Prof. Dr. Patrick Glauner • [redacted]
[redacted]

Deutscher Bundestag
Ausschuss für Digitales
Platz der Republik 1
11011 Berlin

Ihre Nachricht vom	Telefon-Durchwahl	E-Mail	Unser Zeichen	Ort, Datum
26.04.2024	Tel.: +49 991 [redacted]	[redacted]		Deggendorf, 10.05.2024

Schriftliche Stellungnahme[1] von Prof. Dr. Patrick Glauner

Für die am 15.05.2024 stattfindende Anhörung zu

„Nationale Spielräume bei der Umsetzung des europäischen Gesetzes über Künstliche Intelligenz"

Allgemeine Ausführungen

- Die **Definition von Künstlicher Intelligenz** (KI) wurde in den Entwürfen des AI Act zwar mehrfach verändert, ist jedoch in der finalen Version weiterhin **sehr breit und unkonkret**. In Verbindung mit der **vagen Abgrenzung von Hochrisiko-Anwendungsfällen**[2] und den damit verbundenen Auflagen besteht die Sorge vor **erheblicher Bürokratie** bei der Umsetzung des AI Act und den daraus folgenden **Innovationshemmnissen**.
- Unternehmen treffen aktuell KI-Investitionsentscheidungen für die kommenden Jahre und Jahrzehnte. Es besteht daher die zwingende **Notwendigkeit**, den AI Act in Deutschland **innovationsfreundlich, kostenarm und praxisnah umzusetzen**.
- Hierfür müssen die **zuständigen Aufsichtsbehörden zeitnah festgelegt werden** und passende **Standardisierungen** und **Checklisten** erstellt werden. Die Aufsicht sollte nicht durch Daten- oder Verbraucherschützer erfolgen, um nicht die bei der Umsetzung der Datenschutzgrundverordnung gemachten Fehler zu wiederholen.
- Andernfalls würden voraussichtlich **chinesische und US-amerikanische Konzerne** in ihrer Technologieführerschaft **weiter gestärkt**, da sie für die Umsetzung über wesentlich umfangreichere Ressourcen als deutsche mittelständische Unternehmen verfügen.
- Die Umsetzung des AI Act durch Behörden erscheint grundsätzlich herausfordernd und wird vermutlich nur sehr langsam erfolgen. Wahrscheinlicher ist jedoch eine **Vielzahl von zivilrechtlichen Klagen**. Um diese auf Augenhöhe bearbeiten zu können, muss die Justiz zeitnah flächendeckend eigene KI-Kompetenzen aufbauen.
- Der **AI Act ist kein Naturgesetz**. Es muss ein **permanentes Monitoring** stattfinden, um ihn bei Bedarf weiterzuentwickeln, anzupassen oder gar aufzuheben.

[1] Ich möchte mich bei Dr. David Bomhard von der Aitava Rechtsanwaltsgesellschaft mbH, Marieke Merkle von der Noerr Partnerschaftsgesellschaft mbB und weiteren Gesprächspartnern für die umfangreichen Diskussionen während der Vorbereitung dieser Stellungnahme bedanken.

[2] Siehe u.a. http://www.appliedai.de/assets/files/AI-Act_WhitePaper_final_CMYK_ENG.pdf

Beruflicher Hintergrund des Verfassers
Als Hochschullehrer bin ich schwerpunktmäßig in der Lehre und Forschung zu KI tätig. Zudem berate ich Unternehmen, Regierungen und weitere Organisationen beim Einsatz von KI, insbesondere in strategischen, technischen, politischen und regulatorischen Fragestellungen. Dabei implementiere auch weiterhin selbst KI-Anwendungen.

Ausführungen im Einzelnen
1) Wie muss die nationale Aufsicht aufgestellt sein, um eine möglichst kohärente, schlanke Governance zu gewährleisten? Wie gelingt uns trotz sektoraler Zuständigkeiten und föderaler Aufteilung der vielzitierte One-Stop-Shop? Welche genauen Aufgaben sollte die Aufsicht übernehmen?
Siehe Antwort auf 12). Hervorzuheben ist zudem, dass für die Sicherheitsbehörden aufgrund deren besonderen Anforderungen ein separater One-Stop-Shop geschaffen werden muss bzw. deren Aufsicht nicht durch eine gemeinsame Aufsichtsbehörde für alle KI-Anwendungsfälle erfolgt[3]. Andernfalls wäre der Austausch von Daten mit ausländischen Partnern gefährdet. Hier könnte der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) eine Schlüsselrolle zukommen, da sie gemäß des Errichtungserlasses eine zentrale behörden-übergreifende Rolle bei Forschung, Entwicklung und Beratung im Sicherheitsbereich des Bundes hat.

2) Der AI Act eröffnet den Mitgliedstaaten in der nationalen Umsetzung im Bereich Arbeit Spielräume. Wie sollten diese Spielräume im Sinne gestärkter Arbeitnehmer:innenrechte genutzt werden?
Arbeitnehmer verfügen heute schon durch eine Vielzahl von Gesetzen, u.a. der Datenschutzgrundverordnung, über weitgehenden Schutz im digitalen Raum. Es sollten daher keine weiteren KI-spezifischen bürokratischen Auflagen geschaffen werden. KI schützt eher vielmehr Arbeitnehmer vor Gefahren und übernimmt ggf. auch unliebsame Tätigkeiten. Daher sollte KI besser als Chance für Arbeitnehmer gesehen werden, auch mit Hinblick auf die Abfederung des demografischen Wandels und des Fachkräftemangels. Um diesen Wandel mitgestalten zu können, müssen nahezu alle Arbeitnehmer im Bereich KI weitergebildet werden. Hierbei könnten bei staatlich geförderten Weiterbildungsmaßnahmen auch die Gewerkschaften eine maßgebliche und proaktive Rolle einnehmen.

3) Bei der biometrischen Fernidentifizierung im öffentlichen Raum eröffnet der AI Act die Möglichkeit des Nachschärfens der EU-weiten Mindeststandards. Sowohl für Echtzeit-Fernidentifizierungssysteme als auch für nachträgliche biometrische Fernidentifizierung im öffentlichen Raum können die Mitgliedstaaten in nationalen Rechtsgrundlagen auch strengere Regeln erlassen. Wie lässt sich diese Möglichkeit für einen umfassenderen Grundrechtsschutz nutzen, wo könnten entsprechende Vorschriften im nationalen Recht verankert werden und wie sollten diese – etwa im Hinblick auf ein ausnahmsloses Verbot – inhaltlich ausgestaltet sein?
Für den Einsatz biometrischer Echtzeit-Fernidentifizierungssysteme wird innerhalb des AI Act ein grundsätzliches Verbot statuiert. Ausnahmen hierzu sind nur unter strengen verfahrens- und materiell-rechtlichen Voraussetzungen möglich (Art. 5 Abs. 1h - 2). Der Einsatz von biometrischen Echtzeit-Fernidentifizierungssystemen in öffentlichen Räumen zu Strafverfolgungszwecken soll nur bei Vorliegen von restriktiv auszulegenden Voraussetzungen möglich sein, wobei diese zudem in weiten Teilen kumulativ vorliegen müssen.
Jener Erlaubnisvorbehalt ist demnach bereits äußerst restriktiv. Ein absolutes Verbot in nationalem Recht würde die Funktionsfähigkeit der Sicherheitsbehörden gefährden. Für die wenigen zulässigen Ausnahmefälle (z.B. bevorstehender Terroranschlag, entführte Kinder, etc.) benötigen die Sicherheitsbehörden zwingend die Möglichkeit, biometrische Echtzeit-Fernidentifizierungssysteme als ultima ratio einsetzen zu können. Ziel muss es sein, einen erheblichen Schaden für Leib und Leben abzuwenden sowie die Bevölkerung und den Staat zu schützen.
Gesellschaft und Politik haben zu Recht höchste Erwartungen an den Einsatz von KI im sicherheitsbehördlichen Bereich: KI muss vertrauenswürdig sein und verantwortungsvoll eingesetzt werden. Gleichzeitig muss KI für Sicherheitsbehörden einsetzbar bleiben: Der

[3] http://www.europol.europa.eu/publications-events/publications/joint-declaration-of-european-police-chiefs-ai-act

Einsatz von KI erhöht die Effizienz der Tätigkeit von Sicherheitsbehörden und stellt die Handlungsfähigkeit der Sicherheitsbehörden gegenüber potentiell feindlichen Akteuren sicher, die KI zur Schädigung und Bedrohung der Gesellschaft einsetzen wollen. Daher sollte der Handlungsspielraum der Sicherheitsbehörden zur Wahrung der Sicherheit von Gesellschaft und Staat nicht weiter eingeschränkt werden.

4) Inwieweit beinhaltet der AI Act Instrumente zum Kampf gegen Desinformation, wie spielt er mit dem DSA zusammen und inwieweit ergeben sich daraus Handlungsempfehlungen für die nationale Ebene?
Diese erfolgen im AI Act mindestens mit Hinblick auf „General-Purpose AI" (GPAI)-Systeme, wie z.B. ChatGPT. Diese Systeme können für eine Reihe von Anwendungen eingesetzt werden[4], woraus der AI Act potentiell systematische Risiken ableitet, die jedoch überwiegend unbegründet erscheinen. GPAI-Systeme unterliegen besonderen hohen – wenn auch oft nicht praktikablen – Evaluations-, Dokumentations- und Absicherungsanforderungen.

5) Bitte beschreiben Sie die rechtlichen Anforderungen des AI Act an die zuständigen nationalen Behörden: Wie ist insbesondere die Vorgabe auszulegen, dass die Behörden ihre Befugnisse unabhängig, unparteiisch und unvoreingenommen ausüben müssen, und welche Regelungsoptionen zur Aufsichtsstruktur sind im nationalen Umsetzungsgesetz vor dem Hintergrund der bestehenden rechtlichen und organisatorischen Strukturen der Marktüberwachung (MÜ-VO, MÜ-G, RAPEX Informationssystem, Deutsches Forum für Marktüberwachung) denkbar, zulässig und mit Blick auf den Regelungsgegenstand KI-Systeme sachgerecht?
Siehe Antworten auf 1) und 12).

6) Bitte bewerten Sie die im AI Act vorgesehenen Maßnahmen zur Innovationsförderung (Kapitel VI): Wie sollten insbesondere KI-Reallabore und Tests unter realen Bedingungen national geregelt, angeschoben und durch politische Maßnahmen flankiert werden – und welchen Anforderungen muss die nationale und unionsweite Aufsichtsstruktur erfüllen, um zu einer kohärenten Nutzung dieser Instrumente beizutragen?
Der Aufbau von KI-Reallaboren und die Entwicklung von Tests unter realen Bedingungen werden ausdrücklich begrüßt, sind jedoch nicht ausreichend, um den Anforderungen an wirkliche Innovation gerecht zu werden. Reallabore senken die Anforderungen des AI Act ausdrücklich nicht. Da jedoch eine Aufsichtsbehörde eingebunden ist, kann sie ggf. keine Strafen verhängen. Zudem muss jeder Mitgliedsstaat die Rahmenbedingungen dafür schaffen und soll mindestens ein Reallabor errichten (Erwägungsgrund 138).
Da die Arbeit der Reallabore umfangreiche Methodenkenntnis und Einblicke in Arbeitsweise der Kunden benötigt, sollten z.B. Sicherheitsbehörden über ein eigenes KI-Reallabor verfügen, um den Methodenschutz zu gewährleisten und um auf für diesen Bereich spezialisierte Experten zurückzugreifen. Auch der Schutz sensibler Daten bedingt vor dem Hintergrund der Befugnisse eines KI-Reallabors (u.a. Art. 59) eine geschützte Umgebung für die Erprobung von Systemen, welche von oder für Sicherheitsbehörden eingesetzt werden sollen.

*7) Welche politischen und gesetzlichen Maßnahmen sind notwendig, um die im AI Act vorgesehenen harmonisierten Standards, gemeinsamen Spezifikationen und Zertifizierungsmechanismen für KI-Systeme voranzutreiben und das Konformitätsbewertungsverfahren insgesamt so auszugestalten, dass es für Unternehmen effizient umsetzbar ist, für Verbraucher*innen aber zugleich ein hinreichendes Schutzniveau gewährleistet?*
Die Erstellung von anwendbaren Standards, Normen, Checklisten und Best Practices für die Entwicklung, den Betrieb und die Prüfung von KI-Systemen sind von größter Bedeutung, um eine effiziente und effektive Umsetzung des AI Act zu gewährleisten. Für die Erstellung solcher Standards ist eine tiefe technische Expertise und praktische Erfahrung notwendig. Da das Europäische Komitee für elektrotechnische Normung (CENELEC) mit der Erstellung der im AI Act vorgesehenen harmonisierten Normen beauftragt ist, sollte sichergestellt werden, dass Deutschland hier – und in anderen relevanten Standardisierungsgremien – breit und stark vertreten ist. Zudem sollte Deutschland auch in den einschlägigen internationalen

[4] Generalisierung und breite Einsatzmöglichkeiten sind jedoch eigentlich per Definition das Ziel des maschinellen Lernens, weshalb der Begriff GPAI in der Wissenschaft umstritten ist.

Standardisierungsorganisationen (z.B. ISO, ITU, IEEE) vertreten sein. Ein Vorbild für staatliche Hilfsmaßnahmen bildet das amerikanische National Institute of Standards and Technology (NIST).

8) Welche gesetzlichen und politischen Maßnahmen sind notwendig, um die Zusammenarbeit zwischen den zuständigen Behörden in Deutschland und den Einrichtungen auf EU-Ebene (insbesondere AI Office, AI Board, Advisory Forum und Scientific Panel) schlagkräftig und effizient aufzustellen und wie lässt sich gewährleisten, dass zivilgesellschaftliche und interdisziplinäre wissenschaftliche Expertise bei der Auslegung, Konkretisierung, Umsetzung und Weiterentwicklung des AI Acts substantiell Berücksichtigung finden?
Die genaue Abgrenzung der Zuständigkeiten des AI Office und AI Board erscheint aktuell noch schwammig[5]. Eine Schärfung dieser Abgrenzung ist notwendig um die Einrichtungen auf EU-Ebene schlagkräftig und effizient aufzustellen und um Parallelstrukturen zu vermeiden. Das KI-Personal in der Industrie und Wissenschaft ist aufgrund der vielfältigen Anwendungsfälle generell interdisziplinär besetzt, was sich bei einer nach der Bestenauslese folgenden Besetzung der genannten Rollen in den Einrichtungen widerspiegeln sollte.
Bei der Zusammenarbeit mit Einrichtungen auf EU-Ebene sollten z.B. ZITiS oder die Agentur für Innovation in der Cybersicherheit (Cyberagentur) eine wichtige Funktion übernehmen und ihre aufgebauten hohen Kompetenzen in diesem Bereich einbringen.

9) Wie muss die Umsetzung des AI Acts in Deutschland gestaltet werden, um einerseits die Sicherheit und Bürgerrechte zu wahren und andererseits ein innovationsfreundliches Umfeld zu schaffen, das Innovationskraft und privatwirtschaftlichen Wettbewerb auf dem deutschen Markt ideal unterstützt?
Verfahren der KI sind grundsätzlich sicher und funktionieren[6], wenn sie richtig entwickelt werden. Um dies zu gewährleisten, können Aufsichtsbehörden nur eine nachgelagerte, präventive Rolle spielen. Durch Fördermaßnahmen müssen vorgelagerte, proaktive Maßnahmen ergriffen werden. Diese sollten u.a. das Thema Bildung stärken. Bis heute wird in den meisten KI-Vorlesungen z.B. das Thema „Bias"[7] (Verzerrungen, treten auf, wenn die Verteilungen von Trainings- und Testdaten unterschiedlich sind) nicht behandelt bzw. ist es den Lehrenden sogar überhaupt nicht bekannt. Durch eine Verbesserung der Ausbildungsmöglichkeiten würde die nächste Generation von KI-Experten befähigt, bessere und sicherere Verfahren umzusetzen, die zudem auch zu weiterer Innovationskraft und Steigerung der Wettbewerbsfähigkeit führen.

10) Wie sollte die nationale Gesetzgebung zur Umsetzung des AI Acts strukturiert werden, um einerseits detaillierte und spezifische Anforderungen zu adressieren und andererseits genügend Flexibilität für zukünftige Anpassungen und die Berücksichtigung sektorspezifischer Bedürfnisse zu gewährleisten? Welche Vor- und Nachteile wurden sich aus den verschiedenen regulatorischen Ansätzen ergeben?
Siehe Antworten auf 1) und 12).

11) Welche Ideen und Herangehensweisen zur Umsetzung des AI-Act sind Ihnen aus den anderen EU-Mitgliedstaaten bislang bekannt und welche dieser sollten in Deutschland für die Umsetzung genauer betrachtet bzw. einbezogen werden?
Spanien richtete schon im Juni 2022 das erste KI-Reallabor ein[8]. Zudem hat Spanien im November 2023 die Agencia Española de Supervisión de la Inteligencia Artificial (AESIA, Spanish Agency for the Supervision of AI) gegründet. Diese soll die spanische Verwaltung dabei unterstützen, die Pflichten gemäß AI Act umzusetzen[9].
Im Juli 2023 kündigte die französische Datenschutzbehörde CNIL die Einrichtung eines KI-Labors für drei Innovationsprojekte im öffentlichen Sektor an[10].

---

[5] Deutscher Bundestag, Drucksache 20/10599 vom 11.03.2024, http://dserver.bundestag.de/btd/20/105/2010599.pdf
[6] http://www.the-yuan.com/773/Contrary-to-popular-belief-AI-does-actually-work-is-generally-safe.html
[7] Siehe u.a. P. Glauner, P. Valtchev and R. State, "**Impact of Biases in Big Data**", Proceedings of the 26th European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning (ESANN 2018), Bruges, Belgium, 2018. http://www.esann.org/sites/default/files/proceedings/legacy/es2018-7.pdf
[8] http://digital-strategy.ec.europa.eu/en/news/first-regulatory-sandbox-artificial-intelligence-presented
[9] http://www.dataguidance.com/opinion/spain-agency-supervision-ai-overview
[10] http://www.cnil.fr/en/sandbox-cnil-launches-call-projects-artificial-intelligence-public-services

Ende 2022 kündigten die Niederlande spezielle Transparenzanforderungen an im öffentlichen Sektor eingesetzte KI-Systeme[11] an. Zudem wird die Dutch Authority for Digital Infrastructure (RDI) von der Europäischen Kommission bei der Einrichtung einer Überwachung für KI unterstützt[12].
Österreich hat im Januar 2024, im Vorgriff auf den AI Act, die KI-Servicestelle in der Rundfunk und Telekom Regulierungs-GmbH (RTR) eingerichtet, welche die neuen Regelungen des AI Act national koordinieren und kontrollieren soll[13].
Deutschland sollte aktiv in den Austausch mit den anderen Mitgliedsstaaten treten und Erfahrungen mit ihnen austauschen. Ebenso könnte eine Beteiligung Deutschlands am von der Europäischen Kommission eingerichteten AI Pact[14] sinnvoll sein.

12) Wie kann bei der Marktüberwachung mit Blick auf die hohe Zahl in Deutschland existierender Stellen und die aktuell sehr unterschiedliche Verteilung von bundesweiten bis hin zu regionalen Zuständigkeiten eine geographische und sektorale Zersplitterung verhindert werden, im Sinne einer effizienten, möglichst auf Bundesebene koordinierten Aufsicht und welche gesetzlichen Änderungen könnten aus Ihrer Sicht notwendig werden, um dieses Ziel zu erreichen?
Um eine geographische Zersplitterung zu vermeiden und eine bundesweite Harmonisierung bei der Durchsetzung des AI Act zu erreichen, sollte die Marktüberwachung schlank auf Bundesebene erfolgen bzw. dort koordiniert werden. Jedoch ist auch die sektorale Kompetenz für die effektive Umsetzung des AI Act entscheidend. Daher müssen einzelne Aufsichtsbehörden eigene KI-Kompetenzen aufbauen. Diese müssen auch untereinander gemeinsame Best Practices teilen um Doppelstrukturen und uneinheitliche Entscheidungen zu vermeiden. Widersprüchlichkeiten zwischen AI Act, Data Act, Datenschutzgrundverordnung, Digital Services Act, Digital Market Act, etc. werden bei der Umsetzung jedoch eine Herausforderung darstellen.
Art. 3 Abs. 48 definiert, dass eine „«zuständige nationale Behörde» eine notifizierende Behörde oder eine Marktüberwachungsbehörde" sei. Offen ist jedoch aktuell, ob diese oberste nationale Aufsichtsbehörde gleichzeitig eine notifizierende Behörde und eine Marktüberwachungsbehörde sein soll/darf oder ob es für die beiden Funktionen getrennte Behörden geben muss.
Für die Auswahl von Konformitätsbewertungsstellen (Art. 3 Abs. 21) und notifizierenden Stellen (Art. 3 Abs. 22) könnten Challenges der Bundesagentur für Sprunginnovationen (SPRIND) ein geeignetes Mittel sein.

13) Inwiefern lässt der AI-Act, was die Prüfungen von KI-Systemen angeht, Ihrer Ansicht nach genügend Raum für eine fortwährende Anpassung der Prüfschemata- und Kriterien an die sich schnell vollziehende weitere technologische Entwicklung bei KI, an welchen Stellen könnten hier mittelfristig Probleme entstehen und welche Maßnahmen sind bei der Umsetzung des AI-Act von Anfang an mitzudenken, um ausreichenden Spielraum für innovationsorientierte Anpassungen sicherzustellen?
Der AI Act sieht Mechanismen vor, um auch nach Inkrafttreten der Verordnung Anpassungen vorzunehmen. So ist z.B. vorgesehen, dass alle vier Jahre ein umfangreiches Review erfolgen soll, bei dem u.a. die Überwachungs- und Governance-Strukturen angepasst werden können (Art. 112).
Prüfungen von KI-Systemen adressiert der AI Act insbesondere bei GPAI-Systemen. Der AI Act gibt für deren Prüfung nur eine grobe Richtung vor und regelt die detaillierte Umsetzung nicht. Laut einem Kommissionsvertreter sei dies absichtlich nicht genau im AI Act festgelegt[15]. Hierdurch eröffnen sich Spielräume, die innovationsfreundlich ausgelegt sein müssen. Einen Vorschlag zur Präzisierung legte z.B. im April 2024 das ZEW – Leibniz-Zentrum für

[11] http://www.holisticai.com/blog/the-netherlands-ai-regulation
[12] http://reform-support.ec.europa.eu/what-we-do/public-administration-and-governance/supervising-ai-competent-authorities_en
[13] http://www.rtr.at/rtr/service/ki-servicestelle/ki-servicestelle.de.html
[14] http://digital-strategy.ec.europa.eu/en/policies/ai-pact
[15] http://background.tagesspiegel.de/digitalisierung/ein-wirtschaftsmodell-fuer-ki-sicherheitstests

Europäische Wirtschaftsforschung GmbH Mannheim vor[16]. Dieser kann eine sinnvolle Grundlage für weitergehende Diskussionen darstellen.
Zudem ist eine konkrete Gefahr, dass die Entwicklung von Open Source in diesem Bereich durch hohe Auflagen geschwächt bis unmöglich gemacht werden könnte. Ob kommerzielle Konkurrenten genau daran ein Interesse haben könnten, muss kritisch geprüft werden.

14) Steht für die Umsetzung des AI-Act in Deutschland Ihrer Ansicht nach genügend Fach-Personal zur Verfügung und wenn nein, in welchen konkreten Feldern deuten sich aktuell die größten Lücken an, welches sind die wichtigsten Maßnahmen, die von der Politik hier zu ergreifen sind, und wie wichtig wäre aus Ihrer Sicht das zeitnahe Vorliegen einer aktualisierten ressortübergreifenden KI-Strategie, um eine reibungslose und effiziente Umsetzung des AI-Act in Deutschland sicherstellen zu können?
Vor einigen Jahren begann u.a. der Freistaat Bayern damit, KI-spezifische Bachelor- und Masterstudiengänge zu etablieren. Da weitere Bundesländer anschließend einen ähnlichen Weg gingen, steht mittelfristig grundsätzlich viel Fachpersonal zur Verfügung. Dieses sollte jedoch vor allem in der Industrie und Wissenschaft zu Innovationen beitragen und nicht überwiegend in staatlichen Aufsichtsbehörden gebunden sein.
Eine wesentliche Herausforderung für Behörden bei der Gewinnung dieses Fachpersonals ist deren Vergütung. Bisher werden im öffentlichen Dienst viele Stellen für Informatiker (mit Masterabschluss) nur im gehobenen Dienst eingruppiert. Um das passende KI-Fachpersonal gewinnen zu können, müssen die Stellen in den Aufsichtsbehörden im höheren Dienst eingruppiert bzw. außertariflich vergütet werden. Erforderlich ist somit eine Konkretisierung der Abbildung auf Planstellen im Bundeshaushalt und in welchem Umfang dafür Haushaltsmittel erforderlich sind.
Eine aktualisierte und ressortübergreifende KI-Strategie für die Bundesrepublik Deutschland ist unabdingbar. Diese sollte jedoch nicht nur die Umsetzung des AI Act sicherstellen, sondern sich vor allem auf eine Steigerung der Innovation und Wettbewerbsfähigkeit durch KI fokussieren.

15) Ausdrücklich ausgenommen aus dem AI Act sind die Bereiche des Militärs und der Geheimdienste, da sie unter das nationale Recht der Mitgliedstaaten fallen. Wie kann und soll bei der Umsetzung des AI Act gewährleistet werden, dass in diesen Bereichen die mächtigen KI-Modelle etwa zur Gesichtserkennung oder zur Sprachanalyse gesetzeskonform eingesetzt werden?
Die Bundeswehr und die deutschen Nachrichtendienste sind verpflichtet, sich an die gültigen Rechtsnormen zu halten. Darüber hinaus unterliegen sie einer durchgängigen Kontrolle, u.a. durch den Deutschen Bundestag und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Persönlichkeitsrechte sind in Deutschland verfassungsmäßig besonders geschützte Güter, unabhängig vom Einsatz von KI.

16) Das neu einzurichtende Europäische AI-Büro soll „eine Schlüsselrolle bei der Umsetzung des KI-Gesetzes spielen, indem sie die Leitungsorgane in den Mitgliedstaaten bei ihren Aufgaben unterstützt". Sollte mit dieser „Unterstützung" eine Kontrolle und eine Weisungsbefugnis verbunden sein? Wo sollte das AI-Büro angesiedelt und wie sollte es personell, finanziell und organisatorisch ausgestattet sein, damit man es „politisch unabhängig" nennen könnte?
Das AI Office ist gemäß des AI Act der Europäischen Kommission unterstellt. Der AI Act legt die Aufgaben des AI Office, insbesondere auch Kontroll- und Weisungsbefugnisse fest. Es wäre begrüßenswert, wenn Deutschland eine starke Vertretung im AI Office und im AI Board, im Scientific Panel und im Advisory Forum anstrebt, da diese Institutionen die reibungslose und effiziente Umsetzung des AI Act maßgeblich beeinflussen werden. Siehe zudem Antwort auf 8).

17) Welche konkrete Regelung empfehlen Sie für die nationale Umsetzung des AI-Acts, um die im Koalitionsvertrag enthaltene Position eines Verbots biometrischer Fernidentifikationssysteme im öffentlichen Raum umzusetzen für die Sicherung der Grundrechte auf Privatsphäre sowie Datenschutz, auf Nichtdiskriminierung, Meinungs- und Informationsfreiheit, auf Versammlungs- und Vereinigungsfreiheit sowie auf Rechtsstaatlichkeit und inwiefern ergibt es mit Blick auf die genannten

[16] http://www.zew.de/presse/pressearchiv/zew-so-soll-risikoreiche-generative-ki-geprueft-werden

Grundrechte Sinn, dabei hinsichtlich Echtzeit und retrograder Fernidentifikation zu unterscheiden, insbesondere da die Unterscheidung zwischen Echtzeit und retrograd unklar ist?
Siehe Antwort auf 3).

18) Wie sollte und könnte ein nationales KI-Transparenzregister über den Bereich der Hochrisiko-Systeme hinausgehen, um wirksame Transparenz im Sinne des Verbraucherschutzes (Nachvollziehbarkeit, Beschwerdebasis etc.) herzustellen und insbesondere beim Einsatz von KI-Systemen durch die öffentliche Hand dem erhöhten Anspruch an Grundrechtsschutz und bestehende Abhängigkeiten gerecht zu werden und wie sollte generell ein solches Transparenzregister organisiert sein, hinsichtlich:

- *wer sollte es aufbauen und wen dabei einbeziehen*
- *wie sollte es aufgebaut werden*
- *wer sollte es verwalten*
- *welche Informationen sollte es enthalten?*

Der AI Act sieht vor, dass Hochrisiko-KI-Systeme und (zulässige) Systeme zur biometrischen Fernidentifizierung in Echtzeit in einer öffentlichen EU-Datenbank bzw. im Spezialfall von Systemen gemäß Anhang III Abs. 2 in einer nationalen Datenbank registriert werden (Registrierungspflichten gemäß Art. 49, 71). Ebenso müssen KI-Systeme, für die die Ausnahme aus der Hochrisiko-Klassifizierung gemäß Art. 6 Abs. 3 geltend gemacht wird, in der EU-Datenbank registriert werden. Informationen zu sicherheitsbehördlichen Anwendungsfällen (Anhang III Abs. 1, 6, 7) werden gemäß Art. 49 Abs. 4 nur eingeschränkt und in einem nicht-öffentlichen Teil der Datenbank erfasst.
Aufgrund der im AI Act enthaltenen unscharfen Definition der Begriffe „KI" und „Hochrisiko" erscheint die Notwendigkeit und Wirksamkeit solch eines Transparenzregisters fraglich. Es besteht die Gefahr einer erheblichen Bürokratisierung, die zu hohen Kosten und Innovationshemmnissen führen würde. Es gibt bisher aus den gleichen Gesichtspunkten auch kein „Software-Transparenzregister" oder „Computer-Transparenzregister".

Gerne stehe ich für weitergehende Fragen und Diskussionen zur Verfügung.

gez. Prof. Dr. Patrick Glauner

Professor für Künstliche Intelligenz
Fakultät Angewandte Informatik