Jean Monnet Saar

EUROPARECHT ONLINE

Saar Blueprints

Meltem Yildirim

Datenschutz und Künstliche Intelligenz

Die Erhebung von personenbezogenen Daten durch KI-basierte Systeme

DFG Deutsche Forschungsgemeinschaft
German Research Foundation

11/2024 DE

Zur Autorin

Mag. iur Meltem Yildirim, LL.M., ist Doktorandin und wissenschaftliche Mitarbeiterin am Europa-Institut der Universität des Saarlandes. Nach ihrem Studium des Magister juris internationalis in Gießen, Deutschland, absolvierte sie den Master of Laws im Europäischen und Internationalen Recht am Europa-Institut in Saarbrücken, wobei sie sich auf Wettbewerbsrecht, Menschenrechte sowie IT-Recht und Datenschutz spezialisierte. In ihrer Dissertation untersucht sie den Einfluss Künstlicher Intelligenz auf Menschenrechte.

Vorwort

Diese Veröffentlichung ist Teil einer elektronischen Zeitschriftenserie (Saar Expert Papers), welche von Jean Monnet Saar, einem Lehrstuhlprojekt von Prof. Dr. Thomas Giegerich, LL.M. am Europa-Institut der Universität des Saarlandes herausgegeben wird. Die weiteren Titel der Serie können unter https://jean-monnet-saar.eu/ abgerufen werden.

In den Veröffentlichungen geäußerte Feststellungen und Meinungen sind ausschließlich jene der angegebenen Autoren und Autorinnen.

Herausgeber
Lehrstuhl Prof. Dr. Thomas Giegerich Universität des Saarlandes
Postfach 15 11 50
66041 Saarbrücken
Germany

ISSN
2199-0050 (Saar Blueprints)
DOI: 10.17176/20241114-092807-0

Zitierempfehlung
Yildirim, Datenschutz und KI: Die Erhebung von personenbezogenen Daten durch KI-basierte Systeme, Saar Blueprints 11/24, online verfügbar unter: https://jean-monnet-saar.eu/wp-content/uploads/2024/11/Saar-Blueprint_Meltem-Yildirim.pdf.

Gefördert durch die **Deutsche Forschungsgemeinschaft** (DFG) – Projektnummer: 525576645 (DFG) – Projektnummer: 525576645

Inhaltsverzeichnis

A. Einführung

Unser Alltag wird zunehmend durch KI-basierte Systeme geprägt – von digitalen Assistenten bis hin zu einer Vielzahl von Anwendungen in verschiedensten Lebensbereichen. Diese Technologien haben bereits Einzug in viele Bereiche des täglichen Lebens gehalten, sei es durch „smarte“ Zahnbürsten oder automatisierte Fahrzeuge. Ihre Einsatzmöglichkeiten erscheinen nahezu unbegrenzt. Um ihre Funktionen zu erfüllen, greifen diese Systeme jedoch auf enorme Datenmengen (Big Data) zurück und erfassen dabei oft sensible Informationen über die Nutzer.[1] Dies wirft die Frage auf, ob der technologische Fortschritt nicht auch eine Gefahr für den Datenschutz darstellt. Wie kann daher sichergestellt werden, dass diese Technologien, die im Alltag immer präsenter werden, mit dem Schutz personenbezogener Daten im Einklang stehen?[2]

B. Anwendungsbereiche

Die technologische Entwicklung schreitet rasant voran und es scheint kaum noch Grenzen zu geben. Roboter übernehmen Tätigkeiten in der industriellen Fertigung, während selbstfahrende Autos und digitale Assistenten den Alltag erleichtern. Im Zentrum dieser Systeme steht die Künstliche Intelligenz (KI), die durch selbstlernende Prozesse und stetig wachsende Rechenleistung die Funktionsweise von IT-Systemen grundlegend verändert.[3] Diese Technologien sind längst nicht mehr auf Pilotprojekte von Forschungseinrichtungen beschränkt, sondern haben sich fest in unserem Alltag etabliert. Sie basieren auf KI-gesteuerten Prozessen und bieten inzwischen eine wachsende Vielfalt an Anwendungen.[4] Im Folgenden werden einige dieser Anwendungen und ihre datenschutzrechtlichen Implikationen näher betrachtet.

---

[1] *Conrad,* Künstliche Intelligenz – Die Risiken für den Datenschutz, 740.
[2] *Ebd.*
[3] Vgl. *Schonscheck*, Künstliche Intelligenz durchdringt bereits die IT, ZDNet 06.03.2017, https://www.zdnet.de/88288740/kuenstliche-intelligenz-durchdringt-bereits-die-it/# (letzter Abruf am 29.09.2024).
[4] *Conrad,* Künstliche Intelligenz – Die Risiken für den Datenschutz, 740.

I. Erhebung personenbezogener Daten für die Weiterentwicklung und das Training von KI-Systemen

KI-basierte Systeme erheben personenbezogene Daten zu verschiedenen Zwecken, darunter auch zur Weiterentwicklung und zum Training der Modelle. Diese Systeme lernen durch die Daten, mit denen sie trainiert werden. Der Datenschutz sollte dabei entweder durch die Minimierung der Erhebung personenbezogener Daten gewährleistet werden oder, wie zunehmend empfohlen wird, durch die bevorzugte Nutzung von nicht-personenbezogenen Daten. Nicht-personenbezogene Daten sollten für das Training von KI-Systemen grundsätzlich personenbezogenen Daten vorgezogen werden, sofern sie die gleiche Datenqualität aufweisen. Wenn die Verwendung personenbezogener Daten für das Training eines KI-Systems jedoch unvermeidbar ist, muss das Prinzip „Privacy by Design" umfassend gestärkt werden. Dies bedeutet, dass Datenschutz von Anfang an in die Entwicklung integriert wird. Hierfür sind vertiefte Forschung, Standardisierungs- und Zertifizierungsinitiativen sowie technologische Weiterentwicklungen erforderlich. Auch wirtschafts-, forschungs- und bildungspolitische Maßnahmen sowie rechtliche Anerkennung spielen eine zentrale Rolle, um den Schutz personenbezogener Daten in KI-Systemen langfristig sicherzustellen.[5]

II. Personalisierung und prädiktive Analytik

KI-Systeme werden zunehmend zur Personalisierung von Diensten und zur Anwendung sogenannter prädiktiver Analytik eingesetzt. Letztere bezieht sich auf datenbasierte Vorhersagemodelle, die anhand gesammelter Informationen Prognosen über das Verhalten von Individuen erstellen. Diese Modelle können beispielsweise vorhersagen, wie wahrscheinlich es ist, dass eine Person ein bestimmtes Produkt kauft.[6] Diese datengetriebene Personalisierung kann zu einem maßgeschneiderten Angebot an Inhalten, Werbung oder Dienstleistungen führen. Solche Anpassungen gehen jedoch mit Risiken einher, darunter Preismanipulationen oder die

[5] *Müller-Quade/Houdeau et al.*, Datenschatz für KI nutzen, Datenschutz mit KI wahren – Technische und rechtliche Ansätze für eine datenschutzkonforme, gemeinwohlorientierte Datennutzung, https://cta4.plattform-lernende-systeme.de/files/Downloads/Publikationen/AG3_WP_KI_Datenschutz_Datenschatz.pdf (letzter Abruf am 29.09.2024).
[6] *Mühlhoff*, Prädiktive Privatheit: Kollektiver Datenschutz im Kontext von Big Data und KI, S. 31 ff.

Einschränkung des Zugangs zu Informationen. Kritisch ist auch das Potenzial, dass politische Prozesse, wie etwa Wahlen, durch gezielte Manipulation beeinflusst werden können.[7]

III. Weitere Anwendungen

Personenbezogene Daten werden von KI-basierten System darüber hinaus auch in anderen Bereichen genutzt:

- **Verbesserung der Benutzererfahrung:** Durch das Verstehen des Nutzerverhaltens werden Systeme optimiert.
- **Automatisierung von Prozessen:** KI-basierte Systeme automatisieren Aufgaben basierend auf individuellen Daten.
- **Sicherheit und Authentifizierung:** Biometrische Daten wie Fingerabdrücke und Gesichtserkennung werden für die Identitätsprüfung verwendet.

C. Risiken für den Datenschutz

KI-basierte Systeme erfassen und verarbeiten in vielen Fällen eine Vielzahl an Informationen über die Nutzer, die oft so umfangreich und vielfältig sind, dass sie schwer zu interpretieren bleiben. Mit fortschreitender Entwicklung dieser Technologien gewinnen sie jedoch immer tiefere Einblicke in das Verhalten und die Vorlieben des Einzelnen. Zukünftige Analysen und technologische Fortschritte könnten diese Daten noch weiterverarbeiten und nutzen, um umfassendere Erkenntnisse und Prognosen über die Person zu liefern. Dies stellt eine erhebliche Gefahr für den Datenschutz dar. Besonders sensibel sind biometrische Daten wie Fingerabdrücke oder Gesundheitsdaten, die eine besonders hohe Gefahr für die informationelle Selbstbestimmung der Nutzer darstellen.[8]

Wesentliche Datenschutzrisiken bei der Nutzung von KI-basierten Systemen umfassen:

- **Datenmissbrauch:** Gesammelte Daten können missbraucht oder ohne Einwilligung eingesehen werden.

---

[7] *Conrad,* Künstliche Intelligenz – Die Risiken für den Datenschutz, 740 (742).
[8] *Conrad,* Künstliche Intelligenz – Die Risiken für den Datenschutz, 740 (742).

- **Fehlende Transparenz:** Nutzer wissen oft nicht, wie und in welchem Umfang ihre Daten verwendet werden.
- **Übermäßige Datensammlung:** Häufig werden mehr Daten erhoben als nötig.
- **Profiling und Diskriminierung:** Algorithmen können Nutzerprofile erstellen und diskriminierende Entscheidungen treffen, etwa durch fehlerhafte Gesichtserkennung.[9]
- **Unklare Verantwortung:** Oft ist unklar, wer bei Datenschutzverstößen verantwortlich ist.

Diese Risiken zeigen, dass die Erhebung und Nutzung personenbezogener Daten durch KI-Systeme nicht nur technische, sondern auch ethische und rechtliche Herausforderungen für den Datenschutz darstellen.[10]

D. Notwendige rechtliche und technische Voraussetzungen

Um die Potenziale von KI-Systemen zum Wohl der Gesellschaft zu nutzen, muss der Datenschutz gewährleistet bleiben. Dazu sind geeignete technische und rechtliche Maßnahmen erforderlich.

I. KI-Datenschutz durch verteiltes maschinelles Lernen

Bei der Datenanalyse, insbesondere beim Training von KI-Modellen, bietet der Einsatz dezentraler maschineller Lernmethoden (Federated Learning) eine vielversprechende Möglichkeit, Datenschutz und eine gemeinwohlorientierte Datennutzung zu vereinen. Dieser Ansatz, der nach dem Prinzip „*bring computation to data"* funktioniert, erfordert keine vorherige Veränderung personenbezogener Daten, da diese lokal bei den Nutzern verbleiben. Dadurch wird sowohl eine hohe Datenqualität als auch individuelle Datensouveränität gewährleistet, was den Ansatz besonders für KI-Entwickler attraktiv macht.[11]

---

[9] *Vogel*, Künstliche Intelligenz und Datenschutz – Vereinbarkeit intransparenter Systeme mit geltendem Datenschutzrecht und potentielle Regulierungsansätze, S. 68.
[10] *Ottersböck et al.*, Daten und KI-Ethik, 167 (167f.).
[11] *Müller-Quade/Houdeau et al.*, Datenschatz für KI nutzen, Datenschutz mit KI wahren – Technische und rechtliche Ansätze für eine datenschutzkonforme, gemeinwohlorientierte Datennutzung, https://cta4.plattform-lernende-systeme.de/files/Downloads/Publikationen/AG3_WP_KI_Datenschutz_Datenschatz.pdf (letzter Abruf am 29.09.2024).

Da Daten für Unternehmen wertvoll, aber gleichzeitig ein sensibles Thema sind – da viele Nutzer ungern personenbezogene Daten preisgeben – bietet das verteilte maschinelle Lernen eine praktikable Lösung. Es ermöglicht das Training von KI-Modellen, ohne dass persönliche Daten die Geräte der Nutzer verlassen. Stattdessen trainiert jeder Nutzer sein Modell lokal, und nur die trainierten Modelle, nicht die Rohdaten, werden auf einen zentralen Server übertragen und dort kombiniert. Dies verbessert den Datenschutz, reduziert den Bedarf an großen Datenmengen und erlaubt es, auch auf Geräten mit geringer Rechenleistung effizient zu arbeiten, was zusätzlich energieeffizienter ist.[12]

II. Anforderungen an die Daten

KI-Technologien bieten Unternehmen großes Potenzial, um ihre Prozesse, Produktivität und Marktstrategien zu optimieren. Da Künstliche Intelligenz jedoch auf große Datenmengen angewiesen ist, stehen die Unternehmen vor der Herausforderung, qualitativ hochwertige Daten bereitzustellen. Die Datenqualität ist entscheidend, da ungenaue oder fehlerhafte Daten zu unzuverlässigen Ergebnissen und falschen Entscheidungen führen können. Besonders wichtig ist es, faire und unvoreingenommene Daten zu nutzen, um Diskriminierungen durch die KI-Systeme zu vermeiden. KI kann bestehende Vorurteile in der Gesellschaft, wie etwa aufgrund von Hautfarbe oder Geschlecht, übernehmen. Deshalb müssen Unternehmen sicherstellen, dass die Trainingsdaten frei von Diskriminierungen sind. Ebenso wichtig ist, dass die Daten repräsentativ für die jeweilige Zielgruppe sind, um präzise und nachvollziehbare Entscheidungen zu ermöglichen.[13]

III. Gemeinwohlorientierte Datennutzung

Für einen zeitgemäßen und effektiven Rechtsrahmen, insbesondere im Hinblick auf eine flexible, datenschutzkonforme Datennutzung im Interesse des Gemeinwohls, ist es entscheidend, dass Instrumente ermöglicht und gefördert werden, die dazu beitragen, Unsicherheiten in der Rechtsauslegung zu verringern und gleichzeitig sich widersprechende Rechte und Schutzgüter umfassend schützen. Dies erfordert einen ganzheitlichen Ansatz zur rechtlichen Anerkennung einer flexibilisierten Datennutzung im Gemeinwohlinteresse, basierend auf den vorgestellten

---

[12] *Ottersböck et al.*, Daten und KI-Ethik, 167 (169).
[13] *Ebd.*, S. 171 f.

technischen Maßnahmen und einem integrierten Datenmanagement. Dies bedeutet, dass eine einheitliche Definition des Gemeinwohlinteresses notwendig ist.[14]

IV. Recht und Zertifizierung

Gemeinwohlinteresse sollte in konkreten Anwendungskontexten rechtssicher definiert werden, sodass bei Vorliegen dieses Interesses Datennutzungsflexibilisierungen als Rechtsfolge eingeräumt werden können. Dabei muss die Beurteilung des Gemeinwohlinteresses nicht isoliert betrachtet werden, sondern in einem ganzheitlichen Ansatz erfolgen. Dies erfordert die Messbarkeit von Implikationen und möglichen negativen Externalitäten anhand eines klaren Kriterienrahmens. So könnte beispielsweise die Datenfreigabe für gemeinwohlorientierte KI-Systeme durch große Digitalkonzerne auf den ersten Blick gemeinwohlorientiert wirken (wie im Fall von Google Books und der Demokratisierung des Wissenszugangs). Wenn aber durch anschließende Kapitalisierung negative Auswirkungen auf das Gemeinwohl entstehen, etwa durch die Entstehung eines Monopols auf den Wissenszugang, widerspricht dies dem eigentlichen Ziel einer datenschutzkonformen und gemeinwohlorientierten Datennutzung. Ein solcher Kriterienrahmen würde helfen, diese Fälle zu bewerten und angemessene Entscheidungen zu treffen.[15]

V. Privacy by Design stärken

Im Sinne des Datenschutzes bleibt es entscheidend, dass für das Training von KI-Systemen grundsätzlich nicht-personenbezogene Daten personenbezogenen Daten vorgezogen werden, sofern die Datenqualität vergleichbar ist. Um dies zu ermöglichen, sollte die Verfügbarkeit nicht-personenbezogener Daten verstärkt gefördert werden. Dies könnte durch verstärkte Forschungs- und Entwicklungsinitiativen geschehen, beispielsweise durch den Aufbau interoperabler Datenräume. Wenn die Nutzung personenbezogener Daten für das Training eines KI-Systems unvermeidlich ist, muss das Prinzip "Privacy by Design" umfassend gestärkt werden. Dies erfordert vertiefte Forschung und Entwicklung, Standardisierungs- und

---

[14] *Müller-Quade/Houdeau et al.*, Datenschatz für KI nutzen, Datenschutz mit KI wahren – Technische und rechtliche Ansätze für eine datenschutzkonforme, gemeinwohlorientierte Datennutzung, https://cta4.plattform-lernende-systeme.de/files/Downloads/Publikationen/AG3_WP_KI_Datenschutz_Datenschatz.pdf (letzter Abruf am 29.09.2024).
[15] *Ebd.*

Zertifizierungsinitiativen, technologische Weiterentwicklungen sowie politische Maßnahmen in den Bereichen Wirtschaft, Forschung und Bildung. Auch die rechtliche Anerkennung von Privacy by Design als grundlegendes Konzept im Datenschutz sollte gefördert werden.[16]

E. Schlussfolgerung und Ausblick

Die Nutzung von KI-Systemen birgt erhebliche Datenschutzrisiken, insbesondere wenn maschinelle Entscheidungen über Individuen getroffen werden. Dabei wird deutlich, dass der Einsatz solcher Systeme oft in Konflikt mit den Grundwerten des Rechts stehen kann, insbesondere wenn die Entscheidungsprozesse undurchsichtig und schwer nachvollziehbar sind. Das europäische Datenschutzrecht, vor allem die DSGVO, spielt hier eine zentrale Rolle. Es findet Anwendung, wenn KI-Systeme personenbezogene Daten nutzen oder Entscheidungen über Individuen treffen.[17]

Der neu verabschiedete AI-Act der EU verweist ausdrücklich auf die Bedeutung der DSGVO und unterstreicht deren Relevanz für den rechtlichen Rahmen von KI-Systemen. Neben der rechtlichen Einbettung in die DSGVO sind auch technische Maßnahmen wie „Privacy by Design" essenziell, um den Schutz personenbezogener Daten zu stärken. Zukünftige Entwicklungen sollten verstärkt auf nicht-personenbezogene Daten setzen und klare rechtliche und technische Standards schaffen. Nur so kann ein umfassender Datenschutz gewährleistet werden, der Innovation fördert und gleichzeitig die Rechte der Nutzer schützt.

Darüber hinaus ist es interessant zu sehen, dass die Europäische Kommission am 5. September 2024 das Rahmenübereinkommen des Europarats über Künstliche Intelligenz, Menschenrechte, Demokratie und Rechtsstaatlichkeit unterzeichnet hat.[18] Dieses Übereinkommen soll der erste rechtsverbindliche internationale Vertrag werden, der sicherstellen soll, dass der Einsatz von KI-Systemen vollständig im Einklang mit Menschenrechten, Demokratie und

---

[16] *Ebd.*
[17] *Vogel*, Künstliche Intelligenz und Datenschutz – Vereinbarkeit intransparenter Systeme mit geltendem Datenschutzrecht und potentielle Regulierungsansätze, S. 64 ff.
[18] Council of Europe Treaty Series – No. 225, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=225 (letzter Abruf: 28.10.2024).

Rechtsstaatlichkeit erfolgt. Er ist vollumfänglich mit dem Unionsrecht im Allgemeinen und dem AI-Act im Besonderen vereinbar und stellt die weltweit erste KI-Verordnung dar.[19]

Das Übereinkommen enthält eine Reihe von Schlüsselkonzepten, darunter den Schutz personenbezogener Daten. Besonders in Artikel 11 wird festgestellt, dass jede Vertragspartei Maßnahmen ergreift oder beibehält, um sicherzustellen, dass der Schutz der Privatsphäre und personenbezogener Daten über den gesamten Lebenszyklus von KI-Systemen gewahrt bleibt. Gleichzeitig müssen effektive Garantien und Schutzvorkehrungen für Einzelpersonen in Übereinstimmung mit nationalen und internationalen Verpflichtungen sichergestellt werden.

Im erläuternden Bericht zum Übereinkommen,[20] insbesondere in den Randnummern 79 bis 83 zu Artikel 11, wird hervorgehoben, dass der Schutz personenbezogener Daten eine Schlüsselrolle für die Wahrung der Privatsphäre und anderer Menschenrechte in der digitalen Welt spielt. Die Verfasser des Entwurfs haben daher ausdrücklich darauf hingewiesen, dass nationale und internationale Gesetze, Normen und Rahmenwerke zum Schutz personenbezogener Daten berücksichtigt werden müssen. Um die Bedeutung eines wirksamen Schutzes im Zusammenhang mit Künstlicher Intelligenz zu betonen, verweist Artikel 11 Buchstabe b des Übereinkommens auf zusätzliche „Garantien und Schutzmaßnahmen“ für natürliche Personen (in einigen Ländern auch als „betroffene Personen“ bezeichnet).

Das Übereinkommen verfolgt somit einen gemeinsamen Ansatz, um sicherzustellen, dass Tätigkeiten im Lebenszyklus von KI-Systemen im Einklang mit Menschenrechten, Demokratie und Rechtsstaatlichkeit stehen und gleichzeitig Innovation und Vertrauen fördern. In der EU wird das Übereinkommen durch den AI-Act umgesetzt, welcher harmonisierte Vorschriften für das Inverkehrbringen, die Inbetriebnahme und die Nutzung von KI-Systemen enthält. Diese Regelungen können durch weitere relevante EU-Vorschriften ergänzt werden. Mit der Unterzeichnung des Übereinkommens signalisiert die EU ihre Absicht, Vertragspartei des Übereinkommens zu werden. Anschließend wird die Europäische Kommission einen

---

[19] *Europäische Kommission*, Kommission unterzeichnet Rahmenübereinkommen des Europarats über künstliche Intelligenz und Menschenrechte, Demokratie und Rechtsstaatlichkeit, News Article 05.09.2024, https://digital-strategy.ec.europa.eu/de/news/commission-signed-council-europe-framework-convention-artificial-intelligence-and-human-rights (letzter Abruf am 15.10.2024).

[20] Council of Europe Treaty Series – No. 225, Explanatory Report, https://rm.coe.int/1680afae67 (letzter Abruf am 15.10.2024).

Vorschlag für einen Beschluss des Rates über den Abschluss des Übereinkommens vorlegen. Auch das Europäische Parlament muss seine Zustimmung erteilen.[21]

[21] *Europäische Kommission*, Kommission unterzeichnet Rahmenübereinkommen des Europarats über künstliche Intelligenz und Menschenrechte, Demokratie und Rechtsstaatlichkeit, News Article 05.09.2024, https://digital-strategy.ec.europa.eu/de/news/commission-signed-council-europe-framework-convention-artificial-intelligence-and-human-rights (letzter Abruf am 15.10.2024).

Literaturverzeichnis

Conrad, Conrad Sebastian, Künstliche Intelligenz – Die Risiken für den Datenschutz, Datenschutz und Datensicherheit (DuD), 2017, 740-744

Mühlhoff, Rainer, Prädiktive Privatheit: Kollektiver Datenschutz im Kontext von Big Data und KI, in: Friedewald, Michael/Roßnagel, Alexander/Heesen, Jessica/Krämer, Nicole/Lamla, Jörn (Hrsg.), Künstliche Intelligenz, Demokratie und Privatheit, Baden-Baden 2022, S. 31-58

Müller-Quade, Jörn/Houdeau, Detlef et al., Datenschatz für KI nutzen, Datenschutz mit KI wahren – Technische und rechtliche Ansätze für eine datenschutzkonforme, gemeinwohlorientierte Datennutzung, Whitepaper Lernende Systeme, abrufbar unter: https://cta4.plattform-lernende-systeme.de/files/Downloads/Publikationen/AG3_WP_KI_Datenschutz_Datenschatz.pdf (letzter Abruf am 29.09.2024).

Ottersböck, Nicole/Urban, Isabella/Shahinfar, Fatemeh/Terstegen, Sebastian/Schüth, Nora Johanna, Daten und KI-Ethik, in: Stowasser, Sascha (Hrsg.), Künstliche Intelligenz (KI) und Arbeit – Leitfaden zur soziotechnischen Gestaltung von KI-Systemen, Berlin 2023.

Schonscheck, Oliver, Künstliche Intelligenz durchdringt bereits die IT, ZDNet 06.03.2017, abrufbar unter: https://www.zdnet.de/88288740/kuenstliche-intelligenz-durchdringt-bereits-die-it/# (letzter Abruf am 29.09.2024)

Vogel, Paul, Künstliche Intelligenz und Datenschutz – Vereinbarkeit intransparenter Systeme mit geltendem Datenschutzrecht und potentielle Regulierungsansätze, Baden-Baden 2022