WIEBKE WINTER

Big Data und KI im Gesundheitswesen

Studien zum Medizin- und Gesundheitsrecht

Mohr Siebeck

Studien zum Medizin- und Gesundheitsrecht

Herausgegeben von

Steffen Augsberg, Karsten Gaede, Jens Prütting

9

Wiebke Winter

Big Data und KI im Gesundheitswesen

Zwischen Innovation und Informationeller Selbstbestimmung

Mohr Siebeck

Wiebke Winter, Geboren 1996; Studium der Rechtswissenschaften an der Bucerius Law School, Hamburg, und der University of Oxford, UK; Wissenschaftliche Mitarbeiterin am Institut für Medizinrecht der Bucerius Law School; Rechtsreferendariat am Hanseatischen Oberlandesgericht Bremen.

ISBN 978-3-16-162112-3/ eISBN 978-3-16-162191-8
DOI 10.1628/978-3-16-162191-8

ISSN 2699-6855 / eISSN 2699-6863 (Studien zum Medizin- und Gesundheitsrecht)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind über *http://dnb.dnb.de* abrufbar.

Das Buch wurde von Gulde-Druck aus der Times gesetzt, in Tübingen auf alterungsbeständiges Werkdruckpapier gedruckt und von der Buchbinderei Nädele in Nehren gebunden.

Printed in Germany.

Vorwort

Dieses Buch ist die überarbeitete Fassung meiner Dissertationsschrift, die ich im Jahr 2022 an der Bucerius Law School, Hamburg, vorgelegt habe. Die Arbeit soll den Versuch darstellen, eine Brücke zwischen Datenschutz und datengetriebenen Innovationen im Gesundheitswesen zu schlagen. Sie soll dazu beitragen, das aktuelle Datenschutzrecht kritisch zu hinterfragen und neue, vor allem digitale Wege zu beschreiten, um das Recht auf informationelle Selbstbestimmung und die Potenziale von Big Data und Künstlicher Intelligenz im Gesundheitswesen in Einklang zu bringen.

Die Arbeit ist an der Bucerius Law School am Institut für Medizinrecht zwischen den Jahren 2019 bis 2022 entstanden und wurde im März 2022 dort als Dissertation angenommen. Bei der Überarbeitung der Dissertation vor der Veröffentlichung sind die kürzlich aufgekommenen Entwürfe der EU-Verordnungen zur Künstlichen Intelligenz und zu einem Europäischen Gesundheitsdatenraum aufgenommen worden. Die Arbeit konzentriert sich jedoch im Wesentlichen auf die Datenschutzgrundverordnung. Sie ist nun auf dem Stand von Dezember 2022.

Zu dem Gelingen meiner Dissertation haben viele Menschen beigetragen, denen ich an dieser Stelle danken möchte. Mein besonderer Dank gilt meinem Doktorvater Prof. Dr. Jens Prütting. Er hat mich nicht nur für das Medizinrecht begeistern können, sondern sich vor allem jederzeit mit Leidenschaft allen rechtswissenschaftlichen Diskussionen mit mir gestellt und mich stets in all meinen Ideen und Projekten ohne Einschränkung unterstützt und gefördert. Ich möchte mich daher vor allem für die Freundschaft bedanken, die sich in den Jahren unserer Zusammenarbeit entwickelt hat.

Prof. Dr. Benedikt Buchner danke ich für die zügige Erstellung des Zweitgutachtens, für die wertvollen Anmerkungen und für unseren Austausch über Gesundheitsdatenschutzrecht. Zudem möchte ich mich bei Prof. Dr. Karsten Gaede, meinem zweiten Chef am Institut für Medizinrecht an der Bucerius Law School, für die stete Unterstützung und die vielen guten Gespräche bedanken. Ebenso bedanke ich mich bei ihm, Prof. Dr. Steffen Augsberg und meinem Doktorvater für die Aufnahme in diese Schriftenreihe.

Dank gebührt zudem meinen Kolleginnen und Kollegen am Institut für Medizinrecht, die mich insbesondere in der Anfangszeit meiner Promotion, die noch nicht von der Pandemie geprägt war, stets motiviert und unterstützt haben.

Ich danke zudem der Konrad-Adenauer-Stiftung für die großzügige Unterstützung meiner Promotion.

Ein ganz besonderer Dank gilt zum Schluss meiner Familie: Meiner Mutter, Frau Dr. rer. nat. Christine Winter, die das gesamte Werk Korrektur gelesen und mich immer wieder mit pharmazeutischen Hinweisen unterstützt hat; meinem Vater, Dr. med. Martin Winter, mit dem ich immer wieder tiefgehende Diskussionen aus ärztlicher Sicht führen durfte und der mich überhaupt erst auf das Thema „Digitalisierung in der Medizin“ gebracht hat; meinen Großeltern, die sich so sehr über diesen Erfolg gefreut haben wie keine zweiten und für deren Liebe ich so unglaublich dankbar bin, und meiner Schwester Katrin Winter für ihr immer offenes Ohr. Zudem danke ich Alex Schmidtke für all seine Unterstützung und seinen steten Glauben, dass ich dieses Werk trotz allen extracurricularen Engagements noch fertig stelle. Ihnen ist dieses Werk gewidmet.

Bremen, im Januar 2023 *Wiebke Winter*

Inhaltsübersicht

Inhaltsverzeichnis

1. Kapitel:

Big Data und Künstliche Intelligenz im Gesundheitswesen

A. Moderne Verarbeitungstechniken und die Medizin

I. Wachstum und Innovation durch Wissen

Die Welt befindet sich aufgrund der Digitalisierung in einem rasanten Wandel. Neue Technologien bringen ungeahnte Effizienzsteigerungen und neue Erkenntnispotentiale mit sich, die unser Zusammenleben in vergleichbarer Intensität verändern wie die industrielle Revolution im 18. und 19. Jahrhundert.

Neues, datenbasiertes Wissen[1] führt dazu, dass Innovationen im Gesundheitswesen einen Quantensprung machen.[2] Die Verarbeitung und Auswertung von Daten helfen, Krankheiten wie Krebs besser zu verstehen und dadurch besser zu heilen. Datenbasierte Forschung ermöglicht neue, individuelle Therapien. Die sogenannte stratifizierte Medizin[3] schafft nicht nur eine Erleichterung für den Patienten, sondern auch für die zunehmend prekären Finanzierungslage des Gesundheitssystem.[4] Denn die effiziente Nutzung von zielgenauer Medizin und der Einsatz von Daten zur Versorgungsforschung bergen enorme Einsparpotentiale für unsere soziale Versorgung, die ansonsten angesichts des demografischen Wandels und der damit immer älter werdenden Bevölkerung vor der Implosion stünde.[5]

---

[1] Mit datenbasiertem Wissen ist hier ein Wissen gemeint, dass sich auf die Auswertung von Daten beruft und eine Korrelation auf eine bestehen Kausalität hin überprüft hat. Datenbasiertes Wissen kommt regelmäßig in der sog. evidenzbasierten Medizin zum Einsatz, vgl. dazu *Wagner*, in: MüKo BGB, 8. Aufl. 2020, § 630a Rn. 128.

[2] Vgl. *Caliebe/Burger/Knoerzer/Kieser*, DÄBl. 2019, 1534, 1534.

[3] Vgl. mit personifizierter Medizin; hierzu bereits monographisch *Keil*, Rechtsfragen individualisierter Medizin, 2015.

[4] *Ochmann/Albrecht*, Zukünftige Entwicklung der GKV-Finanzierung, 2019.

[5] Vgl. *Ochmann/Albrecht*, Zukünftige Entwicklung der GKV-Finanzierung, 2019; dem kann allerdings mit dem Argument entgegengetreten werden, dass eine Individualisierung der Medizin an einigen Stellen auch höhere Kosten verursachen kann, da Aspekte der Massenproduktion und des einheitlichen Vorgehens ausscheiden. Zudem ist nicht auszuschließen, dass die Forschung bei immer kleiner werdenden Vergleichsgruppen problematisch werden kann.

Moderne Verarbeitungstechnologien wie Big Data und die Nutzung künstlicher Intelligenz sind die passenden Werkzeuge, um die (Gesundheits-)Welt schneller, effektiver und digitaler zu machen. Nicht mehr Produkte, sondern Daten werden zum wertvollsten Gut unserer Zeit.[6] Wer Daten[7] besitzt, besitzt Wissen – und damit Macht. Die neuen Verarbeitungsmethoden führen dazu, dass dieses neue Wissen immer schneller generiert und verwertet werden kann. Die Grundlage Daten ist somit das neue Rohöl unserer Zeit.[8] Und der Hunger nach Daten ist omnipräsent.

Die Preisgabe der benötigten Daten bedeutet für den Einzelnen jedoch stets eine Einschränkung seiner persönlichen Freiheit. Schon im Jahr 1983 beschrieb das Bundesverfassungsgericht, dass derjenige, der nicht wissen könne, wer welche Informationen über ihn besitzt, sich in seiner Persönlichkeit nicht mehr frei entfalten könne. Wer das Gefühl hat, dass stets alles über ihn bekannt werden könnte, der verhalte sich konformistischer – und damit unfreier.[9]

Das gilt insbesondere für Daten, die einen Bezug zum Vitalstatus des Betroffenen aufweisen. Um die besondere Sensibilität dieser Daten wusste schon Hippokrates in der griechischen Antike, der schwor:

„Was ich bei der Behandlung sehe oder höre oder auch außerhalb der Behandlung im Leben der Menschen, werde ich, soweit man es nicht ausplaudern darf, verschweigen und solches als ein Geheimnis betrachten."[10]

Aufgrund seiner potenziellen Freiheitseinschränkung durch die Preisgabe von Informationen wird dem Einzelnen sowohl auf europäischer als auch auf nationaler Ebene ein Grundrecht auf Datenschutz, bzw. informationelle Selbstbestimmung, eingeräumt. Dieses Recht garantiert dem Betroffenen, dass seine perso-

---

[6] So sind die Unternehmen Apple, Microsoft, Alphabet und Amazon, die viele Daten verarbeiten, die wertvollsten Unternehmen der Welt, Stand 03.01.2022. Zum monetären Wert von Daten im Privatrecht jüngst *Nissen*, Der monetäre Wert von Daten im Privatrecht, 2021.

[7] Diese Schlussfolgerung beruht auf der Prämisse, dass zudem entsprechende Datennutzungs- und Datenauswertungssysteme bereitstehen, die die Datenlage in nutzbares Wissen zu verwandeln vermögen.

[8] Vgl. auch die viel zitierte Überschrift des *The Economist*, The world's most valuable resource is no longer oil, but data, 06.05.2017, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (Abrufdatum: 14.11.2022).

[9] BVerfGE 65, 1, 43 f.

[10] Zitiert nach: Eid des Hippokrates, Wikipedia, https://de.wikipedia.org/wiki/Eid_des_Hippokrates (Abrufdatum: 14.11.2022); die Schweigepflicht bezweckt unmittelbar, das Vertrauensverhältnis zwischen Arzt und Patient zu bewahren. Dies bedeutet jedoch auch unmittelbar, dass es dem Patienten unangenehm wäre, wenn diese Informationen Dritten preisgegeben werden würden; vgl. *Weichert*, in: Kühling/Buchner, DSGVO, 3. Aufl. 2020, Art. 4 Nr. 15 Rn. 4.

nenbezogenen Daten nur aufgrund einer gesetzlichen Grundlage oder aufgrund einer von ihm erteilten Einwilligung verarbeitet werden können.[11]

Der Schutz von Daten wird im europäischen Rechtsraum weiter durch die Datenschutzgrundverordnung und die vielen datenschutzrechtlichen Normen, die auf ihrer Grundlage erlassen werden, garantiert. Die Europäische Union ist in den Augen Vieler Vorreiter im Datenschutz.[12]

Der strenge Datenschutz kann jedoch die Generierung neuen Wissens und neuer Gesundheitstechnologien erschweren. Gerade Rechtsunsicherheiten im Datenschutz können für Forscher und Unternehmen zum Innovationshemmnis und dadurch zum Standortnachteil für Europa werden.[13] Daher ist es besonders misslich, dass unklar ist, inwiefern Big Data und die Datenschutzgrundverordnung miteinander in Einklang zu bringen sind. Insbesondere die mit Datenschutzverstößen verbundenen hohen Sanktionen[14] führen dazu, dass Unternehmen und Behörden vor dem Einsatz von Daten zurückschrecken können.[15] Auch die Forschung leidet unter den hohen Voraussetzungen: Da kaum rechtssichere Verarbeitungsgrundlagen bestehen, setzen Viele auf die einzelne Einwilligung[16] – ein langwieriges und kaum zu bewältigendes Verfahren für jeden Forscher, der Big Data nutzen möchte. Zudem bringt dies erhöhten anwaltlichen Beratungsbedarf und damit Zeitaufwand und Zusatzkosten mit sich.

Dabei ist unklar, inwieweit der strenge Datenschutz den Menschen in Deutschland und Europa heutzutage zugutekommt. Viele sind von den unzähligen gestellten Einwilligungsersuchen und der dazugehörigen Menge an Informationsmaterialien überfordert, die ihnen täglich bei der Nutzung des Internets begegnen.[17] Ohne über die Konsequenzen ihrer Handlungen nachzudenken oder sich über die Datenverarbeitungsmodalitäten zu informieren und Datenschutzerklä-

---

[11] Vgl. Art. 8 Abs. 2 GRCh.

[12] BfDI, DSGVO – Texte und Erläuterungen, 2020, S. 8 f.; *Keller*, in: WELT, Warum die DSGVO nur ein Anfang sein kann, 29.05.2018, https://www.welt.de/wirtschaft/bilanz/article176768757/Globaler-Datenschutz-Warum-die-DSGVO-nur-ein-Anfang-sein-kann.html (Abrufdatum: 14.11.2022).

[13] Vgl. den Präsidenten des BDI *Kempf*, in: Pressemitteilung: BDI-Präsident Kempf zur EU-Datenschutzgrundverordnung: Datenschutz darf nicht zum Innovationshemmnis und Standortnachteil werden, 11/2018, 20.05.2018.

[14] Vgl. Art. 83 f. DSGVO.

[15] Vgl. *Lamprecht,* in: Datenschutz PRAXIS, Wirtschaftsvertreter klagen über DSGVO, 17.01.2020, https://www.datenschutz-praxis.de/fachnews/wirtschaftsvertreter-klagen-ueber-dsgvo/ (Abrufdatum: 14.11.2022).

[16] *V. Kielmannsegg,* in: Strech et al., Wissenschaftliches Gutachten – „Datenspende" – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen, 2020, S. 103.

[17] Vgl. dazu extensiv *Hermstrüwer*, Informationelle Selbstgefährdung, 2016.

rungen zu lesen, willigen sie in viele Datenverarbeitungsprozesse ein. Sie geben auf diese Weise mehr Daten preis, als sie eigentlich müssten.

Daher erscheint es zumindest zweifelhaft, ob noch von tatsächlicher informationeller Selbstbestimmung gesprochen werden kann. Eine echte Kontrolle über das, was wir über uns preisgeben, ist aufgrund der Fülle der Daten sowieso kaum mehr möglich. Es ist daher die Frage zu stellen, inwieweit das Recht dem neuen Lebenswandel angepasst ist.

Die aktuelle Rechtslage ist somit weder für innovationssuchende Unternehmen, Forscher oder Einrichtungen noch für die Betroffenen selbst ein optimaler Zustand. Schon die herrschende Dynamik im digitalen Markt und bei der Datenverarbeitung macht offensichtlich, dass das Datenschutzrecht stets weiterzuentwickeln ist. Was 2012 mit der Schaffung der Datenschutzgrundverordnung und zustimmungswürdigen Intentionen begann, scheint heute überholt.

Diese Untersuchung hat daher zum Ziel, die dogmatischen Defizite des Datenschutzrechts sowohl für die informationelle Selbstbestimmung des Einzelnen als auch für die tatsächliche Erforschung und Anwendung von Innovationen aufzuzeigen. Das Ziel der Arbeit ist, punktuell Vorschläge zu unterbreiten, wie diese Defizite aufgelöst werden können.

Die Untersuchung erfolgt anhand des Gesundheitssektors, bei dem ein besonders hohes Innovations- aber auch ein besonders großes Gefährdungspotential für die informationelle Selbstbestimmung besteht. Daher weist der Gesundheitssektor ein besonders gewichtiges und juristisch interessantes Spannungsfeld auf.

Dabei sollen verschiedene Handlungsfelder im Bereich des Medizinsektors untersucht werden; die Konzentration liegt auf den Feldern, die den größten Beitrag zu Innovationen im Gesundheitswesen leisten.

II. Terminologie

Für eine präzise und verständliche Analyse bedarf es in einem so innovativen Feld wie der Datenverarbeitung einer genauen Bestimmung der verwendeten Begriffe Künstliche Intelligenz und Big Data.[18]

1. Künstliche Intelligenz

Der Begriff der Künstlichen Intelligenz ist aufgrund der vielfältigen technologischen Ansätze[19] kaum trennscharf zu definieren.[20] Das erste Mal wurde der Be-

---

[18] M. w. N. *Dochow*, Grundlagen und normativer Rahmen der Telematik im Gesundheitswesen, 2017, S. 56 ff.

[19] S. zu den technologischen Ansätzen *Dettling* MPJ 2019, 176 ff.

[20] *Ernst* JZ 2017, 1026, 1027; *Frost* MPR 2019, 117, 118; *Schael* DuD 2018, 547, 547.

griff der künstlichen Intelligenz durch die „Dartmouth-Konferenz“ geprägt, bei der John McCarthy das erste KI-Projekt anstieß. Nach seiner Definition bedeutete Künstliche Intelligenz:

„The study is to proceed on the basis of the conjecture that every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it.“[21]

Aufgrund der zunehmenden und verbesserten technischen Möglichkeiten der Datenverarbeitung wurde der Begriff in Folge weiterentwickelt. Speicherkapazitäten und Verarbeitungsschnelligkeit erlauben erst seit wenigen Jahren eine gewinnbringende Analyse einer Vielzahl von Daten, die ein Mensch allein nicht bewältigen könnte.

Die KI-Enquete des Deutschen Bundestags definiert den Begriff der Künstlichen Intelligenz so:

„KI-Systeme sind von Menschen konzipierte, aus Hardware- und/oder Softwarekomponenten bestehende intelligente Systeme, die zum Ziel haben, komplexe Probleme und Aufgaben in Interaktion mit der und für die digitale oder physische Welt zu lösen.“[22]

Die von der Bundesregierung eingesetzte Datenethikkomission beschreibt Künstliche Intelligenz als einen

„Sammelbegriff für diejenigen Technologien und ihre Anwendungen, die durch digitale Methoden auf der Grundlage potenziell sehr großer und heterogener Datensätze in einem komplexen und die menschliche Intelligenz gleichsam nachahmenden maschinellen Verarbeitungsprozess ein Ergebnis zur Anwendung gebracht wird.“[23]

Es handelt sich bei KI nach der nationalen Ansicht Deutschlands somit primär um IT-Ansätze, die intelligente, menschenähnliche Verhaltensweisen zeigen[24] und die anders als Big Data nicht die Datenmenge als Ganzes beschreiben, sondern vielmehr eine weitere Technologie, mit der diese Datensätze regelmäßig ausgewertet werden.

Licht in dem Dickicht verschiedener Definitionen vermag der Entwurf der KI-Verordnung der Europäischen Union[25] (KI-VO-E) zu bringen. Diese zum Zeitpunkt der Untersuchung noch in der Vorabstimmung befindliche Verordnung

---

[21] *McCarthy,* A Proposal For The Dartmouth Summer Research Project On Artificial Intelligence, 1955, S. 2; vgl. zu der Entwicklung der Forschung *Lenzen*, Künstliche Intelligenz, 2019, S. 21 ff.

[22] BT-Drs. 19/23700, S. 51 mit weiter- und tiefgehenden Definitionen.

[23] *Datenethikkommission*, Gutachten der Datenethikkommission, 2019, S. 34.

[24] Bitkom/DFKI, Künstliche Intelligenz – Wirtschaftliche Bedeutung, gesellschaftliche Herausforderungen, menschliche Verantwortung, 2017, S. 14.

[25] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intel-

könnte als normenhierarchisch höchstes, für alle Mitgliedstaaten verbindliches Recht Klarheit schaffen.

Nach dem Vorschlag der EU-Kommission werden in Art. 3 Nr. 1 KI-VO-E[26] KI-Systeme definiert als

„eine Software, die mit einer oder mehreren der in Anhang I aufgeführten Techniken und Konzepte entwickelt worden ist und im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren".

Die Definition der Kommission ist weit und kann so auch in der Zukunft neue Technologien umfassen. Die Zukunftssicherheit wird durch die Nennung der entsprechenden Techniken künstlicher Intelligenz, die in „Anhang I – Techniken und Konzepte der Künstlichen Intelligenz[27] gemäß Artikel 3 Absatz 1" genannt werden, gewährleistet.[28] In Art. 3 Abs. 1 lit. a) des Anhangs I KI-VO-E werden die weit verbreiteten Konzepte des maschinellen Lernens genannt. Insbesondere kann hier zwischen unbeaufsichtigtem *(„unsupervised"),* beaufsichtigtem („*supervised*") und bestärkendem („*reinforced*") Lernen differenziert werden:[29] Beim beaufsichtigten Lernen sind die Antworten, zu der eine Intelligenz kommen soll, schon vorgegeben. Die Maschine lernt und optimiert sich anhand ihrer Fehler, die sie durch die schon vorgegebenen Antworten selbst erkennt.[30] Beim unbeaufsichtigten Lernen gibt es indes keine Zielvorgabe oder festgelegte Antworten. Vielmehr ist das Ziel des auch als „*Data Mining*" beschriebenen Vorgangs,[31] große Datenmengen neu zu strukturieren und neue Zusammenhänge und Erkenntnisse zu generieren.[32] Beim bestärkenden Lernen besteht im Gegensatz zum unbeaufsichtigten und beaufsichtigten Lernen keine Ausgangsdatenlage, mit der die Künstliche Intelligenz trainiert werden muss. Ein so trainiertes Sys-

---

ligenz) und zur Änderung bestimmter Rechtsakte der Union vom 21.04.2021, COM(2021) 206 final.

[26] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, COM(2021) 206 final, Stand 21.04.2021.

[27] In der Vorlage steht „Intellizenz", es ist jedoch von einem Tippfehler auszugehen, sodass „Intelligenz" gemeint ist.

[28] *Spindler* CR 2021, 361, 362 f.

[29] Vgl. dazu auch BT-Drs. 19/23700, S. 51 ff.

[30] *Schael* DuD 2018, 547, 548.

[31] *Datenethikkommission*, Gutachten der Datenethikkommission, 2019, S. 58; *Hoffmann-Riem*, (Rechtliche Rahmenbedingungen für und regulative Herausforderungen durch Big Data, in: Hoffmann-Riem (Hrsg.), Big Data – regulative Herausforderungen, 2018, S. 11, 20 f.) beschreibt dies als prädiktive Analytik; *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 2016, S. 25; vgl. *Schael*, DuD 2018, 547, 548.

[32] *Bilski/Schmid* NJOZ 2019, 657, 658.

tem findet vielmehr Lösungen zu komplexen Fragestellungen, indem es versucht, erhaltene Belohnungen zu maximieren. Die erforderlichen Daten werden in einem Trial-and-Error-Verfahren generiert.[33]

Eine Methode, die dazu häufig genutzt und vom Anhang I des Art. 3 Abs. 1 KI-VO-E eingeschlossen wird, ist das sogenannte tiefe Lernen *(„Deep Learning")*.[34] Beim Deep Learning werden künstliche neuronale Netze eingesetzt, die eine Vielzahl von Zwischenschichten, sog. *hidden layers*, zwischen der Eingabeschicht und der Ausgabeschicht besitzen. Aufgrund der verschiedensten Verknüpfungsmöglichkeiten lässt die Methode immer genauere Sachverhalte erfassen: So kann Deep Learning eingesetzt werden, um eine Künstliche Intelligenz auf Bilderkennung zu trainieren. Deep Learning Mechanismen können sich dabei selbst optimieren, indem sie auch ohne Eingabe von Expertenwissen selbst filtern können, welche Features aus den Eingabedaten am effektivsten auf einer bestimmten Ebene transformiert werden können.[35] Für ein effektives Funktionieren von Deep Learning bedarf es jedoch einer besonders großen Datenmenge.[36]

Schließlich wird von starker und schwacher künstlicher Intelligenz gesprochen – je nachdem, ob die künstliche Intelligenz wie ein Mensch lernen und dessen Fähigkeiten übertreffen kann oder rein maschinell lernt, indem Wissen aus Erfahrung generiert wird. Als Unterscheidungsmerkmal dient die Fähigkeit zur Selbstoptimierung.[37]

Bei all diesen Techniken werden Algorithmen eingesetzt. Nach der Definition des Dudens sind die im Rahmen von Künstlicher Intelligenz eingesetzten Algorithmen Verfahren zur schrittweisen Umformung von Zeichenreihen oder Rechenvorgängen nach einem bestimmten, sich wiederholenden Schema.[38] Allgemein gesprochen sind Algorithmen also „Regeln, die bestimmte Aufgaben in definierten Einzelschritten lösen sollen."[39]

---

[33] S. *Baum,* in: Leupold/Wiebe/Glossner, Münchener Anwaltshandbuch IT-Recht, 4. Aufl. 2021, Teil 9.1, Rn. 34 ff; mit dieser Methode konnte *Alpha Go Zero* sich beim komplizierten Brettspiel „Go" gegen die weltbesten Spieler behaupten, s. https://deepmind.com/blog/article/alphago-zero-starting-scratch, (Abrufdatum: 14.11.2022); zuvor wurde die Software Alpha Go noch mit über 30 Millionen Spielzügen aufwendig trainiert, vgl. *Pumperla/Ferguson*, Deep Learning and the Game of Go, 2019.

[34] Vgl. auch *Schael* DuD 2018, 547, 549.

[35] Retresco GmbH, Was ist Deep Learning, https://www.retresco.de/lexikon/deep-learning/ (Abrufdatum: 14.11.2022).

[36] Datasolut, Deep Learning: Definition, Beispiele & Frameworks, https://datasolut.com/was-ist-deep-learning/ (Abrufdatum: 14.11.2022).

[37] *Frost* MPR 2019, 117, 118.

[38] *Duden,* Begriff „Algorithmus", https://www.duden.de/rechtschreibung/Algorithmus (Abrufdatum: 14.11.2022).

[39] *Hoffmann-Riem*, Rechtliche Rahmenbedingungen für und regulative Herausforderungen

2. Big Data

Zentrales Thema dieser Arbeit ist der datenschutzrechtliche Umgang mit Big Data. Daher ist hier genau zu untersuchen, was unter diesem Begriff zu verstehen ist. Zudem müssen die gesteigerten Gefahren, die von Big Data im Vergleich zu „normalen" Datenverarbeitungsvorgängen ausgehen, skizziert werden.

a) Begriffsdefinition

Der aus dem Englischen entliehene Begriff des Big Data erfährt weder eine Legaldefinition noch eine ausdrückliche Erwähnung in der DSGVO und wird in Praxis und Literatur daher uneinheitlich verwendet.[40] Verbreitet wird der Begriff mithilfe von drei „V" umschrieben: *velocity, variety* und *volume*.[41] Kurz beschreibt Big Data damit die Möglichkeit des Zugriffs auf eine besonders große Menge digitaler Daten (*volume*), die eine unterschiedliche Art, Speicherform und Qualität aufweisen (*variety*) und in hoher Geschwindigkeit verarbeitet werden können (*velocity*).[42]

Das englische Wort *velocity* lässt sich mit „Geschwindigkeit" in die deutsche Sprache übersetzen. Das Charakteristikum ist insbesondere einschlägig, wenn große Daten in Echtzeit verarbeitet werden. Ein prominentes Beispiel für eine besonders schnelle Verarbeitung großer Datenmengen im Gesundheitswesen stellt das Phänomen *Google Flu Trends*[43] dar. Der amerikanische Konzern Google versuchte Ende des ersten Jahrzehnts der 2000er, anhand von Suchanfragen zu bestimmen, wo sich die jährlich auftretenden Grippewellen wann und wie schnell ausbreiten würden.[44] Die Vorhersagen waren jedoch nicht immer hinreichend belastbar.[45] Der Ansatz von Google konnte dennoch als Startpunkt für

---

durch Big Data, in: Hoffmann-Riem (Hrsg.), Big Data – regulative Herausforderungen, 2018, S. 11, 14.

[40] *Buchner* ZfME 2018, 131, 132.

[41] Zu Deutsch: Geschwindigkeit, Vielfalt, Volumen; vgl. *pars pro toto Raum*, in: Stiftung Datenschutzrecht, Big Data und E-Health, S. 135 f.; *Augsberg/von Ulmenstein* GesR 2018, 341, 341; *Buchner* ZfmE 2018, 131, 133; *Winkler* Frankfurter Forum, 2017, 22, 22.

[42] Angelehnt an *Hoffmann-Riem*, Rechtliche Rahmenbedingungen für und regulative Herausforderungen durch Big Data, in: Hoffmann-Riem (Hrsg.), Big Data – regulative Herausforderungen, 2018, S. 11, 19.

[43] Dieser wurde mittlerweile eingestellt, *Weber*, in: SZ, Google versagt bei Grippe-Vorhersagen, 14.03.2014, https://www.sueddeutsche.de/wissen/big-data-google-versagt-bei-grippe-vorhersagen-1.1912226 (Abrufdatum 06.01.2022).

[44] *Ginsberg/Mohebbi/Patel et al.* Nature 2009, 1012, 1012.

[45] *Lazer/Kennedy/King/Vespignani* Science 2014, 1203, 1203.

weitere Projekte genutzt werden, die die Grundprinzipien der Verarbeitung weiterentwickelten.[46]

Der Aspekt der Schnelligkeit der Verarbeitung kann jedoch nicht nur bei Echtzeitdaten beobachtet werden. Die Verarbeitung von Echtzeitdaten ist daher keine zwingende Voraussetzung für Big Data. Technische Möglichkeiten und sich stetig vergrößernde Speicherkapazitäten führen vielmehr dazu, dass auch andere große Datenmengen mittlerweile in kürzester Zeit durchforstet werden können.[47]

Variety wird im Kontext von Big Data in dem Sinne verstanden, dass eine Vielfalt von Datentypen und Datenquellen für die Analyse genutzt wird.[48] Insbesondere im Gesundheitswesen kann man auf die unterschiedlichsten Datenquellen treffen. Daten von Wearables,[49] Labortests oder ärztliche Behandlungsdokumentation stellen unterschiedliche Datenquellen in unterschiedlichen Formaten dar, die zusammen ein Bild des Patienten ergeben.

Volume beschreibt den Umfang der Datenmengen, die im Rahmen von Big Data verarbeitet werden. Das Gesundheitswesen stellt dabei eine besonders datenintensive Disziplin dar.[50] Abrechnungs- und Verwaltungsdaten ergänzen die umfangreiche Dokumentationspflicht, sodass gerade in der Medizin besonders viele Daten anfallen, die sich für Big Data-Analysen eignen.

Teilweise werden noch zwei weitere „V", *value* und *veracity*[51] zur Konkretisierung hinzugefügt, die die Wahrhaftigkeit und das Wertschöpfungspotential von Big Data verdeutlichen sollen.[52]

Die Alliteration der fünf „V" besagt zusammenfassend, dass große, vielfältige und in ihrer Aussage korrekte Datenmengen in hoher Geschwindigkeit (erkenntnis-)gewinnbringend verarbeitet werden.

Die ursprüngliche Definition wird von verschiedenen Akteuren aufgegriffen. Der Deutsche Ethikrat hat die fünf „V" in einer Form definiert, nach der Big Data einen Umgang mit großen Datenmengen beschreibt,

---

[46] So Professor Samuel Kou, Harvard University, in: *Gessat*, Neuer Anlauf für die Grippeprognose, Deutschlandfunk v. 18.11.2015, https://www.deutschlandfunk.de/suchmaschinen daten-neuer-anlauf-fuer-die-grippeprognose.676.de.html?dram:article_id=337312 (Abrufdatum: 14.11.2022).

[47] Vgl. dazu *Buchner* ZfME 2018, 131, 132 f.

[48] *Buchner* ZfME 2018, 131, 133.

[49] Wearables sind tragbare Computer, mit denen Körperfunktionen oder Körperaktivitäten, wie Puls oder Schrittanzahl, aufgezeichnet werden können.

[50] *Buchner* ZfME 2018, 131, 133.

[51] Zu Deutsch: Wertschöpfung (durch Informationsgewinn durch Big Data) und Wahrhaftigkeit.

[52] Vgl. *Krüger-Brand* DÄBl. 2015, 1026,1027; *Buchner* ZfME 2018, 131, 132 führt zudem noch die Begriffe Validity, Vulnerability und Volatility an.

„der darauf abzielt, Muster zu erkennen und daraus neue Einsichten zu gewinnen. Dazu sind angesichts der Fülle und Vielfalt der Daten sowie der Geschwindigkeit, mit der sie erfasst, analysiert und neu verknüpft werden, innovative, kontinuierlich weiterentwickelte informationstechnologische Ansätze notwendig."[53]

Auch in den deutschen Krankenkassen wird Big Data maßgeblich mit den fünf „V" charakterisiert. Nach einer Studie zu Big Data im Krankenversicherungsmarkt sind für die Leistungsträger nebst eines großen Datenvolumens[54] vor allem neue IT-Technologien und neue Auswertungsmethoden entscheidend für das Vorliegen von Big Data.[55]

Nach engerer Ansicht in der Literatur ist neben den fünf „V" die nachträgliche Zweckänderung der Datenerhebung kennzeichnendes Element von Big Data.[56] Danach sind Ziel und Zweck der Datenanalyse bei der Anwendung von Big Data nicht im Vorhinein festgelegt. Die Algorithmen sollen vielmehr ohne Ziel- und Zwecksetzung nach Clustern im Datenwald suchen.[57] Dies begründe gerade ihr für die Rechtsordnung disruptives Element.

Diese Ansicht betrachtet jedoch nur einen Teil der Möglichkeiten moderner Verarbeitungstechnologien und spricht vor allem die Datenverarbeitungsfunktion des Data Minings an. Gerade diese Form der Künstlichen Intelligenz birgt ein besonderes Konfliktpotential mit dem datenschutzrechtlichen Zweckbindungsgrundsatz.

In Abgrenzung zu Künstlicher Intelligenz ist jedoch festzuhalten, dass der Begriff von Big Data als neue Verarbeitungsform eine Form des *unsupervised learning* künstlicher Intelligenz umfasst. Er überschreitet den Bedeutungsgehalt künstlicher Intelligenz insoweit, als er auch Bezug auf die Menge der verarbeiteten Daten nimmt und zu Teilen so verstanden wird, dass er sich nur auf Verarbeitungsvorgänge richtet, die kein bestimmtes Ziel oder einen bestimmten Zweck verfolgen. Der Grund dafür liegt darin, dass Big Data sich nicht lediglich in der Verarbeitung von Daten ohne Zwecksetzung erschöpfen kann.[58] Die gezielte Auswertung von Daten birgt nämlich genau die gesteigerte Gefährlichkeit, die

---

[53] *Deutscher Ethikrat,* Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, 2017, S. 11, 54; *Martini* beschreibt Big Data als „eine disruptive technologische Entwicklung, die immer größere, heterogene Datenmengen immer schneller und immer tiefgliedriger auswertbar macht und dadurch einen Paradigmenwechsel in der Datenverarbeitung einläutet" DVBl 2014, 1481, 1482.

[54] Eher größer als Terabytes.

[55] *Radic/Radic* et al, Big Data im Krankenversicherungsmarkt, 2016, S. 6.

[56] *Buchner* ZfmE 2018, 131, 134; *Spindler* MedR 2016, 691, 691.

[57] *Buchner* ZfmE 2018, 131, 134.

[58] Im Gesundheitswesen wäre dann vermutlich kein „Big Data" mehr anzutreffen, s. dazu *Buchner* ZfmE 2018, 131, 134.

vielmehr Charakteristikum und Ursache für eine besondere Behandlung des neuen Datenverarbeitungsphänomens darstellen muss.

b) Gefährdung der informationellen Selbstbestimmung durch Big Data

Die besondere Gefährdung, die Big Data innewohnt, soll nun näher skizziert werden. Sie gibt Aufschluss, warum diese Art der Datenverarbeitung einer qualifizierten Untersuchung bedarf. Der Einzug neuer Verarbeitungsmethoden erschüttert das herkömmliche Datenschutzrecht nämlich in zweierlei Hinsicht: in juristischer und in gesellschaftlich-tatsächlicher Hinsicht.

Offensichtlich ist, dass Big Data eine grundsätzlich höhere grundrechtliche Eingriffstiefe besitzt als die klassische Datenverarbeitung. Die Eingriffstiefe begründet sich in der erhöhten Gefährlichkeit moderner Datenverarbeitungstechniken. Diese resultiert aus dem Ausmaß und der Geschwindigkeit der Datenverarbeitung und der Rekombination teils ungeordneter Daten, die Menschen ohne Hilfsmittel nicht möglich wäre. Während früher zur Erkennung von Korrelationen in tausenden Datensätzen noch viele Menschen beschäftigt werden mussten, gelingt dies einem Algorithmus heute in wenigen Sekunden.[59] Die schnellere, potentiell flächendeckendere und genauere Wissensgenerierung mithilfe von Daten stellt ein Novum für unser normativ-gesellschaftliches Zusammensein dar, das sich auf die Entfaltungsfreiheit des Einzelnen auswirken kann. Denn der Mensch ist Big Data in seinen kognitiven Fähigkeiten grundsätzlich unterlegen.

Von einigen Autoren wird die Gefahr von Big Data insbesondere darin gesehen, dass eine Echtzeitverarbeitung von verschiedenen Daten möglich ist. So könnte eine leistungsstarke Corona-App oder wohl auch Google abbilden, wo sich neue Infektionsherde von Pandemien wie COVID-19 oder Grippewellen bilden.[60] Für staatliche Akteure wie Behörden bietet es die Chance, in Krisensituationen schneller zu reagieren. Auf der Kehrseite bedeutet dies allerdings auch, dass Bürger stärker überwacht werden können. Gesundheitsbehörden können verstärkt kontrollieren, ob sich Personen eines bestimmten Einwohnerkreises an Auflagen halten. Zudem können sie – z. B. im Falle einer Pandemie – Schulen und Geschäfte schließen. Dies bedeutet harte Einschnitte in das Leben der Einzelnen, die ohne die Echtzeitverarbeitung – oder zumindest die sehr schnelle Verarbeitung von Daten – so nicht möglich wäre. Selbst ohne eine Pandemie, bei der die Bevölkerung Beschneidungen der Freiheit zugunsten einer höheren Ge-

[59] Korrelationen sind an dieser Stelle selbstverständlich noch von Kausalitäten, also begründeten Zusammenhängen zu unterscheiden. Korrelationen müssen erst validiert werden, bevor sie als Kausalität beschrieben werden können.

[60] Heute dürfte die Technik dazu auch schon weiter sein als im Jahr 2014, s. zu Google Flu Trends schon oben unter Fn. 43.

sundheitssicherheit hinnehmen mag, bedeutet das durch Big Data mögliche Tracking und Tracing jedenfalls einen tiefen Einblick in den aktuellen Gesundheitszustand und den damit einhergehenden aktuellen Lebenswandel.[61] Unternehmen können dieses Wissen potenziell nutzen, um anfälligere Zielgruppen für Werbung und Angebote für ihre Gesundheitsprodukte auszumachen.

Doch nicht nur aus der zeitnahen Verarbeitung von Daten können Freiheitsbeschränkungen für den Einzelnen resultieren, die der Datenschutz verhindern soll. Auch die erst nachträgliche Verarbeitung von Daten kann zu Nachteilen und Diskriminierung einzelner Personen führen. Kritisch wird dies dann, wenn die Prämienberechnung einer Versicherung auf pauschalisierenden Annahmen beruht. So wäre es hypothetisch möglich, dass im Rahmen einer Krankenversicherung in der Zukunft einem Bewohner eines sozialstrukturschwachen Stadtteils eine höhere Prämie angeboten wird, obwohl er sich selbst stets gesund ernährt, keine Krankheiten hat und viel Sport treibt – aber das generelle Risiko für gesundheitsschädigendes Verhalten in seinem Stadtteil oder seiner Stadt höher ist.[62] Erfolgt die Einordnung einer Person in ein Schema aufgrund einer nur vermeintlichen Kausalität, bedeutet dies einen besonders tiefgreifenden Eingriff.[63]

Zudem sind nicht nur die Betroffenen selbst von Nachteilen durch Datenwissen betroffen, die mit ihrer Datenpreisgabe gleichwohl den ersten Anstoß gegeben haben – auch Dritte, die keine Daten preisgegeben haben, über die aber öffentliche Informationen verfügbar sind, können potenziell in aus anderen Daten gewonnen Statistiken eingeordnet werden und dann ebenfalls Diskriminierung erfahren.[64]

Immer wieder wird zudem die Möglichkeit des erhöhten Risikos des Datenmissbrauchs bei Big Data Verarbeitungen genannt.[65] Grundsätzlich ist aufgrund der großen Datenlage, auf die Big Data Anwendungen regelmäßig gebaut ist, ein

---

[61] Vgl. dazu *Deutscher Ethikrat,* Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, 2017, S. 12.

[62] So etwas wurde bei der SCHUFA befürchtet, vgl. Bundesverband der Verbraucherzentralen, in: Handelsblatt, Ganzen Vierteln droht negative Kreditwürdigkeit, 02.05.2016, https://www.handelsblatt.com/finanzen/steuern-recht/recht/verbraucherschutz-ganzen-vierteln-droht-negative-kreditwuerdigkeit/13532810.html?ticket=ST-13296569-abIbs61gSALgQlMdMzRS-cas01.example.org (Abrufdatum: 14.11.2022); die genaue Berechnung des SCHUFA Scores muss SCHUFA nicht preisgeben, BGHZ 200, 38.

[63] So hat das BVerfG gerade in Fällen der Rasterfahndung hohe Anforderungen an die Rechtfertigung einer solchen Maßnahme gestellt, vgl. BVerfGE 115, 320, 341 ff.; dies ergibt sich zudem aus dem Rückschluss von Art. 22 DSGVO, nach dem nur in Ausnahmefällen Profiling betrieben werden darf.

[64] Vgl. für den medizinischen Bereich *Deutscher Ethikrat,* Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, 2017, S. 267; s. auch *Sackmann* PinG 2019, 277, 277.

[65] Vgl. EGMR NJOZ 2010, 696, 700; darauf verweisend *Spindler* MedR 2016, 691, 693;

tiefer gehender Einblick in die Persönlichkeit und Lebensführung möglich, als dies mit nur punktuellen Informationen denkbar ist. Dadurch erhöht sich das durch Missbrauch vermittelte Gefahrenpotential schon mit der Menge der erhobenen Daten.[66] Der Effekt wird verstärkt, indem Daten in der digitalisierten Gesellschaft einen hohen Wert haben, sodass sich ein Angriff auf eine Vielzahl von Datensätzen besonders lohnt. Dies gilt für sensible und sonst schwer zugängliche, intime Gesundheitsdaten umso mehr.

Insbesondere der Missbrauch durch den Staat wird von einigen Menschen gefürchtet.[67] Die spezifische deutsche Sensibilität erklärt sich gerade aus unserer Geschichte. Es ist kaum mehr als 30 Jahre her, dass in Teilen Deutschlands Einwohner flächendeckend technisch überwacht wurden und ihre persönliche Entscheidung der Lebensführung Konsequenzen für ihr berufliches und gesellschaftliches Fortkommen und ihren Lebensstil hatte.[68] Zwar ist heute gerade die staatliche Datenverarbeitung streng durch das Datenschutzrecht reglementiert und reguliert. Allerdings sind Gesetze nicht in Stein gemeißelt: Es besteht weiterhin die latente Gefahr, dass Gesetze und Regierungen sich so stark wandeln, dass ein geringerer Schutz für die persönliche Selbstbestimmung besteht. Die Daten wären dann indes für eine stärkere Überwachung erhoben.

Zudem dürfen Hackerangriffe fremder Regierungen nicht außer Acht gelassen werden. In China gilt zumindest für die Staatsbürger, dass sie aufgrund eines Scoring-Systems Vorteile erhalten, wenn sie sich in einer bestimmten Form verhalten.[69] Es ist nicht auszuschließen, dass China die Behandlung und die Einreiseerlaubnis von Touristen auch von solchen Informationen abhängig macht, die das Land zuvor – möglicherweise illegaler Weise – erhalten hat.

Schließlich verändert sich das Verhalten des Einzelnen durch die immer stärkere Omnipräsenz des Datenflusses. Er erleidet eine Verminderung der Kontrolle über seine Daten, wenn nicht gar einen Kontrollverlust: Denn der Laie kann oftmals nicht nachvollziehen, zu welchen Zwecken seine Daten verwendet werden könnten. Dazu gesellt sich regelmäßig das Gefühl, ohne Preisgabe der eigenen

---

ebenso *Deutscher Ethikrat,* Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, 2017, S. 17, 106; vgl. *Paal/Hennemann* NJW 2017, 1697, 1699.

[66] *Deutscher Ethikrat,* Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, 2017, S. 17.

[67] Nach einer Umfrage des Umfrageinstituts IfD-Allensbach aus dem Januar 2020 gaben 17 % der Menschen an, Sorge zu haben, dass der deutsche Staat die Bürger zu sehr überwacht, z. B. Internet- oder Telefonverbindung, Allensbacher Archiv, IfD-Umfrage 12014.

[68] S. Stasi-Unterlagen-Archiv mit weiteren Informationen zur Überwachung in der DDR, https://www.stasi-unterlagen-archiv.de (Abrufdatum 06.01.2022).

[69] *Yan*, in: SCMP, The village testing China's social credit system: driven by big data, its citizens earn a star rating, 02.06.2019, https://www.scmp.com/magazines/post-magazine/long-reads/article/3012574/village-testing-chinas-social-credit-system (Abrufdatum: 14.11.2022).

Daten sei die Nutzung bestimmter Dienste nicht mehr möglich. Dies führt schließlich dazu, dass der Einzelne regelmäßig in einen Datenexhibitionismus verfällt und nur noch stumpf in die Verarbeitung seiner personenbezogenen Daten einwilligt, ohne sich der Tragweite oder der Bedeutung der Preisgabe bewusst zu sein.[70]

c) Fazit

Zusammenfassend liegt somit dann Big Data vor, wenn ein Mensch mit seinen natürlichen kognitiven Fähigkeiten die Daten nicht in derselben Weise oder in verhältnismäßig längerer Zeit strukturieren oder auswerten kann wie ein Algorithmus. Die gesteigerte Leistungsfähigkeit kann insbesondere an den von den fünf „V" gesetzten Kriterien festgemacht werden. Die damit konstatierte Weite des Begriffs von Big Data erlaubt eine auch in die Zukunft gerichtete Lösungssuche. Dies ist gerade vor dem Hintergrund der sich immer noch und stetig weiterentwickelnden Datenwelt ein wichtiger Faktor für den Begriff.

Moderne Verarbeitungstechnologien können tatsächliche Gefährdungen der täglichen Freiheit von Betroffenen mit sich bringen. Hinzu kommt, dass viele Menschen aufgrund von Überforderung nur unachtsam ihr Recht auf informationelle Selbstbestimmung ausüben.

Die gesteigerte Gefährlichkeit, die eine besondere Untersuchung von Big Data rechtfertigt, liegt primär in seiner deutlich gesteigerten Leistungsfähigkeit gegenüber dem Menschen.[71] Die gesteigerte Leistungsfähigkeit liegt darin, dass Big Data aufgrund seiner Möglichkeit, riesige, auch aber nicht zwingend unstrukturierte Daten in hoher Geschwindigkeit auszuwerten, neue Optionen der Kontrolle und Überwachung zulässt. Hinzu kommt das Potential eines rasant wachsenden Erkenntnisgewinns über einen bestimmten Sachverhalt, dem ein latentes Diskriminierungspotential innewohnt. Diese neuen Potentiale von Big Data beschränken die freie Entfaltung des Menschen und stellen somit eine potenzierte Gefährdung der informationellen Selbstbestimmung dar. Allein diese Gefährdung rechtfertigt einen gesonderten Umgang von bestimmten Datenverarbeitungsmethoden, die hier unter den Begriff von Big Data fallen sollen.[72] Es bedarf somit regelmäßig einer Funktionsanalyse der eingesetzten Algorithmen.[73] Demgegenüber stehen jedoch Potentiale, die jedem Einzelnen von uns enorm nutzen können und die im nächsten Abschnitt näher erläutert werden sollen. Die

---

[70] Hierzu später ausführlich unter Kap. 3 B. II. d).

[71] Vgl. *Huss*, Künstliche Intelligenz, Robotik und Big Data in der Medizin, 2019, S. 60.

[72] Zu dem Big Data innewohnende Gefahrenpotential vgl. Kap. 1 II. 2. b).

[73] Vgl. *Buchner* ZfmE 2018, 131, 133.