Bewältigung dieser Herausforderung darin bestehen, *„die Entwickler der Algorithmen dazu zu verpflichten, bei Unfällen die Konstruktionsparameter und die Metadaten von Datensätzen offenzulegen“¹⁸⁸;*
- 6) Komplexe Wertschöpfung: Die EU-Produktsicherheitsvorschriften auferlegen den Wirtschaftsakteuren mehrere Verpflichtungen nach dem Grundsatz der „geteilten Verantwortung“. Die geeigneten Bestimmungen sind zu verabschieden, die speziell die Zusammenarbeit zwischen Wirtschaftsteilnehmern und den Verbrauchern fordern. So sollte jeder Wirtschaftsteilnehmer in der Wertschöpfungskette, der die Sicherheit des Produkts beeinflusst, Verantwortung übernehmen und dem nächsten Akteur in der Kette die erforderlichen Informationen und Maßnahmen zur Verfügung stellen.¹⁸⁹

2.5.1. Produktsicherheit für automatisierte Fahrzeuge

Die Technologie automatisierter Fahrzeuge ist überaus eng mit KI-Systemen verbunden. Die EU investiert seit langem in Forschungsprojekte, die zur Entwicklung des automatisierten Fahrens beitragen. Eine Reihe von EU-Mitgliedstaaten hat sich bereits für das automatisierte Fahren geöffnet, um sowohl Testen neuer Fahrzeuge als auch deren Inbetriebnahme zu

¹⁸⁵ Ebenda, S. 10

¹⁸⁶ Ebenda

¹⁸⁷ Ebenda, S. 11

¹⁸⁸ Ebenda

¹⁸⁹ vgl. Ebenda, S. 14

ermöglichen¹⁹⁰, wobei EU bereits über Regulierungsvorschläge verfügt. 2016 veröffentlichte die Europäische Kommission eine Mitteilung über Strategie für Kooperative Intelligente Verkehrssysteme¹⁹¹, in der unter anderem die Festlegung der Vorschriften zur Sicherheit automatisierter Fahrzeuge und der Interoperabilitätsvorschriften vorgeschlagen wurde.¹⁹² Am 17. Mai 2018 veröffentlichte die Europäische Kommission eine Mitteilung zur vernetzten und automatisierten Mobilität¹⁹³, in der eine europäische Strategie zu diesem Thema dargelegt ist, wobei Binnenmarktansatz einzuhalten ist, „um ein Mindestmaß an Harmonisierung und Interoperabilität zu gewährleisten und Rechtssicherheit zu garantieren“.¹⁹⁴

Die Europäische Kommission legte am 17. Mai 2018 den Vorschlag für Richtlinie zur Änderung der Richtlinie 2008/96/EG über das Sicherheitsmanagement der Straßeninfrastruktur¹⁹⁵ vor. Das Ziel dieser Initiative besteht darin, „die Zahl der Verkehrstoten und Schwerverletzten im EU-Straßennetz zu verringern, indem das Sicherheitsniveau der Straßeninfrastrukturen verbessert wird“.¹⁹⁶ Unter anderem sollten die Systeme der Farbenmarkierungen und Verkehrszeichen eingeführt werden, die das reibungslose und sichere Funktionieren der Fahrerassistenzsysteme neben den menschlichen Fahrern ermöglichen.¹⁹⁷ Zur Verankerung der in Frage stehenden Änderungen wurde Richtlinie (EU) 2019/1936 angenommen.¹⁹⁸

¹⁹⁰ European Transport Safety Council, *Prioritising the Safety Potential of Automated Driving in Europe* (2016), abrufbar unter https://etsc.eu/wp-content/uploads/2016_automated_driving_briefing_final.pdf, letzter Zugriff am 30.07.2020

¹⁹¹ Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Eine europäische Strategie für Kooperative Intelligente Verkehrssysteme – ein Meilenstein auf dem Weg zu einer kooperativen, vernetzten und automatisierten Mobilität“ COM (2016) 766 endgültig, abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52016DC0766&from=DE>, letzter Zugriff am 25.07.2020

¹⁹² Ebenda, S. 13

¹⁹³ Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Europa in Bewegung. Nachhaltige Mobilität für Europa: sicher, vernetzt und umweltfreundlich“ COM (2018) 293 endgültig, abrufbar unter https://eur-lex.europa.eu/resource.html?uri=cellar:0e8b694e-59b5-11e8-ab41-01aa75ed71a1.0001.02/DOC_1&format=PDF, letzter Zugriff am 25.07.2020

¹⁹⁴ Ebenda, S. 8

¹⁹⁵ Europäische Kommission, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2008/96/EG über ein Sicherheitsmanagement für die Straßenverkehrsinfrastruktur COM (2018) 274 endgültig, abrufbar unter <https://ec.europa.eu/transparency/regdoc/rep/1/2018/DE/COM-2018-274-F1-DE-MAIN-PART-1.PDF>, letzter Zugriff am 26.07.2020

¹⁹⁶ Ebenda, S. 2

¹⁹⁷ Ebenda, S. 14

¹⁹⁸ Richtlinie (EU) 2019/1936 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zur Änderung der Richtlinie 2008/96/EG über ein Sicherheitsmanagement für die Straßenverkehrsinfrastruktur [2019] ABl L 305/1

Die neue überarbeitete allgemeine Sicherheitsverordnung der EU¹⁹⁹ enthält unter anderem auch spezifische Anforderungen an automatisierte Fahrzeuge und vollautomatisierte Fahrzeuge. Insbesondere sollten sie mit folgenden Systemen bzw. Geräten zusätzlich ausgerüstet werden:

- 1) Systeme zum Ersatz der Kontrolle des Fahrers über Fahrzeug (Signaleinrichtungen);
- 2) Überwachungssysteme des Zustands des Fahrzeugs und der Umgebung;
- 3) Überwachungssysteme der Fahrerverfügbarkeit;
- 4) ereignisbezogene Datenaufzeichnung;
- 5) harmonisiertes Format für den Austausch von Daten;
- 6) Systeme zur Weitergabe von Sicherheitsinformationen an Verkehrsteilnehmer.²⁰⁰

2.5.2. Initiativen zur Marktüberwachung

Die effektive Durchsetzung der EU-Produktsicherheitsvorschriften benötigt ein Vorhandensein eines wirksamen Marktüberwachungssystems, das europaweit einheitlich Anwendung findet. Eine Marktüberwachung soll sicherstellen, *„dass die Produkte den Anforderungen der geltenden Harmonisierungsrechtsvorschriften der Union genügen und das in jenen Rechtsvorschriften erfasste öffentliche Interesse geschützt wird“*.²⁰¹ Zu diesem Zeitpunkt gibt es in der EU einige Versuche zur Feststellung der Notwendigkeit, bestehendes Marktüberwachungssystem in Hinblick auf KI-Anwendung anzupassen.

Am 5. September 2018 veröffentlichten ESAs (European Supervision Authorities (Europäische Aufsichtsbehörde) einen gemeinsamen Bericht über die Ergebnisse der Überwachung zum Thema „Automatisierung in der Finanzberatung“.²⁰² In diesem Bericht wurde festgestellt, dass

¹⁹⁹ Verordnung (EU) 2019/2144 des Europäischen Parlaments und des Rates vom 27. November 2019 über die Typgenehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge im Hinblick auf ihre allgemeine Sicherheit und den Schutz der Fahrzeuginsassen und von ungeschützten Verkehrsteilnehmern, zur Änderung der Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates und zur Aufhebung der Verordnungen (EG) Nr. 78/2009, (EG) Nr. 79/2009 und (EG) Nr. 661/2009 des Europäischen Parlaments und des Rates sowie der Verordnungen (EG) Nr. 631/2009, (EU) Nr. 406/2010, (EU) Nr. 672/2010, (EU) Nr. 1003/2010, (EU) Nr. 1005/2010, (EU) Nr. 1008/2010, (EU) Nr. 1009/2010, (EU) Nr. 19/2011, (EU) Nr. 109/2011, (EU) Nr. 458/2011, (EU) Nr. 65/2012, (EU) Nr. 130/2012, (EU) Nr. 347/2012, (EU) Nr. 351/2012, (EU) Nr. 1230/2012 und (EU) 2015/166 der Kommission [2019] ABl L 325/1

²⁰⁰ Ebenda, Art. 11, Abs. 1

²⁰¹ Verordnung (EU) 2019/1020 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über Marktüberwachung und die Konformität von Produkten sowie zur Änderung der Richtlinie 2004/42/EG und der Verordnungen (EG) Nr. 765/2008 und (EU) Nr. 305/2011 [2019] ABl L 169/1, Art. 3, Abs. 3

²⁰² Joint Committee of the European Supervisory Authorities, Joint Committee Report on the results of the monitoring exercise on “automation in financial advice”, JC 2018-29, abrufbar unter https://esas-joint-committee.europa.eu/Publications/Reports/JC_2018_29_-_JC_Report_on_automation_in_financial_advice.pdf, letzter Zugriff am 01.06.2020

keine sofortigen Maßnahmen erforderlich sind, da derzeit nur eine begrenzte Anzahl von Unternehmen an der Automatisierung der Finanzberatung beteiligt ist und die identifizierten Risiken nicht eingetreten sind. Die ESAs planen allerdings, eine neue Überwachungsmaßnahme durchzuführen, wenn die Entwicklung auf dem Markt dies erfordert.²⁰³

Allerdings warf Europäische Kommission weiter nochmals die Frage zur Notwendigkeit der KI-Marktüberwachung auf. Im Weissbuch „Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen“ geht die Europäische Kommission in Bezug auf die Schaffung der vertrauenswürdig und sicheren KI davon aus, dass *„die geltenden rechtlichen Anforderungen in der Praxis eingehalten und sowohl von den zuständigen nationalen und europäischen Behörden als auch von den betroffenen Parteien wirksam durchgesetzt werden müssen. Die zuständigen Behörden sollten in der Lage sein, Einzelfälle zu untersuchen, aber auch die Auswirkungen auf die Gesellschaft zu bewerten“*.²⁰⁴

Die EU verfügt bereits über Mechanismus für die Durchsetzung des Verbraucherschutzgesetzes sowohl auf EU-Ebene als auch auf Eben der einzelnen Mitgliedsstaaten. In Übereinstimmung mit der Verordnung über die Zusammenarbeit im Verbraucherschutz²⁰⁵ erfolgt die Zusammenarbeit zwischen den für die Durchsetzung der Verbraucherschutzgesetze zuständigen nationalen Behörden in Form eines Netzes für die Zusammenarbeit im Verbraucherschutz.²⁰⁶

Nach der Auffassung der Europäischen Kommission ist eine objektive, vorab vorzunehmende Konformitätsbewertung für KI-Anwendungen mit hohem Risiko für Leben und Gesundheit der Verbraucher erforderlich, um sicherzustellen, *„dass bestimmte der genannten obligatorischen Auflagen für Anwendungen mit hohem Risiko erfüllt sind“*²⁰⁷, die Zertifizierungen und die Inspektionen umfassen beinhalten könnten. Ein solches System sollte auf die Verordnung zur Cybersicherheit²⁰⁸ gestützt werden und technische Merkmale der KI-Systeme berücksichtigen.

²⁰³ Ebenda, S. 4

²⁰⁴ COM (2020) 65 endgültig, S. 27

²⁰⁵ Verordnung (EU) 2017/2394 des Europäischen Parlaments und des Rates vom 12. Dezember 2017 über die Zusammenarbeit zwischen den für die Durchsetzung der Verbraucherschutzgesetze zuständigen nationalen Behörden und zur Aufhebung der Verordnung (EG) Nr. 2006/2004 [2017] ABl L 345/1

²⁰⁶ vgl. Ebenda, Erwägungsgrund 45

²⁰⁷ COM (2020) 65 endgültig, S. 27

²⁰⁸ Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 [2019] ABl L 151/15

Die Konformitätsbewertungen für KI-Anwendungen mit hohem Risiko sollten zum Teil der bestehenden Konformitätsbewertungsmechanismen für die Produkte werden, die in Verkehr EU-weit gebracht werden. Falls es nicht der Fall sein kann, sollten andere geeignete Mechanismen geschaffen werden, die sich auf bewährte Verfahren und Einbeziehung der Europäischen Normungsorganisationen stützen. Zugrunde neuer Systeme sollten objektive, verhältnismäßige und transparente Kriterien liegen.²⁰⁹ Bei der Schaffung der vorab vorzunehmenden Konformitätsbewertungen sollten insb. folgende Aspekte berücksichtigt werden:

- 1) Mögliche weitere Anpassung der Konformitätsanforderungen, falls sie für Überprüfung bei einer vorab vorzunehmenden Konformitätsbewertung nicht geeignet sind;
- 2) Fähigkeit der KI-Systeme wie Maschinelles Lernen und künstliche neuronale Netzwerke zur selbständigen Weiterentwicklung, die mehrere Bewertungen während deren Funktionsdauer erfordert;
- 3) Notwendigkeit der Überprüfung der Trainingsdaten und der verwendeten technischen Methoden bzw. Techniken;
- 4) Notwendigkeit zum Nachtrainieren der KI-Systeme, falls die Nichteinhaltung der Anforderung bei der Konformitätsbewertung festgestellt ist.²¹⁰

²⁰⁹ COM (2020) 65 endgültig, S. 27-28

²¹⁰ vgl. Ebenda, S. 28

Kapitel 3: Initiativen in den USA

3.1. Überblick der bestehenden Initiativen zur Regulierung der KI in den USA

Eine politische Zielsetzung der USA besteht auch in der Aufrechterhaltung und der Stärkung der wissenschaftlichen, technologischen und wirtschaftlichen Führungsposition auf dem Gebiet der KI. Allerdings erfordert die Aufrechterhaltung solcher Führungsrolle in der KI auch *„den Schutz der amerikanischen Technologie, der wirtschaftlichen und nationalen Sicherheit, der bürgerlichen Freiheiten, der Privatsphäre und der amerikanischen Werte sowie Verbesserung der internationalen und industriellen Zusammenarbeit mit ausländischen Partnern und Verbündeten“*.²¹¹

Diese Absicht wurde in der Anordnung des US-Präsidenten Nr. 13859 von 11 Februar 2019 „Aufrechterhaltung der amerikanischen Führungsrolle in der KI“ (Maintaining American Leadership in Artificial Intelligence) dargestellt. Diese Anordnung ruft unter anderem auch auf, die Leitlinien für Regulierung der KI-Technologien und geeignete Standards für KI-Systeme festzulegen. Derartige Leitlinien sollten unter anderem regulatorische und nicht regulatorische Ansätze in Bezug auf Technologien und Industriesektoren beinhalten, die entweder durch KI befähigt oder ermöglicht werden.²¹² Die Regulierung der KI auf Bundesebene unter dem Präsidenten Trump ist durch Bevorzugung eines Ansatzes zur Feststellung der Leitlinien und Standards gegenüber Festlegung der rechtsverbindlichen Regelungen durch zuständige Behörden gekennzeichnet.²¹³

3.1.1. Jüngste Initiativen auf Bundesebene

Kurz nach dieser Anordnung führte das Repräsentantenhaus am 27. Februar 2019 die Entschließung Nr. 153 zur Unterstützung der Entwicklung von Leitlinien für die ethische Entwicklung der KI ein. Mit dieser Entschließung sollte ein Ausgleich zwischen der Förderung des *„Potenzials der KI zur Verbesserung des Wohlbefindens, der Förderung des*

²¹¹Executive Order No. 13859, 84 FR 3967 (February 11, 2019), abrufbar unter <https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence>, letzter Zugriff am 20.06.2020, Abschnitt 1

²¹² Ebenda, Section 6

²¹³ vgl. Brian Higgins, ‘Government Plans to Issue Technical Standards for Artificial Intelligence Technologies’ (2019) Artificial Intelligence Technology and the Law, abrufbar unter <http://aitechnologylaw.com/2019/02/government-plans-to-issue-technical-standards-governing-artificial-intelligence-technologies/>, letzter Zugriff am 30.07.2020

*Wirtschaftswachstums und der Verbesserung der Pflege und Dienstleistungen für viele Menschen*²¹⁴ und der Notwendigkeit einer „sicheren, verantwortungsvollen und demokratischen Entwicklung“²¹⁵ hergestellt werden.

Die Entschließung bietet zehn Ziele, um dieses Gleichgewicht zu erreichen, einschließlich Transparenz und Erklärbarkeit, Schutz der persönlichen Daten, Rechenschaftspflicht und Kontrolle für alle automatisierten Entscheidungen, Zugang und Fairness in Bezug auf technologische Dienstleistungen und Vorteile sowie Sicherheit und Kontrolle von KI-Systemen jetzt und in der Zukunft.²¹⁶ Obwohl die Entschließung noch nicht angenommen wurde, beinhaltet sie einige der Grundsätze, die für die Entwicklung einer ethischen und vertrauenswürdigen KI von Bedeutung sind, insb. Schutz personenbezogener Daten, Kontrolle über ADM-Systeme, Sicherheit jeweiliger KI-Systeme.

Die jüngste Entwicklung auf diesem Gebiet in den USA ist die Leitlinie des Weißen Hauses für 2020 zur Regulierung der KI-Anwendung (auf Englisch „Guidance for Regulation of Artificial Intelligence Applications“)²¹⁷, die sich an die Leiter der Exekutivagenturen des Bundes richtet. Grundsätzlich zielt sie darauf ab, die Öffentlichkeit einzubeziehen, Doppelarbeit und Redundanz zwischen Behörden zu vermeiden, sowie festzustellen, dass eine einheitliche Regulierung bundesweit nicht zu allen Akteuren der KI-Industrie passt.

Dieses Dokument beinhaltet ebenfalls zehn Prinzipien, die die Behörden bei der Formulierung von den regulatorischen und nicht regulatorischen Ansätzen für die Entwicklung, die Bereitstellung und den Betrieb von AI-Anwendungen zu berücksichtigen haben. Diese Prinzipien und deren Inhalt sind wie folgt dargelegt²¹⁸:

- Öffentliches Vertrauen gegenüber die KI – die staatlichen Behörden haben „zuverlässige, robuste und vertrauenswürdige KI-Anwendungen zu fördern“²¹⁹, wobei keine einschlägige Definition bzw. Erläuterung des Begriffes „vertrauenswürdige KI“ (wie etwa in der EU) angeführt ist;

²¹⁴ H.R., Resolution No. 153, 116th Congress (2019), abrufbar unter <https://www.congress.gov/bill/116th-congress/house-resolution/153/text>, letzter Zugriff am 20.09.2020, Erwägungsgrund 4

²¹⁵ Ebenda, Erwägungsgrund 4

²¹⁶ Ebenda

²¹⁷ The White House, Guidance for Regulation of Artificial Intelligence Applications, abrufbar unter <https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf>, letzter Zugriff am 11.06.2020

²¹⁸ Ebenda, S. 3-6

²¹⁹ Ebenda, S. 3

- Beteiligung der Öffentlichkeit - die Öffentlichkeit sollte die Möglichkeit haben, Informationen bereitzustellen und an allen Phasen des Gesetzgebungsprozesses teilzunehmen;
- Wissenschaftliche Integrität und Informationsqualität;
- Risikobewertung und -management – man muss nur solche Risiken behandeln, die *„die Möglichkeit eines inakzeptablen Schadens oder eines Schadens darstellen, bei dem die erwarteten Kosten höher als der erwartete Nutzen sind“*²²⁰;
- Vorteile und Kosten – man muss *„im Einklang mit dem Gesetz die vollständigen Kosten, den Nutzen und die Verteilungseffekte der Gesellschaft sorgfältig abwägen, bevor die Vorschriften in Bezug auf die Entwicklung und Bereitstellung von KI-Anwendungen verabschiedet werden. Zu diesen Überlegungen gehören die potenziellen Vorteile und Kosten des Einsatzes von KI im Vergleich zu den Systemen, die KI ergänzen oder ersetzen sollen...“*²²¹;
- Flexibilität – *„bei der Erstellung der regulatorischen und nicht regulatorischen Ansätze sollten Agenturen leistungsorientierte und flexible Ansätze verfolgen, die sich an schnelle Änderungen und Aktualisierungen von KI-Anwendungen anpassen können“*²²²;
- Fairness und Nichtdiskriminierung;
- Offenlegung und Transparenz – man muss von zusätzlichen Offenlegungspflichten Abstand nehmen, wenn die derzeitige Regulierung ausreicht;
- Sicherheit und Schutz – *„Agenturen sollten potenzielle Sicherheitsrisiken sowie das Risiko einer möglichen böswilligen Bereitstellung und Verwendung von KI-Anwendungen berücksichtigen“*²²³;
- Koordination bzw. Zusammenarbeit zwischen den Behörden.²²⁴

Außerdem wurde der Entwurf von *Artificial Intelligence Initiative Act* am 21. Mai 2019 im US-Kongress vorgelegt, der in erster Linie auf die Beschleunigung der Forschung und Entwicklung im Bereich KI abzielt.²²⁵ Allerdings sieht er vor, dass der Präsident eine nationale KI-Forschungs- und Entwicklungsinitiative einrichtet, deren Aufgaben die Stärkung von

²²⁰ Ebenda, S. 4

²²¹ Ebenda, S. 5

²²² Ebenda

²²³ Ebenda, S. 6

²²⁴ Ebenda

²²⁵ Artificial Intelligence Initiative Act, S. 1558, 116th Congress (2019)

Forschung und Entwicklung in Bezug auf KI umfassen, indem „*unangemessene Verzerrungen in Datensatzalgorithmen und anderen Aspekten der KI identifiziert und minimiert werden*“.²²⁶

3.1.2. Gesetzliche Definition

Auf dem 115. Kongress wurden 93 Gesetzentwürfe eingeführt, die im Text den Ausdruck „KI“ enthalten, wobei vier dieser Gesetzesvorschläge in Kraft getreten sind.²²⁷ Aus diesem Grund entstand eine berechtigte Notwendigkeit, gesetzliche Definition der KI bzw. KI-Systeme zu geben. Vor diesem Hintergrund wurde dieser Ausdruck „*künstliche Intelligenz*“ („artificial intelligence“) in *John S. McCain National Defense Authorization Act for Fiscal Year 2019*²²⁸ definiert. Diese Definition ist wie folgt dargelegt:

- 1) künstliches System, das die Aufgaben unter verschiedenen und unvorhersehbaren Umständen ohne nennenswerte menschliche Kontrolle ausführt oder aus Erfahrungen lernen und eigene Leistung verbessern kann, wenn es den Datensätzen ausgesetzt ist;
- 2) künstliches System, das in Computersoftware, physischer Hardware oder einem anderen Kontext entwickelt wurde und Aufgaben löst, die eine menschliche Wahrnehmung, Erkenntnis, Planung, Lernen, Kommunikation oder physisches Handeln erfordern;
- 3) künstliches System, das so gestaltet bzw. geeignet ist, wie ein Mensch zu denken bzw. zu handeln, inklusiv kognitive Architekturen und neuronale Netze;
- 4) eine Reihe der Techniken, einschließlich maschinellem Lernen, mit denen eine kognitive Aufgabe angenähert werden soll;
- 5) künstliches System für rationales Handeln, einschließlich eines intelligenten Software-Agenten oder eines verkörperten Roboters, der Ziele durch Wahrnehmung, Planung, Argumentation, Lernen, Kommunikation, Entscheidungsfindung und Handeln erreicht.²²⁹

3.1.3. Rolle einzelner Bundesstaaten

Wenn man über bestehende Rechtsvorschriften im Bereich der KI spricht, sollte man bedenken, dass die USA eine Bundesrepublik ist. Deswegen sind sowohl Bund als auch Bundesstaaten

²²⁶ Ebenda, Paragraph 101(6)(F)

²²⁷ The Law Library of Congress, *Regulation of Artificial Intelligence in Selected Jurisdictions* (2019), abrufbar unter <https://www.loc.gov/law/help/artificial-intelligence/regulation-artificial-intelligence.pdf>, letzter Zugriff am 20.07.2020, S. 27

²²⁸ John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232, § 238, 132 Stat. 1658 (2018), abrufbar unter <https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf>, letzter Zugriff am 20.07.2020

²²⁹ Ebenda, Unterabschnitt (g)

befugt, ihre eigenen Gesetze zu erlassen.²³⁰ Vor diesem Hintergrund sind die Bundesstaaten im Vergleich zu Bund bei der Verabschiedung der KI-Gesetzgebung überaus aktiv. Im Jahre 2011 verabschiedete der Bundesstaat Nevada das erste Gesetz zur Regelung automatisierter Fahrzeuge²³¹. Dieses Gesetz legt unter anderem Anforderungen an Prüfung automatisierter Fahrzeuge fest und fordert die Erlassung der Vorschriften für deren Betrieb auf. 2012 verabschiedete Kalifornien ebenfalls Gesetz zur Regulierung dieses Aspektes²³². Vor diesem Hintergrund werden einige Gesetze der Bundesstaaten weiter kurz dargestellt und erläutert.

3.2. Initiativen zum Schutz der grundlegenden Menschenrechte

Die Menschenrechtsaspekte sind für den US-Gesetzgeber bei der Ausarbeitung der Rechtsvorschriften zur Regulierung der KI-Anwendung in der Geschäftstätigkeit von entscheidender Bedeutung. Allerdings ist der amerikanische Gesetzgeber auf diesem Gebiet nicht so überaus aktiv in Vergleich zur EU. Bis jetzt gibt es auf Bundesebene nur einige Initiativen zum Schutz der personenbezogenen Daten und des Privatlebens bei der Anwendung der KI-Systeme, die noch zu verabschieden sind.

In den USA gibt es noch kein einziges allgemeines Datenschutzgesetz auf Bundesebene. Stattdessen gibt es nur sog. sektorspezifische Regelungen und Gesetzgebungsakte als Reaktion auf bestimmte Vorfälle, wie etwa: *Fair Credit Reporting Act* für Kreditauskunfteien, *Gramm-Leach-Bliley Act* für Finanzinstitutionen, *Video Privacy Protection Act* für Anbieter von Videobanddiensten, *Health Insurance Portability and Accountability Act* für Gesundheitsdienstleister.

Es gibt auch staatliche Behörde, die befugt sind Datenschutzgesetze zu durchsetzen. FTC (Bundeshandelskommission, auf Englisch „Federal Trade Commission“) befasst sich unter anderem auch mit den Fragen zum Schutz personenbezogener Daten der Verbraucher und der Durchsetzung der damit verbundenen Gesetze in den USA. FTC ist grundsätzlich auch befugt, bei der Durchsetzung des Wettbewerbsgesetzes und der Förderung des Verbraucherschutzes als Regulierungsbehörde zu agieren. In den USA ist daher ein Datenschutz als ein Teilgebiet des Verbraucherschutzrechtes anzusehen.

²³⁰ Gemäß Art. 6 Abs. 1 Verfassung der USA sind die Bundesstaaten befugt eigene Gesetze zu verabschieden. Allerdings hat das Bundesrecht einen Vorrang vor den Gesetzen einzelner Bundesstaaten.

²³¹ A.B. 511, 76th Legislature, 2011 Reg. Sess. (Nevada 2011), abrufbar unter https://www.leg.state.nv.us/Session/76th2011/Bills/AB/AB511_EN.pdf, letzter Zugriff am 30.07.2020

²³² S.B. 1298, California State Legislature, 2011-2012 Session (California 2012), abrufbar unter https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201120120SB1298, letzter Zugriff am 31.07.2020

Eine wichtige Initiative im Bereich des Schutzes personenbezogener Daten der Verbraucher ist *Algorithmic Accountability Act*.²³³ Es wurde am 10. April 2019 im Kongress vorgelegt. Ein umstrittenes Thema in Hinblick auf dieses Dokument ist sein persönlicher Anwendungsbereich. *Algorithmic Accountability Act* sollte auf die Kategorien natürlicher bzw. juristischer Personen Anwendung finden, die mindestens eine der folgenden Voraussetzungen erfüllen bzw. den folgenden Gruppen (sogenannte „covered entities“ nach Wortlaut von *Algorithmic Accountability Act*) angehören:

- 1) das jährliche Bruttoeinkommen von mehr als 50 Millionen US-Dollar;
- 2) Besitz oder Kontrolle über personenbezogenen Daten von mehr als 1 Million Verbrauchern oder 1 Million Verbrauchergeräten;
- 3) Gesellschaft, deren Betrieb bzw. Kontrolle durch die Personen ausgeübt sind, die eine der oben genannten Voraussetzungen erfüllen;
- 4) ein Datenbroker oder eine Person, die als wesentlicher Teil ihrer Geschäftstätigkeit personenbezogene Daten über eine Person sammelt, zusammenstellt oder verwaltet, die kein Kunde oder Angestellter dieser Person ist, um solche Informationen zu verkaufen bzw. den Dritten den Zugang zu diese bereitzustellen.²³⁴

Innerhalb von zwei Jahren nach Verabschiedung von *Algorithmic Accountability Act* wird die FTC befugt sein, KI-Technologien zu regulieren, indem die betroffenen Unternehmen verpflichtet werden, eine Folgenabschätzung für bestehende oder neue automatisierte Entscheidungssysteme mit hohem Risiko sowie für neue bzw. bestehende Informationssysteme durchzuführen.²³⁵ Der Entwurf sieht ausdrücklich vor, dass es keinen Vorrang über staatliche Gesetze hat.²³⁶ Stattdessen würde es von der FTC gemäß Paragraf 5 des Entwurfes über die Handelskommission durchgesetzt.

Die Definition eines automatisierten Entscheidungssystems mit hohem Risiko ist weit gefasst und umfasst verschiedene Arten automatisierter Systeme, einschließlich, aber nicht beschränkt, folgender: a) die ein „erhebliches Risiko“ für den Datenschutz oder die Sicherheit einer natürlichen Person darstellen oder zu voreingenommenen bzw. unfairen Entscheidungen führen; b) die Entscheidungen treffen, die sich erheblich auf die Verbraucher auswirken, indem sie Daten zu sog. sensiblen Aspekten (z.B. Arbeitsleistung oder Gesundheit) verwenden; c) die

²³³ Algorithmic Accountability Act of 2019, S. 1108, 116th Congress (2019)

²³⁴ Ebenda, Paragraf 2, Abs. 5

²³⁵ Ebenda, Paragraf 3, Abs. b

²³⁶ Ebenda, Paragraf 4

personenbezogene Daten wie Rasse, politische und religiöse Überzeugungen, Geschlechtsidentität und sexuelle Orientierung sowie genetische Informationen bearbeiten; d) die systematisch einen großen öffentlichen Raum überwachen; e) alle andere, die die von FTC festgestellten Kriterien erfüllen.²³⁷

Die von *Algorithmic Accountability Act* vorgesehene Bewertung der Auswirkungen des automatisierten Entscheidungssystems sollte folgenden Mindeststandard beinhalten:

- 1) eine detaillierte Beschreibung des automatisierten Entscheidungssystems, seines Designs, seiner Schulung, seiner Daten und seines Zwecks;
- 2) eine Bewertung des relativen Vorteils und der Kosten des automatisierten Entscheidungssystems im Hinblick auf seinen Zweck unter Berücksichtigung relevanter Faktoren, wie etwa Praktiken zu Datenminimierung, Zugang der Verbraucher zu den Ergebnissen des automatisierten Entscheidungssystems;
- 3) eine Bewertung der Risiken, die das automatisierte Entscheidungssystem für die Privatsphäre oder Sicherheit personenbezogener Daten von Verbrauchern darstellt, und der Risiken, die das automatisierte Entscheidungssystem zu ungenauen, unfairen, voreingenommenen oder diskriminierenden Entscheidungen führen oder dazu beitragen kann, die sich auf die Verbraucher auswirken;
- 4) die Maßnahmen zur Minimierung der oben beschriebenen Risiken, einschließlich technologischer und physischer Schutzvorkehrungen.²³⁸

Diese Gesetzgebungsinitiative soll die Aufsicht des Bundes über KI und Datenschutz verbessern und ähnelt in gewisser Hinsicht der europäischen DSGVO. Allerdings hat sie wenige Chancen, durch den Kongress verabschiedet zu werden. Unabhängig davon erregen die vorgeschlagenen Bundesgesetze häufig die Aufmerksamkeit der Gesetzgeber in einem oder mehreren Bundesstaaten und spornt ähnliche Vorschläge auf Bundesstaatenebene an.²³⁹ In diesem Fall ist es jedoch passiert.

Am 20. Mai 2019 verabschiedete Bundesstaat New Jersey ein ähnliches Gesetz mit der Überschrift *New Jersey Algorithmic Accountability Act*.²⁴⁰ Wie *Algorithmic Accountability Act*

²³⁷ Ebenda, Paragraph 2, Abs. 7

²³⁸ Ebenda, Paragraph 2, Abs. 2

²³⁹ Jennifer Betts, Keeping an Eye on Artificial Intelligence Regulation and Legislation (*Ogletree Deakins*, 14 June 2019), abrufbar unter <https://ogletree.com/insights/keeping-an-eye-on-artificial-intelligence-regulation-and-legislation/>, letzter Zugriff am 29.09.2020

²⁴⁰ New Jersey Algorithmic Accountability Act, A.B. 5430, 218th Legislature, 2019 Reg. Sess. (N.J. 2019)

auf Bundesebene verlangt dieser Gesetzentwurf, dass die betroffenen Unternehmen Folgenabschätzungen für automatisierte Entscheidungssysteme und Informationssysteme mit hohem Risiko durchführen.²⁴¹ Die „automatisierte Folgenabschätzung des Entscheidungssystems“ erfordert eine Bewertung des Entwicklungsprozesses des Systems, einschließlich der Entwurfs- und Schulungsdaten, hinsichtlich der Auswirkungen auf „Genauigkeit, Fairness, Voreingenommenheit, Diskriminierung, Datenschutz und Sicherheit“ und muss eine detaillierte Beschreibung des Systems und eine Kosten-Vorteile-Analyse enthalten.²⁴²

Im Gegensatz zu der EU verfügt der US-Gesetzgeber bereits über die gesetzliche Initiative zur Regulierung der Gesichtserkennungstechnologien. Die Hauptinitiative zur Regulierung in dieser Hinsicht auf Bundesebene ist *Commercial Facial Recognition Privacy Act*²⁴³, das am 14. März 2019 im Senat vorgelegt wurde, um den Verbraucherschutz zu gewährleisten. Im Falle eines Inkrafttretens würde der Gesetzentwurf den betroffenen Unternehmen generell verbieten, die Gesichtserkennungstechnologie zur Erfassung der Gesichtserkennungsdaten von Endbenutzern zu verwenden, ohne für sie zu benachrichtigen und ihre Zustimmung zu bekommen.²⁴⁴

Dieser Gesetzgebungsakt sollte jede Person betreffen, einschließlich verbundener Unternehmen, die Gesichtserkennungsdaten sammelt, speichert oder verarbeitet, unter Ausnahme der Bundesregierung oder eines Staates bzw. einer lokalen Regierung, einer Strafverfolgungsbehörde, einer nationalen Sicherheitsbehörde oder eines Geheimdienstes.²⁴⁵ Die Gesichtserkennungsdaten sind an persönliche Informationen gebunden (dh. „eindeutige persönliche Identifizierung“), aber können auch pseudonymisierte Informationen enthalten („einer eindeutigen, dauerhaften Kennung“ zugewiesen ist).²⁴⁶

Allerdings sollte dieses Gesetz auch der Verhütung der Diskriminierung dienen. Eine Verwendung der Technologie zur Diskriminierung der Verbraucher, zur erneuten Verwendung der Gesichtsdaten oder zur Weitergabe dieser Daten an Dritte ohne weitere Zustimmung der Endbenutzer ist nach diesem Gesetz verboten.²⁴⁷ Die betroffenen Unternehmen dürfen die

²⁴¹ Ebenda, Paragraph 3

²⁴² Ebenda, Paragraph 2

²⁴³ Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Congress (2019)

²⁴⁴ Ebenda, Paragraph 3, Abs. a (1) (A)

²⁴⁵ Ebenda, Paragraph 2, Abs. 3

²⁴⁶ vgl. Ebenda, Paragraph 2, Abs. 6

²⁴⁷ Ebenda, Paragraph 3, Abs. a

Anwendung einer Technologie durch einen Verbraucher von seiner Zustimmung zum Verzicht auf Datenschutzrechte abhängig zu machen, wenn der Einsatz der Gesichtserkennungstechnologie für solche Anwendung nicht erforderlich ist.²⁴⁸ Darüber hinaus müssen die betroffenen Unternehmen eine menschliche Überprüfung durchführen, bevor sie eine endgültige Entscheidung auf der Grundlage der Ergebnisse der Technologie treffen, wenn dies zu einem vernünftigerweise vorhersehbaren Schaden führen oder für einen vernünftigen Endbenutzer „äußerst anstößig“ sein kann.²⁴⁹

Commercial Facial Recognition Privacy Act enthält jedoch eine Reihe der Ausnahmen:

- 1) Sog. „Sicherheitsanwendungen“, die eine KI-Technologie zur Verlustprävention oder zur Aufdeckung oder Verhinderung krimineller Aktivitäten verwenden²⁵⁰;
- 2) Produkt oder Dienstleistung zur Verwaltung personenbezogener Daten oder zum Sortieren oder Speichern von Fotos oder Videos, wenn die Gesichtserkennungstechnologie nicht zur eindeutigen persönlichen Identifizierung einer bestimmten Person verwendet wird;
- 3) bei Identifizierung der Persönlichkeiten des öffentlichen Lebens für journalistische Medien, die für das öffentliche Interesse erstellt wurden;
- 4) Identifizierung der Persönlichkeiten des öffentlichen Lebens in urheberrechtlich geschütztem Material für den Kinostart;
- 5) Verwendung bei einem Notfall, wenn eine unmittelbare Gefahr oder das Risiko des Todes oder einer schweren Körperverletzung vorliegt.²⁵¹

Ein wesentlicher Fortschritt im Schutz des Arbeitnehmers bei dem KI-Einsatz im Bewerbungsprozess ist *Artificial Intelligence Video Interview Act*²⁵², das im Bundesstaat Illinois am 9. August 2019 verabschiedet wurde und im Januar 2020 in Kraft trat. Das Gesetz beschränkt auch die Weitergabe der Videos - nur „mit Personen, deren Fachwissen bzw. Technologie erforderlich ist, um die Eignung eines Bewerbers für eine Position zu bewerten“ - und fordert eine Löschung der Interviewaufzeichnungen innerhalb von 30 Tagen nach Eingang

²⁴⁸ Ebenda, Paragraph 3, Abs. b (3)

²⁴⁹ Ebenda, Paragraph 3, Abs. c

²⁵⁰ Ebenda, Paragraph 3, Abs. e (2)

²⁵¹ Ebenda, Paragraph 3, Abs. e (1)

²⁵² Artificial Intelligence Video Interview Act, H.B. 2557, 101st General Assembly, 2019 Reg. Sess., Public Act 101-0260 (Illinois 2019)

einer Anfrage von solchem Bewerber.²⁵³ Nach diesem Gesetz kann der Arbeitgeber die KI-Systeme bei Videointerview des Bewerbers nur unter solchen Bedingungen einsetzen:

- 1) Ein Bewerber wird vor dem Interview darüber informiert, dass AI zur Analyse des Videointerviews verwendet werden kann;
- 2) Ein Bewerber erhält Informationen zur Funktionsweise der angewandten KI-Systeme;
- 3) Ein Vorliegen der ausdrücklichen Zustimmung eines Bewerbers für dessen Bewertung durch KI-Systeme, die vor dem Interview gegeben wurde.²⁵⁴

Andere prominente Initiative zum Schutz der Menschenrechte und des Privatlebens beim Einsatz der KI-Technologien ist sog. *Bolstering Online Transparency* (auch als „B.O.T.“ bekannt)²⁵⁵ im Bundesstaat Kalifornien, das California Business & Professional Code ergänzt. Dieses Gesetz verbietet grundsätzlich die Verwendung von *„einem Bot zur Kommunikation oder Interaktion mit einer anderen Person in Kalifornien, um die andere Person über ihre künstliche Identität irrezuführen“*, falls der Verarbeiter kommerzielle oder politische Zwecke verfolgt. Allerdings haftet eine Person nicht, wenn sie explizit eine Angabe an eine betroffene Person erstellt, dass sie ein Bot verwendet.²⁵⁶ Eine derartige Angabe muss *„klar, auffällig und angemessen gestaltet sein, um betroffene Personen entsprechend zu informieren“*.²⁵⁷

Nach Wortlaut dieses Gesetzes versteht man unter Bot *„ein automatisiertes Online-Konto, bei dem alle oder im Wesentlichen alle Aktionen oder Beiträge dieses Kontos nicht das Ergebnis einer Person sind“*.²⁵⁸ Außerdem findet dieses Gesetz eine Anwendung nur auf Bot-Kommunikationen, die über öffentlich zugängliche Internet-Websites, Webanwendungen und digitale Anwendungen, einschließlich sozialer Netzwerke oder Veröffentlichungen, bereitgestellt werden²⁵⁹, und sieht ferner ausdrücklich vor, dass *„Diensteanbietern von Online-Plattformen“* keine Pflicht auferlegt wird.²⁶⁰

3.3. Initiativen zur Haftung

In der oben erwähnten Leitlinie des Weißen Hauses für 2020 zur Regulierung der KI-Anwendung wurde unter anderem erwähnt, *„wobei das breitere rechtliche Umfeld bereits für*

²⁵³ Ebenda, Paragrafe 10 und 15

²⁵⁴ Ebenda, Paragraf 5

²⁵⁵ S.B. 1001, California State Legislature, 2017-2018 Session (California 2018)

²⁵⁶ California Business and Professions Code, Paragraph 17941, Abs. a

²⁵⁷ Ebenda, Paragraf 17941, Abs. b

²⁵⁸ Ebenda, Paragraf 17940, Abs. a

²⁵⁹ Ebenda, Paragraf 17941, Abs. b

²⁶⁰ Ebenda, Paragraf 17941, Abs. c

KI-Systeme gilt, kann die Anwendung des bestehenden Rechtsrahmens auf Fragen der Verantwortung und Haftung für Entscheidungen der KI in einigen Fällen unklar sein, was dazu führt, dass Agenturen im Einklang mit ihren Behörden die Vorteile, Kosten und Verteilungseffekte im Zusammenhang mit einer identifizierten oder erwarteten Methode zur Rechenschaftspflicht bewerten müssen“.²⁶¹ Allerdings ist eine umfassende Analyse der Geeignetheit der bestehenden Haftungsmodelle in Bezug auf die durch KI verursachten Schäden (wie etwa die oben bereits betrachteten Initiativen der EU zu diesem Thema) noch nicht durchgeführt.

Derzeit bestehen noch wenige Initiativen in einzelnen Bundesstaaten und Bereichen. Ein Beispiel der Initiative zur Regulierung der Produkthaftung für KI-Systeme gegenüber Verbraucher ist das Gesetz des Bundesstaates Kalifornien *Anti-Eavesdropping Act*.²⁶² Nach dem Inkrafttreten würde dieses Gesetz den Herstellern von intelligenten Lautsprechern verbieten, Geräte zu installieren, ohne den Benutzer „ständig“ zu informieren.²⁶³ Es sollte ferner verbieten, dass Transkriptionen, die „als persönliche Informationen gelten oder nicht identifiziert werden“, für Werbezwecke verwendet, an Dritte weitergegeben bzw. verkauft oder ohne die Zustimmung des Benutzers aufbewahrt werden. Außerdem beinhaltet dieses Gesetz ebenfalls die Vorschriften zur Haftung des Herstellers.²⁶⁴

Die Haftung des Herstellers ist nur auf solche Funktionen beschränkt, „die zum Zeitpunkt des ursprünglichen Verkaufs eines angeschlossenen Fernsehgeräts oder eines Smart-Speaker-Geräts bereitgestellt wurden“.²⁶⁵ Allerdings haftet der Hersteller nicht für die Funktionen, die von Anwendungen bereitgestellt wurden, die der Benutzer in der Cloud verwenden möchte oder die von einem Benutzer heruntergeladen bzw. installiert wurden.²⁶⁶

Was die durch automatisierte Fahrzeuge verursachten Schäden angeht, befreit die Einhaltung des Bundessicherheitsstandards eine Person von der Haftung für Schäden nach allgemeinem Recht nicht.²⁶⁷ Allerdings würde der Bundesstandard den Vorrang haben, falls die Wirkung eines staatlichen Deliktsanspruchs darin bestehen würde, einem Kraftfahrzeug- oder

²⁶¹ The White House, Guidance for Regulation of Artificial Intelligence Applications, abrufbar unter <https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf>, letzter Zugriff am 11.06.2020, S. 4-5

²⁶² Anti-Eavesdropping Act, A.B. 1395, California State Legislature, 2019 Reg. Sess. (California 2019)

²⁶³ Ebenda, Paragraph 3, Abs. 22948.20. (a)

²⁶⁴ Ebenda, Paragraph 3, Abs. 22948.20. (b)

²⁶⁵ Ebenda, Paragraph 3

²⁶⁶ Ebenda, Paragraph 3

²⁶⁷ 49 United States Code, Paragraph 30103 (2011)

Ausrüstungshersteller einen Leistungsstandard aufzuerlegen, der nicht mit dem Bundesstandard vereinbar ist.²⁶⁸

Gegenwärtig verfügen die meisten US-Bundesstaaten über sowohl Deliktshaftungsgesetze, die Fahrer für die von ihnen verursachten Unfälle verantwortlich machen, als auch Gesetze zur Produkthaftung, gemäß denen die Haftung der Hersteller für etwaige Mängel an ihren Produkten eingeführt ist.²⁶⁹ Allerdings beinhalten die Gesetze einzelner Bundesstaaten manchmal ebenfalls die Sonderregelung für die Haftung in Zusammenhang mit den automatisierten Fahrzeugen. Beispielsweise, gemäß der Gesetzgebung von Bundesstaat Michigan zu den automatisierten Fahrzeugen haftet der Hersteller eines Fahrzeuges nicht und wird von jeglichen Klagen wegen angeblicher Schäden abgewiesen, die sich aus der Umwandlung des Fahrzeugs in ein automatisiertes Kraftfahrzeug durch eine andere Person ergeben.²⁷⁰

3.4. Initiativen zur Produktsicherheit

Durch die Anordnung des US-Präsidenten Nr. 13859 von 11 Februar 2019 „Aufrechterhaltung der amerikanischen Führung in der KI“ wurde National Institute of Standards and Technology (NIST, auf Deutsch „Nationales Institut für Standards und Technologie“) des US-Handelsministeriums mit der Herausgabe eines Plans für das Engagement des Bundes bei der Entwicklung technischer Standards und zugehöriger Tools zur Unterstützung *„zuverlässiger, robuster und vertrauenswürdiger Systeme, die KI-Technologien verwenden“*, beauftragt.²⁷¹

Aufgrund dieses Auftrags veröffentlichte NIST seinen Plan für das Engagement des Bundes bei der Entwicklung technischer Standards und verwandter Instrumente.²⁷² In dem Plan wird die Notwendigkeit der *„KI-Sicherheit, des Risikomanagements und einiger Aspekte der Vertrauenswürdigkeit wie Erklärbarkeit oder Sicherheit“* anerkannt.²⁷³ Dieses Dokument

²⁶⁸ U.S. Department of Transportation, Preparing for the Future of Transportation: Automated Vehicles 3.0, abrufbar unter <https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf>, letzter Zugriff am 25.07.2020, S. 6

²⁶⁹ Dentons, *Autonomous Vehicles: US Legal and Regulatory Landscape* (August 2019), abrufbar unter <https://www.dentons.com/en/pdf-pages/-/media/611f20c26f504cbe81cf848a46e5074e.ashx>, letzter Zugriff am 20.07.2020, S. 11

²⁷⁰ S.B. 663, 97th Michigan State Legislature, 2013 Reg. Sess. (Michigan 2013)

²⁷¹ Executive Order No. 13859, 84 FR 3967 (February 11, 2019), abrufbar unter <https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence>, letzter Zugriff am 20.06.2020, Abschnitt 6

²⁷² National Institute of Standards and Technology, *US Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools* (August 9, 2019), abrufbar unter https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf, letzter Zugriff am 10.07.2020

²⁷³ Ebenda, S. 12

beinhaltet gleichfalls drei Bereiche sogenannter „nicht-technischer“ KI-Standards, die politische Entscheidungen beeinflussen, nämlich: gesellschaftliche und ethische Überlegungen, Governance und Datenschutz.²⁷⁴

Auf dem Gebiet der Sicherheit der KI-Systeme sind die US-Regulierungsbehörden vor allem bei der Ausarbeitung der Grundsätze bzw. des Rechtsrahmens für Prüfung und Inverkehrbringen der automatisierten Fahrzeuge überaus aktiv. Mehrere tödliche Unfälle mit automatisierten Fahrzeugen werfen neue Fragen auf, wie Regierungen des Bundes und der einzelnen Bundesstaaten die Fahrzeugtests und die Einführung neuer Technologien in den zum Verkauf angebotenen Fahrzeugen regeln sollten. Ein Fußgänger wurde in Arizona am 18. März 2018 von einem automatisierten Fahrzeug getötet, wobei drei Tesla-Fahrer starben, weil sie nicht auf Gefahren reagierten haben, die von den Fahrzeugen nicht erkannt wurden.²⁷⁵

National Highway Traffic Safety Administration (NHTSA, auf Deutsch „Nationale Behörde für Straßenverkehrssicherheit“) ist die wichtigste Behörde, die für die Sicherheit der Menschen auf Straßen durch die Durchsetzung von Fahrzeugleistungsstandards in den USA zuständig ist. Trotz der Notwendigkeit einer Regulierung hat NHTSA lediglich freiwillige Richtlinien herausgegeben, die nicht durchsetzbar sind und der Industrie kein Mandat auferlegen, automatisierte Fahrzeuge sicher zu entwickeln und zu testen. Darüber hinaus hat die Agentur es versäumt, die bereits festgestellten Mängel der automatisierten Fahrzeugtechnologie zu beheben.²⁷⁶

Im September 2016 veröffentlichte das US-Verkehrsministerium das Dokument unter Bezeichnung „Federal Automated Vehicles Policy“ das einen proaktiven Ansatz der staatlichen Behörden zur Gewährleistung der Sicherheit automatisierter Fahrzeuge und zur Erleichterung der innovativen Tätigkeit auf diesem Gebiet festlegte.²⁷⁷ Außerdem wurde der Ausdruck „automatisiertes Fahrzeugsystem“ als *„Kombination von Hardware und Software (beide Remote und an Bord), die eine Fahrfunktion ausführt, mit oder ohne dass ein Mensch die*

²⁷⁴ Ebenda

²⁷⁵ Bill Canis, *Issues in Autonomous Vehicle Testing and Deployment* (Congressional Research Service 2020), abrufbar unter <https://fas.org/sgp/crs/misc/R45985.pdf>, letzter Zugriff am 25.07.2020, S. 1

²⁷⁶ Joan Claybrook, Shaun Kildare, ‘Autonomous vehicles: No driver...no regulation?’ (2018) 361(6397) Science (New York, N.Y.), abrufbar unter <https://science.sciencemag.org.uaccess.univie.ac.at/content/361/6397/36>, letzter Zugriff am 25.07.2020

²⁷⁷ U.S. Department of Transportation, Federal Automated Vehicles Policy, abrufbar unter <https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf>, letzter Zugriff am 25.07.2020

*Fahrumgebung aktiv überwacht*²⁷⁸ definiert, sowie der Aufbau der Automatisierungsgrade dargestellt, auf die es weiter in diesem Kapitel näher eingegangen wird.

Aufbauend auf dieser Politik und unter Einbeziehung von Rückmeldungen des Kongresses und Industrievertreter veröffentlichte NHTSA im September 2017 „Automated Driving Systems: A Vision for Safety 2.0“.²⁷⁹ Diese Leitlinien stellen einen flexiblen, nicht regulierenden Ansatz für die Sicherheit automatisierter Fahrzeugtechnologien dar, indem sie die Automobilindustrie und andere wichtige Interessengruppen bei der Prüfung und Entwicklung von Best Practices für die sichere Prüfung und Bereitstellung automatisierter Fahrzeuge unterstützen, die den 3-5 Automatisierungsgraden angehören.²⁸⁰ Sie enthält ebenfalls freiwillige Leitlinien für Interessengruppen hinsichtlich der Gestaltung, der Prüfung und des sicheren Einsatzes automatisierter Fahrzeuge.²⁸¹

Im Oktober 2018 veröffentlichte DoT (US-Verkehrsministerium) die Leitlinien unter Bezeichnung „Preparing for the Future of Transportation: Automated Vehicles 3.0“, das auf den im vorherigen Dokument dargelegten freiwilligen Leitlinien aufbaut, diese jedoch nicht ersetzt. Die Leitlinie *„behält den Hauptfokus von DoT auf Sicherheit bei und erweitert die Diskussion auf andere Aspekte und Arte des Landtransports“*.²⁸² Außerdem legte DoT den föderalen Ansatz zur Gestaltung der Politik für automatisierte Fahrzeuge auf der Grundlage von sechs Prinzipien dar:

- 1) Priorisierung der Sicherheit;
- 2) Technologische Neutralität;
- 3) Modernisierung der Regulierung;²⁸³
- 4) Konsistentes regulatorisches und operatives Umfeld;
- 5) Proaktiver Ansatz zur Automatisierung;
- 6) Schutz der Grundrechte und Freiheiten.²⁸⁴

²⁷⁸ Ebenda, S. 10

²⁷⁹ U.S. Department of Transportation, Automated Driving Systems: A Vision for Safety 2.0, abrufbar unter https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf, letzter Zugriff am 25.07.2020

²⁸⁰ Ebenda, S. II

²⁸¹ Ebenda, S. 16

²⁸² U.S. Department of Transportation, Preparing for the Future of Transportation: Automated Vehicles 3.0, abrufbar unter <https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf>, letzter Zugriff am 25.07.2020, S. 2

²⁸³ Ebenda, S. IV

²⁸⁴ Ebenda, S. V

Im Januar 2020 wurde die jüngste Fassung der Leitlinien zum Thema automatisierter Fahrzeuge veröffentlicht²⁸⁵, die die bisherigen und aktuellen Bemühungen der US-Bundesregierung darstellt, diese Problembereiche anzugehen.²⁸⁶ Ein Herzstück der in Frage stehenden Leitlinien stellen folgende Prinzipien dar:

- 1) *Schutz der Benutzer und Gemeinschaften.* Die US-Regierung bemüht sich, die sichere Inbetriebnahme automatisierter Fahrzeuge zu erleichtern, potenzielle Sicherheitsrisiken anzugehen, sich angemessen gegen die Bedrohungen der Sicherheit und der öffentlichen Sicherheit durch kriminelle oder andere böswillige Verwendung zu schützen, sowie die Sicherheit von Daten und die Privatsphäre der Öffentlichkeit zu schützen;²⁸⁷
- 2) *Förderung effizienter Märkte.* Die Öffentlichkeit, nicht die Bundesregierung oder ausländische Regierungen, sollten die wirtschaftlich effizientesten Transport- und Mobilitätslösungen auswählen.²⁸⁸ Das Hauptziel der US-Bundesregierung besteht darin, den wirtschaftlichen Wohlstand und die innovative Wettbewerbsfähigkeit zu schützen, neue Wachstumsmotoren in den USA zu fördern sowie veraltete Vorschriften zu modernisieren bzw. beseitigen;²⁸⁹
- 3) *Erleichterung koordinierter Bemühungen.* Die US-Regierung sollte die Entwicklung und Umsetzung freiwilliger Konsensstandards, harmonisierter technischer Standards und regulatorischer Richtlinien mit internationalen Partnern fördern, wobei ein konsistenter Bundesansatz einzuhalten ist.²⁹⁰

Society of Automotive Engineers International (abgekürzt SAE, auf Deutsch „Verband der Automobilingenieure“), eine internationale Normungsorganisation, entwickelte einen Stufenbau der Automatisierungsgrade für Fahrzeuge, die vom DoT übernommen wurde, um eine standardisierte Nomenklatur zu fördern und Klarheit und Konsistenz bei Diskussionen über Fahrzeugautomatisierung und -sicherheit zu gewährleisten.²⁹¹ Dieser Stufenbau wurde in „Federal Automated Vehicles Policy“ dargestellt und sieht wie folgt aus:

²⁸⁵ National Science and Technology Council & U.S. Department of Transportation, Ensuring American Leadership in Automated Vehicle Technologies: Automated Vehicles 4.0, abrufbar unter <https://www.transportation.gov/sites/dot.gov/files/2020-02/EnsuringAmericanLeadershipAVTech4.pdf>, letzter Zugriff am 20.07.2020

²⁸⁶ Ebenda, S. 1

²⁸⁷ Ebenda, S. 4

²⁸⁸ Ebenda, S. 4

²⁸⁹ Ebenda, S. 5

²⁹⁰ Ebenda, S. 5

²⁹¹ Bill Canis, *Issues in Autonomous Vehicle Testing and Deployment* (Congressional Research Service 2020), abrufbar unter <https://fas.org/sgp/crs/misc/R45985.pdf>, letzter Zugriff am 25.07.2020, S. 2

- 1) Automatisierungsgrad 0 - der menschliche Fahrer macht alles selbst;
- 2) Automatisierungsgrad 1 - ein automatisiertes System eines Fahrzeuges kann dem menschlichen Fahrer *manchmal* dabei helfen, einige Teile der Fahraufgabe auszuführen;
- 3) Automatisierungsgrad 2 - ein automatisiertes System eines Fahrzeuges kann *tatsächlich* einige Teile der Fahraufgabe ausführen, während der Mensch weiterhin die Fahrumgebung überwacht und den Rest der Fahraufgabe ausführt;
- 4) Automatisierungsgrad 3 - ein automatisiertes System kann tatsächlich einige Teile des Systems leiten Fahraufgabe und Überwachung der Fahrumgebung in einigen Fällen, wobei der menschliche Fahrer bereit sein muss, die Kontrolle zurückzunehmen, wenn das automatisierte System diese erfordert;
- 5) Automatisierungsgrad 4 – ein automatisiertes System kann die Fahraufgabe ausführen und die Fahrumgebung überwachen, wobei der menschliche Fahrer die Kontrolle nicht zu übernehmen hat, aber das automatisierte System kann nur in bestimmten Umgebungen und unter bestimmten Bedingungen arbeiten;
- 6) Automatisierungsgrad 5 - ein automatisiertes System kann alle Fahraufgaben unter allen Bedingungen ausführen, unter denen ein menschlicher Fahrer sie ebenfalls ausführen kann.²⁹²

Der vorliegende Stufenbau ist gut geeignet, Fortschritte in der Autonomie der aufkommenden KI-Systeme zu beachten und die Ausarbeitung der gesetzlichen Sicherheitsstandards für jedes Niveau zu erleichtern. Außerdem kann dieses Niveausystem ebenfalls als Basis für die Ausarbeitung der Haftungsmodelle für die Behandlung der Sachverhalte mit den durch automatisierte Fahrzeuge verursachten Schäden.

Allerdings sind die Bundesstaaten hauptsächlich mit gesetzlicher Regulierung der automatisierten Fahrzeuge in den USA beschäftigt. Zum Stand von Februar 2020 erließen 29 Bundesstaaten von USA Gesetze in Bezug auf automatisierte Fahrzeuge.²⁹³ Der Gesetzgeber des Bundesstaates Nevada verabschiedete, Gesetz AB 511 und war damit der erste Staat, der

²⁹² U.S. Department of Transportation, Federal Automated Vehicles Policy, abrufbar unter <https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf>, letzter Zugriff am 25.07.2020, S. 9

²⁹³ Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (*National Conference of State Legislatures* 2020), abrufbar unter <https://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx>, letzter Zugriff am 20.07.2020

fahrerlose Autos legalisierte.²⁹⁴ Diese Gesetzesvorlage genehmigt den Betrieb automatisierter Fahrzeuge auf Autobahnen innerhalb des Bundesstaates Nevada.²⁹⁵ Das im Jahre 2013 verabschiedete Gesetz SB 313²⁹⁶ erfordert ein automatisiertes Fahrzeug, das auf einer Autobahn getestet wird, bestimmte Bedingungen in Bezug auf einen menschlichen Fahrer zu erfüllen, wobei der menschliche Fahrer sollte:

- 1) in einer Position sitzen, die es ihm ermöglicht, das automatisierte Fahrzeug sofort manuell zu steuern;
- 2) in der Lage sein, die Sicherheit des Betriebs des automatisierten Fahrzeuges zu überwachen;
- 3) in der Lage sein, die sofortige manuelle Steuerung des automatisierten Fahrzeuges im Falle eines Ausfalls der automatisierten Technologie oder eines anderen Notfalls zu übernehmen.²⁹⁷

Im Jahre 2012 wurde das Gesetz im Bundesstaat Kalifornien verabschiedet²⁹⁸, das das Gesetzbuch von Kalifornien über Fahrzeuge (California Vehicle Code) ändert bzw. mit Paragraf 38750 ergänzt und kalifornisches Kraftfahrzeugministerium (the California Department of Motor Vehicles) beauftragt, bis zum 1. Januar 2015 Vorschriften für die Prüfung und den Einsatz von „automatisierten Fahrzeugen“ auf öffentlichen Straßen zu erlassen²⁹⁹, sowie „automatisierte Technologie“ als „*Technologie, die in der Lage ist, ein Fahrzeug ohne die aktive physische Kontrolle bzw. Überwachung durch einen menschlichen Bediener zu fahren*“³⁰⁰ definiert (dh. dieses Gesetz findet nur auf automatisierte Fahrzeuge mit mindestens Automatisierungsgrad 3 Anwendung). In Übereinstimmung mit diesem Gesetz sollte der menschliche Fahrer weiterhin die Möglichkeit haben, die Kontrolle auf verschiedene Arten zu übernehmen, unter anderem durch Verwendung der Bremse, des Gaspedals oder des Lenkrads,

²⁹⁴ A.B. 511, 76th Legislature, 2011 Reg. Sess. (Nevada 2011), abrufbar unter <https://legiscan.com/NV/text/AB511/id/330673>, letzter Zugriff am 30.07.2020

²⁹⁵ Ebenda

²⁹⁶ S.B. 313, 77th Legislature, 2013 Reg. Sess. (Nevada 2013), abrufbar unter <https://legiscan.com/NV/text/SB313/id/858221>, letzter Zugriff am 30.07.2020

²⁹⁷ Ebenda, Paragraf 3

²⁹⁸ S.B. 1298, California State Legislature, 2011-2012 Session (California 2012), abrufbar unter https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201120120SB1298, letzter Zugriff am 31.07.2020

²⁹⁹ California Vehicle Code, Paragraph 38750 (West 2014), abrufbar unter https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=VEH§ionNum=38750, letzter Zugriff am 31.07.2020, Abs. d (1)

³⁰⁰ Ebenda, Abs. a (1)

sowie sollte das Fahrzeug den Bediener darauf hinweisen, dass automatisierte Technologie deaktiviert wurde.³⁰¹

Gemäß Paragraf 38750 Gesetzbuch von Kalifornien über Fahrzeuge kann ein automatisiertes Fahrzeug zu Testzwecken auf öffentlichen Straßen von einem Fahrer betrieben werden, der über die entsprechende Lizenzklasse für den betriebenen Fahrzeugtyp verfügt, wenn alle folgenden Anforderungen erfüllt sind:

- 1) ein automatisiertes Fahrzeug wird in diesem Zustand ausschließlich von Mitarbeitern, Auftragnehmern oder anderen vom Hersteller des Fahrzeuges benannten Personen auf Straßen betrieben;
- 2) ein menschlicher Fahrer muss auf dem Fahrersitz anwesend sein, den sicheren Betrieb des automatisierten Fahrzeugs überwachen und in der Lage sein, die sofortige manuelle Steuerung des automatisierten Fahrzeugs im Falle eines Ausfalls der automatisierten Technologie oder eines anderen Notfalls zu übernehmen;
- 3) ein Vorhandensein eines Versicherungsinstruments, einer Bürgschaft oder eines Selbstversicherungsnachweises in Höhe von 5 Millionen US-Dollar.³⁰²

³⁰¹ Ebenda, Abs. c (1), (D)

³⁰² Ebenda, Abs. b

Kapitel 4: Abschließender Vergleich der Initiativen in der EU und den USA

4.1. Vergleich der Initiativen der EU und USA

Die Rechtsvergleichung stellt eine der effektivsten und beliebtesten modernen Methoden der wissenschaftlichen Forschung auf dem Gebiet der Rechtswissenschaft. Die durchgeführte Untersuchung der bestehenden Initiativen zur Regulierung der KI in der EU und USA ermöglicht deren Vergleich und Feststellung der Lücken bzw. Mängel, sowie Erstellung der geeigneten Verbesserungsvorschläge. In diesem Kapitel werden weiter die wichtigsten Ergebnisse der in dieser Master Thesis dargelegten Untersuchung angeführt:

a) Vergleich der Ansätze zur Schaffung des Rechtsrahmens für KI

Die EU ist schon im Besitz der umfassenden Strategie zur Förderung der Entwicklung von KI-Technologien und der ethischen Leitlinien für KI in verschiedenen Branchen des öffentlichen bzw. privaten Lebens, sowie verfügt über die einschlägige Herangehensweise zur Anpassung der bestehenden Unionsvorschriften und Ausarbeitung der neuen Regelungen für die KI-Technologien. Ein Herzstück des Europäischen Ansatzes ist die Schaffung einer „vertrauenswürdigen KI“, die grundsätzlich dem Wohlergehen der Menschen und der Gesellschaft dienen sollte. Im Mittelpunkt der neuen Regelungen für KI sollte der risikobasierte Ansatz stehen, „um die Verhältnismäßigkeit des regulatorischen Eingreifens zu gewährleisten“.³⁰³ Außerdem gibt es einschlägige Initiativen zur Anpassung des europäischen Binnenmarktrechts, um den freien grenzüberschreitenden Verkehr der KI-Produkte und Dienstleistungen zu ermöglichen. Die Erlassung der umfassenden EU-weiten Vorschriften in diesem Bereich wird in den kommenden Jahren erwartet. Im Gegensatz zur europäischen Herangehensweise bevorzugt der amerikanische Gesetzgeber bis jetzt, auf Bundesebene nur allgemeine ethische Regeln bzw. rechtliche Grundsätze für die gesetzliche Regulierung der KI festzulegen (wie etwa durch politische Leitlinien meistens ohne bindende Kraft und technische Standards), wobei die Bundesstaaten grundsätzlich über die Mehrheit der Gesetze zur Regulierung der KI verfügen, z.B. in den Bereichen Datenschutz und automatisierte Fahrzeuge. Vor allem sind Bundesstaaten Kalifornien, Illinois und Nevada überaus aktiv. Die Bundesstaaten konzentrieren sich grundsätzlich mehr auf der Regulierung der einzelnen Arten der KI-Technologie als auf der Schaffung des universellen Rechtsrahmens. Allerdings wurden mehrere Versuche unternommen, KI auf Bundesebene

³⁰³ COM (2020) 65 endgültig, S. 20

zu regulieren, insb. die Leitlinie des Weißen Hauses für 2020 zur Regulierung von Anwendungen der KI, die einschlägige Grundsätze zur Regulierung der KI-Technologien beinhalten. Also die EU ist zurzeit mehr fortgeschrittener bei der Regulierung der KI in der Geschäftstätigkeit als die USA.

b) Vergleich der Initiativen zum Schutz der grundlegenden Menschenrechte

Die EU verfügt bereits über den gut ausgearbeiteten Rechtsrahmen zum Schutz der personenbezogenen Daten und zur Verhütung der Diskriminierung bei dem Einsatz der KI. Das Herzstück der Regulierung in dieser Hinsicht ist Art. 22 DSGVO, der Profiling und automatisierte Entscheidungen betrifft. Nach dieser Vorschrift hat eine Person das Recht, „*nicht einer ausschließlich auf einer automatisierten Verarbeitung (einschließlich Profiling) beruhenden Entscheidung unterworfen zu werden*“.³⁰⁴ Diese Bestimmung dient sowohl dem Schutz personenbezogener Daten als auch der Verhinderung der Diskriminierung beim Einsatz der ADM-Systeme. Außerdem ist der umfassende Rechtsrahmen zum Datenschutz in DSGVO verankert, der auch auf die Verarbeitung personenbezogener Daten durch KI-System Anwendung findet. In den USA besteht derzeit kein einheitlicher Rechtsrahmen zum Schutz der personenbezogenen Daten der Verbraucher. Es gibt nur einige bundesweite Initiativen wie *Algorithmic Accountability Act* und *Commercial Facial Recognition Privacy Act*, die noch durch den Gesetzgeber zu verabschieden sind. In Fall einer Verabschiedung dieser Gesetze werden sie die ersten gesetzgeberischen Fortschritte des Bundes zur Regulierung der KI in verschiedenen Branchen der Geschäftstätigkeit. Grundsätzlich spiegeln diese Gesetzgebungsentwürfe im Wesentlichen den in DSGVO dargestellten Ansatz wider. Allerdings ist der Anwendungsbereich dieser Gesetze in der persönlichen Dimension ungerechtfertigt begrenzt. Deshalb bedürfen sie weiterer Verbesserung. Im Gegensatz zu der EU sind einige US-Bundesstaaten bereits im Besitz der Gesetze zum Schutz der Menschenrechte beim Einsatz einiger KI-Technologien, z.B. Gesichts- und Spracherkennung, Chatbots usw.

c) Vergleich der Initiativen zur Haftung

Zu diesem Zeitpunkt gibt es weder in der EU noch in den USA spezifische gesetzliche Haftungsmodelle, die speziell dazu bestimmt sind, die den durch Anwendung der KI verursachten Schaden zu behandeln. Der Ansicht der europäischen Gesetzgeber nach,

³⁰⁴ Verordnung (EU) 2016/679, Art. 22, Abs. 1

können bestehende Haftungsmodelle zu diesen Zwecken wirksam verwendet werden, insb. die Produkthaftungs- und Gefährdungshaftungsvorschriften. Allerdings sind diese unter Berücksichtigung solcher technischen Eigenschaften der KI-Systeme, die sog. „Black-Box-Effekt“ schaffen (in erster Linie wie Opazität und Autonomie, die diesen Effekt schaffen) entsprechend anzupassen. Die Europäische Kommission vertritt weiter die Ansicht, dass die Anpassung der bestehenden Haftungsvorschriften keine Anerkennung der sog. KI-Rechtspersönlichkeit benötigt. Derzeit verfügen die USA über keine umfassenden Initiativen zur Anpassung der bestehenden Haftungsvorschriften bzw. Ausarbeitung der neuen Bestimmungen für den Umgang mit den durch KI verursachten Schaden. Allerdings sind einige Bundesstaaten schon im Besitz einiger Initiativen zur Produkthaftung in Bezug auf automatisierte Fahrzeuge und intelligente Lautsprecher.

d) Vergleich der Initiativen zu Produktsicherheit und Marktaufsicht

In der EU sind bereits die geeigneten Empfehlungen zur Anpassung der Produktsicherheitsvorschrift, nämlich Berücksichtigung der technischen Eigenschaften, die im Bericht über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung dargestellt sind. Der Meinung der Europäischen Kommission nach, sind bestehende Marktüberwachungsmechanismen ausreichend, um die Sicherheit der KI-Produkte zu gewährleisten. Zur Ergänzung der bestehenden Konformitätsbewertungsmechanismen sollten die neuen „Konformitätsbewertungen für KI-Anwendungen mit hohem Risiko“ geschaffen werden. In den USA wird eine Arbeit in dieser Hinsicht nur auf dem Gebiet der automatisierten Fahrzeuge durchgeführt.

4.2. Empfehlungen zur Verbesserung der untersuchten Initiativen

In Anbetracht der oben angegebenen Ausführungen zum Vergleich der bestehenden Rechtsvorschriften bzw. Initiativen zur Regulierung der KI in der EU und in den USA können deren Nachteile bzw. Lücke festgestellt werden, die ein der Ergebnisse der vorliegenden Master Thesis darstellen. Aufgrund dieser Ergebnisse sind eigene Empfehlungen bzw. Verbesserungsvorschläge erstellt. Diese können wie folgt dargestellt werden:

- 1) Bis jetzt gibt es mehrere Versuche zur juristischen Definierung der KI in Rahmen der verschiedenen internationalen Organisationen. Der EU-Gesetzgeber hat eine einheitliche

Definition der KI auszuarbeiten und sie auf Unionsebene zu verankern, um Inkonsistenzen in der Auslegung bzw. Anwendung des Unionsrechts zu vermeiden;

- 2) Die Anpassung des Binnenmarktrechts der EU zur Ermöglichung des freien grenzüberschreitenden Verkehrs der KI-Waren und Dienstleistung ist derzeit noch nicht fertiggestellt und bedarf daher weiterer Bemühungen der EU-Institutionen. Das Konzept eines digitalen EU-Binnenmarkts sollte auch KI-Produkte und Dienstleistungen umfassen, da sie große Mengen der frei zugänglichen Daten zur Weiterentwicklung erfordern. Allerdings sind dabei die geltenden Rechtsvorschriften zum Schutz personenbezogener Daten zu beachten;
- 3) Die EU verfügt über den umfassenden Rechtsrahmen zum Schutz gegen Diskriminierung aufgrund der bestimmten Merkmale (z.B. Rasse, Geschlecht, Religion, Staatsangehörigkeit, Weltanschauungen) in verschiedenen Bereichen. Allerdings sind die Vorschriften zum Umgang mit einer Diskriminierung speziell beim Einsatz der KI-Systeme (außer ADM-Systeme) in dem EU-Recht noch nicht vorhanden. Solche Bestimmungen sind unter Berücksichtigung der oben angeführten technischen Eigenschaften der KI-Systeme festzulegen. Allerdings sollen die Gesetzgeber auch auf die Möglichkeit zur entsprechenden Anpassung des bestehenden Rechtsrahmens näher eingehen;
- 4) Die bestehenden Produktsicherheits- und Produkthaftungsvorschriften der EU sind unter Einbeziehung der Empfehlungen der Europäischen Kommission anzupassen, die im Bericht über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung dargelegt sind. Der Wert dieser Empfehlungen besteht darin, dass sie die technischen Eigenschaften der KI wie Autonomie, Opazität und Datenabhängigkeit entsprechend berücksichtigen;
- 5) Der europäische Gesetzgeber sollte neben dem vorliegendem universellen Rechtsrahmen, der auf alle Arte der KI-Technologien ausgerichtet ist, auch die Vorschriften zur Regulierung der einzelnen KI-Technologien wie Gesichts- und Spracherkennung, Verwendung von Chatbots usw. ausarbeiten, weil jede einzelne Art der KI-Technologie bestimmte Risiken mit sich bringen, die andere KI-Technologien nicht bewirken können.

Für die Verbesserung der bestehenden Initiativen in den USA betreffend der Regulierung des wirtschaftlichen Einsatzes der KI kann man folgendes empfehlen:

- 1) Zahlreiche unterschiedliche Datenschutzregelungen in verschiedenen Bundesstaaten erschweren deren Einhaltung für die in verschiedenen US-Bundesstaaten tätigen Unternehmen. US-Gesetzgeber ist daher gut beraten, auf Bundesebene einen einheitlichen Rechtsrahmen zum Schutz personenbezogener Daten beim Einsatz der KI-Systeme (insb. bei der Anwendung der ADM-Systeme) der Verbraucher zu schaffen;
- 2) Eine Schwäche von *Algorithmic Accountability Act* ist ein zu enger Kreis der durch dieses Gesetz gedeckten Unternehmen (Anforderungen an Höhe des Einkommens über 50 Millionen US-Dollar oder an Besitz der Daten von 1 Million Verbrauchern³⁰⁵). Wenn ein ernstes Schadensrisiko besteht, ist es nicht sinnvoll, eine große Anzahl von Unternehmen von der Einhaltung der Vorschriften auszuschließen. Deshalb ist US-Gesetzgeber gut beraten, die Anwendung von *Algorithmic Accountability Act* auf alle Unternehmen auszudehnen, die personenbezogene Daten bearbeiten;
- 3) Die amerikanischen Initiativen beinhalten nur wenige Vorschläge zur Verhinderung der Diskriminierung beim Einsatz der KI-Systeme (außer Vorschriften zur Verhinderung der Diskriminierung beim Einsatz der Gesichtserkennungstechnologien in *Commercial Facial Recognition Privacy Act* und Schutz vor der Diskriminierung beim Einsatz der ADM-Systeme in *Algorithmic Accountability Act*). Daher sollte der US-Gesetzgeber diesem Thema mehr Aufmerksamkeit schenken;
- 4) Wie oben angeführt, sind in den USA derzeit keine Initiativen zur Regelung der Deliktaspekte der KI-Anwendung vorhanden. Eine umfassende Analyse der bestehenden Haftungsmodelle in der USA-Rechtsordnung ist notwendig, um festzustellen, ob die Handlungen des Gesetzgebers in dieser Hinsicht erforderlich sind. Eine derartige Analyse sollte sowohl Bundesgesetzgebung als auch Gesetzgebung einzelner Bundesstaaten heranziehen;
- 5) Der US-Gesetzgeber sollte ebenso auf mögliche Anpassung der Produktsicherheitsvorschriften näher eingehen, da er auf diesem Gebiet auch nicht tätig war, außer automatisierter Fahrzeuge. In dieser Hinsicht wäre der einheitliche Rahmen zur Sicherheit der KI-Systeme besser als unterschiedliche Gesetzgebungen je nach Bundesstaat.

³⁰⁵ Algorithmic Accountability Act of 2019, S. 1108, 116th Congress (2019), Paragraph 2, Abs. 5

Fazit

Die Anwendung verschiedener KI-Systeme in der Geschäftstätigkeit ist schon der Alltag für große Anzahl der Unternehmen, weil sie der Beschleunigung und der Effizienzsteigerung der Geschäftsprozesse im Unternehmen dienen. Der Einsatz der KI-Technologien in der Geschäftstätigkeit des Unternehmens ist überaus vielfältig: Automatisierung der Geschäftsprozesse und der Entscheidungsfindung, Einsatz der Roboter in der Industrie, Erstellung der personalisierten Werbungen und Kundensuche, Kundenberatung durch Chatbots usw. Allerdings bewirkt das Aufkommen digitaler Technologien wie KI die Entstehung neuer rechtlicher Herausforderung, insb. beim Schutz der personenbezogenen Daten und der Verbraucherrechte, Verhütung der Diskriminierung, Ungeeignetheit der traditionellen Deliktshaftungsmodelle und Produktsicherheitsvorschriften. Zum Zeitpunkt der Erstellung dieser Master Thesis gibt es jedoch keine allgemein anerkannte rechtliche Definition der KI, was eine Unklarheit in Hinblick auf die Regulierung der KI schaffen kann. Der Begriff der KI umfasst eine breite Reihe der Technologien, unter anderem: maschinelles Lernen, künstliche neuronale Netze (Deep Learning), Roboter, maschinelles Sehen, Expertensysteme usw. Die KI-Technologie wird dadurch gekennzeichnet, dass sie selbstständig Aufgaben erfüllt, von denen sonst angenommen wird, dass sie Heranziehung menschlicher Intelligenz erfordern.

In Anbetracht der potenziellen Risiken bzw. Gefahren der KI bedarf ihre Anwendung, insb. in der Geschäftstätigkeit von Unternehmen, der Regulierung durch spezifische Vorschriften. Jedoch ist eine solche Regulierung dann zulässig, wenn sie gut geeignet ist, die mit der Verwendung von den mit KI verbundenen Risiken zu verhindern bzw. mindern. Der Rahmen für sichere und vertrauenswürdige Anwendung der KI sollte sowohl ethische Leitlinien als auch rechtliche Regelungen beinhalten. Die derartigen Regelungen sollen die wesentlichsten technischen Eigenschaften der KI berücksichtigen, wie Opazität, Autonomie, Konnektivität, Komplexität, Datenabhängigkeit. Diese Eigenschaften unterscheiden im Wesentlichen KI von den anderen aufkommenden digitalen Technologien, da die Ergebnisse ihres Vorgangs meistens unvorhersehbar und nicht immer nachvollziehbar für den Menschen sind.

Genau aus diesem Grund benötigt ein vertrauenswürdiger KI-Einsatz in der Geschäftstätigkeit des Unternehmens die Schaffung des besonderen Rechtsrahmens. Die bestehende Gesetzgebung ist nicht immer geeignet, die sich aus KI ergebenden Herausforderungen zu meistern. Allerdings muss der Gesetzgeber in jedem einzelnen Fall sorgfältig prüfen, ob ein bestehender Rechtsrahmen für KI einschlägig ist, bevor er neue Gesetzgebung in diesem

Bereich erlässt, um die Überlappung bzw. Unstimmigkeiten in der hohen Anzahl der sachlich ähnlichen Regelungen zu vermeiden. Tatsächlich verfolgen die Europäische Kommission und das Europäische Parlament diesen Ansatz bereits.

Im Vergleich zu den USA ist die EU bei der Ausarbeitung des Rechtsrahmens für KI-Anwendung in den letzten Jahren überaus aktiv. Die EU verfügt bereits über den einschlägigen ethischen und rechtlichen Rahmen, die gut geeignet sind, den vertrauenswürdigen und auf den Menschen ausgerichteten Einsatz der KI in der Geschäftstätigkeit von Unternehmen zu fördern bzw. gewährleisten. In den USA dauert mittlerweile noch die Arbeit an den Grundsätzen für die zukünftige ethische und rechtliche Regulierung der KI. Zu gleicher Zeit wird die Verabschiedung der umfassenden Gesetzgebung in der EU zur Regulierung der KI in verschiedenen Lebensbereichen erwartet.

Den größten Fortschritt bei der gesetzlichen Regulierung von KI kann man mittlerweile im Bereich Datenschutz beobachtet werden. Als ein beispielhaftes Datenschutzsystem bei der Anwendung der KI ist DSGVO anzusehen, insb. ihr Art. 22. Diese Vorschrift behandelt Profiling und ausschließlich automatisierte Entscheidungen mit der Anwendung der KI. Im Gegensatz zu der EU liegt in den USA kein allgemeiner Datenschutzrechtsrahmen vor, sondern gelten die verschieden sektorspezifischen Vorschriften. Die bestehenden Initiativen zum Datenschutz bei der KI-Systeme, wie *Algorithmic Accountability Act* und *Commercial Facial Recognition Act*, bedürfen weiterer Verbesserung und Verabschiedung durch Gesetzgeber.

Allerdings ist das Recht auf den Datenschutz und Schutz eines Privatlebens nicht das einzige Menschenrecht, das bei der Verwendung von KI verletzt werden kann. Gleich wichtig sind die Fragen der möglichen Diskriminierung, insb. bei dem Einsatz der ADM-Systeme. Eine derartige Diskriminierung kann vermieden werden, indem eine menschliche Überwachung und Möglichkeit zum Eingreifen einer Person auf jeder Phase dieses Prozesses durch gesetzliche Vorschriften gewährleistet wird.

Die bestehen Haftungsmodelle, die in den meisten modernen Rechtsordnungen verankert werden, sind gut geeignet, die Herausforderung der durch KI verursachten Schäden zu meistern. Besonders wirksam nach Ansicht der EU-Gesetzgeber können zu diesem Zweck Produkthaftungs- und Gefährdungshaftungsvorschriften angewandt werden. Allerdings sollten sie entsprechend angepasst werden, so dass sie technische Eigenschaften der KI-Systeme und deren Funktionsweise entsprechend berücksichtigen sollten. Zur Verschaffung des wirksamen

Haftungsregimes für KI besteht keine Notwendigkeit zur Anerkennung deren Rechtspersönlichkeit.

KI in der Geschäftstätigkeit stellt ebenso eine gewisse Herausforderung für die geltenden Produktsicherheitsvorschriften. Daher sind sie unter Berücksichtigung der Autonomie und Opazität der KI-Systeme angemessen anzupassen. Eine Marktüberwachung ist für die tatsächliche Einhaltung und wirksame Durchsetzung der vorhandenen und zukünftigen Produktsicherheitsvorschriften erforderlich. Die bestehenden Mechanismen zur Marktüberwachung, die Mehrheit der modernen Rechtsordnungen (insb. der EU) kennen, sind gut geeignet, die Sicherheit der KI-Produkte zu gewährleisten. Allerdings sollten nach Ansicht der Europäischen Kommission die Konformitätsbewertungsmechanismen der EU mit den Konformitätsbewertungen für KI-Anwendungen mit hohem Risiko ergänzt werden.

Die Anpassung der Rechtsvorschriften zum Schutz der Menschenrechte, zur Haftung und Produktsicherheit in Hinblick auf KI-gestützte Produkte bzw. Dienstleistungen dienen im Wesentlichen der Effektivierung des europäischen digitalen Binnenmarkts. Da weitere Entwicklung bzw. Funktionsweise vieler KI-Technologien wie Maschinelles Lernen und künstliche neuronale Netzwerke von der Verfügbarkeit des großen Umfangs der Daten abhängen, ist ein digitaler Binnenmarkt mit dem freien EU-weiten Verkehr der Daten für die Förderung der KI von enorm großer Bedeutung.

Die Regulierung automatisierter Fahrzeuge lohnte im Rahmen dieser Master Thesis besondere Aufmerksamkeit, da KI ebenfalls zugrunde dieser Industrie liegt. Sowohl EU als auch USA verfügen über einschlägige Vorschriften in diesem Bereich (in den USA sind grundsätzlich einzelne Bundesstaaten wie Kalifornien aktiv). Besonders regulierungsbedürftig in dieser Hinsicht sind menschliche Überwachung des Betriebs und Anforderungen an Inbetriebnahme.

Aufgrund der in vorliegender Master Thesis durchgeführten Untersuchung bestehender Initiativen in der EU und in den USA zur Regulierung der KI in der Geschäftstätigkeit von Unternehmen kann der Schluss gezogen werden, dass sie die Risiken der Verwendung von KI noch nicht vollständig verhüten bzw. minimieren können. Vor diesem Hintergrund bedürfen sie weiter Verbesserung bzw. Vervollständigung. Allerdings ist es zu beachten, dass die Tätigkeit in der EU und den USA in dieser Richtung zum Zeitpunkt der Beendigung dieser Master Thesis noch andauert. Die in dieser Master Thesis dargestellten Verbesserungsvorschläge bzw. Empfehlungen können jedoch bei der weiteren Ausarbeitung des Rechtsrahmens für KI in der EU und in den USA berücksichtigt werden.

Literaturverzeichnis

Bücher und andere Publikationen:

1. Avron Barr, Edward A. Feigenbaum, *The Handbook of Artificial Intelligence: Volume 1* (Butterworth-Heinemann 1981)
2. Roger Brownsword, Eloise Scotford, Karen Yeung, *The Oxford Handbook of Law, Regulation and Technology* (Oxford University Press; Auflage: 1 2017)
3. Miriam C Buiten, 'Towards Intelligent Regulation of Artificial Intelligence' (2019) 10(1) European Journal of Risk Regulation, abrufbar unter <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/towards-intelligent-regulation-of-artificial-intelligence/AF1AD1940B70DB88D2B24202EE933F1B/core-reader>, letzter Zugriff am 30.04.2020
4. Bill Canis, *Issues in Autonomous Vehicle Testing and Deployment* (Congressional Research Service 2020), abrufbar unter <https://fas.org/sgp/crs/misc/R45985.pdf>, letzter Zugriff am 25.07.2020
5. Joan Claybrook, Shaun Kildare, 'Autonomous vehicles: No driver...no regulation?' (2018) 361(6397) Science (New York, N.Y.), abrufbar unter <https://science-sciencemag-org.uaccess.univie.ac.at/content/361/6397/36>, letzter Zugriff am 25.07.2020
6. Conrad Sebastian Conrad, 'Kann die Künstliche Intelligenz den Menschen entschlüsseln? — Neue Forderungen zum Datenschutz' (2018) 42(9), DuD, 541, abrufbar unter <https://link-springer-com.uaccess.univie.ac.at/content/pdf/10.1007/s11623-018-0996-z.pdf>, letzter Zugriff am 01.06.2020
7. Dentons, *Autonomous Vehicles: US Legal and Regulatory Landscape* (2019), abrufbar unter <https://www.dentons.com/en/pdf-pages/-/media/611f20c26f504cbe81cf848a46e5074e.ashx>, letzter Zugriff am 20.07.2020, S. 12
8. European Transport Safety Council, *Prioritising the Safety Potential of Automated Driving in Europe* (2016), abrufbar unter https://etsc.eu/wp-content/uploads/2016_automated_driving_briefing_final.pdf, letzter Zugriff am 30.07.2020
9. European University Institute, *Department of law Consumer law and artificial intelligence Challenges to the EU consumer law and policy stemming from the business' use of artificial intelligence* (EUI working papers 2018), abrufbar unter

https://pdfs.semanticscholar.org/d15a/13a15d74ce0168293c6477d1eb37c5692744.pdf?_ga=2.75614742.280107500.1590079789-947451715.1590079789, letzter Zugriff am 21.05.2020

10. Lukas Feiler, Nikolas Forró, *EU-DSGVO: EU-Datenschutz-Grundverordnung: Kurzkomentar* (Verlag Österreich 2017)
11. Future of Privacy Forum, *The Privacy Expert's Guide to Artificial Intelligence and Machine Learning* (2018), abrufbar unter <https://fpf.org/wp-content/uploads/2018/10/FPF-Artificial-Intelligence-Digital.pdf>, letzter Zugriff am 30.05.2020
12. Brian Higgins, 'Government Plans to Issue Technical Standards for Artificial Intelligence Technologies' (2019) *Artificial Intelligence Technology and the Law*, abrufbar unter <http://aitechnologylaw.com/2019/02/government-plans-to-issue-technical-standards-governing-artificial-intelligence-technologies/>, letzter Zugriff am 30.07.2020
13. Wolfgang Hoffmann-Riem, *Artificial Intelligence as a Challenge for Law and Regulation, Regulating Artificial Intelligence* (Springer International Publishing 2020)
14. Mario Martini, *Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz* (Springer-Verlag 2019)
15. Eoin Quill, *Irland, Staatshaftung in Europa: Nationales und Unionsrecht* (De Gruyter; Auflage: 1 2013)
16. PwC, *Künstliche Intelligenz als Innovationsbeschleuniger im Unternehmen: Zuversicht und Vertrauen in Künstliche Intelligenz* (2018), abrufbar unter <https://www.pwc.de/de/digitale-transformation/ki-als-innovationsbeschleuniger-in-unternehmen-whitepaper.pdf>, letzter Zugriff am 20.04.2020
17. PwC, *Sizing the prize, What's the real value of AI for your business and how can you capitalise?* (2017), abrufbar unter <https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf>, letzter Zugriff am 21.03.2020
18. Anne Röthel, 'Gefährdungshaftung' (2012) 34(6) *JURA – Juristische Ausbildung*, abrufbar unter <https://doi-org.uaccess.univie.ac.at/10.1515/jura-2012-0095>, letzter Zugriff am 20.06.2020
19. Martin Schnetter, *Robotik und ihre Regulierung: Tendenzen in Technik, Recht und Ethik* (Berliner Wissenschafts-Verlag 2016)

20. Jacob Turner, *Robot Rules: Regulating Artificial Intelligence* (Fountain Court Chamber: London 2019)
21. Rachel Wilka, Rachel Landy, Scott A. McKinney, 'How Machines Learn: Where Do Companies Get Data for Machine Learning and What Licenses Do They Need?' (2018) 13(3) Washington Journal of Law, Technology & Arts, abrufbar unter <https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=1274&context=wjlta>, letzter Zugriff am 01.05.2020
22. Frederik J. Zuiderveen Borgesius, 'Strengthening legal protection against discrimination by algorithms and artificial intelligence' (2020) 22(7) The International Journal of Human Rights, abrufbar unter <https://www.tandfonline.com/doi/full/10.1080/13642987.2020.1743976>, letzter Zugriff am 20.06.2020
23. The Law Library of Congress, *Regulation of Artificial Intelligence in Selected Jurisdictions* (2019), abrufbar unter <https://www.loc.gov/law/help/artificial-intelligence/regulation-artificial-intelligence.pdf>, letzter Zugriff am 20.07.2020

Rechtsakte und deren Entwürfe:

1. A.B. 511, 76th Legislature, 2011 Reg. Sess. (Nevada 2011)
2. Algorithmic Accountability Act of 2019, S. 1108, 116th Congress (2019)
3. Allgemeines bürgerliches Gesetzbuch, JGS Nr. 946/1811
4. Artificial Intelligence Initiative Act, S. 1558, 116th Congress (2019)
5. Artificial Intelligence Video Interview Act, H.B. 2557, 101st General Assembly, 2019 Reg. Sess., Public Act 101-0260 (Illinois 2019)
6. Anti-Eavesdropping Act, A.B. 1395, California State Legislature, 2019 Reg. Sess. (California 2019)
7. California Vehicle Code, Paragraph 38750 (West 2014), abrufbar unter https://leginfo.ca.gov/faces/codes_displaySection.xhtml?lawCode=VEH§ionNum=38750, letzter Zugriff am 31.07.2020
8. Charta der Grundrechte der Europäischen Union [2012] ABl C 326/391
9. Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Congress (2019)
10. Eisenbahn- und Kraftfahrzeughaftpflichtgesetz, BGBl. Nr. 48/1959
11. Entschließung des Europäischen Parlaments vom 16. Februar 2017 mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103(INL))

12. Entschließung des Europäischen Parlaments vom 12. Februar 2019 zur umfassenden europäischen Industriepolitik in Bezug auf künstliche Intelligenz und Robotik (2018/2088(INI))
13. Entschließung des Europäischen Parlaments vom 20. Oktober 2020 zu den Rechten des geistigen Eigentums bei der Entwicklung von KI-Technologien (2020/2015(INI))
14. Executive Order No. 13859, 84 FR 3967 (February 11, 2019), abrufbar unter <https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence>, letzter Zugriff am 20.06.2020
15. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232, § 238, 132 Stat. 1658 (2018), abrufbar unter <https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf>, letzter Zugriff am 20.07.2020
16. New Jersey Algorithmic Accountability Act, A.B. 5430, 218th Legislature, 2019 Reg. Sess. (N.J. 2019)
17. Richtlinie 85/374/EWG des Rates vom 25. Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte [1985] ABl L 210/29
18. Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates vom 3. Dezember 2001 über die allgemeine Produktsicherheit [2001] ABl L 11/4
19. Richtlinie 2010/41/EU des Europäischen Parlaments und des Rates vom 7. Juli 2010 zur Verwirklichung des Grundsatzes der Gleichbehandlung von Männern und Frauen, die eine selbständige Erwerbstätigkeit ausüben, und zur Aufhebung der Richtlinie 86/613/EWG des Rates [2010] ABl L 180/1
20. Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2011 über die Rechte der Verbraucher, zur Abänderung der Richtlinie 93/13/EWG des Rates und der Richtlinie 1999/44/EG des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 85/577/EWG des Rates und der Richtlinie 97/7/EG des Europäischen Parlaments und des Rates [2011] ABl L 304/64
21. Richtlinie (EU) 2019/1936 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zur Änderung der Richtlinie 2008/96/EG über ein Sicherheitsmanagement für die Straßenverkehrsinfrastruktur [2019] ABl L 305/1
22. S.B. 313, 77th Legislature, 2013 Reg. Sess. (Nevada 2013)
23. S.B. 663, 97th Michigan State Legislature, 2013 Reg. Sess. (Michigan 2013)
24. S.B. 1001, California State Legislature, 2017-2018 Session (California 2018)

25. S.B. 1298, California State Legislature, 2011-2012 Session (California 2012)
26. Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) [2016] ABl L 119/1
27. Verordnung (EU) 2017/2394 des Europäischen Parlaments und des Rates vom 12. Dezember 2017 über die Zusammenarbeit zwischen den für die Durchsetzung der Verbraucherschutzgesetze zuständigen nationalen Behörden und zur Aufhebung der Verordnung (EG) Nr. 2006/2004 [2017] ABl L 345/1
28. Verordnung (EU) 2019/1020 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über Marktüberwachung und die Konformität von Produkten sowie zur Änderung der Richtlinie 2004/42/EG und der Verordnungen (EG) Nr. 765/2008 und (EU) Nr. 305/2011 [2019] ABl L 169/1
29. Verordnung (EU) 2019/2144 des Europäischen Parlaments und des Rates vom 27. November 2019 über die Typgenehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge im Hinblick auf ihre allgemeine Sicherheit und den Schutz der Fahrzeuginsassen und von ungeschützten Verkehrsteilnehmern, zur Änderung der Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates und zur Aufhebung der Verordnungen (EG) Nr. 78/2009, (EG) Nr. 79/2009 und (EG) Nr. 661/2009 des Europäischen Parlaments und des Rates sowie der Verordnungen (EG) Nr. 631/2009, (EU) Nr. 406/2010, (EU) Nr. 672/2010, (EU) Nr. 1003/2010, (EU) Nr. 1005/2010, (EU) Nr. 1008/2010, (EU) Nr. 1009/2010, (EU) Nr. 19/2011, (EU) Nr. 109/2011, (EU) Nr. 458/2011, (EU) Nr. 65/2012, (EU) Nr. 130/2012, (EU) Nr. 347/2012, (EU) Nr. 351/2012, (EU) Nr. 1230/2012 und (EU) 2015/166 der Kommission [2019] ABl L 325/1
30. Vertrag über die Arbeitsweise der Europäischen Union (konsolidierte Fassung) [2012] ABl L 326/47
31. Vertrag über die Europäische Union (konsolidierte Fassung) [2012] ABl L 326/13
32. 49 United States Code, Paragraph 30103 (2011)

Offizielle Publikationen:

1. Artikel-29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679

WP251rev.01, abrufbar unter [https://www.dsb.gv.at/dam/jcr:768b9c7f-f0f6-45d7-b2aa-](https://www.dsb.gv.at/dam/jcr:768b9c7f-f0f6-45d7-b2aa-d113d121ea69/Leitlinien%20zu%20automatisierten%20Entscheidungen%20im%20Einzelfall%20einschlie%C3%9Flich%20Profiling%20f%C3%BCr%20die%20Zwecke%20der%20Verordnung%202016-679.pdf)

[d113d121ea69/Leitlinien%20zu%20automatisierten%20Entscheidungen%20im%20Einzelfall%20einschlie%C3%9Flich%20Profiling%20f%C3%BCr%20die%20Zwecke%20der%20Verordnung%202016-679.pdf](https://www.dsb.gv.at/dam/jcr:768b9c7f-f0f6-45d7-b2aa-d113d121ea69/Leitlinien%20zu%20automatisierten%20Entscheidungen%20im%20Einzelfall%20einschlie%C3%9Flich%20Profiling%20f%C3%BCr%20die%20Zwecke%20der%20Verordnung%202016-679.pdf), letzter Zugriff am 21.12.2020

2. Europäische Kommission, Bericht über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung COM (2020) 64 endgültig, abrufbar unter https://ec.europa.eu/info/sites/info/files/report-safety-liability-artificial-intelligence-feb2020_de.pdf, letzter Zugriff am 15.04.2020
3. Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Eine europäische Datenstrategie“ COM (2020) 66 endgültig, abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020DC0066&from=DE>, letzter Zugriff am 30.04.2020
4. Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Eine europäische Strategie für Kooperative Intelligente Verkehrssysteme – ein Meilenstein auf dem Weg zu einer kooperativen, vernetzten und automatisierten Mobilität“ COM (2016) 766 endgültig, abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52016DC0766&from=DE>, letzter Zugriff am 25.07.2020
5. Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Europa in Bewegung. Nachhaltige Mobilität für Europa: sicher, vernetzt und umweltfreundlich“ COM (2018) 293 endgültig, abrufbar unter https://eur-lex.europa.eu/resource.html?uri=cellar:0e8b694e-59b5-11e8-ab41-01aa75ed71a1.0001.02/DOC_1&format=PDF, letzter Zugriff am 25.07.2020
6. Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Koordinierter Plan für künstliche Intelligenz“ COM (2018) 795 endgültig, abrufbar unter https://eur-lex.europa.eu/resource.html?uri=cellar:22ee84bb-fa04-11e8-a96d-01aa75ed71a1.0003.02/DOC_1&format=PDF, letzter Zugriff am 15.04.2020

7. Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Künstliche Intelligenz für Europa“ COM (2018) 237 endgültig, abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52018DC0237&from=DE>, letzter Zugriff am 20.04.2020
8. Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Schaffung von Vertrauen in eine auf den Menschen ausgerichtete künstliche Intelligenz“ COM (2019) 168 endgültig, abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52019DC0168&from=DE>, letzter Zugriff am 01.06.2020
9. Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Strategie für einen digitalen Binnenmarkt für Europa“ COM (2015) 192 endgültig, abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52015DC0192&from=DE>, letzter Zugriff am 20.06.2020
10. Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über die Halbzeitüberprüfung der Strategie für einen digitalen Binnenmarkt „Ein vernetzter digitaler Binnenmarkt für alle“ COM (2017) 228 endgültig, abrufbar unter https://eur-lex.europa.eu/resource.html?uri=cellar:a4215207-362b-11e7-a08e-01aa75ed71a1.0003.02/DOC_1&format=PDF, letzter Zugriff am 15.04.2020
11. Europäische Kommission, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2008/96/EG über ein Sicherheitsmanagement für die Straßenverkehrsinfrastruktur COM (2018) 274 endgültig, abrufbar unter <https://ec.europa.eu/transparency/regdoc/rep/1/2018/DE/COM-2018-274-F1-DE-MAIN-PART-1.PDF>, letzter Zugriff am 26.07.2020
12. Europäische Kommission, Weissbuch „Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen“ COM (2020) 65 endgültig, abrufbar unter

https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_de.pdf letzter Zugriff am 30.05.2020

13. Expert Group on Liability and New Technologies, Report on Liability for Artificial Intelligence and other emerging technologies (2019), abrufbar unter <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608>, letzter Zugriff am 23.05.2020
14. Hochrangige Expertengruppe für künstliche Intelligenz, Eine Definition der KI: Wichtigste Fähigkeiten und Wissenschaftsgebiete (April 2019), abrufbar unter https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60664, letzter Zugriff am 01.05.2020
15. Hochrangige Expertengruppe für künstliche Intelligenz, Ethik-Leitlinien für eine vertrauenswürdige KI (April 2019), abrufbar unter <https://op.europa.eu/de/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1>, letzter Zugriff am 01.05.2020
16. H.R., Resolution No. 153, 116th Congress (2019), abrufbar unter <https://www.congress.gov/bill/116th-congress/house-resolution/153/text>, letzter Zugriff am 20.06.2020
17. Joint Committee of the European Supervisory Authorities, Joint Committee Report on the results of the monitoring exercise on “automation in financial advice”, JC 2018-29, abrufbar unter [https://esas-joint-committee.europa.eu/Publications/Reports/JC_2018_29 - JC Report on automation in financial advice.pdf](https://esas-joint-committee.europa.eu/Publications/Reports/JC_2018_29_-_JC_Report_on_automation_in_financial_advice.pdf), letzter Zugriff am 01.06.2020
18. National Institute of Standards and Technology, US Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools (August 9, 2019), abrufbar unter https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf, letzter Zugriff am 10.07.2020
19. National Science and Technology Council & U.S. Department of Transportation, Ensuring American Leadership in Automated Vehicle Technologies: Automated Vehicles 4.0, abrufbar unter <https://www.transportation.gov/sites/dot.gov/files/2020-02/EnsuringAmericanLeadershipAVTech4.pdf>, letzter Zugriff am 20.07.2020
20. OECD, Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449), abrufbar unter <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>, letzter Zugriff am 15.04.2020

21. The White House, Guidance for Regulation of Artificial Intelligence Applications, abrufbar unter <https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf>, letzter Zugriff am 11.06.2020
22. U.S. Department of Transportation, Automated Driving Systems: A Vision for Safety 2.0, abrufbar unter https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf, letzter Zugriff am 25.07.2020
23. U.S. Department of Transportation, Federal Automated Vehicles Policy, abrufbar unter <https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf>, letzter Zugriff am 25.07.2020
24. U.S. Department of Transportation, Preparing for the Future of Transportation: Automated Vehicles 3.0, abrufbar unter <https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf>, letzter Zugriff am 25.07.2020

Websites und Interviews:

1. Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation (*National Conference of State Legislatures* 2020), abrufbar unter <https://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx>, letzter Zugriff am 20.07.2020
2. Jennifer Betts, Keeping an Eye on Artificial Intelligence Regulation and Legislation, (*Ogletree Deakins*, 14 June 2019), abrufbar unter <https://ogletree.com/insights/keeping-an-eye-on-artificial-intelligence-regulation-and-legislation/>, letzter Zugriff am 30.07.2020
3. Kurt Wagner, Interview with Elon Musk (15 July 2017), abrufbar unter <https://www.vox.com/2017/7/15/15976744/elon-musk-artificial-intelligence-regulations-ai>, letzter Zugriff: 20.03.2020
4. Milad Safar, Einfach erklärt: Was ist Künstliche Intelligenz? (*Weissenberg Solutions*), abrufbar unter <https://weissenberg-solutions.de/was-ist-kuenstliche-intelligenz/>, letzter Zugriff am 20.04.2020
5. Stefan Luber, Nico Litzel, Was ist ein Chatbot? (*Bigdata Insider*, 28. Februar 2018), abrufbar unter <https://www.bigdata-insider.de/was-ist-ein-chatbot-a-690591/>, letzter Zugriff am 30.04.2020

6. The Oxford English Dictionary, Definition of “artificial intelligence” (*Lexico*), abrufbar unter https://en.oxforddictionaries.com/definition/artificial_intelligence, letzter Zugriff am 01.05.2020
7. Was ist künstliche Intelligenz? (Retresco), abrufbar unter <https://www.retresco.de/lexikon/kuenstliche-intelligenz/#was-ist-k%C3%BCnstliche-intelligenz>, letzter Zugriff am 01.05.2020

Eidesstattliche Erklärung

Ich erkläre hiermit an Eid statt, dass ich die vorliegende Arbeit selbstständig und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht. Die Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

Wien, den 31. Dezember 2020