netidee

STIPENDIEN

Künstliche Intelligenz:

Eine grund- und datenschutzrechtliche Untersuchung

Endbericht | Call 15 | Stipendium ID 5110

Inhalt

1 Einleitung

Der aktuelle Stand der vorliegenden Untersuchung entspricht nicht mehr dem ursprünglich avisierten Zeitplan, wodurch sich der Fortschritt des Forschungsprojekts verzögert.
Bereits abgeschlossen wurden die ersten beiden Forschungsblöcke (im aktuellen Meilensteinplan vorgesehen für SS2020; WS2020; SS2021, WS2021); die Abfassung der Hauptteile zum Datenschutzrecht sowie zu Grundrechten (vorgesehen ab SS2022) ist jedoch noch nicht vollendet. Diese Verzögerung ist zT auf den wissenschaftlichen Diskurs mit regen Regulierungsvorschlägen rund um die sog KI-Verordnung, die sich noch vor Einleitung des ordentlichen Gesetzgebungsverfahrens befindet, zurückzuführen.[1] Andererseits hat sich das Forschungsumfeld des Autors verändert: Das Forschungsprojekt wird nunmehr unter selben Titel und mit gleichgebliebenem Inhalt an der Universität Graz fortgesetzt. Hintergrund davon ist, dass der Autor eine vierjährige Stelle als Universitätsassistent an der Universität Graz – Institut für Rechtswissenschaftliche Grundlagen, Fachbereich Recht und IT angenommen hat.[2] Damit ist der weitere Fortgang der Untersuchung finanziell und institutionell langfristig abgesichert.

1.1 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 sog „intelligenten“ Maschinen übernommen wird.[3] Dies gilt in besonderem Maße für den Einsatz von lernenden, selbständig handelnden Systemen, die Daten en masse verarbeiten und durch automatisierte Entscheidungen in die Freiheiten und Rechte von betroffenen Nutzern eingreifen.[4]
Die technischen Charakteristika dieser Systeme erzeugen erhebliche Spannungen, wenn sie in das System des Datenschutzrechts eingeordnet werden. So erfordern Systeme mit Künstlicher Intelligenz (KI) die Verarbeitung großer Datenmengen, und zwar sowohl bei der Entwicklung als auch im (späteren) Einsatz („**Datenintensität**“). Die Entwicklung der (zugrundeliegenden) KI-Modelle erfolgt, ebenso wie dessen spätere Vorhersagen, über statistische Zusammenhänge unter erschwerter Erklärbarkeit und Nachvollziehbarkeit („**Komplexität**“) und darüber hinaus existieren im gesamten Lebenszyklus von KI-Systemen

1 Europäische Kommission, Proposal for a Regulation laying down harmonised rules on Artificial Intelligence, COM(2021) 206 final, abrufbar unter: .
2 https://rewi-grundlagen.uni-graz.at/de/institut/recht-und-it/team/.
3 *Harari*, Sapiens: A Brief History of Humankind (2015); *Yeung/Lodge*, Algorithmic Regulation: An Introduction (2019).
4 *Konferenz der unabhängigen Datenschutzaufsichtsbehörden*, Hambacher Erklärung zur Künstlichen Intelligenz (3.4.2019) 2.

erhebliche Probleme mit der Robustheit bzw Informationssicherheit der Systeme („**Fragilität**“).

1.2 Struktur und Ablauf der (bisherigen) Untersuchung

Die vorliegende Arbeit konturiert und grenzt das Phänomen KI auf eine engere **Arbeitsdefinition** ein und unterzieht vorliegende **(Legal-)Definitionen** einer kritischen Würdigung. Anschließend wird ein Überblick über gängige Entwicklungsverfahren und Systeme gegeben, die in der Praxis als KI bezeichnet werden.

In einer technischen Grundlagenuntersuchung werden die wesentlichen technologischen Rahmenbedingungen von KI-Systemen, für den hier (datenschutz-)rechtlich interessierenden Kontext, umrissen. Die hierbei festgemachten technologischen Eigenschaften zeigen, sowohl bei der Entwicklung als auch beim Einsatz der Technologie, (rechtliche) **Risiken** und **Spannungsfelder** auf: Va die Notwendigkeit der Verarbeitung großer (allenfalls personenbezogener) Datenmengen tritt hierbei augenscheinlich hervor und löst Friktionen mit dem Datenschutzrecht aus („**Datenintensität**“). Weitere Dissonanzen ergeben sich aufgrund der „**Komplexität**“ der Systeme, zumal die Entwicklung von KI-Modellen, ebenso wie dessen spätere Vorhersagen, über **statistische Zusammenhänge** unter **erschwerter Erklärbarkeit** und Nachvollziehbarkeit erfolgt. Verschärfend kommt hinzu, dass im gesamten Lebenszyklus von KI-Systemen erhebliche Probleme mit der Robustheit bzw Informationssicherheit der Systeme bestehen („**Fragilität**“).

Anschließend wird das **Friktionspotenzial** dieser Charakteristika mit (tradierten) datenschutzrechtlichen Grundsätzen untersucht und im Ergebnis gezeigt, dass der vorliegende normative Rahmen (noch) keine vertrauenswürdige Entwicklungs- und Einsatzumgebung für KI-Systeme bieten kann.

2 Allgemeines

Zusammenfassung der Arbeit, Fragestellung, Ziel der Arbeit

2.1 Ziele der Untersuchung

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

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. In diesem Sinne sollen grundrechtliche verbürgte Schutzgüter einer **wertebasierten Betrachtung** unterzogen werden, um sodann konkrete Kriterien für die Entwicklung von vertrauenswürdigen KI-Systemen aufzustellen.

2.2 Forschungsfragen

Das gegenständliche Forschungsprojekt untersucht sowohl die **Trainingsphase von KI (I. Forschungsfrage)**, als auch den **Einsatz von bereits trainierten KI-Modellen (II. Forschungsfrage)** untersuchen (vgl Abbildung 1[5] zur Unterscheidung). Hauptfokus der vorliegenden Arbeit sollen jedoch die Untersuchungen zur **I. Forschungsfrage** bilden, zumal diese Phase in der bisherigen Forschung noch wenig(er) Beachtung gefunden hat.

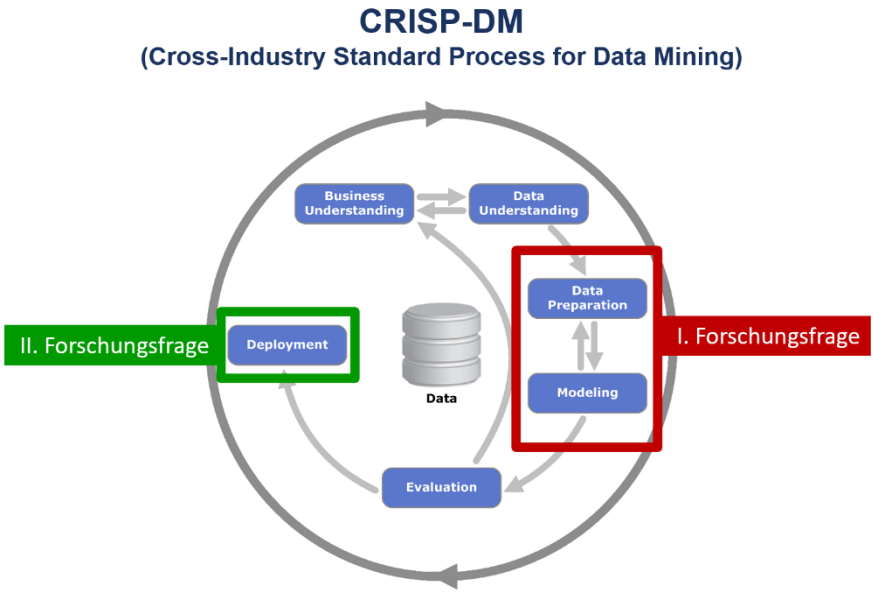

Abbildung 1: Entwicklungszyklus eines KI-Modells nach dem branchenübergreifenden Standard für KI-Entwicklung „CRISP-DM“.

[5] *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>(22.10.2021).

3 Ergebnisse

Beschreibung der erreichten Ergebnisse

Das normative **Spielfeld** für KI ist angesichts der **eklatanten Spannungen mit den Grundsätzen des Datenschutzrechts** (noch) mit erheblicher **Rechts-Unsicherheit** behaftet. Bis dieses Spielfeld geeignete rechtliche und technische (Sicherheits-)Garantien für eine vertrauenswürdige Entwicklung- und Einsatzumgebung bieten kann, sind noch intensive Forschungsanstrengungen erforderlich.

An den zahlreichen legislativen Vorstößen rund um Technologie- und Internetregulierung hat sich immer wieder verdeutlicht, wie schwer innovative Technologien einzuhegen sind. Der legislative Vorstoß des Unionsgesetzgebers rund um die sog „KI-Verordnung“[6] zeigt wieder, dass das (klassisch) datenschutzrechtliche Korsett der DSGVO, die Technologie nicht gebührend zu erfassen vermag. Ähnlich, wie auch bei der Blockchain-Technologie[7], wo sich aufgrund der Unabänderlichkeit der Datensätze ein diametraler Widerspruch mit dem Recht auf Löschung nach Art 18 ergab, tun sich auch iZm der Entwicklung und dem Einsatz von KI-Systemen Spannungsfelder auf:

- So verlangen KI-Systeme schlicht die Verarbeitung von großen Datenmengen als grundlegende Funktionsbedingung; ganz besonders in der Trainingsphase, aber auch beim späteren Einsatz (Stichwort „**Datenintensität**“). Ein vorsorglicher Grundrechtsschutz durch **Datenvermeidung** ist bei der Verarbeitung von personenbezogenen Daten zur KI-Entwicklung somit nur schwer möglich: Die Verarbeitung von nicht-repräsentativen oder unvollständigen Trainingsdaten birgt die Gefahr von fehlerhaften bzw qualitativ schlechten Modellen, die wiederum zur Quelle von schlechten Entscheidungen beim Einsatz werden können. Somit kann sich ein vorgezogener Betroffenenschutz durch Datenvermeidung schließlich erst wieder **diskriminierend oder nachteilig** auf Betroffene auswirken.
- Weiters wird die Herstellung von Transparenz und Nachvollziehbarkeit der Datenverarbeitung durch die „**Komplexität**“ von KI-Systemen maßgeblich erschwert. Insb, weil die „Intelligenz“ der Systeme idR über komplexe **statistische Zusammenhänge** erzeugt wird, die sich dem menschlichen Verstand oft nur schwer erschließen. Gerade in dieser Komplexität der Systeme liegt jedoch ihre Innovationskraft; zumal damit Ergebnisse erzielt

[6] *Europäische Kommission*, Vorschlag für eine Verordnung zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz, COM(2021) 206 final.

[7] Vgl etwa *Piska/Bierbauer*, Datenschutzrechtliche Dimensionen der Blockchain-Technologie, in Piska/Völkel, Blockchain rules (2019) 161.

werden können, die im Wege der (konventionellen) regelbasierten Programmierung nicht möglich wären.

- Die, der relativen Neuartigkeit der Technologie geschuldete, „**Fragilität**“ der Systeme bringt ebenso vielschichtige Risiken für Betroffene mit sich, die den GS des Systemdatenschutzes schwer belasten. Die oben genannten Charakteristika „Datenintensität“ und „Komplexität“ verstärken die Fragilität der Systeme noch weiter: So wird durch die erhöhte Datenmenge mehr Angriffsfläche exponiert und Angriffe bzw Manipulationen sind durch die Komplexität der entwickelten Systeme leichter zu verdunkeln. Diese Risiken sind der Technologie – nach heutigem Stand der Technik – zwar inhärent, es ist aber davon auszugehen, dass sie zukünftig durch rechtliche und technische Schutzmaßnahmen minimiert werden können.

Gleichwohl diese gegenläufige Interessenlage das Datenschutzrecht oft als Hemmschuh für Forschung und Innovation erscheinen lässt, muss dies bei genauerer Betrachtung nicht so sein. Hinter diesen prima facie widerstreitenden Interessen stehen vielfach auch Grundrechtsposition, die miteinander in Einklang zu bringen sind: Primärrechtlich verbürgte Grundrechtsgüter, wie das Grundrecht auf Datenschutz (Art 8 GRC), gewährleisten nämlich nicht nur den Schutz von Betroffenen bei der Verarbeitung ihrer Daten; sie schützen darüber hinaus auch Interessen, welche die Verarbeitung von personenbezogenen Daten einfordern. So etwa bei Verarbeitungen zu kommerziellen Interessen (**Berufsfreiheit** Art 15 GRC, **Unternehmerische Freiheit** Art 16 GRC) oder für ein wissenschaftliches Erkenntnisinteresse (**Wissenschaftsfreiheit** Art 13 GRC).

Ferner heißt es auch in ErwG 4 DSGVO: *„Das Recht auf Schutz der personenbezogenen Daten ist **kein uneingeschränktes Recht**; es muss im Hinblick auf seine gesellschaftliche Funktion gesehen und unter **Wahrung des Verhältnismäßigkeitsprinzips** gegen andere Grundrechte abgewogen werden.“*[8]

Das pauschale Vorziehen von einzelnen Schutzgütern ist daher stets zu vermeiden, wenn damit andere Grundrechtspositionen übermäßig belastet werden. Für die vorliegende Untersuchung heißt das: Die **Technologie-Immanenz** der Charakteristika „Datenintensität“, „Komplexität“ und „Fragilität“ ist in die Auslegung der Datenschutzgrundsätze miteinzubeziehen.

In der Literatur wurde bereits davor gewarnt, dass die tradierten Datenschutzgrundsätze Gefahr laufen von der „normativen Kraft des Faktischen“ untergraben zu werden, wenn sie allzu starr angewendet werden.[9] Tradierte (Datenschutz-)Grundsätze sind daher nach der hier vertretenen Meinung – unter Achtung der Betroffenen(grund)rechte und sämtlicher

[8] [Hervorhebungen nicht im Original].
[9] *Roßnagel* in Simitis/Hornung/Spiecker, DSGVO (2019) Art 5 Rz 30.

Facetten des Einzelfalles – **technologiefreundlich** zu **interpretieren**, wenn sie ansonsten die Innovationskraft der Technologie an sich konterkarieren würden.

4 Geplante weiterführende Aktivitäten

Das vorliegende Dissertationsprojekt wurde an der Universität Wien begonnen und wird nunmehr jedoch an der Universität Graz fortgesetzt. Maßgeblich Ergebnisse von Teilabschnitten wurden bereits in einem österreichischen Sammelband für Datenschutzrecht publiziert;[10] es ist auch für zukünftige Ergebnisse vorgesehen, diese in wissenschaftlichen Beitragen zu veröffentlichen. Ferner wurden Ergebnisse auf wissenschaftlichen Konferenzen vorgetragen;[11] auch diese Vortragstätigkeit soll fortgeführt werden. Weiters ist auch vorgesehen die gewonnen Forschungserkenntnisse im Rahmen von Forschungsprojekten an der Universität Graz, sowie in der universitären Lehre zu verwerten.

Noch ausständig bzw noch nicht vollständig abgeschlossene Forschungsaktivitäten sind zum gegenwärtigen Zeitpunkt: Verfassen des Hauptteils zum Datenschutzrecht und zu Grundrechten (geplanter Abschluss WS2022) sowie Durchführen der Case-Study (SS2023).

5 Anregungen für Weiterführung durch Dritte

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 bestens als Grundlage für weiterführende Forschung im Verfassungs- und Datenschutzrecht, sowie weiteren Rechtsgebieten. Ferner kann die Arbeit auch als rechtliche Leitlinie für technische Arbeiten bzw für Software-Entwickler dienen.

[10] *Bierbauer*, Datenschutzrechtliche Grundsätze bei der Entwicklung Künstlicher Intelligenz, in: Jahnel (Hrsg), Datenschutzrecht. Jahrbuch 2021 (Wien NWV Verlag 2022) 175-196.

[11] Charakteristika von Künstlicher Intelligenz im System des Datenschutzrechts. Online. 12.05.2022;
Künstliche Intelligenz entymstifiziert: technische und datenschutzrechtliche Grundprinzipien bei der Entwicklung von KI-Systemen. Salzburg/Wien, online. 24.02.2022;
AI demystified. Technological and legal foundations of AI technologies. 06.08.2021.