22.01.2026

Transkript

„KI-Regulierung und deutsche Umsetzung des AI Act"

Expertinnen und Experten auf dem Podium

- **Prof. Dr. Patrick Glauner**
  Professor für Künstliche Intelligenz, Technische Hochschule Deggendorf
- **Prof. Dr. Philipp Hacker**
  Professor für Recht und Ethik der digitalen Gesellschaft, Europa-Universität Viadrina Frankfurt (Oder)
- **Prof. Dr. Dr. Christiane Wendehorst**
  Professorin für Zivilrecht und Stellvertretende Institutsvorständin am Institut für Digitalisierung und Recht, Universität Wien, Österreich, und Wissenschaftliche Direktorin des European Law Institute
- **Samantha Hofmann**
  Redakteurin für Digitales und Technologie, Science Media Center Germany
  und Moderatorin dieser Veranstaltung

Mitschnitt

- Einen Audio- und Videomitschnitt finden Sie unter:
  https://sciencemediacenter.de/press-briefings/696dfc13977c1364ed2f3718

Transkript

Moderatorin [00:00:00]

Herzlich willkommen, liebe Journalistinnen und Journalisten, hier zum Press Briefing des Science Media Center zum Thema KI-Regulierung und deutsche Umsetzung des AI Act. Mein Name ist Samantha Hofmann. Ich bin Redakteurin für Digitales und Technologie beim Science Media Center und mit mir hier sind heute eine Expertin und zwei Experten zum Thema KI-Regulierung und KI-Landschaft. Ich stelle sie gleich noch genauer vor, aber erst noch einige Sachen zum Organisatorischen dieses Meetings. Liebe Journalistinnen und Journalisten, stellen Sie bitte Ihre Fragen über das F von Zoom. Ein Kollege von mir sammelt die Fragen im Hintergrund und ich stelle sie dann hier im Gespräch an unsere Expertin und die Experten. Nutzen Sie bitte ausschließlich die F von Zoom und nicht den Zoom-Chat. Das macht es einfach für uns etwas übersichtlicher und so gehen keine Fragen verloren. Außerdem gibt es in dem F die Funktion, Fragen mit einem Daumen nach oben upzuvoten. Machen Sie davon bitte auch viel Gebrauch. So sehen wir nämlich, welche Fragen Sie für besonders wichtig halten und wir können die gegebenenfalls priorisieren, falls wir am Ende nicht genug Zeit haben, alle Fragen zu beantworten. Dieses Meeting wird aufgezeichnet. Deswegen brauchen Sie nichts mitzuschneiden. Wir stellen am Ende so schnell wie möglich ein Transkript, eine Audio-und Videodatei dieses Meetings zur Verfügung, die Sie dann sehr gerne für Ihre Berichterstattung nutzen können. Das waren die organisatorischen Sachen. Jetzt zum Inhalt unseres Meetings. Eigentlich wollten wir zu Beginn über einen Gesetzentwurf zur nationalen Umsetzung des AI Act sprechen. Jetzt hat die Bundesregierung dazu gestern aber keinen Gesetzentwurf veröffentlicht. Das ist überhaupt nicht schlimm. Das Thema ist und bleibt natürlich relevant. KI ist aus unser aller Alltag vermutlich nicht mehr wegzudenken. Die Rahmenbedingungen für ihren Einsatz schafft in Europa der AI Act. Allerdings gibt es weiterhin Fragen zu Datenschutz, Innovation, digitaler Unabhängigkeit und Wettbewerb. Die rechtlichen Bedingungen sind gerade für uns Laien nicht immer übersichtlich. Um Licht in dieses Dunkel zu bringen, sind heute drei Forschende zum Thema hier. Die stelle ich Ihnen jetzt kurz in alphabetischer Reihenfolge vor. Ich möchte gerne beginnen mit Patrick Glauner. Er ist Professor für Künstliche Intelligenz an der Technischen Hochschule Deggendorf. Er beschäftigt sich mit KI-Technik und -Anwendung und kann heute auch einen guten Vergleich zwischen USA, China und Europa herstellen. An zweiter Stelle, Herr Professor Philipp Hacker. Er ist Professor für Recht und Ethik der digitalen Gesellschaft an der Europa-Universität Viadrina Frankfurt (Oder) und er beschäftigt sich mit der Umsetzung des AI Act und KI-Regulierung allgemein. Die Runde abschließt Christiane Wendehorst. Sie ist Professorin für Zivilrecht an der Universität Wien und wissenschaftliche Direktorin des European Law Institute. Sie beschäftigt sich viel mit dem Zusammenspiel verschiedener europäischer Digitalgesetze, zum Beispiel eben dem AI Act, aber auch der DSGVO und insgesamt KI-Regulierung auf europäischer Ebene. Vielen Dank, dass Sie alle hier sind und sich heute die Zeit für unsere Fragen nehmen. Ich habe auch direkt für jeden von Ihnen schon eine Einstiegsfrage vorbereitet und würde gerne mit Herrn Hacker beginnen. In einem Referentenentwurf vom Herbst 2025 wird die Bundesnetzagentur als zentrale Behörde benannt, die für die Einhaltung und Umsetzung des AI Act in Deutschland verantwortlich sein wird. Welche Aufgabe hätte die Bundesnetzagentur als zuständige Behörde und wie könnte sie dieser Rolle gerecht werden?

Philipp Hacker [00:03:17]

Das ist eine gute Frage. Vielen Dank. Ich möchte da vielleicht auf drei Punkte zu sprechen kommen, nämlich erstens: Was ist an dem Entwurf gut? Zweitens: Was ist zu kritisieren? Und drittens: Wie kann es jetzt weitergehen? Gut ist meiner Ansicht nach zunächst mal natürlich das Ziel, das bürokratiearm und innovationsfreundlich zu gestalten. Darauf können wir uns, glaube ich, alle irgendwie einigen. Nicht schlecht ist, finde ich, auch der Versuch, möglichst viel in eine Hand zu

legen, also für Unternehmen gewissermaßen einen One-Stop-Shop bei der Bundesnetzagentur zu etablieren. Wofür überhaupt? Für die Verbote der KI-Verordnung, für die Hochrisikosysteme und auch für die Transparenzanforderungen. Die Regelungen für General-Purpose AI (GPAI), also für allgemeine Systeme wie Large Language Models (LLMs), liegen ja weiterhin bei der EU-Kommission. Und dort beim KI-Büro, also dem AI Office. Sinnvoll finde ich zweitens, dass man zugleich zurückgreift auf sektorale Regulierungsbehörden, die es schon gibt. Zum Beispiel im Bereich der Produktsicherheit, bei Medizinprodukten, da gibt es ja schon die Prüfstellen, und auch im Bereich der Finanzdienstleistungen. Das macht Sinn, dass man da auf bestehende Expertise setzt. Und drittens ist es auch sinnvoll, einen zentralen Koordinierungsmechanismus, ein Gremium sozusagen, einzusetzen bei der Bundesnetzagentur, das dann gepoolt Expertise zur Verfügung stellt. Was macht nicht so viel Sinn? Besonders schwierig oder kritisch zu sehen, meiner Ansicht nach, ist, dass es bestimmte, besonders grundrechtssensible Bereiche gibt. Das sind ganz spezifisch, ganz konkret, Biometrie, Strafverfolgung, aber auch Justiz, Wahlen und Demokratie. Und da sagt die KI-Verordnung eigentlich, dass nach Artikel 74, Absatz fünf und Absatz acht, diese Bereiche den Datenschutzbehörden zugeordnet werden müssen. Das macht das deutsche Umsetzungsgesetz nicht. Stattdessen wird eine unabhängige Marktüberwachungskammer mit dem schönen Kürzel UKIM, bei der Bundesnetzagentur eingerichtet. Meiner Ansicht nach ist das möglicherweise europarechtswidrig. Da handeln wir uns unbesehen Probleme ein. Man kann sozusagen lange darüber streiten: Macht es Sinn oder nicht, die Datenschutzbehörden da zu bevollmächtigen? Aber das ist nun mal geltendes Recht und das ist für einen großen Mitgliedsstaat wie Deutschland kein guter Ausweis, wenn wir sagen, wir setzen das jetzt einfach sehenden Auges falsch um, nur weil uns die generelle Richtung nicht passt. Das erst mal vielleicht so als grobe Einordnung. Wie geht es jetzt weiter? Ganz wichtig, erster Punkt: Die Behörden richtig und gut finanziell ausstatten. Manche Politikerinnen und Politiker denken ja immer, man muss Behörden möglichst wenig ausstatten, damit die die Wirtschaft wenig stören. Das ist meiner Ansicht nach grundlegend falsch, denn dann können sie ihrer Beratungsfunktion gar nicht mehr nachkommen. Die ist hier essenziell. Und das Zweite ist, dass man sich natürlich anschauen muss: Wie funktioniert das jetzt in der Praxis? Ein zentrales Beispiel ist da natürlich Grok und die Nudification-Debatte. Da werden wir jetzt im Bereich des Omnibus-Verfahrens, also des Überarbeitungsverfahrens des AI-Act, viel zu diskutieren haben. Dazu können wir gerne dann später auch noch weiter konkrete Anhaltspunkte geben.

Moderatorin [00:06:25]

Alles klar, vielen Dank. Wir hatten ja jetzt bisher nur einen Referentenentwurf vorliegen und Sie haben gesagt, das, was da drin steht, könnte eventuell europarechtswidrig sein. Können Sie sich vorstellen, dass das in einem Gesetzentwurf so weiter bestehen bleibt oder dass da noch mal nachgearbeitet wird? Gerne kurz antworten.

Philipp Hacker [00:06:39]

Ja, es gab da auch Kritik von vielen Seiten aus der Literatur. Die Lage ist da eigentlich relativ eindeutig, meiner Ansicht nach, dass das anders gehandhabt werden müsste. Insofern könnte ich mir vorstellen – das ist jetzt aber reine Spekulation –, dass vielleicht die Verzögerung damit zu tun hat, dass man da noch einmal darüber nachdenkt, ob man da gewissermaßen sehenden Auges in ein mögliches Vertragsverletzungsverfahren hineinlaufen möchte. Denn man will ja Klarheit für die Unternehmen. Und Klarheit besteht halt leider nicht, wenn man es europarechtswidrig umsetzt.

Moderatorin [00:07:10]

Alles klar, dann gerne weiter mit Frau Wendehorst mit ihrer Eingangsfrage. Was ist grundsätzlich berechtigte Kritik an der KI-Verordnung und was sind Ihre Stärken und Schwächen?

Christiane Wendehorst [00:07:23]

Ja, ganz herzlichen Dank. Auch das ist eine sehr gute Frage, über die man lange sprechen könnte. Ich fange vielleicht mal mit den Stärken der KI-Verordnung an. Gut ist, glaube ich, wirklich dieser risikobasierte Ansatz. Was heißt risikobasierter Ansatz? Risikobasierter Ansatz heißt: Ich reguliere dort strikt, wo ein hohes Risiko besteht. Ein hohes Risiko entweder für die Grundrechte oder auch für Gesundheit und Sicherheit unserer Bürgerinnen und Bürger. Dort, wo aber nur ein niedriges oder geringes Risiko besteht, dort nehme ich Regulierung zurück. Und dieser risikobasierte Ansatz, der ist, glaube ich, ganz wichtig und richtig. Ich halte auch – obwohl hier viele meiner Kollegen und Kolleginnen kritisch sind – grundsätzlich den produktsicherheitsrechtlichen Ansatz für gut oder zumindest gangbar. Was heißt das? Das heißt, ich behandle künstliche Intelligenz wie ein ganz normales Produkt. Freilich mit der Besonderheit, dass es auch zum großen Teil Grundrechtsrisiken schafft und wende aber ansonsten die gängigen Mechanismen des Produktsicherheitsrechts an. Ich glaube, das ist ein gangbarer Weg, und das ist auch in Ordnung. Ich komme jetzt aber zur Kritik, und diese Liste der Kritikpunkte ist auch nicht ganz kurz. Ich will vielleicht nur vier Punkte nennen. Ein Punkt ist die Unklarheit zentraler Begriffe. Und ich fange hier an mit dem ganz wichtigen Begriff: Was ist überhaupt ein KI-System? Dieser Begriff entscheidet über den Anwendungsbereich des gesamten Rechtsakts und nicht nur des Rechtsakts, sondern auch weiterer flankierender Rechtsakte, die sich an dem Begriff des KI-Systems nach der KI-Verordnung orientieren. Und dieser Begriff ist vollkommen unklar. Der Gesetzgeber hat sich hier zum Schluss an der revidierten OECD Definition orientiert, die niemals dafür geschaffen worden ist, tatsächlich den Anwendungsbereich von Gesetzgebung zu definieren. Der Begriff ist vollkommen unscharf und man kann sagen, die Leitlinien der Europäischen Kommission haben die Sache noch schlimmer gemacht. Sie widersprechen sich dauernd, sie vermischen verschiedene Fragen. Sie sind ganz klar durch bestimmte Lobbytätigkeiten auch beeinflusst worden. Das heißt, wir haben jetzt einen vollkommen unklaren Begriff des KI-Systems, vollkommen unklare Leitlinien und wissen daher wirklich nicht im einzelnen, für welche Systeme der ganze Rechtsakt überhaupt gilt. Zweites Problem ist die mangelnde Abstimmung mit anderen Rechtsakten. Man wollte hier bestimmte Rechtsakte, zum Beispiel gerade die Datenschutz-Grundverordnung (DSGVO), bewusst nicht antasten. Die DSGVO war ja lange Zeit bis jetzt zum digitalen Omnibus so eine Art heilige Kuh, die unantastbar ist. Das heißt, man hat hier wieder mal seine Formel gebracht, dass das Datenschutzrecht unberührt bleibt, obwohl wir wissen, es kann nicht unberührt bleiben und obwohl wir wissen, die KI-Verordnung hat große Implikationen für den Datenschutz. Man hat dann an zwei Stellen quasi ein Sonderdatenschutzrecht geschaffen und das führt alles zu Problemen für die Unternehmen, die diese ganzen Rechtsakte parallel anwenden müssen. Ich komme zum nächsten Punkt, dass die KI-Verordnung möglicherweise nicht future-proof ist. Ich darf daran erinnern, als sie vorgestellt wurde, gab es noch kein ChatGPT oder besser gesagt, es war noch nicht ausgerollt. Im November 2022 kam dann eben die Ausrollung von ChatGPT. Man hat gemerkt, der Entwurf ist schon auf generative KI nicht hinreichend abgestimmt. Man hat das dann versucht notdürftig zu reparieren. Die Frage ist: Reicht das? Was ist mit agentischer KI? Ich glaube, viele Probleme, die wir hier jetzt sehen, haben nicht unbedingt was mit der KI-Verordnung selbst zu tun, sondern mit der Kommunikation über die KI-Verordnung. Wir sehen hier ein richtiges Kommunikationsdesaster. Ich war ja in die Anfänge der KI-Verordnung teilweise auch intensiv eingebunden und die Kommission ist angetreten mit der Zielsetzung: wir wollen keine zweite DSGVO. Wir dürfen die Fehler der DSGVO nicht verdoppeln, nicht wiederholen, wir wollen etwas schlankes, klares. Aber diese Kommunikation über die KI-Verordnung ist gekippt. Die KI-Verordnung wird dargestellt als ein Regulierungsmonster, das KI-Entwicklung in Europa verhindert.

Und dieses Kommunikationsdesaster, glaube ich, müssen wir auch wieder einfangen und auch den Leuten erklären, was da wirklich überhaupt drin steht. Danke.

Moderatorin [00:12:37]

Noch eine ganz kurze Nachfrage: Meinen Sie jetzt zum Beispiel auch mediale Kommunikation, wie es dargestellt wird oder geht es Ihnen um die politische Kommunikation, wie das vermarktet wurde?

Christiane Wendehorst [00:12:44]

Ich glaube beides. Das können wir ja nicht voneinander trennen. Der Ausgangspunkt war: Lass uns hier etwas schlankes, klares schaffen, das die Fehler nicht wiederholt und dass der europäischen Industrie die nötige Sicherheit gibt, aber auch Grundrechte unserer Bürger und Bürgerinnen schützt. Rausgekommen ist jetzt ein Regulierungsmonster, das sozusagen KI-Entwicklung in Europa verunmöglicht. Und das stimmt einfach so nicht. Ja.

Moderatorin [00:13:16]

Mhm. Alles klar. Danke schön. Ich denke, Herr Glauner, da können Sie direkt mit Ihrer Einstiegsfrage drauf eingehen, und zwar: Wie beeinflusst der AI Act konkret die KI-Landschaft in Deutschland und der EU? Und wie sicher kann man das überhaupt sagen, weil ja eben auch schon kurz die Rede davon war, dass da zum Beispiel Innovationen gehemmt werden. Gibt es dafür überhaupt Anhaltspunkte, dass dem so sein könnte?

Patrick Glauner [00:13:39]

Ja, herzlichen Dank. Hallo allerseits. Also bezüglich Innovation, Klarheit beziehungsweise Unklarheit stimme ich der Kollegin Wendehorst zu. Es ist schon mal unklar, was ist eigentlich ein KI-System laut der Legaldefinition in dem AI Act. Die hat sich ja auch mehrfach in den Entwürfen geändert. Am Ende kam eine Definition raus, auf die wir Informatiker niemals gekommen wären. Und die Frage ist: Was bedeutet das jetzt alles? Dazu gibt es Kommentarliteratur. Ich habe auch an einem Kommentarwerk von David Bomhard und weiteren Herausgebern mitgeschrieben. Da haben wir zwanzig, dreißig Seiten im Kommentar geschrieben, was diese paar Sätze oder paar Zeilen im AI Act bedeuten. Das hilft bei der Umsetzung nicht. Das erschwert Innovation, es verteuert Innovation, es verlagert Innovation, weil eben die Unternehmen keine Zeit haben, hunderte Seiten Verordnungen zu lesen beziehungsweise Kommentare zu prüfen. Was man braucht bei der praktikablen Umsetzung, sind am Ende Checklisten. Und die werden branchenspezifisch entstehen müssen und sind teilweise am Entstehen. Da sehe ich die Berufsverbände auch in der Pflicht. Und wenn dann die Unternehmen mehrere Seiten Checklisten haben, die sie durchgehen können und dann vielleicht 95 Prozent sicher sind, das hilft. Anderenfalls wird es zu teuer. Es wird Innovation verhindern, und ich glaube, wir sehen da auch schon viele Negativbeispiele. Die Intention des AI Act mag gut sein. Man hätte sich natürlich von Anfang an fragen müssen, wo ist eigentlich die Regelungslücke? Weil es gibt ja auch viel vertikale, also sektorielle Regulierung und die KI-Anwendungen sind diesen immer unterworfen. In der jetzigen Form hilft das nicht. Wir sehen jetzt aber auch auf europäischer Ebene den Omnibus, in dem man versucht, an ein paar Details zu arbeiten. Ich glaube, da muss man noch mal wesentliche Fragen stellen: Wie kann man es verschlanken? Und bezüglich der Aufsicht auch noch ein paar Sätze: Die Gefahr, wenn die Aufsicht bei den Mitgliedstaaten liegt, ist, dass wir in Deutschland versuchen, päpstlicher als der Papst zu sein. Und dass das in anderen Ländern gar nicht erzwungen wird. Da gibt es ja auch so Beispiele mit kleinen Mitgliedstaaten in der EU, die die Datenschutzgrundverordnung eigentlich ignorieren.

Man hat sich jetzt für den Weg entschieden, dass es viel nationale Aufsicht gibt und wenig gebündelt in Brüssel ist. Das ist jetzt so. Vielleicht kann man das über den Omnibus auch noch mal ändern, aber der Kollege Hacker hat ja auch gelobt, dass neben der Bundesnetzagentur die sektoriellen Aufsichtsbehörden einbezogen werden. Das ist sehr sinnvoll, weil dort die Domänenexpertise ist. Die Bundesnetzagentur kann jetzt keine Fragen zu Landwirtschaft oder Maschinenbau beantworten. Dafür braucht man die sektoriellen Experten. Und ja, die finanzielle Ausstattung ist wichtig. Generell werden IT-Experten im öffentlichen Dienst sehr schlecht eingruppiert: A13. Und man muss sagen, jeder Gymnasiallehrer ist A13. Dann sind es oft zeitlich befristete Stellen bei den Behörden, und da muss man natürlich auch Geld auf den Tisch legen, dass man gute Leute gewinnt, die am Ende diese Regelwerke auch verstehen und das technische Wissen mitbringen. Das sollten auch Dauerstellen sein, damit man da nicht so eine permanente Fluktuation hat oder auch Rotation zwischen Industrie und Aufsichtsbehörden.

Moderatorin [00:17:06]

Ja, vielen Dank. Sie haben eben natürlich auch schon die viel zitierte Innovation noch mal angesprochen und meinten, es gibt Negativbeispiele dazu, wie der AI Act, zum Beispiel Unternehmen beeinflussen kann. Haben Sie da zufällig eins parat?

Patrick Glauner [00:17:19]

Es ist Angst, dass man sagt: „Da ist jetzt irgendwas verboten oder irgendwas eingeschränkt. Machen wir jetzt gar nicht mehr. Wir vergessen es und machen keine KI." Das sind so Beispiele, die sieht man immer. Da sage ich auch zu den Unternehmen: Das nicht in der Richtung tun, sondern machen, KI umsetzen. Die Verbote sind überschaubar, glaube ich, und bei allem anderen muss man halt eng mit den Berufsverbänden zusammenarbeiten, dass Checklisten entstehen. Denn die Unternehmen werden nicht hunderte Seiten umsetzen können.

Moderatorin [00:17:49]

Alles klar. Noch einmal ein ganz kurzer Hinweis an die Journalistinnen und Journalisten. Sie können gerne Ihre eigenen Fragen im F stellen. Also das ist auf jeden Fall freigeschaltet. Wenn Sie Fragen haben, posten Sie die gerne da rein, damit wir sie hier auch an die Expertinnen und Experten stellen können. Ich hätte noch eine weitere Frage an Herrn Hacker. Und zwar ging es eben schon ganz kurz darum, dass die DSGVO in verschiedenen Mitgliedsstaaten unterschiedlich umgesetzt wurde. Was kann man denn bisher zur Umsetzung des AI Act in verschiedenen Mitgliedsstaaten sagen?

Philipp Hacker [00:18:21]

Also erstens sind wir in Deutschland relativ spät dran, was einfach mit der Regierungsumbildung zu tun hatte. Da konnte jetzt gewissermaßen im AI-Bereich niemand so wirklich was dafür. Was zu konstatieren ist, ist, dass sehr unterschiedliche Modelle gewählt werden. Teilweise ist es so, dass die Mitgliedstaaten noch stärker auf sektorale Behörden setzen. Teilweise wird versucht, alles bei einer Behörde, teilweise auch den Datenschutzbehörden, zu zentralisieren. Interessant ist zu sehen, dass sich aber viele Mitgliedstaaten an die Zuweisung der besonders grundrechtssensiblen Bereiche – wir zählten sie bereits auf, die Biometrie, Strafverfolgung – an die Datenschutzbehörden halten. Das macht meiner Ansicht nach auch Sinn, weil es eben doch was anderes ist, Strafverfolgungsbehörden oder Unternehmen zu beaufsichtigen. Das sehen wir auch gerade in den USA, dass das teilweise dann doch recht eigene Dynamiken erfahren kann, was da passiert. Insofern macht das vielleicht Sinn, das auch noch mal zu trennen und hier nicht eine reine

Marktaufsicht, sondern eher eine verstärkte Grundrechtsaufsicht zu haben. Da geht es dann auch weniger um Innovation im eigentlichen Sinne, also dahingehend, dass Unternehmen jetzt Produkte an den Markt bringen können. Sondern da geht es darum, wie können einzelne Behörden, wie kann die Polizei, wie kann die Staatsanwaltschaft diese Systeme nutzen? Die werden ja selten in den Behörden auf Weltniveau entwickelt. Da geht es eher um die Anwendung und darum, da eine gute Aufsicht und eine gute Grundrechtsprüfung zu haben. Also insofern haben wir da eine große Heterogenität, aber im Bereich gerade dieser spezifischen und besonders diskutierten Frage ist Deutschland dann doch eher die Ausnahme.

Moderatorin [00:19:59]

Gibt es vielleicht ein Positivbeispiel in Europa, an dem Deutschland sich orientieren könnte, gerade wenn wir noch nicht so weit sind mit der nationalen Ausarbeitung?

Philipp Hacker [00:20:07]

Das ist, glaube ich, schwer, weil wir in Deutschland aufgrund der föderalen Struktur eben so gewisse Besonderheiten haben. Also ein Kritikpunkt an der jetzigen Ausgestaltung im Referentenentwurf ist, dass man versucht, die Aufsicht zu zentralisieren, damit die Unternehmen einen Anlaufpunkt haben. Dadurch greift man gewissermaßen als Nebeneffekt in die eigentlichen Sachkompetenzen der Länder ein. Wir wissen ja, im föderalen Schulsystem ist es beispielsweise so, dass jedes Land ein eigenes Bildungssystem hat und das geht dann mit eigenen Schulämtern und so weiter einher. Wenn jetzt Hochrisiko-KI in Schulen oder Universitäten eingesetzt wird, dann wäre weiterhin die Bundesnetzagentur zuständig und da ist nicht ganz klar, wie das verfassungskonform geschehen kann. Da brauchst du dann bestimmte Abstimmungsmöglichkeiten. Ich würde sagen, da ist es vielleicht in dem Fall wert, zu versuchen, das tatsächlich einheitlich zu regeln. Und dann durch bestimmte nachgelagerte Vereinbarungen mit den Ländern das Ganze verfassungskonform aufzustellen. Das ist aber im Einzelnen tatsächlich ziemlich kompliziert. Das sind aber wiederum Probleme, die aus der spezifischen deutschen Föderalstruktur resultieren. Wir können es also nicht so machen wie die Franzosen, die sagen: Wir machen jetzt einfach alles bei der einen zentralen Datenschutzbehörde. Die haben wir in Deutschland ja gar nicht. Es gibt ja die Bundesbeauftragte für Datenschutz und Informationsfreiheit (BFDI) auf Bundesebene und dann 17 Datenschutzbehörden der Länder. Dass das zu einer nicht ganz unerheblichen Zersplitterung führen würde, ist auch klar. Daher kommt gewissermaßen der Impetus des Bundesministerium für Digitales und Staatsmodernisierung (BMDS) zu sagen: Wir versuchen, das alles an einer Stelle zu bündeln.

Moderatorin [00:21:47]

Ja, vielen Dank. Noch eine Frage an Frau Wendehorst. Und zwar ist der AI Act ja seit 2024 Schritt für Schritt in Kraft getreten. Kann man schon eine erste Bilanz ziehen, wie das bisher angelaufen ist, ob er ein wirksames Instrument gegen Missbrauch von KI ist und ob er auch wirklich durchgesetzt wird, gerade auch mit Blick zum Beispiel auf große Player wie die USA oder China?

Christiane Wendehorst [00:22:09]

Ja, das ist schwierig zu sagen. Also wie wir gerade diskutieren, sind in vielen Mitgliedstaaten noch gar nicht die Begleitgesetze erlassen. Die zuständigen Behörden fangen, soweit sie ernannt sind, erst an zu arbeiten. Ich denke, das kann man momentan noch nicht wirklich absehen. Ja, klar ist, Sie haben ein wichtiges Stichwort genannt: Durchsetzung gegenüber großen Playern aus Drittstaaten. Hier hat sich zweifellos mit der zweiten Amtszeit Trumps deutlich noch mal etwas verschoben. Das

heißt, wir müssen jetzt auch bei europäischer Regulierung sehr viel strategischer denken für den Standort Europa. Das ist etwas, was bislang, muss ich ganz ehrlich sagen, bei europäischer Gesetzgebung nicht immer der Fall war. Und wir werden möglicherweise manche Bestimmungen auch noch einmal unter dem Gesichtspunkt europäischer digitaler Souveränität überprüfen und gegebenenfalls anpassen müssen. Aber ich glaube, für ein Resümee, wie sich das in der Praxis bewährt, ist es momentan noch ein bisschen zu früh.

Moderatorin [00:23:22]

Alles klar. Okay, noch zu früh, sagen zu können, was genau der AI Act dafür jetzt bringt. Wir haben eben auch schon digitale Souveränität angesprochen. Ist ja auch ein sehr großes Thema, gerade eben auch mit Blick auf die USA. Herr Glauner, wie sehen Sie denn die Chancen, dass Deutschland digital souverän wird, zum Beispiel durch eigene große Sprachmodelle?

Patrick Glauner [00:23:49]

Souveränität ist ein schwieriger Begriff. Also wir sind ja gerne so Weltmeister darin, alles schlechtzureden in Deutschland. Jetzt kann man sich fragen: Wo steht Deutschland in der KI? Da gibt es natürlich immer viele Meinungen. Wichtig ist, dass man Studien dazu durchführt. Ich habe auch verschiedene Studien zusammen mit Partnern dazu durchgeführt. Da haben wir gesehen, dass Deutschland bei der Anzahl der KI-Unternehmen, also Unternehmen, die nicht nur KI nutzen, sondern in irgendeiner Form auch entwickeln rund auf Platz fünf steht – teilweise steht Deutschland auf Platz sieben weltweit bei Forschung, Innovation und bei Anzahl der Experten. Also grundsätzlich passiert mal viel. KI ist viel mehr als die großen Sprachmodelle. Es gibt in Deutschland ganz tolle Mittelständler, die KI in ihre Produkte einbauen bis hin zu, sagen wir, Kaffeemaschinen. Es gibt auch tolle Unternehmen in Deutschland, die KI-Chips herstellen. Da gibt es ein Start-Up in Offenburg, das heißt AITAD. Die entwickeln Chips und fertigen die vor Ort. Dadurch sind Lieferketten deutlich einfacher als auf anderem Weg. Also es passiert viel. Wenn wir jetzt auch diese großen Sprachmodelle wollen, sind Energiekosten ein Problem. Das muss man auch beachten. Regulierung erschwert natürlich an manchen Stellen auch die Innovation, das ist gar keine Frage. Aber was ich auch sehe: Wir haben so viele tolle Start-Ups in Deutschland. Viele gehen aber in die USA. Nicht nur wegen der Regulierung, auch teilweise einfach, weil es dort einfacher ist, an Venture Capital zu kommen, also Risikokapital. Wir sitzen in Deutschland regelrecht auf dem Geld. Bei uns verwalten die Versicherer Billionen, dürfen aber nicht in Venture Capital gehen. Der CEO der Allianz hat ja mehrfach auch gesagt, er würde gerne, aber er darf gesetzlich nicht. Aber wir tun uns in Deutschland immer schwer mit Aktienrente und solchen Dingen. Die Leute haben Angst, es würde alles verzockt werden. Die Wahrheit ist, bei Venture Capital haben wir einen deutlich höheren Erwartungswert als bei Staatsanleihen. Würde man da auch ein bisschen Flexibilisierung schaffen, dass die Versicherer auch in Venture Capital gehen dürften in Deutschland, dann würden die Start-Ups hier nicht mehr in die USA müssen wegen dem Geld. Denn wir haben grundsätzlich genug Geld. Wir haben eine gute Basis durch Forschung, durch Ausbildung, durch viel Mittelstand, aber wie gesagt, Venture Capital ist ein Thema, Regulierung natürlich auch. Und es ist jetzt nicht immer alles so schlecht, wie man gerne liest. Wie gesagt, Platz fünf, sechs, sieben.

Moderatorin [00:26:25]

Eine Frage von außerhalb an Herrn Philipp Hacker noch dazu, was Sie eben gesagt hatten. Und zwar könnten Sie noch mal etwas konkreter benennen, inwiefern die Bundesnetzagentur weniger strikt auf Grundrechtseinschränkungen sehen könnte. Bei welchen Anwendungen sehen Sie da zum Beispiel Gefahr?

Philipp Hacker [00:26:44]

Das sind genau die Anwendungen, über die wir gesprochen haben. Das sind eben in sensiblen Bereichen biometrische Anwendungen. Da geht es zum Beispiel um die Überwachung von Demonstrantinnen und Demonstranten. Da geht es um den Einsatz in der Strafverfolgung, Stichwort Predictive Policing. Das sind alles Bereiche, in denen ganz andere Fragestellungen zu Tage treten, als wenn ich jetzt schaue, wie ein LLM beispielsweise im Kundenkontakt genutzt wird. Oder auch wie medizinische Diagnostik funktioniert. Das sind typischerweise die Bereiche, mit denen Marktaufsichtsbehörden zu tun haben. Hier geht es ja aber auch gar nicht um einen Markt. Hier geht es um hoheitliches Handeln. Und das sind deshalb genuin andere Grundrechtseinschränkungen möglicherweise und auch genuin andere Durchsetzungsrobustheitsgrade, die da erforderlich sind. Und da kann man zumindest Zweifel haben, ob das bei der Bundesnetzagentur genauso gemacht würde wie bei den Datenschutzbehörden, die gewissermaßen schon diese DNA des Grundrechtsschutzes über Jahre eingeübt haben. Ich möchte gar nicht in Abrede stellen, wenn man da gute Leute in die UKIM setzt, dass die das auch gut machen könnten. Es ist aber halt so, dass natürlich jetzt schon seit vielen Jahren Expertise gewachsen ist. Das muss man auch sagen. Ich unterhalte mich auch häufig mit den Leuten in den Datenschutzbehörden vor Ort in ganz verschiedenen Konstellationen. Das sind auch vielfach keine Verhinderer, die jetzt einfach immer nur sagen: Wir müssen ja Datenschutz in Deutschland und wir wollen jetzt irgendwie alles platt treten. Sondern ganz im Gegenteil, da gibt es viele vernünftige Leute, die teilweise auch selbst einen informatischen Hintergrund haben. Der Vizepräsident der bayerischen Landesdatenschutzaufsicht zum Beispiel ist selber Informatiker. Die sind da sehr pragmatisch, aber haben eben jetzt schon viele Jahre Erfahrung, die einfach die Bundesnetzagentur nicht hat in dem Bereich. Deshalb wäre es vielleicht der etwas sicherere Weg, wenn wir diese ganz besonders kritischen Szenarien betrachten. Und noch mal gesagt, wir sehen in den USA, wie schnell das kippen kann. Und da ist es vielleicht gut, Behörden zu haben, die darin Erfahrung haben, mit solchen Szenarien umzugehen. Ich möchte aber gar nicht sagen, dass die Bundesnetzagentur das nicht machen kann. Da ist nur, finde ich, ein ein bisschen größeres Risiko dabei.

Moderatorin [00:28:54]

Wir haben noch eine Frage auch von außen, und zwar, wer zuständig ist für LLMs. Welche Aufsichtsbehörde ist eigentlich zuständig, wenn Unternehmen LLMs im Kundenkontakt einsetzen? Wäre das auch das AI Office der EU-Kommission oder ist das dann auch die Bundesnetzagentur zum Beispiel? Gerne entweder Frau Christiane Wendehorst oder Herr Hacker?

Philipp Hacker [00:29:17]

Also ich kann gerne anfangen. Das ist nämlich interessanterweise jetzt gerade zum Teil im Umbruch. Grundsätzlich ist es so: Die EU-Kommission ist zuständig für GPAI-Provider, also Anbieterregulierung. Das kann Xai sein, Meta oder OpenAI, die dieses Modell entwickeln, unabhängig davon, wo es dann eingesetzt wird. Dafür ist das AI Office zuständig. Für die Anwendung wiederum – da gibt es momentan nur Transparenzerfordernisse – dafür ist die nationale Marktaufsichtsbehörde zuständig. Wenn man das jetzt aber in einem Hochrisikobereich einsetzen würde – Kundenkontakt ist kein Hochrisikobereich, aber Recruitment zum Beispiel schon –, dann wäre nach jetzigem Stand auch die nationale Marktaufsichtsbehörde zuständig. Das führt dazu, dass wir dann so eine Zweiteilung haben. Auf der einen Seite das AI Office und auf der anderen Seite für alles, was dann die konkrete Anwendung ist in bestimmten KI-Systemen, wäre es die nationale Behörde. Das soll sinnvollerweise, meiner Ansicht nach, der digitale Omnibus ändern. Da ist es nämlich so, dass bestimmte Sachen im GPAI-Bereich hochgezont werden an die

Kommission. Was ist das? Erstens sind das KI-Systeme, die auf GPAI-Modellen beruhen im Hochrisikobereich. Dafür soll das AI Office zuständig werden. Das wäre nicht der Fall bei Kundenkontakt, weil Kundenkontakt, wie gesagt, kein Hochrisikobereich ist. Aber wenn das Recruitment wäre, dafür würde die Kommission dann zuständig werden, also das AI Office. Und zweitens sind das KI-Systeme in VLOPs und VLOSEs, also in den sehr großen Online-Plattformen, die nach dem Digital Services Act (DSA) geregelt sind. Für die VLOPs und VLOSEs ist auch bisher schon die Kommission zuständig. Nicht das AI Office, aber auch im DG Connect. Und das wird auch hochgezont. Macht meiner Ansicht nach sehr viel Sinn, denn wir sehen auch jetzt in der Praxis, dass häufig Fragen von den zukünftigen nationalen Marktaufsichtsbehörden an die Kommission in kommen. Die kommen schon jetzt. Die fragen: Wie sollen wir das und das regeln? Weil ihr habt es ja oben so und so gemacht. Wie sollen wir es jetzt hier unten machen? Das zu verbinden ist Teil dieser Simplification, die meiner Ansicht nach in dem Bereich viel Sinn macht. Es bleibt aber dabei: Wenn es nicht im Hochrisikobereich eingesetzt wird, dann sind nach jetzigem Stand, nach meinem Kenntnisstand, nur die nationalen Marktaufsichtsbehörden zuständig, weil es da am Ende auch nur nur um die Transparenzanforderungen geht.

Moderatorin [00:31:51]

Ja, man merkt schon, es ist auf jeden Fall kompliziert. Herr Glauner möchte direkt was dazu sagen.

Patrick Glauner [00:31:58]

Ja, also ich stimme dem Kollegen Hacker bei seinen Ausführungen zu und er hat was ganz Interessantes angesprochen. Das AI Office ist dann verantwortlich für General-Purpose AI, also für die Anbieter von solchen Modellen. Und dann hat er auch erwähnt, dass bei den VLOPs und VLOSEs, die Kommission auch verantwortlich ist, aber eine andere Einheit. Jetzt spielt bei VLOPS und VLOSEs oft natürlich KI eine Rolle. Daher wäre es eigentlich sinnvoll, wenn man in dem Omnibus das auch noch mal zusammenzieht und sagt: Wir haben einmal hier das AI Office, oder wir haben eine andere Einheit für große Plattformen, große Suchmaschinen, die heute alle auch KI getrieben sind. Und da entsteht dann so ein Wildwuchs am Ende und solche Doppelstrukturen. Und das könnte man eigentlich im Omnibus zusammenziehen. Das habe ich jetzt auch an verschiedenen Stellen vorgeschlagen. Hoffen wir mal, dass es in Brüssel Gehör findet.

Moderatorin [00:32:57]

Frau Wendehorst, Sie haben eben so wissend gelächelt. Möchten Sie da auch noch was sagen oder war das einfach Zustimmung?

Christiane Wendehorst [00:33:02]

Es ist einfach Zustimmung. Ich meine, es gibt zum digitalen Omnibus viel zu sagen, aber in dem Fall vielleicht.

Moderatorin [00:33:07]

Vielleicht können Sie noch mal ganz kurz zusammenfassen in ein, zwei Sätzen, was der digitale Omnibus ist, dass wir da auf dem neuesten Stand sind und Ihre Einschätzung dazu.

Christiane Wendehorst [00:33:15]

Ja, vielen Dank. Zunächst einmal: Warum Omnibus? Was ist überhaupt ein Omnibus? Ein Omnibus ist ein Gesetzespaket, was sozusagen horizontal verschiedene andere Gesetze ändert, meistens unter einem gewissen gemeinsamen Motto. Und so ist jetzt auch ein Paket auf den Weg gebracht worden, das verschiedenste Digitalgesetze unter dem gemeinsamen Motto der gemeinsamen Zielsetzung Vereinfachung ändern soll. Das zerfällt in zwei große Bereiche. Es gibt einen digitalen Omnibus für KI und es gibt einen digitalen Omnibus für den Rest, für die übrigen Digitalgesetze. Wenn wir uns jetzt mal nur den digitalen Omnibus für KI anschauen, dann sind das punktuelle Änderungen der KI-Verordnung. Und da fällt einmal eine Änderung ganz klar ins Auge. Das ist das zeitliche Hinausschieben von ganz zentralen Vorschriften, nämlich den zentralen Vorschriften für die Hochrisiko-KI-Systeme und dann bestimmten Vorschriften zu Transparenz, nämlich etwa dieses Watermarking. Wie ist das jetzt zu bewerten? Ist das ein Einknicken vor Big-Tech und und den USA? Natürlich hat hier zum Teil ein Lobbying großer Firmen eine gewisse Rolle gespielt. Ansonsten musste man sich aber einfach nur eingestehen, dass man es nicht geschafft hat, in der eigentlich vorgesehenen Zeit die Level-2-Rechtsakte und die Standards auf den Weg zu bringen und damit eine Situation geschaffen hat, die für die Industrie, einschließlich der europäischen Tech-Industrie, eigentlich unzumutbar ist. Das versucht man jetzt eben durch ein Hinausschieben der Geltung einzufangen. Da ist momentan ein relativ problematischer Mechanismus vorgeschlagen, wonach das teilweise von einer Kommissionsentscheidung abhängen soll. Das wird stark kritisiert, auch aus Demokratiegesichtspunkten heraus und da ist wahrscheinlich das letzte Wort noch nicht gesprochen. Darüber hinaus gibt es Vorschläge für punktuelle Anpassungen der KI-Verordnung. Eine Anpassung ist gerade schon diskutiert worden. Ich stimme Philipp Hacker absolut zu. Ich glaube, das ist ein positiver Aspekt, das ist vernünftig. Ich will vielleicht zwei andere Aspekte noch hervorheben, bei denen man geteilter Meinung sein kann. Einmal gab es ja so eine versteckte Datenschutzvorschrift im Artikel zehn, Absatz fünf, die im Prinzip gesagt hat, dass, wenn ich hier Bias und Diskriminierung reduzieren oder verhindern möchte in Hochrisiko-KI-Systemen, dann darf ich dafür ausnahmsweise sensible Datenkategorien nutzen. Unter ganz eingeschränkten Voraussetzungen. Da haben viele, einschließlich meiner Wenigkeit, gesagt: Moment, warum nur für Hochrisiko-KI? Das muss ja auch über Hochrisiko-KI hinaus ein legitimes Anliegen sein, Diskriminierung zu vermeiden. Darauf hat man dann reagiert und will das jetzt vor die Klammer ziehen, sozusagen für alle KI-Systeme gelten lassen. Gut gemeint, handwerklich schlecht gemacht. Denn das müsste man eigentlich in die DSGVO hinüberziehen. Auch von der Formulierung her müsste das adaptiert werden. Aber im Prinzip von der Grundidee her positiv. Es sollte nur anders gemacht werden. Noch ein Punkt: KI-Kompetenz. Artikel vier, der ursprünglich eine der wenigen Vorschriften der KI-Verordnung war, die für alle Anbieter und Betreiber aller KI-Systeme gelten, hat gesagt, dass jedes Unternehmen, das irgendwie was mit KI zu tun hat und sei das auch nur im ganz normalen Büroalltag, seine Mitarbeitenden KI kompetent machen muss. Das hat zu einem Boom in der Beratungsindustrie geführt und natürlich zu Panik bei allen möglichen Unternehmen. Und das will man jetzt ein bisschen zurückfahren, um hier eben auch wahrscheinlich diesen Eindruck, den ich vorhin geschildert habe, die KI-Verordnung sei ein Bürokratiemonster, was jetzt wieder jedem Bäcker um die Ecke und jedem Unternehmen, was überhaupt nicht KI spezifisch arbeitet, jetzt Unmögliches abverlangt. Das will man dadurch ein bisschen einfacher machen.

Moderatorin [00:38:13]

Das ist so ein bisschen ein Anstrich, das Ganze humaner zu machen und einfacher umzusetzen. Wir sprechen gleich, weil es gerade auch aus gegebenen Anlass ein sehr relevantes Thema ist, noch mal über Deepfakes. Aber vorher noch eine Nachfrage zum digitalen Omnibus. Je nachdem, wer von beiden sich berufen fühlt, entweder noch mal an Sie, Frau Wendehorst oder auch an Herrn Hacker. Der Omnibus schwächt private Persönlichkeitsrechte, und es wirkt so, als ob die EU den alten Pfad von USA und China jetzt angeht, dass eben diese Persönlichkeitsrechte nicht so wichtig

sind, obwohl genau diese Länder laut Aussage des Journalisten oder der Journalistin genau in eine andere Richtung steuern, also eher hin zu mehr Datenschutz oder Persönlichkeitsschutz. Wie schätzen Sie das ein?

Christiane Wendehorst [00:39:00]

Ja, also wie gesagt, dieser öffentliche Aufschrei, der hier passiert ist, auch schon im Vorfeld des digitalen Omnibus und als der digitale Omnibus veröffentlicht worden ist, den halte ich für absolut übertrieben. Im Grundsatz muss ich ganz ehrlich sagen, sehe ich es positiv, dass man den Mut hat, auch die alte heilige Kuh Datenschutzgrundverordnung einmal anzufassen und punktuell abzuändern. Ich gehöre zu denjenigen, die sich sehr dafür eingesetzt haben, auch im Hinblick auf KI-Entwicklung in Europa. Auch mit dieser Tagung, die ich im Dezember 2024 hier in Wien veranstaltet habe und einem wissenschaftlichen Diskussionsentwurf für eine KI-Datenschutzverordnung, die dann später vom European Law Institute und anderen aufgegriffen wurde. Also ich ich sehe hier im Grundsatz vieles von dem, was im digitalen Omnibus steht, nicht als Einknicken vor den USA, vor den Tech-Konzernen, nicht als sozusagen Aufweichen von Individualrechten, sondern als überfällige Adaptierung unseres Rechtsrahmens. Aber ich hätte mir gewünscht, dass es teilweise anders durchgeführt wird. Und ich hätte mir tatsächlich gewünscht, dass es nicht nur in eine Richtung durchgeführt wird, nicht nur in Richtung Abbau von Hürden. Sondern ich hätte mir gewünscht, dass man auch Lücken schließt, die derzeit in der DSGVO und anderen Digitalrechtsakten bestehen. Lücken bei Hochrisikodatenverarbeitungen bei großen Akteuren, weil hier meines Erachtens die DSGVO momentan nicht ausreicht. Das heißt, unser Vorschlag war, in beide Richtungen zu arbeiten, die DSGVO echt risikobasiert ausgestalten. Was wir jetzt sehen, ist nur in eine Richtung. Aber mal besser als nichts.

Moderatorin [00:41:09]

Okay, also ein Anfang, aber noch nicht perfekt. Herr Hacker, Sie möchten gerne schnell ergänzen.

Philipp Hacker [00:41:14]

Ja. Also Christiane Wendehorst ist da wirklich absolut die Expertin und hat auch einen tollen Entwurf vorgelegt. Ich will nur anmerken, dass ich auch der Meinung bin, dass vieles von dem sinnvoll ist. Weil das Problem ist im Datenschutzrecht schon lange diskutiert worden, es aber wirkt manchmal so, als sei mit Kanonen auf Spatzen geschossen worden. Zum Beispiel jetzt konkret: Die Frage scheint mir anzuknüpfen an sensible Daten, die nach Artikel neun DSGVO besonders geschützt sind. Die werden, wenn man so will, fast pauschal ausgenommen. Immer dann, wenn etwas passiert im Kontext von KI. Und das ist natürlich eine extrem weite Formulierung. Man kann durchaus sagen, dass es Regelungen braucht, wie man grundrechtskonform auch mit sensiblen Daten KI-Systeme trainieren kann. Denn wir brauchen Gesundheitsdaten für Gesundheits-KI-Systeme. Und der Begriff der sensiblen Daten ist ohnehin so breit, dass fast alle Daten darunter fallen. Das ist in der Tat ein Problem. Das Training ist momentan in der EU nicht ganz einfach rechtssicher möglich. Was dann zum Beispiel aber nicht mehr sinnvoll ist, meiner Ansicht nach, ist dieses grundsätzliche Verbot der Nutzung von sensiblen Daten für die Anwendung der KI-Systeme aufzugeben. Das würde nämlich bedeuten, dass es einen Unterschied macht, ob ich jetzt ein nicht-KI-System, also eine normale Software, oder ein KI-System nutze. Und da haben wir ja gar kein generisches Problem, das typischerweise bei dem Training zu Tage tritt. Da habe ich eben große Datenmengen. Aber bei der Anwendung, da sehen wir auch noch mal, gerade in Ländern, die jetzt nicht mehr so stark an der Rechtsstaatlichkeit hängen, dass man da versucht, sehr große Mengen sensibler Daten durch KI zu füttern. Um dann entsprechende Maßnahmen gegen Personen zu erwirken. Und da wäre ich sehr zurückhaltend, das so breit aufzufächern. Ich glaube, wenn man das

targetiert macht für KI-Training und da gute Schranken und Safeguards einzieht, dann ist das eigentlich etwas, was ganz vernünftig ist.

Moderatorin [00:43:06]

Frau Wendehorst, Sie möchten noch mal was ergänzen, aber bitte wirklich kurz. Wir haben noch ein paar Fragen, die wir auch außerhalb davon klären möchten.

Christiane Wendehorst [00:43:12]

Alles klar. Vielleicht nur ganz kurz. Ein Teil des Problems liegt auch darin, wie breit der Europäische Gerichtshof (EuGH) den Begriff der besonderen Kategorien personenbezogener Daten auslegt. Ich will jetzt nicht vertiefen, weil wir keine Zeit haben, aber nur als Anmerkung: Da liegt etwas und da muss möglicherweise die EuGH-Judikatur einfach korrigiert werden.

Moderatorin [00:43:32]

Okay, vielen Dank. Dann die nächste Frage auch von außerhalb an Herrn Glauner, und zwar aus der Praxis betrachtet: laufen KI-Regulierungen nicht insgesamt viel zu spät an und legt die Debatte zu viel Wert auf die Bremsen und weniger auf den Schutz?

Patrick Glauner [00:43:46]

Ja, ich bin grundsätzlich immer sehr kritisch, wenn es um KI-spezifische Regulierung geht, weil am Ende, was wir ja regulieren wollen, sind Anwendungsfälle, nicht das Werkzeug. Wenn ich eben KI in ein Atomkraftwerk einbaue oder in ein Flugzeug oder in ein anderes Produkt, zählt für mich vor allem die sektorale, also die vertikale Regulierung, in der es Prozesse und Systeme gibt. Und die KI ist ja immer nur ein kleiner Teil solcher Systeme und Prozesse und ist natürlich diesen vertikalen Anforderungen unterworfen. Wenn man jetzt versucht, KI-spezifisch zu regulieren, ist man natürlich nie up to date. Man hat ja schon gesehen, wie lange es auch gedauert hat, bis der AI Act verabschiedet wurde. Der erste Entwurf war im April 2021. Er wurde dann im Sommer 2024 verabschiedet und es gab ja davor schon verschiedene Bestrebungen. Und auch der erste Entwurf des AI Act wurde permanent umgeschrieben in diesen drei Jahren, weil dann ChatGPT dazu kam, was man vorher nicht hatte. Es gab schon Modelle dieser Art, die waren vielleicht noch nicht so beliebt. Die Kollegin Wendehorst hatte ja auch so was kurz erwähnt in ihrem Eingangsstatement. Und deshalb ist es mit technologiespezifischer Regulierung sehr schwierig, up to date zu sein, weil der Markt sich eben rapide ändert. Und deshalb würde ich deutlich mehr noch in Anwendungsfällen denken und viel weniger im Sinne von Technologie. Und da, wo es vielleicht Fragen gibt, etwa rund um Deepfakes, wenn es da einen Regulierungsbedarf gibt, auch aus strafrechtlicher Sicht, kann man das ja schließen. Das würde ja völlig unabhängig von KI gehen, weil KI nur ein Werkzeug ist, so was zu erstellen. Man kann es händisch erstellen. Manipulierte Fotos gibt es seit Beginn der Fotografie und es gibt ja auch diverse andere Gesetze, die Schutz bieten, etwa Antidiskriminierungsgesetze. Wenn es da eine Lücke gibt, schließen, aber vielleicht völlig unabhängig von KI.

Moderatorin [00:45:44]

Das ist ein sehr guter Punkt, den Sie ansprechen. Wir haben nämlich auch direkt schon eine Frage zu den Deepfakes beziehungsweise Kennzeichnungspflichten für möglicherweise täuschende KI-

Bilder. Ist es realistisch, dass da in nächster Zeit ein Standard kommt, vielleicht in der EU, vielleicht in Deutschland? Herr Hacker, gerne.

Philipp Hacker [00:46:01]

Ja, da ist gerade eine Arbeitsgruppe eingesetzt worden. Also die arbeiten da dran. Das wird hoffentlich innerhalb der nächsten wenigen Monate der Fall sein und dann wird man sehen, wie schnell die sind und ob dann die Pflichten auch im Sommer in Kraft treten, wofür ich persönlich sehr wäre. Wir sehen die großen Probleme mit Deepfakes gerade. Zu der Regulierung von Deepfakes allgemein können wir gerne gleich auch noch was sagen. Da würde ich gerne noch was zu sagen, aber die Frage wäre jetzt ganz spezifisch.

Moderatorin [00:46:30]

Genau. Vielleicht erst mal, wenn es zu der speziellen Frage Ergänzungen gibt von Herrn Glauner und Frau Wendehorst, Sie haben sich eben auch noch gemeldet. Gerne erst Herr Glauner.

Patrick Glauner [00:46:36]

Ja, für so eine Kennzeichnungspflicht gibt es, glaube ich, gute Gründe. Gibt ja dann auch Aussagen, nicht nur für Bilder, auch für Texte. Aber ich habe dann auch mal in Berlin einer Reihe von Abgeordneten vorgeschlagen, man könnte das ja generalisieren jenseits von KI und vielleicht sagen: Diese Inhalte sind nicht von mir, ob die jetzt eine KI erstellt hat oder jemand anderes. Das wäre wirklich ehrlich. Aber wenn dann die Abgeordneten in ihrer Rede anfangen sagen zu müssen, sie haben ihre Rede nicht geschrieben, sondern die Mitarbeiter, dann macht man sich da natürlich keine Freunde. Es wäre aber wesentlich ehrlicher und auch wieder nicht nur KI-spezifisch.

Moderatorin [00:47:14]

Frau Wendehorst, gerne ergänzen? Gerne auch kurz.

Christiane Wendehorst [00:47:18]

Wir haben ja seit Dezember auch hier einen Draft-Code-of-Practice zur Markierung und ich denke auch, dass wir hier bald etwas haben werden. Andere Frage ist, wie sinnvoll ist es tatsächlich, hier alle Personen zu zwingen, alles zu kennzeichnen? Führt das zu Produktivitätsverlusten und ist vielleicht das, was wir hier damit erreichen, gar nicht so wichtig. Aber das will ich jetzt nicht ansprechen, weil es wäre eine größere Diskussion.

Moderatorin [00:47:55]

Okay, wir haben noch eine Frage direkt zu Deepfakes und der Kennzeichnungspflicht. Und zwar fangen wir gerne wieder mit Ihnen an, Herr Hacker. Welche Behörden, national oder auch auf EU-Ebene, werden zuständig für die Durchsetzung von Artikel 50 sein, der jetzt auch dieses Jahr in Kraft tritt, also Deepfakes maschinell lesbar zu kennzeichnen?

Philipp Hacker [00:48:16]

Ja, danke. Also das sind in der Tat regelmäßig auch die nationalen Marktüberwachungsbehörden. Es sei denn, wie gesagt, der Omnibus kommt so wie geplant und es handelt sich um VLOPs oder VLOSEs, dann ist durchaus möglich, dass das an die Kommission geht. Aber bisher sind das die nationalen Behörden. Was insgesamt, wir sehen die europaweite Tragweite dieser Skandale, die da teilweise entstehen, vielleicht auch nicht der ganz richtige Weg ist. Auch da kann es dann, Stichwort Erpressbarkeit, Probleme geben, wenn beispielsweise die deutsche oder die französische Behörde da besonders gegen sagen. Wenn man gegen Grok oder andere vorgeht, stellt man sich natürlich stärker ins Schussfeld und dann können wieder Zölle kommen, wie wenn 13 oder 15 Soldaten nach Grönland fliegen. Also insofern macht das manchmal schon Sinn, auch aus geostrategischer Perspektive, glaube ich, das in Europa zu zentralisieren. Und das wäre dann auch stärker der Fall, wenn man diese VLOP- und VLOSEs-Regelung nimmt. Denn das betrifft momentan ja vielfach Systeme, die gerade integriert sind oder werden in diese Plattform. Noch interessant ist, dass es auch Erwägungen gibt, jetzt im Rahmen des digitalen Omnibus die Vorschriften für Deepfakes noch einmal erheblich nachzuschärfen. Das halte ich grundsätzlich, ehrlich gesagt, auch für sehr sinnvoll. Da muss man aber schon im Einzelnen noch mal differenzieren. Also das Problem ist ja wahrscheinlich allen bekannt mit Grok und Nudification. Auf der einen Seite kann man sagen, man setzt einen neuen Verbotstatbestand auf. Und zwar für Modelle, die spezifisch dafür geschaffen sind, pornographische und andere Deepfakes, die sexualisiert herabwürdigen, zu erstellen. Da gibt es leider tausende davon. Es gibt ein tolles Paper von Brent Mittelstadt darüber. Die haben das, angeguckt bei GitHub und anderen, großen Plattformen wie Hugging Face. Da sind diese Modelle zu haben und damit kann man dann allerlei Unsinn anstellen, der wirklich für die Betroffenen sehr harmvoll ist. Da wäre ich persönlich sehr dafür bei allgemeinen Modellen, GPAI-Modellen, die ganz viele verschiedene Sachen machen. Das wird aber kompliziert. Da ist es typischerweise, im Einzelnen nicht so einfach zu sagen, ist das ein Verstoß gegen Artikel 55, also gegen die Risikominderungspflichten der Modellbetreiber. Wie gesagt, das ist im Einzelnen relativ schwierig. Was hier vielleicht schwierig wäre, wäre zu sagen, jedes Modell, das grundsätzlich so etwas tun kann, ist verboten. Weil dann in der EU im Grunde sämtliche Bildgeneratoren sofort vom Markt gehen müssten. Das wäre wiederum ein bisschen mit Kanonen auf Spatzen geschossen, auch wenn es hier vielleicht eher Raubvögel sind. Aber ich würde sagen, man könnte an einen Verbotstatbestand denken, der grundsätzlich dieses auch in allgemeinen Modellen verbietet, aber dann eine Ausnahme hat, wenn State-of-the-Art-Safeguards beachtet wurden. Also es ist eben nicht in allen Fällen möglich, das zu verhindern, aber es müssen eben hinreichende Vorkehrungen getroffen werden.

Moderatorin [00:51:41]

Okay, also es muss auf jeden Fall noch mal nachgeschärft werden im Gesetz. Entschuldigung, dass ich Sie unterbreche. Aber wir sind schon über der Zeit und ich würde gerne noch ein paar Fragen durchkriegen, und zwar an Frau Wendehorst. Vielleicht geht es ja auch, die in einigen wenigen Sätzen zu beantworten. Es geht um Urheberrechtsschutz. Wie werden kreativ arbeitende Menschen und ihre Werke im AI Act geschützt? Werden KI Anbieter dafür eine regelmäßige Abgabe zahlen müssen, wenn sie kreative Werke als Trainingsmaterial nutzen müssen oder nutzen möchten?

Christiane Wendehorst [00:52:10]

Also zunächst mal in der KI-Verordnung steht da nicht so viel drin. Es steht im Artikel 53 für die Anbieter großer KI-Modelle mit allgemeinem Verwendungszweck, dass sie eben unter anderem eine Strategie zur Einhaltung des Urheberrechts der Union vorlegen müssen. Einschließlich, da wird Bezug genommen auch auf die Vorschriften zum Text and Data Mining, der sogenannten DSM-Richtlinie, also der Digital-Single-Market-Richtlinie. Da geht es darum, unter welchen Umständen

man eben hier Text and Data Mining betreiben kann. Im Großen und Ganzen ist das derzeit eben noch eine Frage des Urheberrechts. Wie dieses geltende Urheberrecht auszulegen ist, ist zurzeit hoch umstritten. Vor kurzem ist ja die Entscheidung des Landgericht (LG) München zur GEMA durch die Medien gegangen. Da ging es darum, dass eben hier eine KI mit Liedtexten, die urheberrechtlich geschützt waren, trainiert wurde und man mit dieser generativen KI dann diese urheberrechtlich geschützten Liedtexte rekonstruieren konnte mit gewissen Prompts. Also wenn man dann gesagt hat, wie schön, dass du geboren bist, dann hat die KI mit ganz hoher Wahrscheinlichkeit als nächste Zeile ausgespuckt: Wir hätten dich sonst sehr vermisst. Und das hat hier Rolf Zuckowskis Rechte verletzt. Das ist noch nicht rechtskräftig, dieses Urteil. Da werden wir mal sehen, wie es ausgeht. Jedenfalls hat das LG München gesagt, im Modell selbst ist hier ein potenzieller Urheberrechtsverstoß erfolgt. Das ist eine Vervielfältigung von Werken, die eigentlich der Zustimmung bedürfte, als auch nachher bei den Outputs, wenn da eben sozusagen mit hoher Wahrscheinlichkeit bei alltäglichen Prompts der Liedtext herauskommt. Wie das ausgeht, werden wir sehen. Es ist derzeit sehr spannend. Aber keine Frage der KI-Verordnung selber, sondern bestimmter Vorschriften des Urheberrechts.

Moderatorin [00:54:29]

Wenn es keine Frage der KI-Verordnung selber ist, Herr Hacker, möchten Sie dann da noch was substanzielles zu beitragen? Sonst springe ich zur nächsten Frage.

Philipp Hacker [00:54:37]

Ganz kurz wollte ich nur den Journalistinnen und Journalisten nahelegen, es läuft jetzt die Revision der zugrunde liegenden DSM-Richtlinie. Und deshalb glaube ich, ist dieses Jahr relativ entscheidend für Urheberrecht und KI. Wie Christiane Wendehorst gesagt hat, nicht im Rahmen und nicht primär im Rahmen des AI Act. Aber da tut sich soviel, dass es auch noch mal vielleicht was für ein eigenes Press Briefing wäre. Das ist extrem spannend und das hat wirklich das Potenzial, auch die KI-Nutzung und die KI-Entwicklung in Europa nachhaltig zu verändern, weil es da wirklich die großen Geldbeträge gibt.

Moderatorin [00:55:13]

Okay, dann schaffen wir vielleicht noch ein oder zwei Fragen. Erst mal an Sie, Herr Glauner. Und zwar angesichts der sozialen Probleme, die wir derzeit als Folge einer stark profitorientierten digitalen Industrie beobachten, stellt sich die grundlegende Frage, ob die Finanzierung der Entwicklung von KI-Systemen über Venture Capital noch zeitgemäß ist. Und gibt es da alternative Finanzierungsmodelle aus Ihrer Sicht?

Patrick Glauner [00:55:36]

Ja, wenn heute ein Start-Up schnell wachsen möchte, ist Venture Capital eine der Lösungen. Es ist eben ein Ansatz, der jetzt in Deutschland nicht so beliebt ist wie in den USA. Die Idee durch Venture Capital ist ja erstmal, dass die Start-Ups am Anfang große Verluste einfahren, und die Investoren natürlich das Ziel haben, dass die Unternehmen profitabel werden, dass die Geschäftsanteile an Wert steigern. Das ist in den USA, in China sehr stark ausgeprägt und dem können wir uns auch nicht entziehen. Ich habe selbst mein Beratungsunternehmen. Ich bin immer froh, Profit zu machen und nicht abhängig von anderen zu sein. Wenn man eben jetzt nicht Beratung macht, sondern High-Tech entwickelt, muss man schnell wachsen können und dafür ist Venture Capital relevant. Und das ist einfach, glaube ich, ein Ansatz, dem wir uns nicht entziehen

können und nur hoffen, organisch zu wachsen. Das geht so langsam und dann ziehen eben die Unternehmen in China und den USA oder in Großbritannien an uns vorbei.

Moderatorin [00:56:46]

Mhm. Okay, alles klar. Gut, dann wir haben schon sieben Minuten überzogen. Dann würde ich sagen, ist das vielleicht jetzt kein besonders positiver Abschluss für das Ganze, aber doch zumindest ein Abschluss und vielleicht auch ein Blick auf die Zukunft, was noch wichtig sein könnte. Ich weiß nicht, Herr Hacker, ist Ihre Hand noch oben, weil Sie noch was dazu ergänzen möchten? Okay, also einfach nur noch so. Alles klar. Gut, dann haben wir ein bisschen überzogen. Danke, dass Sie das mitgemacht haben. Danke, dass Sie sich überhaupt Zeit für unsere Fragen genommen haben. Danke auch an die Journalistinnen und Journalisten, dass sie so eifrig Fragen gestellt haben. Im Laufe des Tages werden wir eine Audioaufzeichnung, eine Videodatei und ein maschinell erstelltes Skript vermutlich innerhalb der nächsten halben Stunde zur Verfügung stellen nach diesem Meeting. Darauf können Sie zugreifen über den Link in der Reminder-Mail, die Sie bekommen haben. Wir werden im Laufe des Tages über einen von diesen Links auch noch ein redigiertes Transkript zur Verfügung stellen, das Sie dann gerne dazu benutzen können. Danke, dass Sie dabei waren. Ich wünsche Ihnen noch einen schönen Tag und bis zum nächsten Mal. Tschüss.

Ansprechpartnerin in der Redaktion

Samantha Hofmann
Redakteurin für Digitales und Technologie

Telefon +49 221 8888 25-0
E-Mail redaktion@sciencemediacenter.de

Impressum

Die Science Media Center Germany gGmbH (SMC) liefert Journalisten schnellen Zugang zu Stellungnahmen und Bewertungen von Experten aus der Wissenschaft – vor allem dann, wenn neuartige, ambivalente oder umstrittene Erkenntnisse aus der Wissenschaft Schlagzeilen machen oder wissenschaftliches Wissen helfen kann, aktuelle Ereignisse einzuordnen. Die Gründung geht auf eine Initiative der Wissenschafts-Pressekonferenz e.V. zurück und wurde möglich durch eine Förderzusage der Klaus Tschira Stiftung gGmbH.

Nähere Informationen: **www.sciencemediacenter.de**

Diensteanbieter im Sinne MStV/TMG
Science Media Center Germany gGmbH
Schloss-Wolfsbrunnenweg 33
69118 Heidelberg
Amtsgericht Mannheim
HRB 335493

Redaktionssitz
Science Media Center Germany gGmbH
Rosenstr. 42–44
50678 Köln

Vertretungsberechtigter Geschäftsführer
Volker Stollorz

Verantwortlich für das redaktionelle Angebot (Webmaster) im Sinne des §18 Abs.2 MStV
Volker Stollorz

science
media center
germany