

Nationale Spielräume bei der Umsetzung des europäischen Gesetzes über Künstliche Intelligenz

Schriftliche Stellungnahme von Lajla Fetic

Zur Öffentlichen Anhörung des Ausschusses für Digitales
am Mittwoch, 15. Mai 2024, 14:30 - 16:30 Uhr,
Marie-Elisabeth-Lüders-Haus (MELH), Saal 3.101

Vorbemerkungen

- Ich bedanke mich bei der Vorsitzenden und den Mitgliedern des Ausschusses für Digitales für die Einladung, eine schriftliche und mündliche Stellungnahme zu den nationalen Spielräumen bei der Umsetzung des europäischen Gesetzes über Künstliche Intelligenz abzugeben.
- Meine Ausführungen basieren im Wesentlichen auf den Arbeiten zu einer noch unveröffentlichten Publikation, die ich gemeinsam mit dem freien Researcher Amin Oueslati anfertige. Ich bedanke mich insbesondere bei meinem Co-Autoren für die einsichtsreichen und bereichernden Impulse. Die Beantwortung von Frage 6 ist unmittelbar seiner Autorenschaft zuzuordnen, wenngleich alle ausgeführten Punkte die Ergebnisse einer gemeinsamen Arbeit darstellen.

Fragenkatalog

- 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?*

Einführung

Deutschland hat eine einzigartige Chance die zentrale(n) Institution(en) und komplementierende Strukturen zur Umsetzung der KI-Verordnung (KIVO) im Sinne der nationalen Bedarfe und Gegebenheiten aufzubauen, da deren Ausgestaltung in weiten Teilen den nationalen Mitgliedsstaaten der EU überlassen ist. Dabei wird entscheidend sein, in der politischen Diskussion und Ausgestaltung nicht nur auf die Frage zu fokussieren, welche (bestehende(n)) Organisation(en) die Aufgaben der KI-Aufsicht übernehmen soll(en), sondern vor allem wie die Vorgaben erfüllt und die Aufgaben übernommen werden. Im Folgenden erläutere ich die Vorgaben aus dem EU AI Act, gebe eine Übersicht über die Aufgaben und gebe Empfehlungen für eine effektive KI-Aufsicht für Deutschland.

Grundlegend nimmt die nationale KI-Aufsichtsstruktur eine wichtige Rolle bei der Umsetzung der KIVO ein. Da es sich bei der KIVO im Wesentlichen um Produktsicherheitsrecht handelt, wird die Aufsicht durch ein Zusammenspiel verschiedener Behörden auf Basis von technischen Normen übernommen. Hier zu nennen ist die Marktüberwachungsbehörde, die notifizierende Stelle und die notifizierten Behörden. In diesem Kontext gehe ich insbesondere auf die Marktüberwachungsbehörde ein. Die technischen Normen werden aktuell auf europäischer Ebene erarbeitet, dazu in den weiteren Ausführungen unter Frage 13.¹

¹ Zu der Struktur der notifizierenden Behörde und der notifizierten Stellen, die ebenso zur KI-Aufsicht zu zählen sind, verweise ich an dieser Stelle an eine Publikation, die in der zweiten Jahreshälfte 2024 in dieser Sache erscheinen wird: Fetic, L. und Oueslati, A. (2024) [Forthcoming]. KI-Regulierung made in Germany? Sechs Handlungsfelder für eine erfolgreiche nationale Umsetzung der Europäischen KI-Verordnung. Berlin.

Zusammenfassung der Ableitungen aus der KI-Verordnung

- Deutschland muss eine Marktüberwachungsbehörde als zentrale Anlaufstelle für die Koordinierung auf europäischer Ebene benennen. Es können allerdings darunter liegende Behörden existieren, die sich national koordinieren. Marktüberwachung ist in Deutschland insbesondere in der Zuständigkeit von Landesbehörden und wird in der Regel auf der Bundesebene koordiniert.
- Die Behörde muss innerhalb von 12 Monaten benannt werden, idealerweise früher, um mit der Einstellung des geeigneten Personals zu beginnen und Vorbereitungen in Hinblick auf die komplexen Aufgaben zu treffen.
- Die Behörde muss unabhängig, unparteiisch und unvoreingenommen ihren Aufgaben nachkommen. Dafür sollte die Behörde frei von Weisungen sein und über einen eigenen Haushalt verfügen.
- Die Behörde übernimmt im Kern Beobachtungs- und Überwachungsaufgaben, Beaufsichtigungsaufgaben für das Reallabor, den Schutz der Grund- und Verbraucherrechte im Rahmen der KIVO und Anleitungs- und Beratungsfunktionen für KMUS und Startups.

Vorgaben aus der KI-Verordnung

Gestaltung der Behörde (Artikel 70, Abs. 1 und 2 KIVO):

Deutschland ist angehalten mindestens eine notifizierende Behörde und mindestens eine Marktüberwachungsbehörde einzurichten oder zu benennen. Letztere ist bereits grundsätzlich durch die Verordnung (EU) 2019/1020 und das nationale Marktüberwachungsgesetz geregelt. Ähnlich wie bei anderen Produkten, die den Harmonisierungsvorschriften der EU unterliegen, soll diese nationale Behörde sicherstellen, dass KI-Systeme den Anforderungen an Produktsicherheit und weitere Anforderungen erfüllen, bevor diese auf den europäischen Binnenmarkt gebracht werden. Die Behörden **müssen spätestens 12 Monate nach Inkrafttreten der KI-Verordnung benannt werden**. Genauer muss eine Marktüberwachungsbehörde als zentraler Kontaktknotenpunkt zur EU-Kommission benannt werden, um den Austausch auf europäischer Ebene und mit anderen Mitgliedsstaaten zu gewährleisten. Die EU-Kommission empfiehlt mit der Einrichtung oder Benennung dieser Behörden noch deutlich früher zu beginnen.²

Deutschland kann basierend auf diesen Vorgaben frei entscheiden, ob eine neue Behörde geschaffen wird oder eine existierende Behörde benannt wird. Denkbar ist auch eine Erweiterung einer existierenden Behörde um bereits existierende Marktüberwachungsbehörden im sektoralen Bereich (siehe Behörden zur Durchsetzung der Medizingeräterichtlinie). Bei der Wahl der Gestaltungsoption gilt es die Vorgaben, Bedingungen und Aufgaben zu bedenken, ebenso wie die bereits existierende Ausgangslage in Deutschland.

Vorgaben und Bedingungen (Artikel 70, Abs. 3 KIVO):

Vorgaben zur Arbeit der Marktaufsicht:

² https://www.euronews.com/next/2024/04/03/commission-presses-governments-to-appoint-ai-regulators?utm_source=substack&utm_medium=email

- Unabhängig (Die MÜB muss laut Vorgaben unabhängig sein, was im Idealfall bedeutet, dass die MÜB ihren Aufgaben weisungsfrei und auch mit eigenem Haushalt nachgehen können muss.³)
- Unparteiisch
- Unvoreingenommen
- Vertraulich (Rechte des geistigen Eigentums sowie Geschäftsgeheimnisse sollen geschützt werden.)

Dazu erforderliche Bedingungen:

- Angemessene technische und finanzielle Mittel
- Geeignetes Personal und Infrastrukturen
 - Ausreichende Zahl von Mitarbeitenden
 - Kompetenzen und Fachwissen (zu KI-Technologien, Daten und Datenverarbeitung, Schutz personenbezogener Daten, Cybersicherheit, Grundrechte, der Gesundheits- und Sicherheitsrisiken) und Kenntnisse der bestehenden Normen und rechtlichen Anforderungen
 - o Die MÜB muss die EU Kommission alle zwei Jahre darüber informieren, ob sie die Bedingungen adäquat erfüllt.

Weiter zu beachten:

Sollte die Organe und Einrichtungen der EU KI-Systeme einsetzen, so übernimmt der Europäische Datenschutzbeauftragte die Funktionen der Aufsicht. Bei Hochrisiko-KI-Systemen im Bereich der Finanzdienstleistungen ist im Wesentlichen die bereits benannte, nationale Behördenstruktur als Marktüberwachungsbehörde vorgesehen. Davon kann allerdings unter geeigneten Umständen abgewichen werden, wenn die alternative Aufsichtsstruktur an die Europäische Zentralbank alle notwendigen Informationen vermittelt. Für Hochrisiko-KI-Systeme im Bereich der Strafverfolgung, dem Grenzmanagement und Justiz und Demokratie kann die für den Datenschutz zuständige Aufsichtsbehörde als MÜB benannt werden.

Übersicht der Aufgaben:

Beobachtungs- und Überwachungsaufgaben für Hochrisiko-Systeme:

- Die MÜB kann, wenn sie eine Nicht-Konformität feststellt, Anbieter auffordern, dies zu beheben oder bei bestehender Nichtkonformität die Bereitstellung des KI-Systems am Markt beschränken, verbieten oder es vom Markt zurückrufen (Art. 80).
- Nimmt die MÜB an, dass von einem KI-System ein Risiko für die Gesundheit und Sicherheit oder für die Grundrechte ausgeht, so prüft sie, ob das System die Anforderungen und Pflichten erfüllt (insbesondere mit Blick auf Gruppen schutzbedürftiger Personen) und kann im Falle des Falles Korrekturmaßnahmen einfordern, die die Konformität wiederherstellen sollen, das Produkt vom Markt nehmen oder zurückrufen lassen (Art. 79).

³ In diesem Fall sind die Ausführungen von Dr. Jaurisch zu den Vorgaben an den Digital Service Coordinator hilfreich. Die Parallelen zum Digital Service Koordinator zeigen auf, wie auch vor dem Hintergrund von Kompromissen eine abgewogene Wahl getroffen werden kann.

- Nimmt eine MÜB an, dass ein KI-System fälschlicherweise nicht als hochriskant eingestuft wurde, kann sie das System überprüfen und erforderliche Maßnahmen durch die Anbieter einfordern.
- Die Marktüberwachungsbehörde meldet der Kommission und den nationalen Wettbewerbsbehörden jährlich die Informationen, die sie im Rahmen ihrer Tätigkeiten gesammelt hat. Insbesondere berichtet sie zu verbotenen Praktiken und über die ergriffenen Maßnahmen (Art. 74, Abs. 2).
- Die MÜB kann gemeinsam mit der Kommission Untersuchungstätigkeiten vorschlagen oder durchführen, um Konformität zu fördern oder Nicht-Konformität festzustellen, zu sensibilisieren oder Orientierung zu bieten (Art. 74, Abs. 11).
- Die Beobachtungs- und Überwachungsaufgaben für KI-Systeme mit allg. Verwendungszweck gelten nicht für die nationale MÜB, sondern sind dem europäischen Amt für künstliche Intelligenz übertragen. (Art. 75, Abs. 1)
- Sollte die nationale MÜB ihre Ermittlungen nicht abschließen können, so kann sie das Amt für künstliche Intelligenz ersuchen, den notwendigen Zugang zu Informationen durchzusetzen (Art. 75, Abs. 3).

Beaufsichtigung von Tests unter realen Bedingungen:

- Die MÜB muss die Kompetenzen und Befugnisse besitzen, sicherzustellen, dass die Tests unter realen Bedingungen richtig durchgeführt werden (Reallabor) (Art. 76)

Schutz der Grundrechte und der Verbraucher:innenrechte:

- Verbraucher:innen dürfen bei der MÜB begründete Beschwerde einlegen, wenn sie Grund zur Annahme haben, dass gegen die Anforderungen verstoßen wird.
- Behörden, die mit dem Schutz der Grundrechte beauftragt sind (z.B. die Datenschutzbehörden oder die Antidiskriminierungsstelle des Bundes) dürfen in Bezug auf Hochrisiko-Systeme Dokumentationen anfordern und einsehen, um ihrer Aufgabe nachzukommen. Sie informieren in dem Fall die MÜB von dieser Anfrage (Art. 77). Gegebenenfalls kann die MÜB in begründeten Fällen in diesem Sinne technische Tests durchführen (Art. 77, Abs. 3).

Anleitungen und Beratung zur Umsetzung der Vorgaben (insbesondere für KMUs und Start-ups)

Empfehlungen

- **Die Entscheidung darüber, ob eine neue Behörde geschaffen wird oder eine existierende Behörde benannt wird, sollte auf Basis der in der KIVO beschriebenen Vorgaben, Bedingungen und Aufgaben getroffen werden.** Ebenso sollte abgewogen werden, wie aufwendig sich die Schaffung einer neuen Behörde gestalten würde. Vor dem Hintergrund das notwendige Kompetenzen und finanzielle Ressourcen rechtzeitig zur Verfügung gestellt werden müssen, ist davon derzeit abzuraten. Langfristig könnte eine Bündelung bestehender Aufsichtsbehörden für den Digitalbereich angeraten sein und sollte im Prozess als ein Szenario diskutiert werden. Bei der Benennung einer bereits existierenden Behörde ist eine zentrale Herausforderung, wie es gelingt bei der Ausübung der Aufgaben Unabhängigkeit zu wahren und gleichzeitig die notwendigen

vielfältigen Kompetenzen für eine effektive und effiziente Aufsicht sicherzustellen.

- **Da sektorale bzw. fachspezifische Marktüberwachungsbehörden bereits in der KIVO empfohlen werden (s. Finanzdienstleistungen und Grundrechte), gilt es auf den Strukturen aufzubauen, ohne eine unübersichtliche Verästelung für Anbieter und Betreiber zu verstärken.** Die zentrale Marktüberwachungsbehörde sollte hierfür keine parallelen Strukturen schaffen, sondern bestehende Stellen in ihre Arbeit integrieren. Bei Anbietern von KI-Systemen für bereits geregelte Produkte sollte insbesondere die sektorale Aufsicht weiterhin Anlaufstelle bleiben. Die zentrale KI-Aufsicht sollte hingegen auf der Bundesebene konzentriert werden und die Arbeiten der sektoralen und föderalen Behörden bündeln und die Koordinierung mit der supranationalen Ebene übernehmen. Darüber hinaus ist ein grundsätzliches Umdenken in der Aufteilung von Zuständigkeiten wichtig. So sollten Anbieter und Betreiber von Hochrisiko-Systemen idealerweise nur einen Kontaktpunkt haben und ihre Anliegen fallspezifisch diskutieren können. Dabei ist es unerlässlich, dass die Behörden kollaborativ im Hintergrund zusammenarbeiten. Auch wenn eine One-Stop-Shop-Lösung vor dem Hintergrund aktueller Gesetzgebung und bestehender Strukturen auf dem Papier nicht möglich sein wird, so sollte es sich für die Anbieter und Betreiber zumindest in der Praxis so anfühlen. Damit sind also nicht die Benennung der zentralen Ankerinstitution allein, sondern die dahinterliegenden Abstimmungs- und Koordinierungsprozesse für eine kohärente und effektive Aufsicht entscheidend. Bestehende Austauschpunkte wie das Forum für Marktüberwachung können bereits genutzt werden, müssen aber dringend um Zugänge für zivilgesellschaftliche Perspektiven ergänzt werden.
- **Die Marktüberwachungsbehörde übernimmt in großen Teilen klassische Aufgaben innerhalb der Produktsicherheitslogik. Somit wäre eine Erweiterung bestehender Marktüberwachungsbehörden (wie z.B. der Bundesnetzagentur) denkbar.** Insbesondere Beobachtungs- und Überwachungstätigkeiten sind in diesem Zusammenhang in ihrer Art keine Neuheit für diese Behörden, müssen allerdings in Hinblick auf die Eigenheiten von KI-Systemen erweitert werden. Hier ist insbesondere die kontinuierliche Überprüfungsnotwendigkeit zu erwähnen, als auch der soziotechnische Charakter von KI-Systemen. Die Marktüberwachungsbehörde übernimmt allerdings nicht nur klassische Produktsicherheitsaufgaben. Sie ist ebenso für den Schutz der Grundrechte mitverantwortlich und dient als Anker für die von Betreibern einzureichende Grundrechte-Folgenabschätzung. Für letzteres eignet sich insbesondere die Expertise der Datenschutzbehörden. Allerdings wäre eine geteilte Verantwortung nach Aufgabentyp eine Überforderung für Anbieter und Betreiber von KI-Systemen sowie für die Aufsicht selbst, die die Informationen gebündelt an die europäische Kommission versenden muss. Eine zentrale Stelle ist für die Bündelung der Kompetenzen und Informationen unverzichtbar.
- **Aktuell werden vor diesem Hintergrund insbesondere zwei Optionen diskutiert: Die Bundesnetzagentur (BNetzA) und der Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI) bzw. die Datenschutzbehörden.** In puncto Unabhängigkeit sticht im positiven Sinne der

BfDI hervor. Die BNetzA kann dies nur im begrenzten Maße vorweisen.⁴ Die BNetzA kann, wie erwähnt, auf teilweise sektorale und produktsicherheitsbezogene Expertise zurückgreifen und hat im Kontext des DSA bereits zentralisierte Aufgaben übernommen und erwartet einen Personalzuwachs. Ebenso führt die BNetzA bereits die Geschäfte des Deutschen Marktüberwachungsforums (DMÜF), was bei der Koordinierung der sektor- und föderalübergreifenden Marktüberwachung hilfreich sein könnte. Die Datenschutzbehörden wären für die Aufgaben einer klassischen Marktüberwachung eine ungewöhnlichere Wahl, üben sie schließlich bislang keine Marktüberwachungsfunktion für bereits regulierte Produkte aus. Sie können allerdings vor dem Hintergrund der Aufgabe des Grundrechtsschutzes auf langjährige Erfahrung zurückgreifen und finden in der KIVO an mehreren Stellen direkte Erwähnung. Ebenso obliegen ihnen Überwachungsfunktionen im Rahmen der DSGVO.

- **Die Wahl der geeigneten Behörde lässt sich unter zur Hilfenahme wissenschaftlicher und fachlicher Expertise und Perspektiven nicht eindeutig ableiten. Es bleibt eine normative, eine politische Entscheidung.**
 - **Es gilt deshalb den Prozess der Gestaltung der deutschen KI-Aufsicht deliberativ zu gestalten.** Neben wissenschaftlichen Stimmen sollten zivilgesellschaftliche Perspektiven und Praxiseinblicke von Unternehmen in transparenter Weise konsultiert werden. Hierfür sollte ein transparenter Prozess mit Zeitrahmen und vielfältigen Beteiligungsformen gestaltet werden. Die Zielstellung für die führenden Bundesministerien sollte es sein, bis Ende des Jahres den Konsultationsprozess aufgesetzt und durchgeführt zu haben. Bislang sind insbesondere Stakeholder- Gespräche mit wirtschaftlichen Akteuren geführt worden. Die Einbindung der Zivilgesellschaft ist vor dem Hintergrund des Anspruchs Grund- und Menschenrechte zu schützen unabdingbar. In der ersten Jahreshälfte 2025 sollten auf dieser Basis die administrativen Schritte gegangen werden, um geeignetes Personal einzustellen und oder zu schulen und Prozesse und Strukturen für die Koordinierung aufzusetzen.
 - **In jedem Fall wird eine existierende Behörde um Kompetenzen erweitert werden müssen.** Im Falle der BNetzA sind dies im Kern Kenntnisse und Fähigkeiten, die dem soziotechnischen Charakter von KI-Systemen gerecht werden und Wissen im Bereich des Grundrechtsschutzes. Bei KI-Systemen handelt es sich nicht um klassische Produkte, ihre Implikationen können mitunter systemische Risiken für Mensch und Gesellschaft bedeuten. Dies muss eine Marktüberwachungsbehörde ebenso verantworten, wie sie die technischen Konformitätsbewertungen koordiniert. Im Falle des Datenschutzbehörden gilt es die klassischen Marktüberwachungsaufgaben so zu gestalten, dass ihre Anforderungen für Anbieter und Betreiber bewältigbar bleiben. Aus Fehlern bei der Umsetzung der Datenschutzgrundverordnung sollte gelernt werden. Hier müsste dezidiert technische Kompetenz zur Konformitätsüberprüfung aufgebaut werden und einer Verästelung im föderalen System

⁴ Vgl. hierzu die Ausführungen zum Kriterium der Unabhängigkeit für den DSC von Dr. Jaursch:

<https://www.stiftung->

[nv.de/sites/default/files/snv_warum_deutschland_eine_starke_plattformaufsicht_braucht.pdf](https://www.stiftung-nv.de/sites/default/files/snv_warum_deutschland_eine_starke_plattformaufsicht_braucht.pdf)

entgegengewirkt werden. Viele der Anforderungen werden auf Basis technischer Normen überprüft und entsprechen in ihrer Natur nicht den Vorgaben, die die Behörden im Rahmen der DSGVO überprüfen. Die beiden Szenarien geben den Blick frei auf unterschiedliche Schwerpunktsetzungen: Die Wahl der BNetzA ist die klassische Wahl für ein Produktsicherheitsgesetz und muss erweitert werden um rechtsbasierte Ansätze. Vice versa betont die Wahl der Datenschutzstellen die rechtsbasierten Ansprüche der KIVO und sollte um Produktsicherheitslogiken erweitert werden.

- **Unabhängig von der Frage, welche Institution die Aufsicht übernimmt, ist die zentrale Herausforderung die Sicherstellung ausreichenden Personals mit geeigneten und diversen Kompetenzen.** Hier gibt die KIVO kaum genaue Vorgaben. Allerdings kann davon ausgegangen werden, dass die Personalgewinnung einen möglichen Flaschenhals darstellen wird. Die spanische Aufsichtsbehörde setzt Berichten zu Folge etwa auf 50 Neueinstellungen (s. Frage 11). Im Vergleich sind für die Aufgaben des Digital Service Koordinators in der Bundesnetzagentur 70 Stellen vorgesehen (21 zusätzliche für Querschnittsaufgaben⁵). Diese Stellen sollen erwartungsgemäß 5000 kleinere und mittlere Dienste überwachen. Durch den horizontalen Ansatz der KIVO kann davon ausgegangen werden, dass die KI-Aufsicht deutlich mehr Fälle zu betreuen hat. Folglich muss in mindestens ähnlicher Größenordnung für den Personalaufwand gerechnet werden. In Bezug auf die Kompetenzen wird es sozialwissenschaftliche und regulative Fachkenntnisse im breiteren Sinne neben Wissen über technische Aspekte der KI-Systeme brauchen. Um es deutlich zu machen: Die Beurteilung technischer Konformitätsbewertung unter Bezugnahme ausgewiesener technischer Normen erfordert ein gänzlich anderes Profil als die Beurteilung einer Grundrechte-Folgenabschätzung auf Basis von Grund- und Menschenrechten. Ferner braucht es in jedem Fall Übersetzer:innen, die zwischen den Disziplinen und Anforderungen vermitteln können.
- **Für die Erweiterung existierender Behörden und die Einstellung geeigneten Personals werden Finanzmittel in Millionenhöhe notwendig sein. Gleichzeitig gilt es eine langfristige und nachhaltige Finanzierungsstrategie für die laufenden Kosten zu entwickeln.** Erfahrungen, die die BaFin macht, können hierfür herangezogen werden, da sie die Unabhängigkeit der Institution sichern könnten. So finanziert diese MÜB ihre Ausgaben durch Umlagen, Gebühren und Erstattungen. Die Ausgaben der BaFin wurden für das Jahr 2022 auf ca. 540 Millionen Euro geschätzt.⁶ Ob die Aufgaben der KI-Aufsicht diese Ausmaße annehmen, muss vor Benennung und Aufgabenschärfung geklärt werden. Dafür ist eine Abschätzung notwendig, wie viele Hochrisiko-Fälle mitunter untersucht werden müssen. Zusätzlich sollten Aufgaben, wie die Beaufsichtigung des Reallabors und die Koordinierungsaufgaben in Hinblick auf die Grundrechte-Folgenabschätzung durch die Betreiber eingepreist werden.

⁵ <https://background.tagesspiegel.de/digitalisierung/digital-services-coordinator-startschuss-auf-raten>

⁶ BaFin Jahresbericht 2022:

https://www.bafin.de/DE/PublikationenDaten/Jahresbericht/jahresbericht_node.html;jsessionid=E87EB751CF0407E9727756647F2D5C.internet952

- 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?*

Von einer Beantwortung der Frage wird abgesehen.

- 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?*

Biometrische Fernidentifizierungssysteme stellen eine besonders große Herausforderung für Grund- und Menschenrechte dar. So führen die Erkennungssysteme beispielsweise zur massiven Überwachung von Demonstrant:innen und damit zur Einschränkung ihrer Grund- und auch Menschenrechte.⁷

Regulativ muss auf europäischer Ebene neben der KIVO auch die DSGVO und die Law Enforcement Directive herangezogen werden. Die KIVO sieht zwar vor, Echtzeit-Fernidentifizierungssysteme im Einsatz für die Strafverfolgung zu verbieten, allerdings bleibt die Nutzung der nachträglichen Identifizierung weiterhin erlaubt. Dabei spielt es aus Sicht des Grundrechtsschutzes in der Praxis kaum eine Rolle, ob es sich um Echtzeit oder eine retrograde Identifizierung handelt. Ebenso weichen zahlreiche Ausnahmeregelungen und Unklarheiten das eigentlich von der Regierungskoalition vorgesehene Verbot der biometrischen Überwachung auf. Folglich ist zu empfehlen, diese Lücken auf nationaler Ebene zu schließen und einen effektiven Schutz vor Massenüberwachung zu ermöglichen.

Offene Fragen, die zur Nachschärfung der EU-Regelungen beantwortet werden müssen:

- Ab wie viel vergangener Zeit kann von einer nachträglichen Erkennung gesprochen werden? (Mitunter könnten sogar wenige Minuten und Stunden Unterschied ausreichen) Kann Deutschland auf das unklare und einschränkende Attribut der „Echtzeit“ in einem nationalen Gesetz verzichten?
- Ab wann spricht man von einer Fernidentifizierung? Zwar ist die Abgabe von Fingerabdrücken keine Fernidentifikation im Sinne einer sich dem Individuum entziehenden Kontrolle, doch sind insbesondere marginalisierte Gruppen von möglichen Machtungleichgewichten selbst bei einer unter dieser Definition „nicht-remote“ Identifizierung in ihren Grundrechten eingeschränkt. Kann Deutschland die Definition von Fernidentifikation vor diesem Hintergrund schärfen?
- Welche Behörden und Einsatzgebiete sollen neben den Strafverfolgungsbehörden noch von einem Einsatz gehindert werden? Hier wäre eine Ausweitung der Anwendungsakteure und -gebiete geboten.

⁷ <https://restofworld.org/2024/ Facial-recognition-government-protest-surveillance/#/an-end-to-privacy>

Auf nationaler Ebene ist es somit geboten, eine Klärung der vagen Einschränkungen und ein strenges Verbot biometrischer Massenüberwachung zu erwirken. Aus meiner Sicht ist dafür das deutsche KI-Gesetz zur Umsetzung der europäischen KI-Verordnung nur bedingt hilfreich. Möglicherweise können Überlegungen dazu in die Neustrukturierung des Bundespolizeigesetzes einfließen. Empfehlenswert ist eine enge Abstimmung mit Datenschutzbehörden zur weiteren Identifikation der national notwendigen Rechtsgrundlagen.

- 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?*

Desinformation findet explizit nur dreimal Erwähnung in der KIVO. Unter regulativen Gesichtspunkten ist für den Kampf gegen Desinformation im Wesentlichen der DSA entscheidend. Allerdings ist die Anforderung an eine Kennzeichnung von KI-Systemen mit allgemeinem Zweck mitunter als Instrument gegen Desinformation zu verstehen. Eine nationale KI-Aufsicht hat folglich zur Aufgabe diese Überlappungen direkt anzugehen und die in den Behörden verankerte Expertise zu bündeln oder zu koordinieren. Insgesamt wird es eine politische Gestaltungsaufgabe sein, die verschiedenen Digitalgesetze in ihrer Gänze zu beurteilen und in der Umsetzung kohärent zu gestalten. Denkbar wäre eine übergreifende Taskforce gegen Desinformation, die auf Basis der vielen Gesetzesinitiativen geeignete Maßnahmen verfolgt. Zusätzlich kann erwogen werden, zusätzliche Anforderungen an KI-Anbieter von Systemen mit allgemeinem Zweck zu formulieren, so z. B. das Watermarking. Allerdings hat diese Maßnahme nachweislich Wirkungslücken, sodass allein auf regulative Vorgaben nicht zu setzen ist. Folglich ist der Aufbau von Vertrauen in (digitale) Informationen durch einen systemischen Ansatz zu verfolgen: Kompetenzaufbau, die Stärkung bereits vertrauenswürdiger Medienintermediäre und die Stärkung der Verbraucher:innenrechte (so wie z.B. das neu geschaffene Center for User Rights der GFF).

- 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?*

Im Rahmen der Antwort zur Frage 1 diskutiert.

- 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?*

Die Beantwortung dieser ist eine gekürzte Version der schriftlichen Ausführungen von Amin Oueslati im Rahmen unserer gemeinsamen Publikation zur nationalen Umsetzung der KIVO:⁸

Einführung

Derzeit gibt es über 100 Reallabore weltweit. KI-Reallabore bieten einen kontrollierten Rahmen, um innovative KI-Systeme vor dem Markteintritt zu testen und weiterzuentwickeln. Das erste Reallabor wurde 2016 von der UK Financial Conduct Authority (FCA) gegründet, mit dem Ziel, FinTech Innovation zu fördern. Derzeit gibt es über 100 Reallabore in sehr unterschiedlichen Bereichen, von FinTech über Datenschutz bis hin zu Blockchain.

Das primäre Ziel von KI-Reallaboren ist es, Innovation zu stärken. Anstatt alle regulatorischen Auflagen zu erfüllen, die für einen vollständigen Markteintritt erforderlich wären, spezifizieren Unternehmen und Behörde die Auflagen in einem Testplan, was es ermöglicht, bestimmte Auflagen vorläufig abzuschwächen. Nehmen wir den hypothetischen Fall eines 5-Personen-Startups, das eine neue KI-Anwendung zur Unterstützung von HR-Prozessen entwickelt: Eigentlich müsste die Anwendung eine Protokollierung aller Ereignisse durchführen (Art. 12). Es gibt aber noch Unklarheiten, wie genau diese Anforderung datenschutzkonform umgesetzt werden kann. Da der Testplan vorsieht, die Kund:innen auf ein einziges Unternehmen zu beschränken, kann auf die Dokumentationspflicht für die Dauer der Testphase zum Teil verzichtet werden. Erfüllt das Unternehmen die im Testplan festgelegten Bedingungen, garantiert das die Rechtssicherheit, während das Unternehmen das KI-System unter Realbedingungen testen und mit echten Nutzer:innen iterieren kann. Andererseits begleiten die zuständigen Behörden die Testphase und unterstützen die Unternehmen beim Übergang in den Echtbetrieb (Art. 57, Abs. 7).

Als sekundäres Ziel ermöglichen Reallabore das regulatorische Lernen. Die Geschwindigkeit des Fortschritts bei transformativen Technologien wie KI stellt eine Herausforderung für den Staat dar. Häufig geschieht die Innovation im Privatsektor und die zuständigen Behörden müssen die Innovation erst in einem zeitintensiven Prozess verstehen lernen, um sie richtig zu überwachen. Das Reallabor ermöglicht es, die Entwicklung von KI-Systemen und regulatorisches Lernen zu synchronisieren: Expert*innen der Behörde erhalten fortlaufend Einblicke in die Anwendung und stehen im direkten Austausch mit den Entwickler:innen.

⁸ Fetic, L. und Oueslati, Amin. (2024) [Forthcoming]. KI-Regulierung made in Germany? Sechs Handlungsfelder für eine erfolgreiche nationale Umsetzung der Europäischen KI-Verordnung. Berlin.

Gestaltungsräume

Deutschland kann aktiv an der Ausgestaltung des Durchführungsrechtsakts mitwirken. Zwar werden die meisten Modalitäten einheitlich in der EU geregelt, jedoch kann sich Deutschland aktiv in diesen Prozess einbringen.

Deutschland muss eine geeignete Behörde mit der Umsetzung des KI-Reallabors beauftragen. Der EU AIA lässt offen, ob das Reallabor innerhalb oder außerhalb der Marktüberwachungsbehörde angesiedelt ist.

Deutschland kann die nationale Vernetzung von Reallaboren mit weiteren Innovationsstrukturen steuern. Die KI-Verordnung unterstreicht zwar die Vorteile einer Zusammenarbeit mit anderen einschlägigen Akteuren, wie z.B. TEFs, lässt die Details der Zusammenarbeit jedoch offen. Hinsichtlich Modus und Intensität der Zusammenarbeit gibt es aber große nationale Spielräume.

Zur Wahl der richtigen Stelle für ein Reallabor

Die richtige Behörde/Stelle mit dem Reallabor betrauen aufgrund von (i) Expertise, (ii) Schnittstellen, (iii) Skalierbarkeit, (iv) Evidenz aus anderen Industrien. Neben der Marktüberwachungsbehörde wären grundsätzlich andere Stellen denkbar. Beispielsweise wird auch eine Umsetzung des Reallabors als Öffentlich-Private-Partnerschaft politisch diskutiert. Angenommen die Beauftragung von staatlicher Seite erfolgt durch die Marktüberwachungsbehörde, würde so die operative Durchführung ausgelagert.

Zur Beurteilung der Eignung unterschiedlicher Stellen haben wir einen Entscheidungsraster entwickelt. Mithilfe des Rasters können Stellen, die für die Rolle infrage kommen, hinsichtlich ihrer Eignung bewertet werden. Wir haben die Dimensionen aus einer Analyse bestehender Reallabore abgeleitet. Das übergeordnete Raster der Dimensionen gestaltet sich wie folgt:

1. **Expertise:** Regulatorische und technische Expertise helfen vor allem die Sicherheit der KI-Anwendungen im Reallabor zu gewährleisten
2. **Schnittstellen:** Je enger eine Stelle mit anderen relevanten Akteur:innen verknüpft ist, desto schneller und effizienter gestalten sich die Prozesse im Reallabor.
3. **Skalierbarkeit:** Wenn ein Reallabor einfach skaliert, kann es flexibel auf Markttrends reagieren. Nehmen wir an, dass infolge eines technologischen Durchbruchs eine Vielzahl neuer AI-Startups gegründet wird. Das Reallabor könnte entsprechend reagieren und die Anzahl der betreuten Unternehmen im Labor erhöhen.
4. **Evidenz aus anderen Industrien:** Ein Proxy für all jene Faktoren, die wir nicht explizit als Dimension anführen. Wenn eine bestimmte Art von Stelle auch in keiner anderen Industrie in über 100 Fällen das Reallabor verantwortet, gibt es dafür wohl auch eine Grundlage.

Welche Stelle am besten geeignet ist, kann gegebenenfalls mit dem Zielbild des Reallabors variieren. Dieses Zielbild könnte definiert sein durch die Anzahl der

teilnehmenden Unternehmen pro Jahr oder die Abwägung von Sicherheit vs. Innovation vs. regulatorischem Lernen.

In den meisten Szenarien ist die Marktüberwachungsbehörde aufgrund ihrer Expertise und der vielen fachlichen Schnittstellen am besten geeignet, das Reallabor zu verantworten. Die wichtigste Schnittstelle ist die Marktüberwachungsbehörde. Eine enge Anbindung eröffnet Zugang zu zentraler Expertise, vereinfacht prozessuale Abstimmung und ermöglicht regulatorisches Lernen. Daher erscheint der Aufbau des Reallabors in der Marktüberwachungsbehörde als optimale Governance-Option. Dies spiegelt auch die Evidenz anderer Reallabore wider: Typischerweise ist das Reallabor bei der zuständigen Behörde organisatorisch aufgehängt, z.B. UK Financial Conduct Authority Regulatory Sandbox.

Wird die Zielsetzung im Reallabor sehr stark auf Innovation und enge Betreuung ausgelegt, entsteht möglicherweise eine Fallkonstellation, die eine Öffentlich-Private-Partnerschaft begünstigt. Die Zielsetzung wäre charakterisiert durch: (i) Aufnahme einer signifikanten Anzahl an Unternehmen in das Reallabor, (ii) intensive, ressourcenintensive Betreuung, (iii) zusätzlich Unterstützung zu unternehmerischen Fragestellungen.

- 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?*

Von einer Beantwortung der Frage wird abgesehen.

- 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?*

Grundsätzlich im Rahmen der Antwort zur Frage 1 diskutiert. Es ist überdies empfehlenswert den im Rahmen des DSA eingeplanten Beirat für zivilgesellschaftliche Perspektiven auf die KI-Aufsicht zu erweitern.

- 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?*

Einführung

Die nationale Umsetzung des AIA entscheidet über das Gelingen der digitalen Transformation. Damit einher geht auch eine Verschiebung der Verantwortung von der europäischen auf nationalstaatliche Ebene der Mitgliedsländer. Zwar werden einige Maßnahmen weiterhin auf europäischer Ebene koordiniert, beispielsweise die Entwicklung von technischen Normen, an vielen Stellen gibt es aber umfangreiche Gestaltungsspielräume für die nationale Politik. Welche nationale Behörde übernimmt die Marktüberwachung? Wie schafft man ein effektives Ökosystem für KI-Audits? Wie können KI-Reallabore Räume für Innovation schaffen?

Die Übersetzung der europäischen Anforderungen birgt eine einmalige Chance. Deutschland, häufig Schlusslicht in Digitalisierungsfragen, kann sich durch eine effektive Umsetzung der nationalen KI-Regulierung hervortun und damit im europäischen und globalen Wettbewerb führend positionieren. Mit den richtigen Weichenstellungen heißt es: Vorangehen statt aufholen. Um KI vertrauenswürdig und zugleich innovationsfördernd zu regulieren, muss Deutschland einerseits auf der langjährigen Expertise in der technischen Produktsicherheit aufbauen („TÜV als Exportschlager“), andererseits regulatorische Sicherheit und Innovationsmaßnahmen so ausrichten, dass sie die Innovationsfähigkeit der deutschen Wirtschaft fördern.

Amin Oueslati und ich argumentieren in einer in diesem Jahr erscheinenden Publikation, dass Deutschland eine führende Rolle bei der KI-Regulierung einnehmen kann, dafür die nationale Umsetzung aber konsequent planen und vorbereiten muss. Mit dem Inkrafttreten des EU AIA in 2026 – in Teilen sogar früher – gilt es, vor die Welle regulatorischer Anforderungen zu kommen. Damit die deutsche Bundespolitik in dieser Sache aktiv und entschlossen agieren kann, formulieren wir sechs Handlungsfelder, die unerlässlich für eine erfolgreiche Umsetzung des EU AIA sind:

1. Gestaltung einer effektiven nationalen Marktüberwachungsbehörde
2. Schaffen von Innovationsräumen: KI-Reallabore, Test- und Versuchseinrichtungen
3. Aufbau eines Ökosystem für KI-Audits bzw. Konformitätsbewertung und notifizierte Stellen
4. Einbindung von Wissenschaft und Zivilgesellschaft in die Standardisierungsgremien
5. Entwicklung eines effizienten und effektiven Vorgehens zur Grundrechte-Folgenabschätzung
6. Ausgestaltung der Beschwerde- und Regressmöglichkeiten

Auf Handlungsfeld 1 gehe ich unter Frage 1 ausführlich ein. Handlungsfeld 2 und 3 werden in Teilen unter Frage 6 und 7 erörtert. Handlungsfeld 4 wird unter Frage 13 diskutiert. Folglich möchte ich mich im weiteren Verlauf insbesondere mit Handlungsfeld 5 beschäftigen und Empfehlungen formulieren zur Ausgestaltung einer effektiven und effizienten Grundrechte-Folgenabschätzung.

Vorgaben aus der KI-Verordnung

In Artikel 27 der KI-Verordnung definiert der Gesetzgeber die Anforderung, den Umfang und die Bedingungen unter denen die sogenannte Grundrechtefolgeabschätzung (GFA) durchzuführen ist. Die nun in der Verordnung erwähnte Abschätzung geht in ihrer Ausrichtung im Wesentlichen auf die Forderung von

über 150 europäischen Professor:innen zurück ([Brussels Privacy Hub](#)). Die Anforderung war lange Zeit kein expliziter Bestandteil des ursprünglichen Vorschlags der Europäischen Kommission, bevor sie im Oktober 2023 im Trilog durch das Europäische Parlament vorgeschlagen wurde ([Bertuzzi, 2023](#)), um den Schutz der Grundrechte zu stärken.

Die GFA bildet eine Brücke zwischen den vornehmlich technischen Standards und dem Anspruch menschenzentrierte KI in Europa zu fördern. Das Ziel der Abschätzung ist, die möglichen Folgen auf die vornehmlich in der Charta der der EU definierten Rechte, Freiheiten und Grundsätze zu erfassen und sie im Kontext der Anwendung zu bewerten. Die Anforderung eine GFA durchzuführen wird 24 Monate nach Inkrafttreten der KI-Verordnung von Betreibern von Hochrisiko-Systemen umgesetzt werden müssen.

Die GFA ist eine ex-ante Folgenabschätzung und komplementiert bestehende Grundrechtsvorgaben. Die Abschätzung stellt eine Erweiterung bereits bestehender und obligatorischer Ansätze dar, die wiederum nur Teile der Grundrechte abdecken. Hier ist vor allem die Datenschutz-Folgenabschätzung (DSFA) zu erwähnen (Artikel 35, Datenschutzgrundverordnung (DSGVO)), die in ihrer Methodik zwar ähnlich aufgebaut ist, allerdings vor allem auf den Schutz der personenbezogenen Daten fokussiert (Artikel 8, Grundrechtecharta (GRC)). Insgesamt bildet die in der KI-Verordnung vorgesehene Grundrechtfolgeabschätzung einen der umfassendsten Ansätze, den soziotechnischen Charakter von KI-Systemen zu erfassen und ihn im spezifischen Anwendungsfall zu kontextualisieren.

Empfehlungen

Um eine bedarfsgerechte Umsetzung der GFA zu ermöglichen, ist es notwendig, Muster und Anleitungen partizipativ zu entwickeln. Da sich die Anforderung eine GFA durchzuführen vor allem an Betreiber im öffentlichen Sektor richtet, ist eine Einbindung dieser Behörden auf allen Ebenen empfehlenswert. Dabei haben Behörden auf Bundes- und Landesebene und kommunaler Ebene unterschiedliche Kompetenzen und Ressourcen, sodass auch die Bedarfe unterschiedlich ausfallen können. An dieser Stelle kann die Einbindung des IT-Planungsrates bzw. der Föderalen IT-Kooperation (FITKO) und anderer bestehender Koordinationsstellen wie das NExT Netzwerk hilfreich sein. Wichtig wird es dabei auch sein, fallbasiert vorzugehen. Die Vielfalt der möglichen Anwendungsfälle macht die Anwendung des Musters komplex. Bereits existierende Best Practices zeigen, wie Folgenabschätzungen im Kontext von polizeilicher Arbeit durchgeführt werden können. Dabei ist augenscheinlich, dass es mitunter große Unterschiede im Bearbeiten der Abschätzungen geben wird, sollte es sich dabei um Fälle im polizeilichen, administrativen oder auch versicherungstechnischen Bereich handeln. Hier gilt es also nicht nur überföderal und ressortübergreifend zu agieren, sondern auch innerhalb der Behörden hierarchieübergreifend vorzugehen, um die den Fällen zugeordneten Beamten in eine fallsensitive Erarbeitung der Muster einzubeziehen.

Zusätzlich zur Perspektive auf die Verwaltung wird es eine wichtige Aufgabe sein, Betroffenengruppen und ihre Repräsentanten einzubeziehen. Die Folgeabschätzung dient dem Schutz der Grund- und Menschenrechte von möglichen betroffenen Personen und Gruppen, ihre Perspektive sollte deshalb in die Ausgestaltung der Abschätzung einbezogen werden. Antidiskriminierungsstellen, Gewerkschaften und weitere Verbände könnten bei der Erstellung der Muster hilfreiche Einsichten geben,

insbesondere vor dem Hintergrund, dass die Ergebnisse der Folgenabschätzungen Teil weiterer Transparenzmaßnahmen sein könnten. So fordert die Organisation AlgorithmWatch eine Einbindung der Folgeabschätzungen in ein mögliches KI-Transparenzregister, das Bürger:innen und Stellvertreter über die Einsätze im öffentlichen Sektor informieren könnte. Vor dem Hintergrund bereits geäußelter Kritik durch einen Zusammenschluss zahlreicher zivilgesellschaftlicher Organisationen⁹, wäre die proaktive Einbindung dieser Organisation in die Erstellung des Musters anzuraten.

Abschließend wird die partizipative Erarbeitung des Musters und der Anleitungen eine zentrale Koordinierung benötigen. An dieser Stelle könnte die Marktüberwachungsbehörde eine Scharnierfunktion zwischen den verschiedenen Ebenen der Behörden, den Betroffenengruppen und Expert:innen der Wissenschaft einnehmen.

Die obligatorische Einbindung (zivilgesellschaftlicher) Stakeholder bei der Durchführung der GFA muss auf nationaler Ebene verhandelt werden. Der europäische Gesetzgeber sieht nach einigen Verhandlungen nicht vor, dass externe Stakeholder bei der Durchführung einer GFA obligatorisch einbezogen werden müssen. Dies bedeutet jedoch nicht, dass sie nicht beteiligt werden können. Zudem obliegt es den Mitgliedsstaaten weitere Vorgaben vor dem Hintergrund nationaler Interessen zu beschließen. Angesichts zivilgesellschaftlicher Kritik, die zu Teilen auch von der Wissenschaft aufgegriffen wurde, ist zu empfehlen, auf deutscher Ebene zumindest in Rahmen der Diskussion eines Referentenentwurfs für die nationale Umsetzung der KIVO eine solche Verschärfung zu prüfen und eine Einigung zu erwirken.

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 würden sich aus den verschiedenen regulatorischen Ansätzen ergeben?

Von einer Beantwortung der Frage wird abgesehen.

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?

Zur KI-Aufsicht:

- Das von der EU geförderte Projekt „Supervising AI by Competent Authorities“ von der Niederländischen „Authority for Digital Infrastructure“ und der UNESCO erforscht seit Oktober 2023 die Frage, wie eine effektive Aufsicht für KI institutionell aufgebaut werden sollte. Zu erwarten ist ein Report, der verschiedene Erfahrungen zum Aufbau der entsprechenden Strukturen zusammentragen wird.¹⁰ Eine Verzahnung deutscher Überlegungen mit diesem

⁹ <https://www.amnesty.eu/wp-content/uploads/2024/04/EUs-AI-Act-fails-to-set-gold-standard-for-human-rights.pdf>

¹⁰ <https://www.rdi.nl/onderwerpen/kunstmatige-intelligentie/nieuws/2023/10/05/unesco-ec-netherlands-ai-supervision-collaboration>

Projekt ist empfehlenswert. Insgesamt ist ein europäischer Austausch über die Ideen einer effektiven Aufsicht notwendig, trotz aller nationaler Eigenheiten.

- In diesem Zusammenhang legt eine Studie der niederländischen Datenschutzbehörde dar, dass bereits viele sektorale Aufsichtsorganisationen vor Inkrafttreten der KIVO KI-Systeme überprüfen und oder sich der Risiken der Systeme bewusst sind.¹¹ Zusätzlich investiert die niederländische Regierung in den Aufbau der Datenschutzbehörde, um die Aufgaben der KIVO umzusetzen. So wurde 1 Million Euro für das Jahr 2023 vorgesehen. Bis 2026 stehen insg. 3,6 Millionen Euro zur Verfügung. Ein fachlicher Fokus liegt insbesondere auf Anwendungen der öffentlichen Hand aufbauend auf ersten Erfahrungen eines KI-Registers. Hier kann Deutschland von den konkreten Erfahrungen zur Ausgestaltung eines KI-Registers profitieren. Ebenso wird die Ausweitung der Kompetenzen der Datenschutzbehörden für die unter Punkt 1 erläuterten Fragestellung relevant sein.
- In Spanien wurde dagegen eine neue KI-Agentur im Herbst 2023 etabliert.¹² Die spanische Regierung investiert laut Angaben etwa 5 Millionen Euro für die Einrichtung dieser Behörde. Die weitere Finanzierung ist allerdings nicht abschließend geklärt.¹³ Neben den Strukturen, die eine Alternative zur niederländischen Variante darstellen, ist der Entscheidungsprozess über den Sitz der Aufsicht beachtlich. So wäre es denkbar, dass Deutschland die Wahl der Aufsichtsstruktur auf Basis vorab definierter Kriterien in einem transparenten Bewerbungsprozess zwischen den alternativen Aufsichtsstrukturen vornehmen könnte. Ebenso lehrreich sollte die zu kritisierende ausbleibende Beteiligung der Zivilgesellschaft in diesem Prozess sein. Da insbesondere zivilgesellschaftliche Organisationen stellvertretend für marginalisierte Personen und Gruppen Belange und Ansprüche an den Grundrechtsschutz vorbringen, sollten sie bei der Gestaltung der Aufsichtsstruktur inkludiert werden.

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?

Im Rahmen der Antwort zur Frage 1 diskutiert.

¹¹ <https://www.autoriteitpersoonsgegevens.nl/uploads/2024-01/AI%20%26%20Algorithmic%20Risks%20Report%20Netherlands%20-%20winter%202023%202024.pdf>

¹² <https://www.engage.hoganlovells.com/knowledgeservices/news/ai-algorithms-part-6-spain-to-create-europes-first-supervisory-agency-for-artificial-intelligence#:~:text=Spain%20to%20create%20Europe's%20first%20supervisory%20agency%20for%20artificial%20intelligence>

¹³ <https://algorithmwatch.org/en/what-to-expect-from-europes-first-ai-oversight-agency/>

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?

Von einer ausführlichen Beantwortung der Frage wird abgesehen. Insgesamt ist darauf hinzuweisen, dass die regulativen Anforderungen im Wesentlichen auf die Konkretisierung in technischen Normen und Standards setzen sowie auf die Konformitätsüberprüfungen durch notifizierte Stellen. Dadurch entstehen ausreichend innovationsfreundliche Freiheitsgrade für die Prüfungsgrundlage. Allerdings sei an dieser Stelle ausdrücklich auf die Herausforderungen in der technischen Normierung in Normierungsorganisationen verwiesen. Die demokratische Legitimität der Organisationen und ihre Zusammensetzung ist dabei ein wesentlicher Kritikpunkt, der insbesondere Nachteile für KMUs und Startups einerseits und zivilgesellschaftliche Organisationen andererseits birgt. Hierzu seien meine Ausführungen aus der Arbeit in der deutschen Normungsroadmap KI sowie die Ausführungen der Autor:innengruppe um Dr. Baeva, Puntschuh und Binder empfohlen.¹⁴¹⁵ Zusätzlich sind die Kapazitäten der notifizierten Stellen als möglicher Engpass beachtenswert.

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?

Es braucht eine Erweiterung des KI-Kompetenzbegriffs und Klärung der KI-Kompetenzprofile für eine effektive KI-Aufsicht. Sicherlich gibt es viele Studien zu den fehlenden KI-Kompetenzen in der Wirtschaft bzw. zur Entwicklung und Gestaltung von KI-Systemen. Meines Wissens gibt es allerdings keine belastbaren Zahlen zur Quantität und Passung des Personals für eine effektive KI-Aufsicht, wie sie in der KIVO vorgesehen ist. Ausgehend von den konkreten Vorgaben der KIVO müssten zunächst unterschiedliche Kompetenzprofile erstellt werden. Auf Basis der Vorgaben gibt es mindestens drei Kompetenzbereiche: technische (u.a. mit Blick auf KI, Datenverarbeitung, digitale Infrastrukturen), soziotechnische (u.a. mit Blick auf die Einbindung von KI in Organisationen, die Ausgestaltung der Mensch-Technik-Interaktion und den Schutz von Menschen- und Grundrechten) sowie regulative Kompetenzen (u.a. mit Blick auf das Wissen zu existierenden digitalspezifischen Gesetzen und technischen Normen). Ferner besteht ein Bedarf an Übersetzer:innenfähigkeiten, die zwischen den verschiedenen Kompetenzprofilen und Disziplinen vermitteln können. Folglich werden mindestens technische, juristische und sozialwissenschaftliche Hintergründe die Grundlage für Einstellungsprofile bilden. Insbesondere die Einstellung technischer Profile unter Berücksichtigung der begrenzten Möglichkeiten bestehender Tarifstrukturen im Öffentlichen Dienst ist herausfordernd.

¹⁴ <https://background.tagesspiegel.de/digitalisierung/wir-brauchen-ungewoehnliche-koalitionen>

¹⁵ <https://www.zvki.de/zvki-exklusiv/fachinformationen/zvki-whitepaper-power-to-the-standards>

Gleichzeitig wird es vor dem Hintergrund lukrativer Alternativen in der Privatwirtschaft zur Beratung der KIVO-Umsetzung womöglich ebenso schwierig sein, juristische und sozialwissenschaftliche Perspektiven für die nationale Umsetzung zu gewinnen. Hier stellen sich also grundlegende Fragen zur Attraktivität der öffentlichen Hand als Arbeitgeberin. Den Startpunkt bildet hierfür, wie ausgeführt, aber zunächst eine transparente Erstellung von Kompetenzprofilen und Abschätzung des konkreten Personalaufwands.

Die Anpassung der KI-Strategie bzw. des KI-Aktionsplans kann allgemein hilfreich sein. Allerdings braucht es an dieser Stelle nicht mehr Strategie, sondern wirkungsorientierte politische Fördermaßnahmen und eine Flexibilisierung der Einstellungspraxis des öffentlichen Sektors. Inwiefern die bereits bestehenden Fördermaßnahmen im KI-Aktionsplan hilfreich sind, kann aufgrund fehlender Empirie nicht beurteilt werden. Zusätzlich können aufgrund föderaler Strukturen insbesondere die Länder für Teile der KI-Aufsicht zuständig sein. Hier gilt es einen föderalübergreifenden Ansatz zu bevorzugen.

Daneben ist eine Erweiterung von Weiterbildungsangeboten für bereits bestehendes Personal angeraten. Allgemeine KI-Aufklärungskurse sind an dieser Stelle nicht hilfreich. Konkrete Anleitungen, wie die Vorgaben der KIVO zu übersetzen sind, müssen auf Basis konkreter Fallbeispiele und Best Practice Sammlungen erarbeitet werden. Hierfür ist eine Unterstützung von Communities of Practice, wie des NEXt Netzwerks unabdingbar.

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?

Von einer Beantwortung der Frage wird abgesehen.

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?

Zur Ausgestaltung der nationalen KI-Aufsicht siehe Ausführungen zur Frage 1. Eine Kontrolle oder Weisungsbefugnis einer supranationalen Behörde (in Form des Amtes für Künstliche Intelligenz) erscheint vor dem Hintergrund der nationalen Souveränität in diesen Fragen nicht durchsetzbar und ratsam. Allerdings sei an dieser Stelle erwähnt, dass bei allen Vorteilen einer nationalen KI-Aufsicht die Gefahr eines innereuropäischen Wettbewerbs um die geringsten Anforderungen an die Anbieter und Betreiber von KI-Systemen, entstehen könnte. Folglich sollten sich eine supranationale Behörde ebenso wie ihre nationale Kontaktpunkte für eine kohärente Umsetzung der KI-Verordnung

einsetzen. Hier können Erfahrungsaustausch zwischen den Aufsichtsbehörden und die Erstellung von Mustern hilfreich sein.

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 Grundrechte Sinn, dabei hinsichtlich Echtzeit und retrograder Fernidentifikation zu unterscheiden, insbesondere da die Unterscheidung zwischen Echtzeit und retrograd unklar ist?

Im Rahmen der Antwort zur Frage 3 diskutiert.

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?*

Nach meinem aktuellen Kenntnisstand ist bereits ein Minimum Viable Product für ein nationales KI-Transparenzregister im Beratungszentrum für Künstliche Intelligenz unter Federführung des Bundesministeriums des Inneren und für Heimat erarbeitet worden. Überlegungen dazu finden sich auch in aktuellen Arbeiten der FITKO wieder. Folglich sollte der Prozess der Erarbeitung eines solches Registers nicht nur den Mitgliedern des Ausschusses für Digitales offengelegt werden, sondern ebenso für weitere wissenschaftliche und zivilgesellschaftliche Perspektiven geöffnet werden. Dennoch erscheint eine zentralisierte Erstellung des Musters grundsätzlich sinnvoll, um parallele Arbeiten an einem Muster zu verhindern.

Eine Ausweitung des Registers auf Landesbehörden und die kommunale Ebene erscheint vor dem Hintergrund eines konsequenten Verbraucher:innenschutzes notwendig. Dabei sollten dann entsprechend auch die Perspektiven der Länder und der Städte gehört werden. Insbesondere letztere Gruppe verfügt in der Regel über nur über wenige Finanzmittel und sollte von einem einheitlichen Register-Muster profitieren. Sinnvoll erscheint beispielsweise die Einbindung des Deutschen Städtetags in die weiteren Prozessschritte. Insgesamt sei ein verbesserter Austausch zwischen Bund, Ländern und Kommunen nicht für die Erarbeitung eines KI-Transparenzregisters, sondern insgesamt für die Umsetzung der KI-Verordnung empfehlenswert.

Zum Aufbau eines effektiven KI-Transparenzregisters gibt es bereits viele Ausführungen.¹⁶ In Kürze zusammengefasst, ist ein modulartiger Aufbau je nach Zielgruppe zu empfehlen. Vor dem Hintergrund der nationalen Umsetzung der KIVO liegt eine Kopplung an die Ergebnisse der Grundrechte-Folgenabschätzung und die dahinterliegenden Prozesse nahe. So sind es insbesondere die Betreiber der öffentlichen Hand, die die Grundrechte-Folgenabschätzung durchführen und gleichzeitig auch das KI-Transparenzregister verwalten sollten. Insbesondere CDOs oder entsprechende KI-Beauftragte sollten innerhalb der Behörden für die Eintragungen verantwortlich sein. Ebenso wie bei der Grundrechte-Folgenabschätzung wird es für den Betrieb des KI-Transparenzregisters notwendig sein, auch auf die Informationen der Anbieter der KI-Systeme zurückzugreifen. Folglich sollten künftige Ausschreibungen der öffentlichen Hand proaktiv auf die Informationspflichten zwischen Anbietern und Betreibern hinweisen.

Eine Ausweitung der Idee eines KI-Transparenzregisters über die Aufzählung der Hochrisiko-Systeme hinaus ist empfehlenswert, da selbst als a-priori nicht riskant eingestufte Systeme in ihrer Folge Implikationen für die Grundrechte von Menschen haben können. Dennoch erscheint es aus bürokratischen Gesichtspunkten sinnvoll eine schrittweise Ausweitung des Geltungsbereichs eines KI-Transparenzregisters vorzunehmen. Eine Klärung über die Verzahnung mit der in der KIVO vorgesehen europäischen Datenbank ist ebenfalls notwendig.

Kontakt

Lajla Fetic



@LinkedIn: <https://www.linkedin.com/in/lajlafetic/>

¹⁶ <https://algorithmwatch.org/de/reaktionen-transparenzregister/>