

Digitalgespräch Folge 71

Was sind und was leisten KI-Reallabore?

Mit Johannes Buchheim von der Philipps-Universität Marburg, 28. Oktober 2025

<https://zevedi.de/digitalgesprach-071-johannes-buchheim/>

[Der Vorspann mit Musik und Ausschnitten aus dem Gespräch beginnt.]

Marlene Görger [mg]: Herr Buchheim, Sie sind Jurist an der Philips-Universität Marburg. Wir möchten heute von Ihnen erfahren, was wir uns unter einem KI-Reallabor vorstellen können und welche Fragen sich diejenigen stellen müssen, die so etwas entwickeln sollen.

[Buchheim]: Es ist wahrscheinlich so ein bisschen gedacht, wir regulieren erst mal sehr viel und können dann möglicherweise im Laufe der Zeit zurückschrauben, aber es ist genauso gut in die andere Richtung denkbar. Man beobachtet ein System in einem solchen geschützten Raum mit enger Aufmerksamkeit der jeweiligen Regulierungsbehörde und die sieht, wir haben hier ja zusätzliche Probleme.

Petra Gehring [pgg]: Irgendwas mit Innovationsförderung muss es doch zu tun haben, sonst will gar kein Unternehmen da rein, oder?

[Buchheim]: Jeder, auch nur allgemeine Erkenntnisse, Mehrwert aus der Sandbox ist ein Wettbewerbsvorteil gegenüber anderen Unternehmen, die nicht in der Sandbox waren. Wenn die Öffentlichkeit sieht, hier wurde folgende, zum Beispiel Grenzüberwachungs-KI- Drohnensystem entwickelt. Wir wollen das nicht. Auch dafür brauche ich erst mal die Information, was wird denn da getestet. Ich glaube, das ist schon eine Chance. Also ich kann mir nicht vorstellen, dass das keine Effekte hat.

[Der Vorspann endet, das Gespräch beginnt.]

[mg]: Der 2. August 2026 – eine Deadline für die KI-Regulierung in Europa. Bis zu diesem Datum, so sieht es der AI-Act der EU vor, müssen alle Mitgliedstaaten sogenannte KI-Reallabore oder im englischen Text AI-Regulatory Sandboxes eingerichtet haben. Das englische Sandbox würden wir wohl mit Sandkasten übersetzen und beide Begriffe befeuern die Fantasie. Labor, das klingt nach planvollem Entwickeln und systematischem Testen. In diesem Fall soll das auch gleich real, also in der Wirklichkeit erfolgen, jedenfalls nicht im Spiel. Allerdings meint Sandbox, auch in der Informatik, eine abgeschirmte, sichere Umgebung, in der Fehler keine schlimmen Folgen haben. Worum geht das also im Fall der Reallabore, von denen der AI-Act spricht? Was klar zu sein scheint, KI soll einerseits wirksam reguliert und als äußerst riskante Technologie kontrolliert in den Verkehr gebracht werden. Andererseits will die EU aber auch Innovationen fördern und die Entwicklung neuer, möglicherweise sehr nützlicher Technologien nicht grundsätzlich behindern. Die Idee ist also nicht bloß, neue KI-Technologien so sicher wie möglich zu machen, wie auch immer das im Einzelfall gelingt, sondern es geht auch darum zu lernen, wie die Regulation selbst optimal funktioniert. Dass Testumgebungen in einem derart verschränkten Prozess hilfreich sein können, klingt plausibel. Dennoch, wie soll das in der konkreten Umsetzung aussehen? Was kann man sich unter den KI-Reallaboren vorstellen, die die EU von ihren Mitgliedsstaaten fordert? Und wer kümmert sich darum, dass sie am 2. August 26 zur

Verfügung stehen? Das ist unser Thema heute im Digitalgespräch. Mein Name ist Marlene Görger, ich bin Physikerin und Technikphilosophin und arbeite für das Zentrum Verantwortungsbewusste Digitalisierung.

[pgg]: Mein Name ist Petra Gehring. Ich bin Professorin für Philosophie an der Technischen Universität Darmstadt. Als Gast und Experten in unserer Videokonferenz dürfen wir heute Prof. Dr. Johannes Buchheim begrüßen. Er ist uns aus Marburg zugeschaltet. Herzlich willkommen im Digitalgespräch Herr Buchheim. Wir freuen uns sehr, dass Sie sich Zeit für uns genommen haben.

[Buchheim]: Vielen Dank für die Einladung. Ich freue mich, hier zu sein.

[mg]: Herr Buchheim, Sie sind Jurist an der Philips-Universität Marburg und im dort angesiedelten Institut für das Recht der Digitalisierung. Sie legen also in Forschung und Lehre ein Schwerpunkt auf rechtliche Aspekte der Digitalität und Sie arbeiten daneben auch zu Themen des Verwaltungs- und Verfassungsrechts sowie theoretischen Grundlagen des Rechts. Die Entstehung des AI-Acts haben Sie verfolgt und sich dazu als Experte auf EU-Ebene eingebracht. Zudem begleiten Sie ein Pilotprojekt des Bundes zur Einrichtung der von der EU eingeforderten KI-Realabore. Wir möchten heute von Ihnen erfahren, was wir uns unter einem KI-Real-Labor vorstellen können und welche Fragen sich diejenigen stellen müssen, die so etwas entwickeln sollen. Erklären Sie uns zum Einstieg doch bitte, was der AI-Act da genau von den EU-Mitgliedstaaten fordert.

[Buchheim]: Ja, vielen Dank. Ich kann es mal versuchen. Die Regelungen zu den KI-Reallaboren finden sich in Artikel 57 folgende der KI-Verordnung. Überschriften ist dieser ganze Abschnitt Maßnahmen zur Innovationsförderung, womit schon eine erste Idee verbunden ist, was sich der EU-Gesetzgeber davon verspricht andererseits auch Raum für erste Missverständnisse oder jedenfalls Auseinandersetzungen, um die Rolle dieser KI-Reallabore angelegt ist. Diese Idee der Innovationsförderung ist, denke ich, darauf zurückzuführen, dass die KI-Verordnung natürlich verschiedene, auch durchaus strenge regulatorische Anforderungen macht. Auch ein bisschen, wenn man so etwas flapsig sagen will, ins Blaue hinein, ohne noch wirklich zu wissen, was die KI-bezogenen Gefahren sind, und man kann die KI-Reallabore wahrscheinlich am besten verstehen als ein Versuch, diesen regulatorischen Schuss ins Blaue dann nachträglich im Laufe der Zeit über diese besonderen Testräume, die man damit einrichten möchte, sozusagen nachzujustieren, Wissen zu generieren, um dann im Laufe der Zeit zu einer immer zielgenaueren Regulierung zu gelangen. Gleichzeitig ist aber natürlich die Erwartung, die insbesondere auch für den Rechtsverkehr und für die Hersteller von KI-Technologie damit verbunden ist, oft eine andere, gerade wenn man das eben als Innovationsförderung vorstellt, dann denken die natürlich in erster Linie, ja, hier soll es darum gehen, dass ihre schönen KI-Technologie ertüchtigt werden kann und in der Stadt, in diesen geschützten Räumen irgendwie dabei hilft. Und das ist so ein gewisse... Grundspannung, die in den Vorschriften angelegt ist und die eben auch durch das Framing schon im Gesetzgebungsakt angelegt ist, auch angelegt ist, wenn man in den Artikel 57, glaube, Absatz 9, sind fünf Ziele genannt und weisen in diese zwei unterschiedlichen Richtungen. Und das ist wahrscheinlich sozusagen die große Frage und der große Deutungsstreit, der sich dann hier im Verlauf der praktischen Konkretisierung dessen was, solche KI-Reallabore. Sind und wie sie funktionieren, herausentwickeln wird.

[pgg]: Wenn wir jetzt mal an den Gesetzgeber denken, das ist eine spannende Vorstellung, der schafft eine Regulierung, auch eine straffe Regulierung und gleichzeitig baut er ins Gesetz ein, dass er vielleicht selbst nochmal nachsteuert oder das Ganze irgendwie im Einzelfall vielleicht irgendwie doch weicher gestaltet werden könnte, um dann quasi zu lernen, wie taste ich mich an den Gegenstand KI gut ran, in der Umsetzung von Regeln, warum macht ein Gesetzgeber das? Der Gegenstand K.I. Tatsächlich noch so ein bisschen in der Zukunft liegt, das haben wir eben angedeutet. Also so Schuss ins Blaue mäßig mal sehen, wie das funktioniert. Oder ist die Sorge, dass es zu straff ausgefallen ist, das Gesetz. Also ist die Idee am Anfang stramm regulieren und dann später einfach schrittweise lockern. Oder gibt es noch andere Gründe, warum macht man das? Normalerweise könnte man sich vorstellen, Recht soll sicher sein und sicher ist ja, wenn es nicht irgendwie reingedeutet werden kann, dass es auch anders sein könnte, als man in Gesetzestext findet.

[Buchheim]: Ja, also vielleicht erläutere ich nochmal ganz kurz den Globalkontext der KI-Verordnung, die eben im Wesentlichen verschiedene Risikoklassen für verschiedene KI-Systeme und KI-Verwendungen vorschreibt und in verschiedenen Anhängen zur KI-Verordnung werden dann bestimmte Arten von KI-Verwendung diesen Risikoklassen zugeordnet. Und es gibt dann eine Risikoklasse, die beschreibt eben schlechthin. Für unerträglich angesehenen Risiken, die sind in Artikel 5 KI-Verordnung geregelt, diesen konstant, da gibt es auch keine Anpassungsmöglichkeit. Also zum Beispiel subliminale Beeinflussungstechniken, die im öffentlichen Diskurs eingesetzt werden würden. Solche KI wäre davon unter anderem erfasst.

[pgg]: Also Propaganda und versteckte Werbung und so was.

[Buchheim]: Genau in diese Richtung geht das da bei dem Artikel 5. Dort kann man nichts anpassen, aber alle anderen Risikoklassifizierungen sind als anpassbar konzipiert. Da gibt es dann Konkretisierungsbefugnisse der Kommission in näher geregelten Verfahren, in denen man dann eben eine Umklassifizierung vornehmen kann im Laufe der Zeit, je nachdem, was man über die Funktionalität und die praktischen Risiken der jeweiligen KI-Systeme im Verlauf der Zeit feststellt. Also zum Beispiel ist denkbar, dass Gesichtserkennungssysteme im Moment noch ganz gradierende Fehlleistungen aufweisen. Zum Beispiel gibt es diesen Own-Race Bias bei Gesichtserkennung, dass man dann anhand kaukasischer Physiognomie trainierter Gesichtserkennungsmechanismus bei im weiteren Sinne kaukasischer aussehenden Physiognomie da eine treffsichere Zuordnung trifft, aber dann eben alle, die irgendwie etwas anders aussehen, dann eben fehlkategorisiert. Und das wäre so ein Risiko, das natürlich denkbar ist im Verlauf der Entwicklung durch Verbesserung der Technologie einfach in den Griff zu bekommen, sodass möglicherweise dann so ein Gesichtserkennungssystem nicht mehr dieselben gravierenden Fehlzuordnungsrisiken, die ja dann auch, wenn das zum Beispiel polizeilich verwendet wird, mit schweren ... Bei Eingriffsmaßnahmen einhergehen kann, wenn sich solche Probleme dann im Laufe der Zeit – man hofft ja generell auf eine Verbesserung dieser KI-Systeme – verändert, dann kann man dort natürlich die Regulierung etwas lockern, weil man eben beobachtet hat, dass hier doch bestimmte Risiken nicht in der Weise bestehen. Aber dasselbe kann natürlich in die andere Richtung auch passieren. Und das ist auch eine Funktion dieser KI-Reallabore oder jedenfalls eine mögliche Folgerung. Man beobachtet ein System in einem solchen geschützten Raum mit enger Aufmerksamkeit der jeweiligen Regulierungsbehörde und die sieht, wir haben hier ja zusätzliche Probleme. Vielleicht müssen wir darauf hinwirken, dass dieser Art von KI-System in Zukunft sogar in eine

strengere Risikokategorie eingeordnet wird. Und damit kommt natürlich dann da sozusagen keine Erleichterung bei raus, sondern eher eine Verschärfung des Regulierungswerks. Und diese Zwei-Wertigkeit, diese Möglichkeit, in beide Richtungen zu gehen, die, würde ich denken, ist in der Idee der KI-Reallabore, Regulierungsreallabore. Angelegt. Anders meine ich, kann man es nicht verstehen, aber das hat natürlich mit kurzfristig gedachter Innovationsförderung dann natürlich nichts zu tun, weil es effektiv erst mal dafür sorgt, dass bestimmte KI-Systeme dann zusätzliche Anforderungen konkret. Erfüllen müssen. Deswegen würde ich sagen, es ist wahrscheinlich von der gesetzgeberischen Hoffnung so ein bisschen gedacht, wir regulieren erst mal sehr viel und können dann möglicherweise im Laufe der Zeit zurückschrauben, aber es ist genauso gut in die andere Richtung denkbar. Und man hat auch in diesem Gesetzgebungsprozess, ich war bei einem Workshop im Europäischen Parlament dazu, gemerkt, dass sich die politischen Entscheidungsträger anderes im ersten Zugriff erhofft hatten. Die hatten das eben gedacht, ja, wir ertüchtigen da KI und haben diesen regulatorischen Lernmechanismus nicht wirklich verstanden. Die Kommission, die das Ganze konzipiert hat, hat das natürlich verstanden, aber die ist ja nicht sozusagen der politische Entscheidungsträger, der dann am Ende die Calls macht in die eine oder andere Richtung. Und den politischen Entscheidungsträgern, man merkt das in diesem Workshop, dass die dann auch verstanden, dass natürlich immer nur ein sehr kleiner Teil der KI-EntwicklerInnen überhaupt zu so einer Sandbox wieder zugelassen werden können. Man kann diese Infrastruktur, weil sie eine besondere behördliche Aufmerksamkeit erfordert, gar nicht in der Breite allen zur Verfügung stellen. Und auch das war so ein Punkt, den die noch gar nicht verstanden hatten. Die dachten, ah ja, okay, wir regulieren recht scharf, aber dann haben wir ja für alle so ein großartiges Reallabor. Diesen Zahn, musste man den Entscheidungsträgern in gewisser Weise ziehen. Ich glaube auch, dass der Groschen dann tatsächlich gefallen war. Jedenfalls lässt sich das an den Regelungen zu den Artikel 57 folgenden beobachten, weil man nämlich dann im Verlauf des Gesetzgebungsverfahrens noch eine Testmöglichkeit eingeführt hat ohne Reallabor. Da braucht es einen Plan. Also man muss einreichen bei einer Regulierungsbehörde, wie man sich diese Testung, zum Beispiel einer KI ertüchtigten Drohne, vorstellt. Und dann darf man die aber tatsächlich unter Realbedingungen, unter bestimmten Voraussetzungen testen, ohne dass da eine Behörde sozusagen näher draufguckt, mit denen das alles ausmacht. Und das ist sozusagen ein zweiter Mechanismus. Und der ist tatsächlich so ausgestaltet. Da soll es eine Genehmigungsfiktion geben. Also man bringt diesen Plan ein, wenn die Behörde nichts macht, dann kann man irgendwann loslegen nach ein paar Monaten mit dieser Testreihe, so wie sie beschrieben ist, in diesem Plan. Und damit nimmt man natürlich Druck raus aus diesen besonderen KI-Reallaboren im engeren Sinne, bei denen die Behörden dann eng dabei sind, weil man andere Testmöglichkeiten, Ertüchtigungsmöglichkeiten parallel dazu schafft, die dann andersrechtlich ausgestaltet sind, aber die auch das Interesse zumindest bedienen, erst mal testen zu können. Und nicht jeder Test muss dann eben behördlich beaufsichtigt werden. Meines Erachtens ist das eine sehr kluge Ergänzung, die da im Verlauf des Gesetzgebungsverfahrens reingekommen ist. Und dieses andere Mittel, das kann tatsächlich auch dann in die Breite wirken, während die KI-Reallabore werden, dadurch meines Erachtens dann stärker wieder in Richtung eines besonderen Testraums, der auf das regulatorische Lernen stärker blickt, dann wieder zugeschnitten, so wie es meines Erachtens ursprünglich auch der Gedanke der Kommission gewesen wäre.

[mg]: Da haben wir jetzt ganz viele Punkte, in denen wir vielleicht nochmal so zum Entpacken ansetzen könnten. Also was das Reallabor schon mal nicht sein soll, das hat

man jetzt ja deutlich rausgeholt, ist so eine Art TÜV für KI-Produkte. Alle müssen ihr neues Produkt da abgeben und dann kommt hinterher der Daumen hoch, der Daumen runter oder hier nochmal nachbessern. Jetzt hatten sie aber schon angedeutet, es gibt so viele Vorstellungen, was das... Die die Reallabor leisten soll, also es soll Innovationen fördern, es soll vielleicht auch im Entwicklungsprozess schon unterstützen, vielleicht Produkte auch schon gleich so zu entwickeln, dass sie die Zulassungen dann auch bekommen können, aber eben auch die Regulierung selbst noch mal testen dabei gleich. Ist denn klar, dass das alles im Reallabor erfolgt, oder wird die Aufsicht auch noch mal drangehängt, also dass bestimmte Schritte nur zum Beispiel im Reallabor erfolgen, also dass man das Reallabor zum Beispiel sehr technisch ausrichtet und dann der russische Anteil. Zu sagen, arbeitsteilig anderswo erfolgt oder so, da ist das schon so gedacht. Das ist eine geschlossene Organisation, wie auch immer man die dann aufgebaut hat und die erreicht dann dieses Ziel, das da vor Augen steht.

[pgg]: Gibt es irgendwo ein Gebäude, wo drauf steht KI Real Labor und da passiert alles unter einem Dach.

[Buchheim]: Ja, das ist auch eine schwierige Frage. Ich glaube, es gibt verschiedene Arten von KI-Reallaboren, wenn man sich die Vorschriften näher ansieht. Also generell ist es so, dass die echte, sagen, Erforschung und Entwicklung in die Nähe der Marktreife zu kommen, das soll noch nicht von den KI-Reallaboren geleistet werden. Also es wird immer noch echtes Technik-Sandboxing geben. Und das ist sozusagen ja ein Element des Entwicklungsprozesses, der typischerweise weit vor oder weiter vor der Marktreife kommt. Das wird ohnehin nicht von den KI-Reallaboren abgedeckt. So, wenn wir dann eine schon der nahen Möglichkeit nach, sagen, marktgängige KI haben, dann beginnen wir in den Bereich der KI-Reallabore zu kommen. Und da gibt es natürlich unterschiedliche KI-Anwendungen und je nachdem, also eine Drohne, die wird man nicht in einem geschlossenen Raum des KI-Reallabors unter Realbedingungen testen können, sondern da muss man wahrscheinlich, wenn das zur Grenzüberwachung, die drohen werden, sollen ja immer gleich schön für die Migrationssteuerung mitverwendet werden. Also das ist einer der Hauptanwendungsfelder, den sich auch die Politik davon verspricht. Unabhängig davon, was man davon hält, wenn man das in dieser Weise testen möchte unter Realbedingungen, da muss man ins Terrain, muss man gucken, wie fliegen die da rum, was erfassen die, können die effektiv einen Grenzverlauf irgendwie überblicken oder nicht. Diese Art von Testung, die auch im Reallabor, das ist explizit gesetzlich geregelt, möglich sein soll, zwingt eigentlich dazu, dass manche Reallabore nicht in einem geschlossenen Raum, in einem bestimmten Haus durchgeführt werden. Also das ist klar. Und dann gibt es andere. KI-Reallabore, die mit einer bestimmten datenschutzrechtlichen Privilegierung ablaufen sollen. Da sollen nämlich dann Datensätze, die man nach normalen Regeln eben aufwendig, müsste man jede einzelne Datenverarbeitung personenbezogener Daten, die darin stattfinden soll, sozusagen rechtfertigen können gegenüber dem jeweiligen Datensubjekt. Und von dieser kleinteiligen datenschutzrechtlichen Rechtfertigungspflicht sollen, die dann im Reallabor ein Stück weit enthoben werden. Weil das ein Grundproblem ist bei Big Data, man weiß noch nicht genau, was dabei rauskommt bei dem Datenverarbeitungsprozess. Deswegen sind diese datenschutzrechtlichen Rechtfertigungen nicht so leicht zu leisten. Und davon soll dann eben eine Art von KI-Reallabor entheben von dieser Schwierigkeit und in diesem KI-Reallabor. Und das ist dann letztlich eine Datenverarbeitungsumgebung. Da kann man sagen, das ist eine Rechenumgebung, ein bestimmter Ort stattfinden. Da haben dann auch die Datenschutzbeauftragten eine besondere Rolle. Und das ist sozusagen eine zweite Art

von KI-Reallabor. Und dann gibt es eine dritte Art, die letztlich ein rein ideelles Reallabor ist. Zum Beispiel eine KI-gestellte Anwendung, die beim An- und Verkauf auf Finanzmärkten irgendwie unterstützen soll, die natürlich gewisse systemische Risiken aufweisen kann und sowas würde man dann eben regulatorisch überwachen in enger Zusammenarbeit. Ja, was sind die möglichen systemischen Risiken, die dabei entstehen können und wie wäre darauf zu reagieren und würde das dann vielleicht ein paar Monate in dieser Form beobachten und dann daraus seine Schlüsse ziehen. Das wäre aber dann jetzt nicht ein konkreter Ort, an dem das Stattfinden und das wäre, jetzt auch eine besondere Datenverarbeitungs Umgebung, sondern da wäre es sozusagen die Geschehnisse auf einem Finanzmarkt oder einem Teil des Finanzmarktes, auf dem eben dieses Produkt, das KI-Gesteuerte, dann genutzt wird, die man dann in dieser besonderen Weise überwachen würde. Und dieses Spektrum der Reallabore. Macht es eben auch schwierig, diese Frage so klar zu beantworten. Wie sieht das aus? Ist das ein Haus oder eine Computerumgebung?

[pgg]: Sowohl, wenn da Recht mal außer Kraft gesetzt werden soll oder jedenfalls ein Stück weit gelockert zum Zweck des Testens oder um so ein Henne-Ei-Problem mit Daten zu lösen oder wie auch immer, als auch, wenn es eigentlich darum geht, vielleicht die Anwendung zu präzisieren. Also das, was das Recht will, sozusagen im konkreten Fall scharf zu stellen. In beiden Fällen stellt man sich vor, dass da Juristen eine große Rolle spielen. Also sitzen in diesen Reallaboren oder sind bei diesen Prozessen, die dann da durchgeführt werden, immer vor allem die Juristen, die steuernden Personen oder ist das doch eher technisch und am Ende gibt es eine dicke Dokumentation und die geht dann irgendwo zu Juristen zu entscheiden.

[Buchheim]: Ja, das ist eine sehr gute Frage. Wenn ich recht entsinne, gibt es keine Vorschriften dazu, wie die Personen, die an einem solchen Reallabor und an seiner Beaufsichtigung beteiligt sind, welche Qualifikationen, die mitbringen müssen. Also es ist klar, es sind jedenfalls behördliche Akteure dabei. In Deutschland soll zum Beispiel die Bundesnetzagentur da eine wichtige Rolle spielen bei der tatsächlichen Implementierung und bei Aufsicht der KI-Reallabore. Zu einem hohen Teil sind solche Referentenposten durch Juristinnen und Juristen besetzt. In Frankreich wird es ähnlich sein, da ist aber letztlich die Verwaltungsausbildung so generalistischer als weniger spezifisch juristisch im Deutschen. Das klassische Staatsexamen führt zu dem Ergebnis, dass da häufig Juristinnen und Juristen sitzen. Das ändert sich, hat sich aber auch in den letzten 30, 40 Jahren schon verschoben. Es gibt immer mehr Ökonominen. Die in Ministerien arbeiten und natürlich auch andere Qualifikationshintergründe. Aber ich denke, dass dadurch gerade in Deutschland implementierten Reallaboren der juristische Blick darauf besonders prominent sein wird. Und da natürlich auch die Frage, ob das dann gerade in Deutschland gut funktionieren kann, weil Juristinnen und Juristen natürlich ein bestimmtes typisches Mindset haben. Da geht es eben in erster Linie darum, dass alles eben hinreichend sicher rechtmäßig ist, was man da tut und man hat einfach keine relativ risiko-averse während, wenn jemand, der nicht in erster Linie normativ rechtlich darauf blickt, sondern wir müssen doch jetzt irgendwie dieses Ding zum Laufen bekommen und müssten irgendwelche Ergebnisse produzieren, die gehen da möglicherweise mit einer anderen Hemdsärmeligkeit ran, die vielleicht Voraussetzung dafür ist, dass diese KI-Reallabore überhaupt sinnvoll zum Laufen kommen und nicht nur sozusagen eine Art Schattenboxen sind, in der man sich dann irgendwelche Excel-Tabellen rumschickt und irgendwelche komplexen Ablaufpläne und am Ende hat das aber mit dem, wie dann tatsächlich so ein Testprozess funktioniert, relativ wenig zu tun. Also zum Beispiel die Datenschutzbeauftragten, die haben ja schon

seit Jahrzehnten Erfahrungen an dieser Schnittstelle von rechtlich normativer technischer Regulierung, weil das ganze Datenschutzrecht letztlich aus einer technologischen Entwicklung heraus entstanden ist und diese Akteure sind strukturell technikaffin und technikoffen und bereit, darüber nachzudenken. Ich glaube, das ist jedenfalls sicherlich ein wichtiger Akteur, der muss da rein in diese Regulierungs-Sandboxen. Die Bundesnetzagentur eben auch, die ist ja beim Wirtschaftsministerium angedockt, hat eine starke ökonomische Prägung, auch dadurch nicht so juristendominiert wie andere Ministerien. Und ich glaube auch, dass die Sandboxen eben auch eine sinnvolle Funktion haben, um bei den KI-Entwicklerinnen einfach ein Verständnis frühzeitig zu wecken. Es gibt da diese regulatorischen Herausforderungen, über die müssen wir nachdenken. Die sind nicht in Stein gemeißelt. Es gibt oft auf Seiten der Gesellschaft unterkomplexe Vorstellungen von Recht. Ja, das sind wir klar. Was ist denn jetzt meine Checkliste? Und dann muss ich sie halt erfüllen, dass das so nicht ist. Gerade im Bereich KI, das muss natürlich den Leuten auch irgendwie vermittelt und sichtbar werden. Und KI-Reallabor ist eine Möglichkeit, dieses Verständnis zu wecken. Und auch dadurch entsteht ja eine Form von Interdisziplinarität, weil dann auf einmal Diskurse und KI-Entwickler, die natürlich eher ein technisches Mindset haben, schon immer mitdenken, es gibt hier normative Anforderungen und wie sind die denn ausgestaltet? Wo sind da die entscheidenden Fragen? Wie kann ich das schon technisch implementieren? Ich glaube, das ist schon eine Chance und hat sozusagen eine performative Wirkung schon für sich genommen, dieses Instrument, die Interdisziplinarität. Einfach weil sie diese Perspektiven der Regulierungsbehörde und des Regulierten, der erstmal nur über die Technik nachdenkt, zwangsläufig zusammenbringt. Also ich kann mir nicht vorstellen, dass das keine Effekte hat.

[pgg]: Der AI-Act fordert ja mindestens ein KI-Reallabor in jedem Mitgliedsstaat der EU. In Deutschland denkt man da an den Bund, dass nur ein einziges Reallabor geben wird, ist unwahrscheinlich. Das liegt schon in der Materie, in der ganzen komplexen Aufgabenstellung, das haben wir schon diskutiert. Wie wird das denn bei uns im föderalen Zusammenhang aussehen? Wird das eher so eine Bundesangelegenheit sein, so eine Landschaft von KI-Reallaboren zu etablieren oder haben die Länder da auch eine wichtige Rolle? Sagen wir mal Landschaft, wie wird die vielleicht werden?

[Buchheim]: Ja, die Marktüberwachungsbehörde, die nach der KI-Verordnung die Hauptregulierungslast der KI-Verordnung erfüllen muss, die ist im deutschen Kontext auf jeden Fall die Bundesnetzagentur, also auf Bundesebene findet das statt und die kann jedenfalls auch und im Moment läuft das darauf hinaus. Dann gleichzeitig diese federführende Stelle für jedenfalls ein KI-Reallabor sein, also auch auf Bundesebene. Allerdings ist die datenschutzrechtliche Regulierung eben im deutschen Kontext auf der Ebene der Länder, sodass tatsächlich ein Unternehmen, das aus Hamburg kommt und in einer solchen Regulierungs-Sandbox eine Testreihe, die mit personenbezogenen Datenverarbeitungen verbunden ist, durchführen möchte, die ist auch in dieser Konstellation von der hamburgischen Datenschutzbeauftragten dann zu überwachen. Die muss in irgendeiner Form da eingebunden werden, in dieses Reallabor. Und die Bundesdatenschutzbeauftragte, die hat im deutschen Kontext nur eine Regulierungsaufgabe für Bundesbehörde und eine Koordinationsaufgabe, aber sie hat keine originäre eigene Regulierungszuständigkeit datenschutzrechtlicher Art für Wirtschaftsakteure, die natürlich ja immer diejenigen sind, die in letzter Konsequenz den Reallaborversuch verantworten müssen und die Datenverarbeitung, die dabei stattfindet, verantworten müssen. Das heißt, ich vermute, wir werden erst mal ein Reallabor haben von der Bundesnetzagentur federführend, die dann

außenverantwortlich diese Infrastruktur bereithält. Und da müssen aber eben auf jeden Fall verschiedene Datenschutzbeauftragte dann einbezogen werden, die tatsächlich dann die materiellen Letztentscheidungsrechte haben über personenbezogene Datenverarbeitungen. Die müssen wahrscheinlich nach außen dann wieder von der Bundesnetzagentur getroffen werden. Aber so ist das materielle Entscheidungsrecht nicht wohl bei den jeweiligen Datenschutzbeauftragten. Und das sind eben unterschiedliche. Und da ist natürlich naheliegend, dass es dann Koordinationsprobleme auch mal geben wird, weil die Datenschutzbeauftragten eben unterschiedlich strenge Policies, unterschiedliche Vorstellungen haben können. Es gibt eine deutsche Datenschutzkonferenz, an der dann auch die Bundesdatenschutzbeauftragte beteiligt ist. Also es gibt diverse Koordinationsmechanismen, die darauf gehen, dass man so eine Zersplitterung, die allzu groß wird, dann wieder in den Griff bekommt. Und ich würde sagen, das gelingt der datenschutzrechtlichen Regulierung eigentlich auch relativ gut. Aber es ist natürlich eine zusätzliche Herausforderung, die in allen föderalen Mitgliedstaaten der EU besteht, weil man es eben auf jeden Fall mit dem Datenschutzrecht irgendwie übereinbringen muss und den datenschutzrechtlichen Aufsichtszuständigkeiten. Und das ist wahrscheinlich so ein zentraler Kritikpunkte gegenüber der KI-Verordnung, dass sie natürlich hochrelevant für personenbezogene Datenverarbeitungsprozesse ist und deren Aufsicht und dann eben in Anwendungsartikeln sagt, das Datenschutzrecht bleibt unberührt, weil man damit natürlich weiter delegiert die Probleme an die Praxis, die dann irgendwie Rechtsakte miteinander übereinbringen muss, die fingieren, dass sie einander nicht betreffen, aber es natürlich trotzdem tun.

[mg]: Das heißt, die Realabore zeigen dann auch die Bedeutung von Verwaltungsakten dann für die Wirksamkeit unserer Gesetze. Sie hatten früh am Anfang schon mal erwähnt, dass gar nicht alle KI-Entwickler geeignet sind, auch an so einem KI-Reallabor getestet zu werden, wenn ich das richtig verstanden habe. Wir hatten geklärt, es gibt jetzt nicht die Pflicht, es im Reallabor zu machen. Es gibt auch andere Möglichkeiten. Aber sie hatten auch gesagt, man kann die Reallabor gar nicht allen zur Verfügung stellen. Was ist denn der Hintergrund dieser Feststellung?

[Buchheim]: Da meinte ich jetzt eher den Kapazitätsgrenzen, also die KI-Reallabore sind auch rechtlich darauf verpflichtet, einen gleichheitsgerechten Zugang zu gewähren. Im Text geht es um Zugangsvoraussetzungen und Auswahlkriterien. Und Auswahlkriterien impliziert eben, dass es da eine Auswahl geben muss, dass also nicht alle in den Genuss dieser besonderen Testinfrastruktur gelangen können. Das hat mit begrenzten behördlichen Ressourcen zu tun. In KI-Reallabor, wo unterschiedlich die Modelle sind, dazu, ist immer mit hoher behördlicher Aufmerksamkeit verbunden. Da werden Pläne gemacht, gemeinsam ausgearbeitet zwischen Referentinnen einer Behörde und KI-Entwicklerinnen, die eine solche KI regulatorisch testen und ertüchtigen möchten. Solche Verträge müssen ausgehandelt werden, Pläne müssen gemacht werden, müssen natürlich innerhalb einer Behörde ordentlich beaufsichtigt werden. Und all das bindet personelle Ressourcen und Zeit und Geld. Dass diese Ressourcen begrenzt sind, wäre auch völlig unangemessen, wenn man jetzt für eine Sache, nämlich KI-Erstellung und Ertüchtigung, sagen, sämtliche Ressourcengrenzen über Bord werfen würde. Das wäre normativ völlig unsinnig in Polizei, Justiz, Sozialverwaltung, überall verweist man auf, wir haben nur begrenzt Geld und dann soll bei KI-Ertüchtigung auf einmal unendliche Mittel da hineingesteckt werden. Das kann nicht sein. Deswegen wird es immer eine begrenzte behördliche Aufsichtskapazität geben und die muss dann eben verteilt werden nach irgendwelchen Kriterien. Und das ist natürlich auch dem

europäischen Gesetzgeber klar. Der hat so hineingeschrieben, dass es eine hinreichende finanzielle Ausstattung geben muss und dass auch die KI-Reallaborkapazitäten der Nachfrage entsprechend sich fortentwickeln müssen. Aber darin impliziert ist eben immer, dass wir die Auswahl treffen müssen, dass die Ressourcen begrenzt sind. Ich denke, realistischerweise wird vielleicht dann irgendwann so 1 bis 5 Prozent der KI-Entwicklungsvorhaben maximal in irgendwelchen KI-Reallaboren beaufsichtigt werden können. Das ist ein ganzer Wirtschaftszweig. Da können die staatlichen Behörden, die in dieser Breite an die Hand nehmen und denen irgendwie helfen, ihre KI-Systeme marktüchtig zu machen und dazu gehört eben auch Regulierungsanforderungen zu erfüllen.

[pgg]: Da kann man sich natürlich zwei ganz unterschiedliche, extremen Situationen vorstellen. Zum einen die Unternehmen drängeln da rein und rangeln, wer darf jetzt ins KI-Reallabor, wer darf sozusagen das glückliche Testkaninchen sein und dann vielleicht auch so ein bisschen mit beeinflussen, wie die Gesetzgebung umgeht mit einer konkreten, typischen Lösung. Oder das andere Szenario aufwendiger Prozessbehörden und so weiter. Und kein Unternehmen möchte da rein, und wen es dann trifft, der sagt, "oh Gott, ich muss jetzt ja noch ins Reallabor". Also zwei unterschiedliche Ideen dann nachher vom Funktionieren dieses Mechanismus. Irgendwas mit Innovationsförderung muss es doch zu tun haben, sonst will gar kein Unternehmen da rein, oder?

[Buchheim]: Genau, also sicherlich geht es um Innovationsförderung, weil die dann in so einer Sandbox sind, jedenfalls besondere behördliche Aufmerksamkeit bekommen. Man hilft ihnen dabei, eben einen rechtlich tragfähigen Testplan zu entwickeln. Man macht sie darauf aufmerksam, muss sie auch rechtlich darauf aufmerksam machen, welche regulatorischen Risiken man im Moment sieht. Es gibt auch eine, und das ist, würde ich sagen, die einzige harte rechtliche Begünstigung, die diejenigen, die in so einer Sandbox getestet haben. Das ist nämlich, dass sie, wenn sie sich an den Testplan halten und dann dabei irgendwas schief läuft, irgendein Risiko sich materialisiert, das man nicht hat kommen sehen, aber man hat sich sozusagen an diesen Testplan gehalten, dann können einem dafür keine behördlichen Bußgelder aufgebremst werden. Und diese Bußgelder sind im europäischen Regulierungskontext in den letzten Jahren einfach höher geworden. Die können bis in die Prozentbereich des Jahresumsatzes gehen, also wesentlich höher als so in der deutschen Bußgeldpraxis, in der klassischen üblich war, sodass da wirklich ein bisschen Drohpotenzial hintersteckt. Und dieses Drohpotenzial muss man dann eben nicht befürchten. Während zum Beispiel private Schadensersatzklagen, also die Grenzüberwachungsdrohne, die KI-Gesteuerte, die macht irgendwas falsch und es kommt jemand zu Schaden, da sind Schadensersatzansprüche zum Beispiel von Privatrechtssubjekten, die sind dadurch nicht irgendwie eingehegt. Und wenn man eben an die KI-Verordnung, in diese Regelungen näher blickt, dann sieht man, dass man schon ziemlich zurückhaltend war. Hier echte rechtliche Vergünstigungen für die Reallabor-Teilnehmerinnen zu schaffen, jenseits der besonderen behördlichen Aufmerksamkeit. Und das ist die zentrale Frage, reicht das, um hier einen Anreiz zu schaffen, KI-Reallabore aktiv zu nutzen. Und wenn das eben niemand tut, dann funktioniert das alles nicht, weder Innovationsförderung noch regulatorisches Lernen. Man braucht die Akteure da. Und eine Frage wird sein, wie sehr. Schießt man sich darauf ein, auf regulatorischer Seite, dass man seine Start-ups fördern möchte. Da gibt es eben eine Vorschrift, dass die KMU, die kleinen und mittelständischen Unternehmen, kostenlos daran teilnehmen dürfen, bis auf bei besonders erhöhten Stellen vor, irgendwie eine KI-Testung kann nur im Weltraum durchgeführt werden. Das wäre so der Fall, dann müsste auch das KMU diese

Sonderkosten mittragen. Aber sonst sollte es dann grundsätzlich kostenfrei sein. Auch daraus würde ich wiederum sagen, folgt eigentlich, dass die KI-Reallabore aber nicht spezifisch auf kleine und mittelständische Unternehmen zugeschnitten sein sollen, weil ja klar ist, dass der regulatorische Nutzen und die Breite der Beobachtungsfläche, die die Beobachtungen, die man machen kann, in einem Reallabore sind natürlich viel größer, bei einem schon professionelleren, breitenwirksameren, was weiß ich, wenn dann die deutsche Telekom, also irgendein großes Unternehmen, ein KI-System nutzt, auch schon in der Breite nutzen möchte und da dann regulatorische Risiken testen will, ist das ein viel besserer Partner in jeder Hinsicht. Die wissen auch rechtlich mehr, die sind professioneller und sind deswegen auch regulatorisch natürlich unendlich viel nützlicher als irgendein kleines Startup mit fünf Mitarbeitenden, die so gerade gehört haben, dass es überhaupt so was wie ein KI-Verordnung gibt. Und das gibt es ja auch und ist ja auch völlig legitim, aber wenn jetzt die Regulierung oder die Umsetzung des Ganzen in die Richtung geht, dass man eben das nur als Start-up-Förderung begreift, dann ist natürlich diese Möglichkeit regulatorischer Erkenntnisgewinne sehr gering. Und gleichzeitig ist aber natürlich auch den großen Unternehmen muss man vielleicht mehr bieten, denn die haben sowieso eine Rechtsabteilung und die haben sowieso, können auch Anwälte bezahlen, die sie dann beraten, was sind da die rechtlichen Risiken. Das heißt, die haben von der besonderen behördlichen Aufmerksamkeit vielleicht weniger als so ein Start-up, und dann ist eben die Frage, welche Restvorteile haben dann eben die eigentlich besonders interessanten Sandbox-Entwickler?, Und da hat man eben jetzt, wenn man zum Beispiel mit den Regulierungs-Sandboxen im britischen Finanzmarktrecht, das ist sozusagen eines der Pilotbeispiele, was man immer nennt, im Bereich der Regulierungs-Sandboxen, was die im Bereich der Finanzmarktregulierung gemacht haben. Und da gab es eben *echte Letters of Non-Enforcement*, dass man bestimmte Teile des Regulierungsprogramms dann den betreffenden Akteuren versprach, nicht gegenüber ihnen durchzusetzen. Nicht nur nicht bußgeldrechtlich, sondern gar nicht. Und dass man sozusagen echte Dispense erteilt, hat von ganzen Teilen einer Regulierung. Das hat man in der KI-Verordnung gerade nicht gemacht. Sicherlich auch, weil sich dafür dann eben keine Mehrheiten gefunden haben. Man will gerade KI effektiv regulieren, da will man jetzt nicht gleich wieder mit Distanzen fröhlich die verteilen gehen. Aber das ist natürlich die Frage, kriegt man damit die interessanten Player hinreichend angelockt? Und das ist, ja, glaube ich, eine große Frage, die dann die Praxis erst zeigen wird. Ich vermute eher das Kapazitätsproblem in dem Sinne, dass die KI-Entwickler in den die Türen einrennen werden, das wird sich erst mal nicht stellen, glaube ich, bis dann eine gewisse Erfahrung erwachsen ist und man gesehen hat, dass das Ganze funktioniert. Also ich glaube, in den nächsten vier bis fünf Jahren wird man nicht in das Problem kommen, besonders harte Auswahlentscheidungen darüber zu treffen, wer denn jetzt da mitmachen darf.

[mg]: Jetzt müssen die Reallabore ja nicht in vier bis fünf Jahren da sein, sondern es ist relativ wenig Zeit. Ich habe am Anfang schon erwähnt, der 2. August ist so eine Deadline. Was genau muss denn dann stehen? Wann hat man diese Anforderung erfüllt, als jetzt z.B. Deutschland das Reallabore entwickelt?

[Buchheim]: Also letztlich braucht es dann eine Verfahrensinfrastruktur in dem Sinne, ich kann einen Antrag stellen, ich weiß an wen ich den stellen kann. Da gibt es auch für die datenverarbeitungsbezogenen KI-Projekte vielleicht eine gewisse Dateninfrastruktur, Verarbeitungsinfrastruktur, die dann eben für so eine Sandbox-Testung zur Verfügung gestellt würden. Ich denke, sowas müsste man dann eben gegenüber der EU-Kommission oder diesem KI-Gremium melden, was es da gibt. Ob

das dann schon läuft und irgendjemandem was bringt, da ist diese Frist, würde ich sagen, völlig unrealistisch kurz. Im Sinne einer Infrastruktur und eines Erfahrungsschatzes, der schon irgendwie die Ziele eines solchen KI-Reallabors umsetzen kann, das kann ich mir nicht vorstellen, dass das ein einziger Mitgliedsstaat innerhalb der Frist schafft. Ich meine, es ist ja auch oft so, dass man eben bestimmte Dokumentation einreichen muss und die konstituiert dann in gewisser Weise das Reallabor und natürlich dabei kann es nicht stehen bleiben und da wird sicherlich auch die Kommission dann eben irgendwann sagen so ihr habt doch hier diese Pflicht ein echt praktikables Reallabor herzustellen und da werden die auch irgendwann drauf hinwirken aber ich glaube die sind auch hinreichend realistisch dass sie wissen dass sie da einfach ein völlig neues, gedankliches Ding, eine Abstraktion erst mal gesetzlich da abverlangt haben, die bestimmte Dinge schaffen muss, aber dass sich all das ja erst entwickeln muss. Und es muss ja auch noch von der Kommission ein Rechtsakt geben zur Durchführung dieser Reallabore. Wie ist da auszuwählen? Was sind die Zulassungsvoraussetzungen? Den gibt es noch gar nicht. Der ist noch nicht erlassen worden. Der ist zentrale Orientierung dann und Konkretisierung dessen, wie so ein KI-Reallabor aussehen soll. Und das wiederum kann man natürlich dann nicht in drei Monaten wieder umsetzen in der Praxis. Also ich denke, die Umsetzungsfrist formuliert einen Anspruch, die als praktische Umsetzung nicht realistisch ist. Alle Beteiligten wissen das. Es sind auch teilweise auf Seiten der Kommission sogar noch eben Zwischenschritte erforderlich, rechtlich. Das sind normale Startschwierigkeiten, gerade bei so eine neue, erstens gänzlich neue Regulierung wie der KI-Verordnung und dann aber auch einem ganz neuen regulatorischen Instrument wie den KI-Reallaboren. Man braucht auf jeden Fall nachweisbare Anstrengungen in die Richtung, dass man das irgendwie versucht. Auf deutscher Ebene hat man damit angefangen. In anderen Mitgliedstaaten gibt es auch schon Versuche, gab auch schon gewisse Pilotprojekte. Aber sowas braucht Zeit. Aber das ist auch normal und ich glaube auch allen beteiligten Akteuren dann klar.

[pgg]: Wie sieht denn das so aus rechtswissenschaftlicher Sicht aus? Ist das jetzt eine spannende Neuerung und ist man neugierig, wie das funktioniert? Oder ist das einfach was sehr Aufwendiges, ein zusätzlicher Apparat, der jetzt halt durch diese komplexe Technologie nötig wird? Und dann wird es halt zähneknirschend irgendwie schrittweise auch umgesetzt.

[Buchheim]: Ich glaube, das ist juristisch sehr interessant, dass es auch ein zunehmendes Interesse in der Breite, auch bei anderen, nicht jetzt besonders technikaffinen Akteuren für dieses Instrument gibt. Letztlich ist es eine besondere Form von Verwaltungsverfahrenrecht, dass man bestimmte Abweichungsräume schafft, dass man Möglichkeiten schafft, eben regulatorische Erfahrungen zu sammeln und es gibt diese Idee experimenteller Gesetzgebung und experimenteller Regulierung, die gibt es schon länger. Das neue jetzt der KI-Regulierungssandbox ist, also es geht nicht nur der KI-Sandbox um regulatorisches Lernen, sondern eben regulatorisches Lernen und gleichzeitig der Gegenstand, der reguliert werden soll, sondern natürlich eben auch ertüchtigt werden, und diese Wechselbezüglichkeit, die ist glaube ich das Neue und die ist eben das Interessante eigentlich an den KI-Reallaboren. Generell ein Erprobungsgesetz des Bundes ist in Arbeit, in dem man eben das als Instrument nicht nur für KI-Regulierung, sondern generell für Entwicklung und eben Regulierung einsetzen möchte. Man versucht sich also da an einer rechtlichen Formalisierung und Abstrahierung und möglicherweise wird das dann irgendwann Regelungen geben, die spezifisch solche Erprobungsmöglichkeiten einrichten.

[pgg]: Reallabor ist ja auch ein plakativer Begriff oder Sandbox oder so, das können sich Bürgerinnen und Bürger gut vorstellen, Unternehmen wahrscheinlich sowieso. Also was der Witz der Sache ist, welche Rolle spielt, überhaupt die Öffentlichkeit dessen, was da gemacht wird? Also gerade, wenn man sagt, es gibt nicht so beliebig viele Einzelfälle, die das volle Programm von so einem Reallabor dann irgendwie bekommen, dann wäre ja wichtig, dass die anderen lernen können, dass man das als Beispiel nimmt und das auch voll transparent ist, was in dem Reallabor im Einzelnen passiert ist, verhandelt wurde, was das Ergebnis ist. Sowohl auf der Seite des Gesetzgebers oder der Verwaltung, die lernt, oder auf der anderen Seite dann eben auch, was hat das Unternehmen mitgenommen, was ist dabei jetzt im Detail rausgekommen, wo sind die Grenzen der Vorschrift. Ist das mitgedacht, dass da so ein transparentes Vorgehen aufgesetzt wird, dass alle sich da informieren können, das als Beispiel funktionieren kann, vielleicht sogar öffentliche Diskussionen darüber geführt werden, was jetzt gerade spektakulär in einem bestimmten Reallabor Thema ist.

[Buchheim]: Ja, also das ist tatsächlich mitgedacht und findet sich auch an zahlreichen Absätzen dieser Vorschriftenartikel 57 folgend wieder. Man kann das als ein Informationssystem verstehen, in dem KI-Reallabor wird eben Wissen produziert über Abschlussberichte, über konkrete Beobachtungen. Und da gibt es sozusagen mehrstufige Informationspflichten. Also der Abschlussbericht muss eben vom Reallabor selbst oder der Reallabor führenden Stelle erstellt werden. Der geht dann an die Teilnehmer des Reallabors. Die können mit diesem Abschlussbericht zum Beispiel auch zur Aufsichtsbehörde in einem anderen Mitgliedsstaat und sagen, hier, ich habe das ertastet, das dabei rausgekommen. Also ich habe hier meine Due Diligence erledigt. Auch das ist eine Form der Wissensverbreitung. Also es wird tatsächlich eine Dokumentation geben. Die dann diese Wirtschaftsakteure nutzen können an verschiedenen Stellen. Und dann wird aber dieser Reallaborbericht, der muss eben in verschiedenen Stufen an das KI-Gremium der Kommission und die Mitgliedsstaaten müssen mit der Kommission berichten. Die Kommission muss auch der Öffentlichkeit berichten. Diese Berichte sollen auch dann anderen Akteuren in der KI-Kontext zur Verfügung gestellt werden können. Allerdings gibt es eben verschiedene Reservationen in den Regelungen. Die sowas wie Geschäftsgeheimnisse der Beteiligten betreffen. Und die Beteiligten haben natürlich auch unabhängig von Geschäftsgeheimnissen von diesem aktiven Informationssystem, das dann bis zur Öffentlichkeit reicht. Daran haben sie strukturell kein Interesse, weil jeder auch nur allgemeine Erkenntnismehrwert aus der Sandbox einen Wettbewerbsvorteil ist gegenüber anderen Unternehmen, die nicht in der Sandbox waren. Das wird, glaube ich, interessant sein zu beobachten, wie diese Informationspflichten, wie dicht wird da berichtet, wie dicht wird wem berichtet, welche Berichte werden abgelegt und hinterlegt und ich habe es jedenfalls bei meiner Kommentierung der Vorschriften als meine Aufgabe angesehen sein, darauf hinzuweisen, dass wir müssen sagen, überall maximale Öffentlichkeit und maximale. Jedenfalls die Möglichkeit der Kenntnisaufnahme anderer schaffen, ob die davon Gebrauch machen oder nicht, ist dann eine andere Frage. Damit das als regulatorisches System, was dann bis zur Öffentlichkeit reicht, weil natürlich auch, wenn die Öffentlichkeit sieht, hier wurde folgende, zum Beispiel Grenzüberwachungs-KI-Drohnen entwickelt. Wir wollen das nicht, dass es das gibt, kann ja die europäische Öffentlichkeit sagen. Auch dafür brauche ich erst mal die Information, was wird denn da getestet. Und relativ konkret, was, wie soll das eingesetzt werden, nicht irgendwelche Allgemeinheiten, da wurden so und so viele KI-Systeme im Bereich Sicherheit, so und so viele im Bereich Gesundheit. Typischerweise sind dann so öffentliche Berichte, haben dann solche

Informationen. Aber ja, vielleicht ist es auch ein sinnvoller Kontrollmechanismus, was man sagt. Nein, zwar wird in dieser Weise allgemein berichtet, aber wer will, kann das dann auch noch vertiefen, indem man eben guckt, ja, wo sind denn die Reallaborberichte, was ist denn das technische System? Und meine Vermutung ist, dass da wahrscheinlich eher die Unternehmen versuchen werden, informatorisch zu mauern. Teilweise haben sie auch formelle Blockaderechte. Sie müssen zustimmen in einer Veröffentlichung. Ich würde sagen, das sind vielleicht formelle Blockade-Positionen. Aber man könnte zum Beispiel in einen KI-Reallabor-Vertrag oder in sozusagen die Startdokumentation sagen, sie dürfen die nur ausnutzen, eben zur Sicherung bestimmter Geschäftsgeheimnisse, aber nicht einfach nur zur schlichten Absicherung ihrer informatorischen Wettbewerbsvorteile. Ich kenne jetzt noch nicht die Kommentierungslage bei anderen. Ich vermute, dass da nicht alle ähnlich sensibel sind hinsichtlich dieses Informationsproblems, sondern es andere gibt, die dann eher denken, okay, wir müssen hier unsere Wettbewerbsvorteile sichern. Und das ist doch auch legitim. Damit geht auch möglicherweise wieder ein Teil des Anreizes verloren für die Akteure. Also wir sehen, wir haben ein sehr komplexes System, in dem die Voraussetzungen dafür, dass das Ganze überhaupt das bringt, was es bringen soll, wiederum es schwieriger machen, die Voraussetzungen zu schaffen, dass das System überhaupt ins Laufen kommt, weil dann die Anreize schmelzen. Ja, deswegen ist es wirklich ein sehr spannendes Realexperiment, wie diese Regelungen, ob sie in eine sinnvolle Weise zu laufen kommen wird. Ich würde sagen, in der Handhabung müsste man eben informatorisch sehr offen das praktizieren und nur dann hat es eben eine sinnvolle Funktion auch als Lernen der Öffentlichkeit über KI-Risiken. Weil das ist, glaube ich, unerlässlich. Es muss die Öffentlichkeit eben auch. Irgendwie ertüchtigt werden, nicht jeder über jedes KI-System ist sicherlich nicht sprechfähig, aber die Öffentlichkeit als Ganze soll daran teilhaben, Grenzen zu ziehen, zu sagen, so möchten wir KI einsetzen und so nicht. Und wir dürfen das nicht quasi in eine reine technokratische Regulierung sich entwickeln lassen. Und sowas erreicht man durch Informationspflichten und Informationsmöglichkeiten der Öffentlichkeit. Aber es ist natürlich ein hohes Risiko. Sie haben auch gefragt, wer ist das dann, der solche KI-Reallabore betreibt? Ist das dann technische Expertise? Es ist insgesamt ein technokratischer Regulierungsansatz. Das muss man wohl schon sagen, aber ich glaube, man muss eben versuchen, ihn auch als Ermöglichung, sagen, informierterer öffentlicher KI-Regulierung einzusetzen, weil nur das meines Erachtens dann auch auf Dauer demokratisch legitim ist, es ist eben nicht einfach nur eine technische Frage, welche KI-Risiken bestehen und ob sie untragbar sind, sondern es ist eben auch eine normative Frage und die steht eben der Öffentlichkeit zu, zu entscheiden.

[pgg]: Wäre dann aber jedenfalls noch mal eine ganz andere Form von Sandkasten, die diskutierende Öffentlichkeit rund um den Einsatz von KI oder KI-Produkten, Ausgestaltung von KI-Produkten. Wenn wir jetzt an so ein Beispiel wie die Diskussion über die Software Palantir im Polizeibereich denken, dann sehen wir, dass Öffentlichkeiten auch Interesse haben, wenn es griffig dargestellt wird, was dann aber auch heißt, das muss genau beschrieben sein, um was es da geht.

[Buchheim]: Und ich glaube, das muss irgendwie sichtbar werden, ob das so interpretiert wird, das wird sich erst zeigen.

[mg]: Und damit ist dieses Digitalgespräch zu Ende und wir bedanken uns bei Johannes Buchheim von der Philips Universität Marburg für diese spannenden Einblicke und die interessante Diskussion. Viele Grüße und wie immer auch vielen Dank an Sie, liebe

Zuhörerinnen und Zuhörer, für das Interesse und die Aufmerksamkeit. Wenn Sie mögen, hören wir uns in drei Wochen wieder zur nächsten Folge des Digitalgesprächs, einem Podcast von ZEVEDI, dem Zentrum für verantwortungsbewusste Digitalisierung.

[Der Abspann mit Musik und Ausschnitten aus dem Gespräch endet.]



This work is licensed under CC BY-NC-ND 4.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by-nc-nd/4.0/>