universität wien

E X P O S É
zur
D I S S E R T A T I O N

Vorläufiger Arbeitstitel

Künstliche Intelligenz:
Eine grund- und datenschutzrechtliche Untersuchung

Dissertationsgebiet
IT-Recht

verfasst von

Mag. David Bierbauer

angestrebter akademischer Grad

Doctor iuris (Dr. iur.)

Wien, Februar 2020

Matrikelnummer	01404011
Studienkennzahl lt. Studienblatt	UA 992 942
Studienrichtung lt. Studienblatt	Doktoratsstudium der Rechtswissenschaften
Betreut von:	ao. Univ.-Prof. Dr. Christian M. Piska

Künstliche Intelligenz:
Eine grund- und datenschutzrechtliche Untersuchung

Machine-Learning-Verfahren und KI-gestützte Algorithmen
im Spannungsfeld der Rechtsordnung

Inhaltsverzeichnis

"We don't have better algorithms than anyone else;
we just have more data"[1]
Peter Norvig, director of research at Google

I. Problemaufriss

Die industrielle Revolution führte zu einer sukzessiven Übernahme von menschlichen Arbeiten durch Maschinen. Ähnliches Potenzial wird auch der **Digitalisierung** zugeschrieben. Wir sehen nun zum ersten Mal, dass nicht bloß mechanische, sondern auch geistige Arbeit, die bis dato dem Menschen vorbehalten war, von intelligenten Maschinen übernommen wird.[2] Dies gilt in besonderem Maße für den Einsatz von selbstlernenden, autonom handelnden Systemen, die Daten en masse verarbeiten und durch **automatisierte Entscheidungen** in die **Freiheiten** und **Rechte** von betroffenen Nutzern eingreifen.[3]

In diesem Zusammenhang gilt aber: Nicht alles was technisch möglich bzw wirtschaftlich gewünscht wird, ist rechtlich auch zulässig. Die vorliegende Arbeit soll die **grund- und datenschutzrechtlichen Grenzen** bei der Entwicklung von Künstlicher Intelligenz (KI) im weiteren Sinn aufzeigen, um eine gesunde, dem Menschen dienliche Nutzung dieser Technologie zu fördern.[4]

II. Forschungsstand

Die Forschung zu rechtlichen Fragen der künstlichen Intelligenz ist in Österreich noch nicht allzu weit fortgeschritten, beginnt sich aber, wohl auch aufgrund von politischen Impulsen[5] und der Etablierung einer Vielzahl von einschlägigen Institutionen,[6] stärker zu

---

1 *Norvig*, zitiert nach *Cleland*, Google's "Infringenovation" Secrets, Forbes 3.10.2011, abrufbar unter: <https://www.forbes.com/sites/scottcleland/2011/10/03/googles-infringenovation-secrets/?sh=682cfb4f30a6>(26.02.2021).

2 *Harari*, Sapiens: A Brief History of Humankind (2015); *Yeung*/*Lodge*, Algorithmic Regulation: An Introduction (2019).

3 *Konferenz der unabhängigen Datenschutzaufsichtsbehörden*, Hambacher Erklärung zur Künstlichen Intelligenz (3.4.2019) 2.

4 *Martini*, Blackbox Algorithmus - Grundfragen (2019) 27.

5 Für eine Übersicht zu Regulierungsinitiativen innerhalber der EU siehe *FRA*, AI policy initiatives (2016-2020), abrufbar unter: <https://fra.europa.eu/en/project/2018/artificial-intelligence-big-data-and-fundamental-rights/ai-policy-initiatives>(26.02.2021).

6 Für eine weltweite Übersicht nationaler Strategien zu AI siehe: *OECD*, AI Strategies & Public Sector Components, 23.1.2020, abrufbar unter: <https://oecd-opsi.org/projects/ai/strategies https://oecd-opsi.org/projects/ai/strategies/>(26.02.2021).

verdichten.[7] Auf europäischer Ebene kann auf eine große Anzahl von Policy Papers zurückgegriffen werden, welche das Thema auf abstrakter Ebene behandeln.[8] Ferner wurden bereits umfangreiche Gutachten erstellt, welche die Thematik aus verschiedenen (rechtlichen) Blickwinkeln beleuchten.[9] Es besteht aber weiterhin **dringender Forschungsbedarf** zu konkreten rechtlichen Fragestellungen: Bestehende Literatur beschäftigt sich vor allem mit bereits fertig erstellten KI-Modellen.[10] Wenig, bis gar nicht untersucht wurde bis dato die **Trainingsphase**, in der das eigentliche KI-Modell entwickelt wird.[11] Gerade diese Phase ist jedoch aus Gesichtspunkten der **Transparenz**, **Sicherheit** und **Erklärbarkeit** besonders relevant.[12] Die gegenständliche Dissertation soll daher den **gesamten Lebenszyklus** eines KI-Systems, angefangen mit der Erhebung der Trainingsdaten bis hin zum Einsatz des fertigen Modells bzw Algorithmus untersuchen, und hierbei einen besonderen Fokus auf die **Trainingsphase** von KI-Modellen legen.

III. Ziel des Forschungsprojekts

1. Allgemeine Ziele

Ziel der vorliegenden Arbeit ist die Förderung von **vertrauenswürdigen**, **transparenten KI-Systemen**. KI-Systeme stellen (für Internetnutzer) oftmals eine **Blackbox** dar: Es ist für den Nutzer meist nicht ersichtlich (i.) ob KI-Systeme zum Einsatz kommen und (ii.) wie diese Systeme entwickelt wurden bzw ob auch personenbezogene Daten der Nutzer selbst für die Entwicklung verarbeitet wurden. Darüber hinaus stand bis vor kurzem die **technische Innovation** der Technologie so stark im Vordergrund, dass **Transparenz**, **Datensicherheit** und **Manipulationspotenzial** bis dato eher vernachlässigt wurden. Verschärfend kommt hinzu, dass die Rechtslage durch die Neuartigkeit des Phänomens, bzw die starke Verflechtung mit

---

7 Kritisch *Veale*, A Critical Take on the Policy Recommendations of the EU High-Level Expert Group on Artificial Intelligence, European Journal of Risk Regulation 2020, 1; vgl auch *Eisenberger*, Innovation im Recht (2016) 61.

8 Siehe Literaturverzeichnis.

9 Vgl etwa *Datenethikkommission der dt. Bundesregierung*, Gutachten der Datenethikkommission (2019); *Aichroth* et al, Anonymisierung und Pseudonymisierung von Daten für Projekte des maschinellen Lernens (Fraunhofer 2020); *Gesellschaft für Informatik*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren. Studien und Gutachten im Auftrag des Sachverständigenrats für Verbraucherfragen (2018); *Europarat*, A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework, MSI-AUT(2018)05 rev, 22.5.2019.

10 Va Haftungsfragen wurden bereits eingehend thematisiert: vgl bspw *Reinisch*, Haftungsfragen 4.0, ÖJZ, 298; *Expert Group on Liability for New Technologies*, Liability for Artificial Intelligence (2019).

11 Auf diese Problematik hinweisend ua *Lehr/Ohm*, Playing with the Data: What Legal Scholars Should Learn About Machine Learning, University of California, Davis, Vol 51:6, 656.

12 Aus datenschutzrechtlicher Sicht insb Art 5, 25, 32 DSGVO.

der Informationstechnologie, in vielen Fragen ungeklärt ist. Es braucht daher dringend klare Regeln für den Umgang mit dieser Technologie. Das Dissertationsprojekt soll die undurchsichtige Rechtslage erhellen, und Lösungsansätze zu relevanten Problemen herausarbeiten, ohne den **Innovationsgehalt** der Technologie zu untergraben.

2. Forschungsfragen

Das gegenständliche Forschungsprojekt soll sowohl die **Trainingsphase von KI (Forschungsfrage I.)**, als auch den **Einsatz von bereits trainierten KI-Modellen (Forschungsfrage II.)** untersuchen (vgl Abbildung 1[13] zur Unterscheidung). Hauptfokus der vorliegenden Arbeit sollen jedoch die Untersuchungen zur **Forschungsfrage I** bilden, zumal diese Phase in der bisherigen Forschung noch wenig(er) Beachtung gefunden hat.

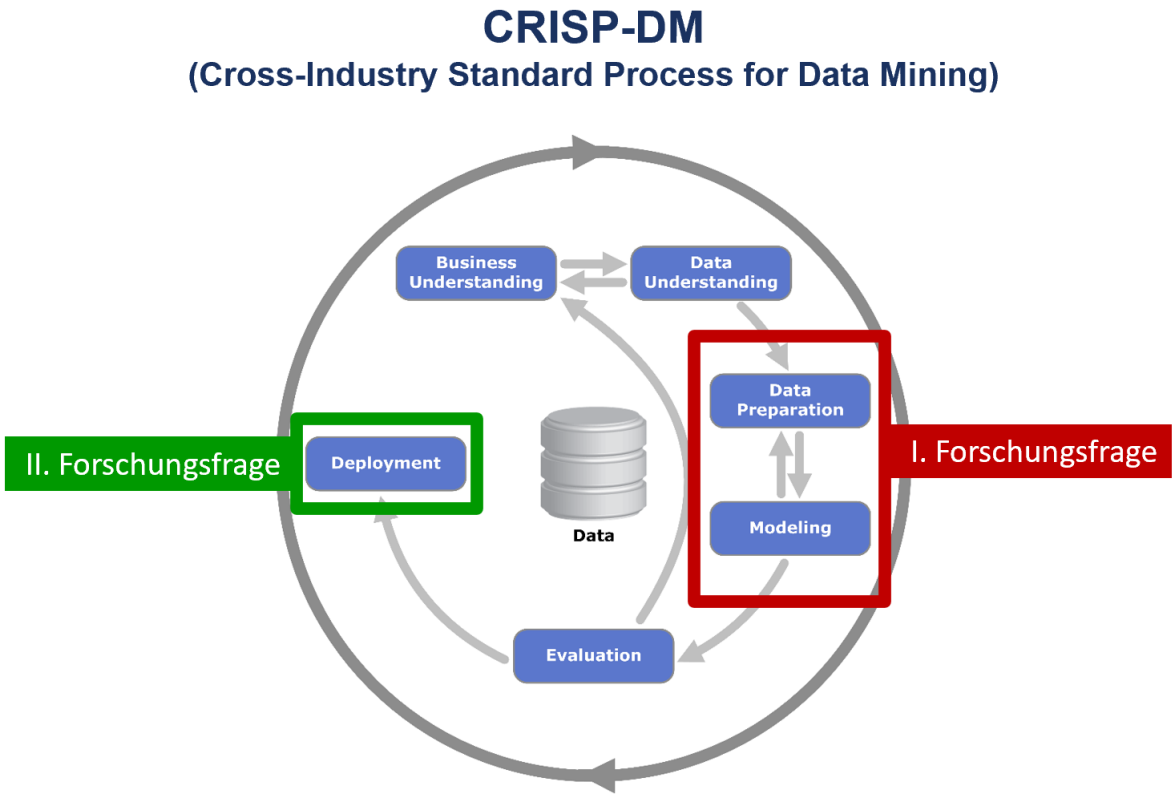

Abbildung 1: Entwicklungszyklus eines KI-Modells nach dem branchenübergreifenden Standard für KI-Entwicklung „CRISP-DM“.[1]

[13] *IBM Corporation*, IBM SPSS Modeler CRISP-DM Guide (2016) 1, abrufbar unter: ftp://public.dhe.ibm.com/software/analytics/spss/documentation/modeler/18.0/en/ModelerCRISPDM.pdf.

I. Welche grund- und datenschutzrechtlichen Rahmenbedingungen sind bei der Entwicklung von Machine Learning-Modellen in der Trainingsphase zu beachten?

Insb folgende Fragestellungen sollen in diesen Teil der Untersuchung einfließen:[14]

- Wann liegt ein Personenbezug iSd DSGVO vor (relativer vs absoluter vs risikobasierter Ansatz)?[15]
- Welche (gängigen) Anonymisierungstechniken genügen den Ansprüchen der DSGVO?[16]
- Ist Anonymisierung bereits eine Verarbeitung iSv Art 2 DSGVO?[17] Ist das Erstellen von synthetischen Trainingsdaten bereits eine Verarbeitung?
- Wann liegt Personenbezug in Federated Learning-Umgebungen vor?
  Wie ist Secure-Multiparty-Computation datenschutzrechtlich einzuordnen?
- Wie kann den Prinzipien von Privacy by Design/Privacy by Default nach Art 25 DSGVO im Modellierungsprozess entsprochen werden?
- Sind die Grundsätze der Erklärbarkeit und Transparenz in KI-Umgebungen überhaupt umsetzbar? Wenn nicht, wie kann trotzdem ein hinreichendes Schutzniveau de lege ferenda erreicht werden.
- Welche praktischen (datenschutzrechtlichen) Probleme stellen sich bei der Verwendung von Pre-Trained-Models?
- Wie sind "vergiftete" Trainingsdaten zu qualifizieren und welche rechtlichen Konsequenzen lösen Sie aus?[18]

II. Welche grund- und datenschutzrechtlichen Rahmenbedingungen sind beim Einsatz von Machine Learning-Modellen zu beachten?

Insb folgende Fragestellungen sollen in diesen Teil der Untersuchung einfließen:[19]

- Wie kann den Vorgaben der automatisierte Entscheidungsfindung nach Art 22 DSGVO beim Einsatz von KI-gestützten Systemen entsprochen werden?

---

[14] Die angeführten Fragestellungen sind als beispielhafte Aufzählung zu verstehen und stellen keine finale Abgrenzung der Untersuchung dar.

[15] *Klar/Kühling* in *Kühling/Buchner*, DS-GVO[3], Art 4 Nr. 1; *Finck/Pallas*, They who must not be identified – Distinguishing Personal from Non-Personal Data under the GDPR, Max Planck Institute for Innovation and Competition Research Paper No. 19-14; *Gellert*, The risk-based approach to data protection (Oxford University Press 2020); *Gonçalves*, The risk-based approach under the new EUdata protection regulation: a critical perspective, Journal of Risk Research 2020, 23:2, 13; EuGH 19.10.2016, C-582/14 (Breyer).

[16] *Art-29-Datenschutzgruppe*, WP 216, Opinion 05/2014 on Anonymisation Techniques.

[17] So etwa *Knyrim*, Datenschutz & Coronakrise, Dako 2020, 391.

[18] *Biggio*/*Roli*, Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning, ArXiv 19.7.2018.

[19] Die angeführten Fragestellungen sind als beispielhafte Aufzählung zu verstehen und stellen keine finale Abgrenzung der Untersuchung dar.

- Welche Rechtfertigungsgründe kommen beim Einsatz von KI-Modellen in Betracht?
  Wie ist sind die Ausgangs-(Interessen) bei Abwägungen nach Art 6 verteilt und gewichtet?
- Wie können Betroffenenrechte wahrgenommen werden? Welche Auswirkungen hat diese Wahrnehmung auf das zugrundeliegende Modell? Wie ist etwa mit einem Löschungsanspruch nach Art 17 DSGVO umzugehen, wenn das KI-Modell bereits vollständig trainiert wurde?
- Inwieweit ist Überwachung (etwa mit Facial-Recognition-Software) durch KI-Systeme zulässig?

IV. Relevanz und Breitenwirkung

1. Für Internetnutzer

Internetnutzer haben sich mittlerweile daran gewöhnt, dass viele Online-Services und Plattformen "**gratis**" sind. Es ist für Nutzer in diesem Zusammenhang aber oftmals nicht klar, dass ihre personenbezogenen Daten in erheblichem Ausmaß als **Trainingsdaten** für KI-Systeme herangezogen werden, bzw, dass sie damit einhergehend **automatisierter Entscheidungsfindung** und **Profiling** ausgesetzt sind. Die Nutzer exponieren sich dadurch besonders stark, weil die Entwicklung von KI-Systemen zum jetzigen Zeitpunkt die nötige Sensibilität und Sicherheit in der Verarbeitung von Nutzerdaten (noch) vermissen lässt. Hierbei profitieren die Plattformbetreiber von der **unklaren Rechtslage** und vom regulatorisch schwer einzufangenden **Problempotential** der Technologie. Die Forschungsergebnisse der Arbeit sollen durch konkrete Untersuchung der zugrundeliegenden Datenverarbeitungen klare Grenzen für die Entwicklung und den Einsatz von KI ziehen, und darüber hinaus Möglichkeiten für eine effektive Wahrnehmung der **datenschutzrechtlichen Betroffenenrechte** aufzeigen.[20]

2. Für KI-Entwickler

In der Praxis ergeben sich für Software-Entwickler eine Vielzahl von ungeklärten Fragen.[21] Wie ist etwa vorzugehen, wenn eine betroffene Person aus den Trainingsdaten einen

[20] Vgl etwa zur Anspannung der verschiedenen Grundsätze in der DSGVO etwa: *Veale/Binns/Ausloos,* When data protection by design and data subject rights clash, International Data Privacy Law 2018, 105.

[21] *Spindler/Schmechel,* Personal Data and Encryption in the European General Data Protection Regulation, JIPITEC 2016, 163.

Löschungsanspruch nach Art 17 DSGVO geltend macht? Aus dem fertig-trainierten Modell kann der einzelne Datensatz nicht mehr herausgelöst werden. Muss das KI-Modell dann – ohne den relevanten Datensatz – neu trainiert werden? Wie viele identifizierende Elemente müssen aus einem Datensatz entfernt werden, um eine Anonymisierung zu erreichen?[22] Wie muss ein KI-Modell unter Berücksichtigung von Privacy by Design und Datensicherheit DSGVO-konform trainiert werden?[23] Die vorliegende Arbeit soll auf Basis der technischen Realität konkrete Antworten auf diese und ähnlich gelagerte Fragen herausarbeiten.

3. Soziale und gesellschaftliche Aspekte

KI-Systeme können selbst bei guten Absichten **ungewollten Schaden** anrichten. **Diskriminierende Ergebnisse**, die von KI-Systemen generiert wurden, waren in der Vergangenheit keine Seltenheit. So erkannte eine KI etwa Menschen mit schwarzer Hautfarbe als Affen, weil sie ungewolllt mit **rassistischen Trainingsdaten** aus sozialen Medien entwickelt wurde.[24] Die **Erklärbarkeit** von KI-gestützten Entscheidungen stellt daher ein großes Spannungsfeld dar und fordert die technischen Möglichkeiten der KI-Entwicklung in besonderem Maße heraus.[25]

Ferner ergibt sich in Bereichen wo Entscheidungen an automatisierte Systeme ausgelagert werden, wie etwa beim **autonomen Fahren**, ein sehr hohes **Risikopotenzial**: Falsch erkannte Verkehrszeichen können so zu lebensgefährlichen Situationen führen.[26] Daneben kommt automatisierte Entscheidungsfindung in anderen Rechtsordnungen auch bei Gerichten schon zur Anwendung.[27] KI-Systeme sollten daher, neben der vielfach geforderten **Erklärbarkeit**, auch gegenüber **Angriffen** und **Manipulation** möglichst resistent sein, und zwar sowohl in technischer als auch rechtlicher Hinsicht.

---

22 *Art-29-Datenschutzgruppe*, WP 216, Opinion 05/2014 on Anonymisation Techniques*; Haimberger/Geuer*, Dako 2018, 57; *Pordesch/Steidle*, Entfernen des Personenbezugs mittels Verschlüsselung durch Cloudnutzer, DuD 2015, 536.

23 *EDSA*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 13.11.2019.

24 *Devlin*, AI programs exhibit racial and gender biases, research reveals, TheGuardian, 13.3.2017, abrufbar unter: <https://www.theguardian.com/technology/2017/apr/13/ai-programs-exhibit-racist-and-sexist-biases-research-reveals>(26.02.2021).

25 *Wachter/Mittelstadt/Russell*, Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI, SSRN Electronic Journal 2020, 4; *Mittelstadt/Russell/Wachter*, Explaining Explanations in AI (2018).

26 Für eine Übersicht zu Angriffen auf KI-Modelle vgl *Biggio*/*Roli*, Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning, ArXiv 19.7.2018.

27 *Susskind*, Online Courts and the Future of Justice (2019) 273.

4. Basis für weitere Forschung

Die stetig fortschreitende Digitalisierung strahlt als **disruptive Strömung** in sämtliche Lebensbereiche des Menschen aus. Es ist daher davon auszugehen, dass sich die Fragen rund um Künstliche Intelligenz in Zukunft noch weiter verästeln und vertiefen werden. Die Arbeit eignet sich daher als Grundlage für weiterführende Forschung im Verfassungs- und Datenschutzrecht, sowie in weiteren Rechtsgebieten. Ferner kann das Vorhaben auch als **rechtliche Leitlinie** für technische Arbeiten dienen.

V. Angewandte Methode

Zur Verwirklichung der Ziele des Projekts wird ein **interdisziplinärer Ansatz** verfolgt, indem sowohl technische als auch rechtliche Aspekte untersucht werden. Hierbei soll der **gesamte Lebenszyklus** des KI-Systems, von der Entwicklung bis hin zum Einsatz des fertigen Systems, behandelt werden. Zur Erarbeitung der technischen Grundlagen sind Teilnahmen an Lehrveranstaltungen der TU Wien, respektive Gespräche mit Experten dieses Bereichs, vorgesehen. Nach Klärung der **technischen Rahmenbedingungen** erfolgt die eigentliche rechtliche Untersuchung, welche den Hauptteil der Arbeit darstellt. Die Analyse der relevanten Rechtsnormen geschieht hierbei unter Zuhilfenahme des Kanons, der in der Rechtswissenschaft anerkannten Interpretationsmethoden. In dieser Phase soll auch auf Policy Papers von europäischen Institutionen zurückgegriffen werden. Abschließend soll ein Use-Case definiert werden, auf den die erarbeiteten Erkenntnisse beispielhaft angewendet werden.

VI. Geplanter Gang der Untersuchung

Im letzten Semester wurde bereits eine umfassende Literatur- und Judikaturrecherche zum Dissertationsvorhaben durchgeführt. Außerdem wurden einschlägige technische Lehrveranstaltungen an der TU Wien besucht. Auf Basis der dadurch gewonnen Erkenntnisse wurde das Dissertationsvorhaben bereits erfolgreich fakultätsöffentlich präsentiert. Die Verfassung der Dissertation steht damit kurz vor ihrem eigentlichen Beginn. Der vorläufige weitere Zeitplan des Projekts gestaltet sich wie folgt:

Zeitplan der Untersuchung

Sommersemester 2020	• Besuch von technischen Lehrveranstaltungen an der TU Wien - 184.735 Einführung in die Künstliche Intelligenz - 184.702 Machine Learning - 194.055 Sicherheit, Privacy und Erklärbarkeit in Maschinellem Lernen • Umfassende Recherche zu einschlägiger Literatur
Wintersemester 2020	• Besuch von weiterführenden Lehrveranstaltungen an der TU Wien • Verfassen des Kapitels zu den technischen Grundlagen von KI • Grundlagenarbeit zu den rechtlichen Ausführungen
Sommersemester 2021	• Verfassen des Hauptteils zu Datenschutzrecht • Verfassen des Hauptteils zu Grundrechten
Wintersemester 2021	• Durchführen der Case-Study • Abgabe der Erstfassung und Abstimmung mit dem Betreuer • Vornahme von Korrekturen
Sommersemester 2022	• Abgabe der Endfassung • Öffentliche Defensio und Abschluss

VII. Vorläufige Gliederung

I. Einleitung und Problemaufriss
   A. Arbeitsdefinition von KI
      1. Technische Definition
      2. Rechtliche Definition
   B. Machine Learning
      1. Classification
      2. Regression
   C. Unsupervised Learning
      1. Deep Learning
      2. Neuronale Netzwerke

II. Technische Rahmenbedingungen
   A. CRISP-Modell
   B. Trainingsdaten
   C. Informationssicherheit im Machine Learning-Prozess
      1. Angriff: Vergiftete Trainingsdaten
      2. Angriff: Trigger in Trainingsdaten
   D. Informationssicherheit beim Einsatz von bereits trainierten KI-Modellen
      1. Angriff: Manipulierte Eingabedaten
      2. Angriff: Model Stealing

III. Datenschutzrechtliche Untersuchung
   A. Personenbezug
      1. Historische Hintergründe
      2. Absolute Theorie
      3. Relative Theorie
      4. Risikobasierter Ansatz
      5. Personenbezug nach der DSGVO
   B. Verarbeitung
   C. Grundsätze für die Verarbeitung
      1. Transparenz und Erklärbarkeit der Verarbeitung
      2. Zweckbindung
   D. Rollenverteilung nach der DSGVO
      1. Betroffene Person
      2. Verantwortlicher

3. Auftragsverarbeiter

E. Rechtmäßigkeit der Verarbeitung

1. Einwilligung
2. Berechtigtes Interesse

F. Betroffenenrechte

1. Recht auf Auskunft
2. Recht auf Berichtigung
3. Recht auf Löschung
4. Recht auf Widerspruch

G. Privacy by Design / Privacy by Default

H. Datensicherheit

I. Automatisierte Entscheidungsfindung

IV. Grundrechtliche Untersuchung

A. Vertrauenswürdige KI

1. Europäische Zielsetzungen
2. Rechtmäßig, ethisch und robust?

B. Achtung der Menschenwürde

C. Liberales Grundprinzip

D. Grundrecht auf Datenschutz

E. Grundrecht auf Achtung des Privat- und Familienlebens

V. Case-Study Machine Learning: Von Trainingsdaten bis zum fertigen Modell

A. Rechtmäßigkeit der Verarbeitung in der Trainingsphase

1. Personenbezug
2. Minimierung der Rückführbarkeit auf natürliche Personen
3. Verantwortlichkeit in der Trainingsphase
4. Rechtfertigungsgrundlage
5. Wahrnehmung der Betroffenenrechte in der Trainingsphase

B. Rechtmäßigkeit beim Einsatz des KI-Modells

1. Verarbeitung
2. Verantwortlichkeit beim Einsatz des Modells
3. Rechtfertigungsgrundlage
4. Automatisierte Entscheidungsfindung nach Art 22 DSGVO
5. Wahrnehmung der Betroffenenrechte

VIII. Vorläufiges Literaturverzeichnis (Auswahl)

1. Technische Literatur

Biggio Battista / Rolia Fabio, Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning, ArXiv 19.7.2018

Bishop Christopher, Pattern Recognition And Machine Learning (Springer 2006)

Brundage Miles / Avin Shahar / Clark Jack / Toner Helen / Eckersley Peter / Garfinkel Ben / Dafoe Allan / Scharre Paul / Zeitzoff Thomas / Filar Bobby / Anderson Hyrum / Roff Heather / Allen Gregory / Steinhardt Jacob / Flynn Carrick / hÉigeartaigh Seán / Beard Simon / Belfield Haydn / Farquhar Sebastian / Amodei Dario, The Malicious Use of Artificial Intelligence: Forecasting Prevention and Mitigation (Oxford University Press 2018)

Carlini Nicholas/ Tramer Florian/ Wallace Eric/ Jagielski Matthew/ Herbert-Voss Ariel/ Lee Katherine/ Roberts Adam/ Brown Tom/ Song Dawn/ Erlingsson Ulfar/ Oprea Alina/ Raffel Colin, Extracting Training Data from Large Language Models, arXiv 2020, abrufbar unter: < https://arxiv.org/abs/2012.07805>()

Ethem Alpaydin, Machine Learning: The New AI (MIT Press 2016)

McCarthy John, What is Artificial Intelligence, 12.11.2007, abrufbar unter: <http://jmc.stanford.edu/articles/whatisai.html>(13.1.2021)

McCarthy John / Minsky Nathaniel / Rochester Nathaniel / Shannon Claude E, A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31 1955, AI Magazine 2006, Vol 27 (No 4), 12

Pfitzmann Andreas / Hansen Marit, Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology, 15.2.2008

Russell Stuart / Norvig Peter, Artificial Intelligence: A Modern Approach[3] (Pearson Education 2010)

Turing Alan, Computing and Machinery, Mind 1950, Vol 59, No 236, 433

Witten Ian H / Frank Eibe / Hall Mark A / Pal Christopher J, Data Mining Practical Machine Learning Tools and Techniques[4] (Elsevier Inc 2017)

2. Policy Papers, Gutachten

Aichroth Patrick / Battis Verena / Dewes Andreas / Dibak Christoph / Doroshenko Vadym / Geiger Bernd / Graner Lukas / Holly Steffen / Huth Michael / Kämpgen Benedikt / Kaulartz Markus / Mundt Michael / Rapp Hermann / Steinebach Martin / Sushko Yurii / Swarat Dominic / Winter Christian / Weiß Rebekka, Anonymisierung und Pseudonymisierung von Daten für Projekte des maschinellen Lernens (Fraunhofer 2020), abrufbar unter: < http: / /publica.fraunhofer.de /documents /N-605681.html>(26.02.2021)

Bitkom Bundesverband Informationswirtschaft, Anonymisierung und Pseudonymisierung von Daten für Projekte des maschinellen Lernens (Bitkom 2020)

Datenethikkommission der dt. Bundesregierung, Gutachten der Datenethikkommission (2019), abrufbar unter: <https://datenethikkommission.de/wp-content/uploads/191028_DEK_Gutachten_bf.pdf>(26.02.2021)

Dede G / Hamon R / Junklewitz H / Naydenov R / Malatras A / Sanchez I, Cybersecurity challenges in the uptake of artificial intelligence in autonomous driving, EUR 30568 EN (Publications Office of the European Union 2021), doi:10.2760/551271, JRC122440

Europäische Kommission, WHITE PAPER. On Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65 final, abrufbar unter: <https://ec.europa.eu/info/files/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en>

Europäische Kommission, Künstliche Intelligenz für Europa, COM(2018) 237 final, abrufbar unter: <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52018DC0237&from=EN>

Europarat, Towards a Regulation of AI Systems, DGI (2020)16, abrufbar unter: <https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da>

Europarat, Feasibility Study on a legal framework on AI design, development and application based on CoE standards, CAHAI(2020)23, abrufbar unter: <https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da>

Europarat, A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework, MSI-AUT(2018)05 rev, 22.5.2019

Expert Group on Liability for New Technologies, Liability for Artificial Intelligence (2019)

Gesellschaft für Informatik, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren. Studien und Gutachten im Auftrag des Sachverständigenrats für Verbraucherfrag (2018), abrufbar unter: <https://www.svr-verbraucherfragen.de/wp-content/uploads/GI_Studie_Algorithmenregulierung.pdf>(26.02.2021)

Hochrangige Expertengruppe für Künstliche Intelligenz (HEG-KI), Ethik-Leitlinien für eine vertrauenswürdige KI, 8.4.2019

Hochrangige Expertengruppe für Künstliche Intelligenz (HEG-KI), A Definition of AI: Main Capabilities and Disciplines, 8.4.2019

Hochrangige Expertengruppe für Künstliche Intelligenz (HEG-KI), Policy and investment recommendations for trustworthy AI, 26.6.2019

Zuboff Shoshana, The Age of Surveillance Capitalism (Profile Books 2019)

3. Juristische Literatur

3.1 Kommentare

Brink Stefan / Wolff Heinrich Amadeus (Hrsg), BeckOK Datenschutzrecht (Stand 1.11.2020)

Ehmann Eugen /Selmayr Martin (Hrsg), Datenschutz-Grundverordnung[2] (Wien 2018)

Kneihs Benjamin / Lienbacher Georg (Hrsg), Rill-Schäffer-Kommentar Bundesverfassungsrecht. 23. Lieferung (Wien 2020)

Knyrim Rainer, Der DatKomm. Praxiskommentar zum Datenschutzrecht, DSGVO und DSG (Wien 2018)

Korinek Karl / Holoubek Michael / Bezemek Christoph / Fuchs Claudia / Martin Andrea / Zellenberg Ulrich E. (Hrsg), Österreichisches Bundesverfassungsrecht (Loseblattausgabe inkl 15. Lfg), (Verlag Österreich 2019)

Kühling Jürgen / Buchner Benedikt, DS-GVO. Datenschutz-Grundverordnung – Kommentar[3] (München 2020)

Paal Boris / Pauly Daniel (Hrsg), Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO BDSG[3] (Beck 2021)

Simitis, Spiros / Hornung, Gerrit / Spiecker, *Indra* (Hrsg), Datenschutzrecht - DSGVO mit BDSG (Baden-Baden 2019)

3.2 Stellungnahmen, Leitlinien, Monografien, Sammelwerke

Art-29-Datenschutzgruppe, WP 260 rev.01, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 11.4.2018

Art-29-Datenschutzgruppe, WP 259 rev.01, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679

Art-29-Datenschutzgruppe, WP 251 rev.01, Leitlinien zu automatisierten Entscheidungen im Einzelfall 2016/679, 06.02.2018

Art-29-Datenschutzgruppe, WP 247, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)

Art-29-Datenschutzgruppe, WP 240, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)

Art-29-Datenschutzgruppe, WP 216, Opinion 05/2014 on Anonymisation Techniques

Art-29-Datenschutzgruppe, WP 169, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter"

Art-29-Datenschutzgruppe, WP 136, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ 01248/07/DE

Barfield Woodrow / Pagallo Ugo, Research handbook on the law of artificial intelligence (Edward Elgar Publishing 2018)

Ebers Martin / Heinze Christian / Krügel Tina / Steinrötter Björn / Beck Susanne, Künstliche Intelligenz und Robotik: Rechtshandbuch (C.H.Beck 2020)

Eisenberger Iris, Innovation im Recht (Springer 2016)

Europäischer Datenschutzuausschuss (EDSA), Guidelines 07/2020 on the concepts of controller and processor in the GDPR

Europäischer Datenschutzuausschuss (EDSA), Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 13.11.2019

Gellert Raphaël, The risk-based approach to data protection (Oxford University Press 2020)

Haase Martin, Datenschutzrechtliche Fragen des Personenbezugs: eine Untersuchung des sachlichen Anwendungsbereiches des deutschen Datenschutzrechts und seiner europarechtlichen Bezüge (Mohr Siebek 2015)

Holzinger Andreas, Kieseberg Peter, Tjoa A Min, Weippl Edgar (Hrsg), Machine Learning and Knowledge Extraction (Springer 2020)

Kaulartz Markus / Braegelmann Tom, Rechtshandbuch Artificial Intelligence und Machine Learning (C.H.Beck 2020)

Krapinger Gernot (Hrsg), Aristoteles Nikomachische Ethik übersetzt (Reclam 2018)

Krönke Christoph, Öffentliches Digitalwirtschaftsrecht. Grundlagen – Herausforderungen und Konzepte – Perspektiven (Mohr Siebeck 2020)

Jahnel Dietmar / *Sramek,Jan*, NZR. Neue Zitierregeln[2] (Wien 2017)

Martini Mario, Blackbox Algorithmus - Grundfragen (Springer-Verlag 2019)

Yeung Karen / *Lodge Martin* (Hrsg), Algorithmic Regulation (Oxford University Press 2019)

3.3 Beiträge in Fachzeitschriften

Apel/*Kaulartz*, Rechtlicher Schutz von Machine Learning-Modellen, RDi 2020, 24

Bygrave Lee A, Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements, Oslo Law Review 2017, Vol 4, 105

Dettling/Krüger, Digitalisierung, Algorithmisierung und Künstliche Intelligenz im Pharmarecht, PharmR 2018, 513

Dettling/Krüger, Erste Schritte im Recht der Künstlichen Intelligenz, MMR 2019, 211

EAID, Sprachassistenten und das KI-Dilemma, ZD-Aktuell 2019, 06780

Finck/Pallas, They who must not be identified – Distinguishing Personal from Non-Personal Data under the GDPR, Max Planck Institute for Innovation and Competition Research Paper No. 19-14

Gaede, Künstliche Intelligenz - Rechte und Strafen für Roboter? (2019)

Gausling, Künstliche Intelligenz im digitalen Marketing, ZD 2019, 335

Gellert Raphaël, Understanding the notion of risk in the General Data Protection Regulation, Computer Law & Security Review 2018, Volume 34, Issue 2, 279

Gonçalves Maria Eduarda, The risk-based approach under the new EUdata protection regulation: a critical perspective, Journal of Risk Research 2020, 23:2, 13

Grapentin, Algorithmen, Künstliche Intelligenz und Wettbewerb, NJW 2019, 181

Graf von Westphalen, Das erschöpfte liberale Recht, IWRZ 2019, 61

Graf von Westphalen, Tastende Versuche, Rechtsrisiken künstlicher Intelligenz einzuhegen, IWRZ 2018, 193

Guggenberger, Einsatz künstlicher Intelligenz in der Verwaltung

Härtel, Digitalisierung im Lichte des Verfassungsrechts – Algorithmen, Predictive Policing, autonomes Fahren, LKV 2019, 49

Heldt, Algorithmen und künstliche Intelligenz in der Verwaltung, NVwZ 2019, 862

Herberger, Künstliche Intelligenz und Recht

Hoeren/Niehoff, KI und Datenschutz – Begründungserfordernisse automatisierter Entscheidungen, RW Rechtswissenschaft 2018/1, 47

Keßler, Intelligente Roboter – neue Technologien im Einsatz, MMR 2017, 589

Klaas, Demokratieprinzip im Spannungsfeld mit künstlicher Intelligenz

Lehr David / Ohm Paul, Playing with the Data: What Legal Scholars Should Learn About Machine Learning, University of California, Davis, Vol 51:6, 653

Meyer, Künstliche Intelligenz und die Rolle des Rechts für Innovation, ZRP 2018, 233

Mittelstadt Brent / Russell Chris / Wachter Sandra, Explaining Explanations in AI (2018)

Nugel, Auslesen von Fahrzeugdaten auf Grundlage der DS-GVO

Ohm Paul, Broken promises of privacy: responding to the surprising failure of anonymization, UCLA LAW REVIEW 2010, 1701

Ory/Sorge, Schöpfung durch Künstliche Intelligenz, NJW 2019, 710

Pieper, Wenn Maschinen Verträge schließen Willenserklärungen beim Einsatz von Künstlicher Intelligenz, GRUR-Prax 2019, 298

Pordesch/Steidle, Entfernen des Personenbezugs mittels Verschlüsselung durch Cloudnutzer, DuD 2015, 536

Schindler, Künstliche Intelligenz und Datenschutz-Recht, ZD-Aktuell 2019, 06647

Schliesky, Digitalisierung – Herausforderung für den demokratischen Verfassungsstaat, NVwZ 2019, 693

Schliesky, Eine Verfassung für den digitalen Staat, ZRP 2015, 56

Schwintowski, Wird Recht durch Robotik und künstliche Intelligenz überflüssig

Spindler Gerald / Schmechel Phillip, Personal Data and Encryption in the European General Data Protection Regulation, JIPITEC 2016, 163

Steege, Autonomes Fahren und die staatliche Durchsetzung des Verbots der Rechtswidrigkeit, NZV 2019, 459

Tinnefeld, Künstliche Intelligenz – ein digitales Glasperlenspiel, ZD 2019, 333

Von Graevenitz, „Zwei mal Zwei ist Grün“ – Mensch und KI im Vergleich, ZRP 2018, 238

Veale Michael, A Critical Take on the Policy Recommendations of the EU High-Level Expert Group on Artificial Intelligence, European Journal of Risk Regulation 2020, abrufbar unter: <http://dx.doi.org/10.2139/ssrn.3475449 >(26.02.2021)

Veale/Binns/Ausloos, When data protection by design and data subject rights clash, International Data Privacy Law 2018, 105

Villaronga Eduard Fosch / Kieseberg Peter / Li Tiffany, Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten, Computer Law & Security Review 2018, Volume 34, Issue 2, 304

Wachter Sandra / Mittelstadt Brent / Russell Chris, Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI, SSRN Electronic Journal 2020

Wachter Sandra / Mittelstadt Brent, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI, Columbia Business Law Review 2019, abrufbar unter: <https://ssrn.com/abstract=3248829>

Wachter Sandra, Data protection in the age of big data, Nature Electronics 2019

Wachter Sandra / Mittelstadt Brent / Russell Chris, Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR, Harvard journal of law & technology 2018

Wachter, Sandra / Mittelstadt, Brent / Floridi, Luciano, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, SSRN Electronic Journal 2016

Waltl Bernhard / *Vogl Roland*, Explainable Artificial Intelligence - The New Frontier in Legal Informatics, in Schweighofer ua (Hrsg), IRIS 2018 (2018) 113

Weber/Kiefer/Jobst, Künstliche Intelligenz und Unternehmensführung

Werner, Schutz durch das Grundgesetz im Zeitalter der Digitalisierung, NJOZ 2019, 1041