JURISTISCHE FAKULTÄT

UNIVERSITÄT
HEIDELBERG
ZUKUNFT
SEIT 1386

Zusammenfassung der Dissertation mit dem Titel

„Datenschutzgrundverordnung – Rechtlicher Vorreiter oder Innovationsbremse? Eine Betrachtung der Entwicklung und Anwendung künstlicher Intelligenz unter der Datenschutz-grundverordnung“

Dissertation vorgelegt von Julia Dokara

Erstgutachter: Prof. Dr. Christian Duve
Zweitgutachter: Prof. Dr. Hanno Kube

Institut für Finanz- und Steuerrecht

„Wer Angst vor Daten hat, wird bei der künstlichen Intelligenz nicht mitmachen können. Denn künstliche Intelligenz ohne Daten ist so wie Kühe ohne Futter: Sie erreichen keinen Zuchterfolg.“ So beschrieb Angela Merkel das Verhältnis von der Entwicklung künstlicher Intelligenz zum Datenschutz im Frühjahr 2018. Die Entwicklung künstlicher Intelligenz läuft auf Hochtouren, sie gilt als die Schlüsseltechnologie der Zukunft. Ob digitale Sprachassistenten, autonome Fahrsysteme oder Chatbots im Kundenservice – schon heute ist unser Alltag von diversen Systemen künstlicher Intelligenz geprägt. Die „global Players“ forschen und entwickeln schon seit längerem, mittlerweile sehr erfolgreiche Systeme künstlicher Intelligenz. So hilft die künstliche Intelligenz von IBM „Watson“ nicht nur Banken, den Scoring-Wert verschiedener Verbraucher zur Einstufung der Kreditwürdigkeit zu ermitteln. Watson kann auch Menschen in logischen Spielen, wie zuletzt in der Quizshow Jeopardy bewiesen, schlagen. Watson besitzt hierbei eine Art menschlicher Intelligenz, mit welcher das System schneller und präziser als Menschen agieren kann. Watson wird mittlerweile auch in der Medizin eingesetzt und stellt anhand verschiedener Patientendaten Diagnosen. Sundar Pichai, CEO von Google, prognostizierte sogar, dass die künstliche Intelligenz für den Menschen „wichtiger als Feuer oder Elektrizität“ sein wird. Entsprechend arbeitet Google mit Hochdruck an der Entwicklung künstlicher Intelligenz, welche den neuen Unternehmensschwerpunkt darstellen soll, wofür man sich das Motto „AI first“ gesetzt hat. Auch für Deutschland hat die Entwicklung künstlicher Intelligenz wirtschaftlich eine große Bedeutung. Die Bundesregierung plant, Deutschland zum weltweit führenden Standort für künstliche Intelligenz zu machen. Hierbei diene die Datenschutzgrundverordnung (DSGVO) als verlässlicher Rahmen für innovative Technologien und Anwendungen auch im Bereich der künstlichen Intelligenz. Die am 25.05.2018 in Kraft getretene Datenschutzgrundverordnung regelt Rechte Betroffener. Es ist jedoch fraglich, ob die Datenschutzgrundverordnung insoweit als verlässlicher Rahmen für die Entwicklung und Anwendung künstlicher Intelligenz gesehen werden kann oder ob nicht vielmehr festgestellt werden muss, dass die Datenschutzgrundverordnung in ihrer heutigen Form der Anwendung und Entwicklung innovativer Techniken im Bereich künstlicher Intelligenz zuwiderläuft.

Die Dissertation beschäftigt sich daher mit der Vereinbarkeit der Entwicklung und Anwendung künstlicher Intelligenz vor dem Hintergrund der seit Mai 2018 geltenden Datenschutzgrundverordnung. Denn obgleich die Entwicklung und Anwendung künstlicher Intelligenz mit Blick auf den technologischen Fortschritt unausweichlich ist, stellt die Datenschutzgrundverordnung konkrete Anforderungen an die Verwender künstliche Intelligenzen, die dem technologischem Fortschritt entgegenstehen können.

Zur Verdeutlichung der technischen Besonderheiten eines Systems künstlicher Intelligenz wird im ersten Teil der Dissertation die künstliche Intelligenz selbst beleuchtet. Dabei wird insbesondere dargestellt, dass wir uns aktuell auf der Stufe der schwachen künstlichen Intelligenz (Artificial Narrow Intelligence „ANI“) befinden und in welchen Zeitabständen die nächsten Stufen künstlicher Intelligenz erreicht werden könnten. Um die juristischen Probleme bei der Entwicklung und Anwendung künstlicher Intelligenz genauer untersuchen zu können, wird sodann der Vorgang des Antrainierens eines Systems künstlicher Intelligenz genauer untersucht. Hierbei wird zwischen einem überwachten (supervised) und unüberwachten (unsupervised) Lernen der künstlichen Intelligenz unterschieden. Anschließend wird die

besonders zukunftsträchtige Form des Deep Learnings näher betrachtet. Bei diesem nutzt das System künstlicher Intelligenz selbst – ähnlich dem menschlichen Gehirn – ein neuronales Netz. Hierdurch werden Informationen auf verschiedenen Ebenen verarbeitet und jeweils an die nachfolgende Ebene (Layer) weitergegeben. Der Verarbeitungsprozess der einzelnen Layer, bzw. die terminierte Weitergabe ist dabei bisher nicht nachvollziehbar; aus diesem Grund wird der Vorgang in den sogenannten Hidden Layern, also den Layern zwischen dem Input- und Output Layer auch Blackbox genannt. Da sich diese Blackbox gerade in juristischer Hinsicht zu einem Problem entwickeln kann, werden auch verschiedene Lösungsansätze zur Entschlüsselung der Blackbox betrachtet und dargestellt. Hierbei wird insbesondere die durch das Fraunhofer Institut entwickelte Spectral Relevance Analysis (SpRAy), die den Entscheidungsfindungsprozess der künstlichen Intelligenz sichtbar macht, untersucht.

Der zweite Teil der Dissertation beschäftigt sich sodann mit der Datenschutzgrundverordnung an sich. Um die Problematiken für Systeme künstlicher Intelligenz vor dem Hintergrund der Datenschutzgrundverordnung zu verstehen, wird zunächst der Anwendungsbereich der Datenschutzgrundverordnung beleuchtet. In diesem Zusammenhang wird auch die Harmonisierungswirkung der Verordnung und mögliche Beschränkungen nach Art. 23 DSGVO untersucht. Insbesondere wird untersucht, ob von möglicherweise problematischen Normen der Datenschutzgrundverordnung aus wichtigen Gründen i.S.d. Art. 23 DSGVO abgewichen werden könnte. In einem nächsten Schritt wird sodann das Schutzgut der Datenschutzgrundverordnung untersucht und insbesondere eine Betrachtung der bisher geltenden Schutzzwecke auf EU-Ebene und Bundesebene angestellt, um einen Auslegungsrahmen für die seit Mai 2018 geltende Datenschutzgrundverordnung zu entwickeln. Sodann werden die Grundziele der Datenschutzgrundverordnung sowie die Schutzzwecke zur Bestimmung eines verlässlichen Auslegungsrahmens untersucht. Hierbei wird insbesondere auf die der Datenschutzgrundverordnung innewohnenden Grundprinzipien der Rechtmäßigkeit, der Verarbeitung nach Treu und Glauben, des Transparenzgebots, der Zweckbindung, der Datenminimierung, der Richtigkeit, der Speicherbegrenzung, der Integrität und Vertraulichkeit sowie der Rechenschaftspflichten eingegangen und deren Inhalt genauer beleuchtet.

Nachdem die Grundprinzipien der Funktionsweise eines Systems künstlicher Intelligenz sowie die Grundprinzipien und der Auslegungsrahmen der Datenschutzgrundverordnung an sich beleuchtet wurden, beschäftigt sich der dritte und letzte Teil dieser Dissertation mit der Kernfrage, ob die Entwicklung und Anwendung künstlicher Intelligenz vor dem Hintergrund der Datenschutzgrundverordnung überhaupt möglich ist oder nicht vielmehr durch diese verhindert wird.

Hierbei wird zunächst auf das Problem des Art. 22 I DSGVO innewohnenden Generalverbots mit Erlaubnisvorbehalt für automatisierte Entscheidungen einschließlich Profiling eingegangen. Dort wird normiert, dass die betroffene Person das Recht hat, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling - beruhenden Entscheidung unterworfen zu werden. In diesem Zusammenhang wird untersucht, was unter einer automatisierten Entscheidung zu verstehen ist und ob hierbei bereits vollständig automatisiert *vorbereitete* Entscheidungen gefasst werden können oder nur vollständig durch eine künstliche Intelligenz automatisierte Entscheidungen betroffen werden. Denn jedenfalls dann, wenn unter einer automatisierten Entscheidung nicht auch eine automatisiert vorbereitete

Entscheidung, die ein menschlicher Verwender ohne eigene Sachprüfung erlässt, zu verstehen wäre, würde sich das Verbot ad absurdum führen.

In der Folge wird untersucht, welche Auswirkungen das gefundene Ergebnis auf die Entwicklung und Anwendung künstlicher Intelligenz hat, wobei insbesondere auch die in Art. 22 DSGVO selbst genannten Erlaubnisvorbehalte beleuchtet werden.

Anschließend werden die besonderen Auskunftspflichte und -Rechte, die die Datenschutzgrundverordnung in Art. 13 II f, Art. 14 II g und Art. 15 II H DSGVO normiert sind, kritisch betrachtet. Hiernach ist der Verantwortliche einer Datenverarbeitung im Anwendungsbereich der Datenschutzgrundverordnung verpflichtet, das Bestehen einer automatisierten Entscheidung einschließlich Profiling anzuzeigen und – zumindest in diesen Fällen – *aussagekräftige Informationen über die involvierte Logik* zur Verfügung zu stellen. Vor dem Hintergrund des einem System künstlicher Intelligenz innewohnenden Algorithmus wird hierdurch ein Spannungsfeld zwischen den besonderen Auskunftspflichten der Datenschutzgrundverordnung und dem – zumindest verfassungsrechtlich geschütztem – Geschäftsgeheimnis in Form des Algorithmus geschaffen. In diesem Zusammenhang wird zunächst der Anwendungsbereich der zitierten Normen überprüft. Hierbei wird insbesondere untersucht, ob die besonderen Auskunftspflichten bei jeder automatisierten Entscheidungsfindung oder nur bei solchen, die auf einem Profiling beruhen („zumindest in diesen Fällen“) zur Verfügung zu stellen sind.

Darüber hinaus wird der Begriff der aussagekräftigen Informationen über die zugrundeliegende Logik ausgelegt. Es wird dargestellt, dass grundsätzlich drei verschiedene Auslegungen dieser aussagekräftigen Informationen über die zugrundeliegende Logik möglich sind. Hierunter könnte zum einen eine *Transparency* zu fordern sein, bei welcher den Betroffenen nur sehr allgemeine Informationen über die Wirkweise des Systems künstlicher Intelligenz zur Verfügung zu stellen sind. Es könnte allerdings auch eine *Explainability* zu fordern sein. Bei dieser wäre jedenfalls zu fordern, dass Auskunft über die konkret in die Entscheidung geflossenen Parameter sowie deren Gewichtung offengelegt werden. Schließlich könnte auch eine *Provability* anzustreben sein. Diese Stufe wäre erst bei einer Nachrechenbarkeit des Algorithmus, also bei einer vollständigen Offenlegung des Algorithmus erreicht.

Um zu untersuchen, wie diese Auskunftspflichten vor dem Hintergrund der drei verschiedenen Stufen zu erfüllen sind, wird untersucht, ob das Betriebs- und Geschäftsgeheimnis in Form des einer künstlichen Intelligenz zugrundeliegenden Algorithmus in der Datenschutzgrundverordnung selbst oder sonst auf EU- oder Verfassungsebene geschützt wird und wann in technischer Hinsicht das Geschäftsgeheimnis offengelegt wird. Dabei wird auch die bisherige Rechtsprechung des BGH zu § 34 Abs. 4 S. 1 Nr. 4 BDSG beleuchtet und untersucht, ob diese Rechtsprechung in Ansehung der Änderungen durch die Datenschutzgrundverordnung aufrecht erhalten bleiben kann. Des Weiteren werden die Erwägungsgründe zur Datenschutzgrundverordnung betrachtet, um zu untersuchen, ob das Spannungsverhältnis durch den Verordnungsgeber selbst aufgelöst wurde.

Vor dem Hintergrund des gefundenen Ergebnisses wird sodann die derzeitige technische Umsetzung der besonderen Auskunftspflichten betrachtet, um hiervon einen Rückschluss auf

den zukünftigen möglichen Umgang schließen zu können. Hierbei werden verschiedene Interviews sowie Datenschutzanfragen gegenüber verschiedenen Unternehmen ausgewertet.

Anhand des Ergebnisses wird in der Folge untersucht, wie sich dieses auf die Entwicklung und Anwendung künstlicher Intelligenz auswirkt und wie eine Umsetzung dieser neuartigen Technologien vor dem Hintergrund der Datenschutzgrundverordnung in der Praxis möglich wäre. Hierbei wird insbesondere geprüft, ob der nationale Gesetzgeber von den Anforderungen der Art. 13 II f, Art. 14 II g und Art. 15 II h DSGVO abweichen kann und sollte sowie wie er sonst eine für den Betroffenen transparente Verarbeitung seiner Daten ermöglichen kann. Insofern wird eine Beschränkung der besonderen Auskunftsrechte und -Pflichten gegenüber den Betroffenen und die Etablierung von unabhängigen Aufsichtsstellen, gegenüber welchen weitergehende Auskünfte zu erteilen sind, vorgeschlagen. Darüber hinaus wird für den Einsatz künstlicher Intelligenzen trotz des derzeit bestehenden Blackbox-Problems ein abgestuftes System empfohlen, welches sich an dem spezifischen Risiko des Systems künstlicher Intelligenz orientiert.

In einem Folgeschritt werden die Grundprinzipien der Datenschutzgrundverordnung, welche enumerativ in Art. 5 DSGVO aufgezählt sind, beleuchtet und untersucht, ob diese für die Entwicklung und Anwendung künstlicher Intelligenz hinderlich sind. Die Datenschutzgrundverordnung ist auf den Prinzipien der Datenminimierung und der Datensparsamkeit aufgebaut. Die Datenverarbeitung muss das Gebot der Transparenz, der Zweckbindung, der Richtigkeit, der Integrität und Vertraulichkeit sowie der Rechenschaft erfüllen. Darüber hinaus ist Art. 6 I DSGVO ein Generalverbot zur Datenverarbeitung zu entnehmen, welches mit Erlaubnisvorbehalt versehen ist. Vereinfacht gesagt normiert die Datenschutzgrundverordnung, dass nur die für einen bestimmten Zweck unabdingbaren Daten erhoben und diese nur für eine bestimmte Dauer gespeichert werden dürfen, soweit die Datenverarbeitung fehlerfrei erfolgt, für den Nutzer jederzeit in einer transparenten Art und Weise erklärbar ist und der Verantwortliche diverse Rechenschaftspflichte erfüllt.

Was aus negativen Erfahrungen mit großen Datenverwendern wie Facebook und co. als Schutz der menschlichen Betroffenen gedacht war, könnte aufgrund der Regelungsdichte jedoch leicht den innovativen und technischen Fortschritt der Gesellschaft verhindern und insoweit als überschießende Regelungsthematik das Fortkommen der Gesellschaft mehr hindern als es zu schützen. Vor diesem Hintergrund wird in der Dissertation untersucht, ob künstliche Intelligenz, welche immense Datenmengen benötigt, überhaupt datensparsam entwickelt werden kann und wie eine solche Datensparsamkeit in praktischer Hinsicht erreicht werden kann.

Auch die Transparenz- und Rechenschaftspflichten bieten Konfliktpotential, sodass diese in der Dissertation detailliert betrachtet werden. Insofern wird untersucht, welche Transparenzpflichten die Datenschutzgrundverordnung konkret stellt und ob diese in einem System künstlicher Intelligenz technisch überhaupt umsetzbar sind. Ebenso wird untersucht, welche Anforderungen die Datenschutzgrundverordnung an die Rechenschaftspflichten der Verantwortlichen stellt. Denn jedenfalls dann, wenn mit den Rechenschaftspflichten ein Dokumentationsaufwand einhergehen sollte, der den eigentlichen Sinn einer künstlichen Intelligenz, nämlich die Vereinfachung von Arbeitsabläufen, überlagert, würde dieses

Grundprinzip der Entwicklung und Anwendung künstlicher Intelligenz entgegenstehen. Insofern wird untersucht, wie die Rechenschaftspflichten in rechtlicher und tatsächlicher Hinsicht erfüllt werden können und ob hierfür selbst eigenständige Systeme künstlicher Intelligenz eingesetzt werden können.

Darüber hinaus werden auch die Anforderungen der Datenschutzgrundverordnung an die technischen Voreinstellungen beleuchtet. Die Datenschutzgrundverordnung fordert, dass bereits in technischer Hinsicht sichergestellt wird, dass die Grundprinzipien und Regelungen der Datenschutzgrundverordnung eingehalten werden (data protection by design und data protection by default). Diesbezüglich untersucht die Dissertation die Frage, ob diese datenschutzfreundliche Gestaltung der Technik bei der Entwicklung künstlicher Intelligenz überhaupt möglich ist und wie die Einhaltung in technischer Hinsicht erfolgen kann. Denn zumindest auf den ersten Blick scheint die Technik einer künstlichen Intelligenz, welche gerade immense Datenmengen benötigt, diesen Anforderungen konträr entgegenzustehen.

Schließlich werden in der Dissertation Folgeaspekte, die die Datenschutzgrundverordnung und teilweise das Bundesdatenschutzgesetz normiert, auf deren Vereinbarkeit mit künstlicher Intelligenz hin untersucht. So spricht §31 I Nr. 2 BDSG-neu, welcher in Abweichung von Art. 22 I DSGVO Regelungen zum Scoring trifft, davon, dass die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sein müssen. Die Dissertation widmet sich der Frage, welche Anforderungen diese Nachweisbarkeit an die Verwender einer künstlichen Intelligenz im Finanzbereich bei der Verwendung von Scoring stellt und ob hiermit andere Auskunftspflichten als bei der Datenschutzgrundverordnung zu erteilen sind sowie welche Bedeutung dies für das Geschäftsgeheimnis, die Datenschutzgrundverordnung und die Entwicklung und Anwendung künstlicher Intelligenz hat. Im Übrigen wird untersucht, ob die Verwender einer künstlichen Intelligenz der nach Art. 35 I, III DSGVO normierten Datenschutzfolgenabschätzung unterworfen sind und ob diese unter Berücksichtigung des Blackbox-Problems überhaupt durchgeführt werden kann, oder ob diese nicht dadurch unmöglich ist, dass die Risiken für die Betroffenen aufgrund des Blackbox-Charakters vor der eigentlichen Durchführung der Datenverarbeitung schlichtweg unbekannt sind und daher zuvor nicht antizipiert bewertet werden können.

Im Übrigen werden verschiedene nationale und internationale Handlungsempfehlungen zum datenschutzrechtlichen Umgang mit künstlicher Intelligenz betrachtet, um beurteilen zu können, ob die Ziele, die mit der Datenschutzgrundverordnung im Hinblick auf die Entwicklung und Anwendung einer künstlichen Intelligenz in datenschutzrechtlicher Hinsicht verfolgt werden, umsetzbar sind oder die Entwicklung künstlicher Intelligenz faktisch verhindern.

Insgesamt beschäftigt sich diese Arbeit inhaltlich daher mit der Frage, ob die Datenschutzgrundverordnung ein verlässlicher Rahmen für innovative Technologien im Bereich der künstlichen Intelligenz ist oder ob die Datenschutzgrundverordnung nicht vielmehr eine Viehzucht ohne Futter, ein unmögliches Unterfangen, für die Entwicklung künstlicher Intelligenz darstellt.