25.01.2024

Transkript

„Endspurt beim AI Act – Was steckt drin in der KI-Regulierung der EU?"

Experten auf dem Podium

- **Prof. Dr. Philipp Hacker**
  Professor für Recht und Ethik der digitalen Gesellschaft, Europa-Universität Viadrina Frankfurt (Oder)
- **Prof. Dr. Björn Ommer**
  Leiter der Computer Vision & Learning Group, Ludwig-Maximilians-Universität München (LMU)
- **Bastian Zimmermann**
  Redakteur für Digitales und Technologie, Science Media Center Germany,
  und Moderator dieser Veranstaltung

Mitschnitt

- Einen Videomitschnitt finden Sie unter: https://www.sciencemediacenter.de/alle-angebote/press-briefing/details/news/endspurt-beim-ai-act/
- Falls Sie eine Audiodatei oder eine Sprecheransicht des Videomittschnitts benötigen, können Sie sich an redaktion@sciencemediacenter.de wenden.

Transkript

Moderator [00:00:00]

Hallo liebe Journalistinnen und Journalisten, herzlich willkommen zu unserem zweiten virtuellen Press Briefing zum AI Act. Ich bin Bastian Zimmermann, ich bin Redakteur beim Science Media Center und bei mir habe ich heute die beiden Experten Herrn Hacker und Herrn Ommer. Erst einmal vielen Dank, schön, dass Sie da sind. Die Besetzung hat sich wie Sie sehen geändert, Herr Kettemann konnte leider aus einem privaten Grund nicht und Björn Ommer ist noch spontan dazu gekommen. Also erstmal noch mal vielen Dank an Sie, dass das so schnell geklappt hat.

Die EU hat sich jetzt auf die wahrscheinlich finale Version des AI Acts geeinigt, die wurde dann auch am Montag prompt geleakt. Anfang Dezember gab es die erste Einigung, wir hatten dazu ein Press Briefing. Trotzdem ist es danach noch zu Änderungen gekommen, insbesondere bei der Gesichtserkennung wurden die erst verkündeten Beschränkungen zum Teil noch aufgeweicht. Um jetzt den aktuellen Stand, letzte Änderungen und auch die Einschätzung aus KI-Forschungsperspektive zu besprechen, habe ich heute die beiden Experten hier.

Bevor ich gleich zur Vorstellung komme, noch kurz an Sie da draußen ein Hinweis: Stellen Sie Ihre Fragen bitte über die Fragefunktion von Zoom, also den F&A-Knopf da unten, stellen Sie die auch gerne jetzt schon, dann können wir die gleich im Gespräch stellen.

Dann noch mal vielen Dank an Sie beide, dass Sie da sind, ich stelle Sie kurz vor. Wir haben hier einmal Prof. Dr. Philipp Hacker. Er ist Professor für Recht und Ethik der digitalen Gesellschaft an der Europa-Universität Viadrina in Frankfurt an der Oder. Und Prof. Dr. Björn Ommer, Leiter der Computer Vision & Learning Group an der Ludwig-Maximilians-Universität in München.

Wie immer haben wir auch kurze Eingangsfragen für unsere Experten. Wir fangen mit Ihnen an, Herr Hacker. Was ist denn eigentlich jetzt der aktuelle Stand des AI Acts und was hat sich auf den letzten Metern noch verändert?

Philipp Hacker [00:01:49]

Vielen Dank, dass ich dabei sein darf. Wir haben jetzt den wahrscheinlich finalen Text des AI Acts, der so sehr wahrscheinlich verabschiedet werden wird und das ist auch gut so. Ich denke, wir stehen insgesamt mit diesem Text besser da als ohne und man muss auch festhalten, dass die deutsch-französisch-italienische Fundamentalopposition, die sich da in den letzten Wochen und auf den letzten Metern aufgebaut hat, sehr wahrscheinlich gescheitert ist und auch das würde ich persönlich begrüßen. Der Text ist trotzdem ein politischer Kompromiss und als solcher alles andere als perfekt, das ist klar. Er ist aber insgesamt besser als gar keine Regelung. Warum? Es gibt dafür drei Gründe.

Das erste ist: Wir haben Mindestvorschriften für Basismodelle, sogenannte Foundation Models, die eng zugeschnitten sind, gewisse Praktiken der AI Safety, also der auch öffentlichen Sicherheitsaspekte, berücksichtigen und die relativ verhältnismäßig sind.

Das Zweite ist: Es gibt gewisse Mindestvorschriften für den Schutz der Privatsphäre personenbezogener Daten aber auch von politischen Freiheiten bei der besonders umstrittenen Frage der biometrischen Fernidentifizierung, RBI, Remote Biometric Identification. Da insbesondere wären weitere Schutzmaßnahmen möglich und auch sehr wünschenswert, aber man muss sagen, auch diese Mindestvorschriften, die wir jetzt haben, sind besser als nichts.

Und der dritte positive Aspekt ist der, dass es möglich sein wird, dass Unternehmen sich zusammenfinden – oder auch Entwickler und Entwicklerinnen – und Verhaltenskodizes aufschreiben, die dann an die Kommission übersandt werden und die Kommission kann das dann prüfen und

letztlich diese [Kodizes] für allgemeingültig erklären. Und das ermöglicht eine gewisse Flexibilität und auch die Integration von Branchenkenntnissen und letztlich auch sektorale spezifische Implementierungen des manchmal noch recht vagen Textes des AI Act.

Was sind jetzt kritische Punkte? Und dann kommen wir auch gleich zu den Dingen, die vielleicht ein bisschen überraschend oder neu sind. Ein kritischer Punkt, den ich sehe, ist die Verflechtung mit anderen bestehenden Regelungen. Es ist ja nicht so, dass der AI Act ins Nichts fällt, dass hier Tabula rasa herrscht, sondern er muss eingebettet werden in ein bestehendes, dichtes Geflecht von anderen Regulierungsinstrumenten. Und das ist momentan wirklich noch nicht besonders gut gelungen, finde ich. Wenn wir da an die Medizinprodukte-Verordnung denken, an Banking, an Kreditvergabe, an das Versicherungsrecht, an andere Regelungen in den hoch regulierten Bereichen, dann führt diese Dopplung dazu, dass man einerseits das sektorale Recht hat und jetzt den AI Act obendrauf und das nicht richtig verzahnt ist. Diese Doppelung führt meiner Ansicht nach zu unnötiger und tatsächlich auch innovationsschädlicher Bürokratie.

Das zweite Problem ist, dass wir schon signifikante Compliance-Kosten haben. Das ist für die großen Unternehmen kein Problem, das ist typischerweise auch für Startups kein Problem, die wirklich High Level Foundation Models entwickeln, denn die sind in der Entwicklung sehr teuer. Aber gerade für KMU ist das doch eine erhebliche Hürde, gerade wenn die im Hochrisikobereich sind. Ich finde, den Hochrisikobereich sollte man besser High Impact oder Große-Möglichkeiten-Bereich nennen. Das sind ja auch gerade die Bereiche, wo wir dringend KI brauchen: Medizin, Bildung und Ähnliches, wo auch erheblicher Fachkräftemangel herrscht.

Und das dritte Problem ist tatsächlich, das RBI, also Remote Biometrical Identification. Hier ist es so, dass eine wirklich kohärente europäische Aufsicht nicht gewährleistet ist. Das heißt, momentan ist es so, dass nationale Regulierungsbehörden die Umsetzung dieser Vorschriften und die Einhaltung der Mindestregeln gewährleisten müssen und da haben wir das erhebliche Problem, dass wir in einigen Ländern der EU, zum Beispiel Ungarn, große Rückschritte konstatieren müssen, was den Rechtsstaat anbelangt. Und wenn dann am Ende des Tages eine ungarische Behörde die ungarische Polizei dabei kontrollieren soll, ob sie jetzt Oppositionelle auf Demonstrationen mithilfe von Gesichtserkennung brandmarkt und dann möglicherweise verfolgt, das ist etwas, das nicht zureichend bedacht wurde und wo wir noch stärkere Möglichkeiten des europäischen Eingriffs brauchen, um Missbrauch in solchen Ländern mit demokratischen Rückschritten zu vermeiden. Da ist sonst tatsächlich Missbrauch Tür und Tor geöffnet.

Was sind jetzt überblicksartig, bevor wir dann später im Gespräch zu den Einzelheiten kommen, einige Änderungen oder Überraschungen gegenüber dem politischen Kompromiss, der im Dezember gefunden wurde? Das Erste, was schon mal spannend ist, sind Übergangsfristen. Es ist nämlich so, dass für Basismodelle, Foundation Models, die eigentliche Frist bis zur Umsetzung der Vorschriften des AI Acts zwölf Monate beträgt. Wenn aber diese [Modelle] schon existieren zum Zeitpunkt des Inkrafttretens des AI Acts, dann sind es 24 Monate. Da gibt es also eine größere Gnadenfrist, auch eine gewisse Bevorzugung muss man sagen für Anbieter, die bereits am Markt sind. Da kann man sich fragen, ob das so sinnvoll ist. Ich finde das nicht besonders sinnvoll, aber es ist zunächst mal eine gewisse Überraschung und etwas, das man konstatieren muss. Es gibt weiterhin auch eine sehr spezifische Ausnahmeregelung versteckt in Artikel 83, Absatz 2 für am Markt befindliche Hochrisikomodelle. Die sind nämlich erst einmal vollständig ausgenommen, wenn sie nicht eine signifikante Veränderung erfahren, nachdem der AI Act in Kraft getreten ist. Auch das entspricht eigentlich nicht wirklich den Prinzipien des Sicherheitsrechts. Im Produktsicherheitsrecht ist es sonst eigentlich so, dass [sich] alles, was am Markt befindlich ist, auch zu dem Zeitpunkt, in dem eine Verordnung beispielsweise in Kraft tritt, dann daran halten muss.

Zweite Änderung ist im Urheberrecht. Da ist es so, das würde ich auch sehr begrüßen, dass da klargestellt wurde, dass diese Dokumentation, die die Foundation Model Provider bieten müssen, um zu sagen, welche Daten sie genutzt haben, stark in den Anforderungen zurückgeschraubt wurde. Es ist also jetzt nicht so, dass man bei 20 Milliarden Datenpunkten bei jedem einzelnen Datenpunkt

untersuchen muss, ob da möglicherweise urheberrechtlich geschütztes Material genutzt wurde oder nicht, sondern es ist ausreichend, wenn man eine Zusammenfassung bietet über die Datensätze, die benutzt wurden und noch bestimmte Erläuterungen dazu gibt. Da wird es auch ein Template geben, also ein Muster seitens des AI Office, das vereinfacht das Ganze ganz erheblich und das ist sehr sinnvoll.

Dritter Punkt: Nachhaltigkeit. Das ist leider fast komplett rausgeflogen. Das ist vielleicht ein bisschen überraschend, aber dann auch nur beschränkt, weil das sicherlich ein Punkt war, der auf dem politischen Parkett geopfert wurde, um eine Einigung zu erhalten. Wir haben lediglich eine Informationspflicht hinsichtlich des Energieverbrauchs bei den General Purpose AI Models, ansonsten keine Bestimmung darüber. Das finde ich eine verpasste Gelegenheit.

Und schließlich das, was wahrscheinlich die meisten beschäftigen wird: RBI. Dazu noch mal ganz kurz als Einordnung: Das sind Regeln, die einen gewissen Mindestschutz vorsehen und die Mitgliedsstaaten können auch noch weitergehen und noch weitere Schutzvorschriften verankern. Die Regeln im AI Act bieten keine eigene Rechtsgrundlage für die Mitgliedstaaten oder für die Polizeibehörden. Es ist also mitnichten so, dass etwas, was jetzt nach dem AI Act möglich ist, deshalb auch schon erlaubt wäre. Diese Erlaubnis müssen die Mitgliedstaaten erst noch selbst erteilen und die muss dann explizit in den Rechtsvorschriften der Mitgliedstaaten verankert werden. Dennoch gibt es da drei Hauptkritikpunkte. Das erste ist, dass es reicht, dass eine unabhängige Verwaltungsbehörde Echtzeit-RBI genehmigt. Das ist schwierig, weil natürlich eine Verwaltungsbehörde nicht typischerweise unabhängig ist wie eine Justizbehörde und wir haben auch in einigen Ländern [wie] Polen, Ungarn gesehen, dass es da sehr schnell gehen kann, dass auch formell unabhängige Behörden eben nicht mehr wirklich materiell unabhängig sind. Dann haben wir das schon angesprochene Problem der Überwachung der Einhaltung der Vorschriften durch die Mitgliedstaaten selbst. Das ist problematisch. Und wir haben das generelle Problem, dass es so einen Function Creep geben kann. Wenn eine Überwachungsarchitektur einmal eingerichtet ist, dann gibt es verständlicherweise seitens der Sicherheitsbehörden immer das Bedürfnis, das dann noch für andere Fälle einzusetzen und das ist auch in dem Fall leider nicht auszuschließen. Und schließlich was nicht die Echtzeitüberwachung anbelangt, sondern die Post RBI, so nennt man das, also die Gesichtserkennung im Nachhinein und ähnliche Remote-Biometrical-Idenitication-Techniken, da sind die Mindestvorschriften sehr vage und sehr zurückgenommen, viel zu schwach meiner Ansicht nach. Da gibt es jetzt im Erwägungsgrund 58e lediglich einen allgemeinen Verweis auf die Verhältnismäßigkeit. Es gibt ein Verbot der wahllosen Überwachung und ein Verbot der Umgehung von den Vorschriften, die für Echtzeit-RBI vorgesehen sind. Das ist meiner Ansicht nach zu wenig, da hätte man auch noch klarer sicherstellen müssen, dass hier gewisse weitere Mindestanforderungen gewährleistet sind, einfach um zu verhindern, dass dann ein paar Tage oder so gewartet wird und dann beispielsweise zu politischen Zwecken diese Vorschriften missbraucht werden.

Moderator [00:11:44]

Vielen Dank, Herr Hacker. Sie haben schon einige von den Fragen, die ich mir aufgeschrieben habe, im Eingangsstatement erschlagen. Aber das ist ja kein Problem. Dann kommen wir jetzt zu Herrn Ommer mit der Frage: Wie beurteilen Sie den AI Act aus KI-Forschungsperspektive?

Björn Ommer [00:11:58]

Vielen Dank. Freut mich, dass ich auch in dieser Runde mit Ihnen über den AI Act diskutieren kann. Wie wir alle wissen, gingen die Trilogverhandlungen eine gute Weile und in dieser Zeit hat sich viel verändert. Ich glaube, auf alle Partner ist mit der Zeit etwas zugekommen, mit dem sie zu Beginn vermutlich nicht gerechnet haben. Diese Technologie hat sich so schnell so exponentiell weiterentwickelt, dass viele Dinge, über die am Anfang des Diskurses gesprochen wurde, am Ende nicht mehr so recht zusammengepasst haben. Gerade im letzten Jahr gab es dabei eine Menge an

Bewegung und ich denke, einige Bewegungen auch im Vertragstext, die deutlich positiv gewesen sind, wie Philipp Hacker gerade eben schon zum Ausdruck gebracht hat. Wir kommen im letzten Jahr aus einem Punkt heraus, bei dem noch darüber geredet wurde, dass es böse Algorithmen und gute Algorithmen gibt und mittlerweile haben wir bei dem Text jetzt etwas vorliegen, das diskutiert hat, dass es die Anwendungsgebiete sind, die als kritisch zu beurteilen sind. Denn, jetzt kommen wir zu einer technologischen Fragestellung, bei generativer KI, um die es hier primär gehen wird bei den kritischen Punkten, handelt es sich um eine mächtige Ermöglichungstechnologie. Eine Ermöglichungstechnologie, der wir nicht um ihrer selbst willen nachgehen, sondern wegen den Dingen, die auf sie aufbauend hinten heraus möglich gemacht werden. Und das macht es so unendlich schwierig, im Vergleich zu anderen Technologien, zu sagen: Die wollen wir nicht oder die mögen wir haben, weil wir damit effektiv einen gesamten Blumenstrauß eliminieren würden oder auch zulassen würden. Und dementsprechend begrüße ich es, dass in diesem Diskurs jetzt immer mehr in die Richtung gegangen wird, sich auf Applikationsfelder zu konzentrieren.

Der Diskurs und das Verhandeln hat allerdings ein paar fundamentale Probleme gehabt, mit denen er sich auseinandersetzen sollte, bei denen die Quadratur des Kreises nur hinreichend schwierig gelingen kann und die befinden sich genau in dieser Schnittmenge von sehr mächtigen Modellen, insbesondere Foundation Models, die sehr divers einsetzbar sind, bei denen man dementsprechend sehr diverse Anwendungen hat, die dadurch möglich sind. Anwendungen, die von der Gesellschaft als solche gewünscht werden und von der Wirtschaft auch und solche, [bei denen das nicht] der Fall wäre. Da man jetzt nicht eine Technologie eliminieren kann und damit die Probleme als Ganzes im Kern erschlagen kann, ist es schwierig, diese auseinanderzudividieren.

Gleichzeitig möchte der AI Act Transparenz schaffen, was ich sehr begrüße und was auch wichtig ist für eine Technologie, die von unserer Gesellschaft in einem demokratischen Konsens von verschiedenen Staaten akzeptiert werden sollte. Es ist enorm wichtig, dass diese Transparenz aufgebaut wird, um nicht größeren Fallout als solches zu produzieren, während wir auf der anderen Seite viele Firmen haben, die in einer anderen Liga spielen, als es vielleicht die wenigen großen Tech-Firmen in den USA sind und die als solche, weil sie noch eher kleinere Pflänzchen sind, zuerst einmal unterstützt werden sollen. Das führt dazu, dass wir uns gerade bei diesen sehr mächtigen Modellen in einem Schnittfeld befinden, was relativ schwierig aufzulösen ist. Der AI Act versucht dort [eine] gewisse Balance einzugehen, indem er zum einen die Schwellen gesetzt hat bei Compute, das heißt nur bei Modellen, die eine gewisse Größe überschreiten, geht man davon aus, wenn es jetzt Foundation Models sind zum Beispiel, dass sie per definitionem schon kritisch sind.

Dann stellt sich die Frage: Wie gehen wir mit SMEs und mit Open Source um. Gerade bei Open Source argumentiert das aktuelle Papier, was verfügbar ist, dass das für Transparenz sorgen würde, was sicherlich viele Forscher in der letzten Zeit als solches auch nochmal an die Kommission und an andere Partner herangetragen haben und begrüßt das und gewährt deswegen Ausnahmen – mit der Einschränkung jedoch: Wenn es sicherheitskritische Dinge sind, dann gilt das wiederum nicht. Und hier sieht man schon ein Spannungsfeld: Was machen wir jetzt mit sehr mächtigen Modellen, die Open Source sind, aber potenziell kritisch angewendet werden können?

Und das führt uns in den Bereich, den ich als solches hier gerne kurz hervorheben würde. Uns liegt jetzt ein Textentwurf vor, der wahrscheinlich als solches dann auch verabschiedet wird, aber es gibt noch einiges, wie Philipp Hacker gerade eben indirekt erwähnt hat, noch zu klären, wenn das nachher ausgeführt werden soll. Und in diesem Ausführungsprozess, der dann auch noch nationalstaatlich natürlich durchgebracht werden muss, liegt nach hinten heraus eine Menge an Potenzial, dass das in die eine oder in die andere Richtung gehen kann.

Und hier kommt jetzt der Kern, nach dem Sie gerade eben gefragt haben, Herr Zimmermann: Wie schätze ich das aus technologischer Sicht ein. Wir wollten mit dem AI Act Rechtssicherheit schaffen, die ich als solche sehr stark begrüßen würde für unseren europäischen Bereich, damit Verbraucherinnen und Verbraucher wissen, was auf sie zukommt mit dieser Technologie. Und damit gleichzeitig die Firmen, insbesondere die kleinen Firmen, die wir in Europa haben – und die Startups –

wissen, worauf sie sich einlassen und entsprechend Gelder einwerben können oder gewisse Technologien auch nicht verfolgen, weil die hier nicht als solche gewünscht werden. Da jetzt allerdings vieles genau in diesen Schnittfeldern, die ich gerade angefangen habe zu umreißen, über die wir sicherlich gleich noch ein bisschen mehr reden werden, noch nicht ausbuchstabiert ist, nachher Verfahrensvorschriften sind, die noch im Nachhinein potenziell auch sogar noch nationalstaatlich diskutiert werden müssen, sehe ich genau dieses Grundziel, schwarz und weiß, klare Regeln zu schaffen, noch etwas kritisch in dem aktuellen Entwurf, wie er dort ist.

Das ist das eine Problem. Man kann natürlich aus politischer Sicht sagen, dass man sich jetzt um sehr, sehr viel gekümmert hat und hier auch sicherlich mit einem guten Impetus dahinter. Die Frage ist nur, inwiefern es jetzt den Akteuren hilft und welchen Akteuren es hilft, wenn wir so viele Graustufen in diesem Bereich noch drin haben. Große Firmen werden sich diese Regulatorik sicherlich leisten. Wie sieht das mit kleineren Firmen in diesem Fall aus? Wir möchten nicht noch einen Moat, einen Wassergraben produzieren, bei dem diejenigen, die sich sowieso schon auf Regulatorik einstellen mussten, in der Lage sind, aber es den Kleineren in diesem Fall dann doch zu riskant wird. Das ist im Moment nicht beantwortet worden, das wird sich jetzt erst in der weiteren Ausgestaltung zeigen. Dementsprechend würde ich sagen, dass noch nicht das letzte Wort gesprochen ist, was die wirklichen Implikationen für unseren Wirtschaftsraum hier auf unserem Kontinent sein werden mit diesem Text.

Und das ist etwas schade. Man hätte sich natürlich jetzt gewünscht, dass wir nach diesen ganzen Diskussionen möglichst wenig Graustufen in diesem Bereich haben. Das ist auch der Tatsache geschuldet, dass man möglichst breit an alles denken möchte. Bei einer Technologie, die sich rapide weiterentwickelt, nimmt man damit in Kauf, dass man über gewisse Dinge nur fuzzy [unscharfe] Aussagen macht. Wenn das passiert, dann hilft das vermutlich weder den Verbrauchern noch den entsprechenden Firmen, die in diesem Bereich tätig, sind. Die Ausnahmen, die eingebaut sind, insbesondere zum Beispiel auch für kleine und mittelständische Firmen, begrüße ich als solches, dass jetzt an diese explizit gedacht wurde und sie im aktuellen Entwurf als solche hervorgehoben werden, aber wie das genau umgesetzt worden ist, dazu sagt der aktuelle Text nichts.

Und der letzte Punkt von meiner Seite ist, dass in vielen Rechtskontexten – hier in Europa ein bisschen weniger, in den USA noch viel mehr – bei den Implikationen, die KI mit sich bringt, ein wesentliches Problem gewesen ist, dass zuerst klargestellt werden muss, was überhaupt dann erlaubt ist, wenn negative Dinge herauskommen, die als solche auch verurteilen zu können. Ich hoffe, dass mit dem Text hier mehr Klarheit darüber entsteht, dass zumindest Post hoc gewisse Dinge verfolgt werden können. Ich glaube, bei vielen Fragestellungen, über die wir reden, ist das der kritischste Teil, dass wir entscheiden können, was wir haben wollen und was wir nicht haben wollen. Mit welcher Technologie Dinge, die nicht rechtskonform sind, erzeugt werden, ist dafür in vielen Fällen sekundär. Und da kann man noch mal hinterfragen, was man dann wirklich alles in so einem Papier ausbuchstabieren möchte. Wenn es mir schlussendlich egal ist, mit welcher Technologie etwas Schlimmes gemacht wurde, ich nur definieren möchte, dass das nicht meinem Rechtsverständnis entspricht, dann sollte man das als solches eher noch nach vorne stellen als Technologien, Herangehensweisen, entsprechende Limitierungen.

Moderator [00:20:57]

Vielen Dank erst mal, das hat auch schon einiges von den weiteren Sachen, die ich noch ansprechen wollte, bereits erwähnt. Sie haben das jetzt sehr differenziert klar gemacht. Es gab die Kritik, dass der AI Act jetzt der Forschung und Wirtschaft im KI-Bereich in der EU schaden würde. Sie haben jetzt gesagt, Herr Ommer, das kann man jetzt noch gar nicht so genau sagen. Habe ich das richtig verstanden oder sehen Sie da vielleicht schon eine Tendenz, weil das ja schon eine Kritik ist, die häufig geäußert wurde?

Björn Ommer [00:21:25]

Man sieht gewisse Tendenzen. Ich bin allerdings noch vorsichtig zu sagen, was schlussendlich herauskommt, weil natürlich auch die Kommission, alle Partner an diesem Trilog sich dieses Problems bewusst sind. Auf Nationalstaatenebene – wir haben das gerade eben mit Deutschland, Frankreich, Italien gesehen – ist auf der letzten Meile erkannt worden, welche potenziellen Probleme das bedeutet, wie man damit umgehen muss und wie das zu bewerten ist. Das sind alles noch einmal andere Dinge, aber zumindest ist mittlerweile erkannt worden, dass es auch potenzielle Konsequenzen geben kann. Wenn wir eine enorm mächtige Technologie haben, die sehr breit einsetzbar ist, haben wir dieses Problem, wie wir das entsprechend regulieren wollen. Bei der Atombombe, als die sie bezeichnet worden ist, ist das relativ einfach. Die hat einen Zweck, etwas zu zerstören, aber sie ist für etwas Konstruktives nicht wirklich gedacht. Bei generativer KI, nicht nur eine Dual-Use-Technologie, sondern eine Multi-Use-Technologie, die unendlich viele Möglichkeiten hat, Millionen von verschiedenen Möglichkeiten, ist das natürlich unendlich schwieriger und ich denke, viele kleine Firmen sehen hier gewisse Probleme und sehen aber vor allen Dingen, was Compliance-Regelungen angeht das Problem auf sie zukommen, dass sie etwas polemisch ausgedrückt nachher mehr Anwälte brauchen, als dass sie Entwickler brauchen. Ich hoffe nicht, dass es so weit kommt, aber das ist natürlich die Gefahr, die im Moment als solche gesehen wird.

Moderator [00:22:49]

Herr Hacker noch dazu.

Philipp Hacker [00:22:51]

Daran anknüpfend. Ich sehe das auch genauso, dass es ein ganz erhebliches Problem ist, das mir auch immer wieder berichtet wird, wenn ich jetzt in Berlin mit Startups oder ähnlichen Personen aus der KI-Szene spreche. Ich glaube, das Recht hat da gewisse Möglichkeiten, Rechtssicherheit zu schaffen. Eine gewisse Rechtsunsicherheit ist unvermeidbar, wenn man natürlich so einen Akt auch entwicklungsoffen gestalten will. Rechtsbegriffe sind häufig unscharf, gerade wenn sie mit neuen Technologien zu tun haben und dass es jetzt keine jahrzehntelange Jurisprudenz dazu, Rechtsprechung des BGH oder sowas gibt. Worauf man gespannt sein muss, und das würde ich genau so sehen wie Björn Ommer, ist, wie wird das jetzt umgesetzt erstens in der Standardisierung, also ISO, CEN-CENELEC. Es gibt ja den Normsetzungsauftrag an Standardisierungsorganisationen und diese Standards, die werden dann nach Artikel 40 auch ganz entscheidend sein, um einen Transmissionsriemen zwischen dem Recht und der Technik darzustellen. Wenn dann diese Standards gut sind, wenn die so sind, dass ML engineers die auch verstehen und sagen können: Ah, jetzt weiß ich, was ihr damit meint mit diesem Human-in-the-loop oder so was, nicht irgendwie so fuzzy legal words, sondern dass man sagt, okay, da kommen jetzt konkrete Metriken raus und daran können die Leute sich orientieren. Dann wäre sehr viel gewonnen. Das ist das Eine.

Und das Zweite ist: Es gibt Leitlinien, die dann vom AI Office und vom AI Board, zwei großen Behörden-Instanzen, die jetzt neu geschaffen werden, veröffentlicht werden sollen. Und da wäre auch die Hoffnung, dass die versuchen, möglichst schnell gute Beispiele zu bringen: Das ist das, was wir meinen, was darunter fällt, das ist was, was nicht erlaubt ist und das, was erlaubt ist. Das kennen wir aus dem Data Protection Bereich und das ist häufig auch sehr hilfreich. Diese Anwendungsrichtlinien haben keine Rechtsqualität, aber häufig orientieren sich die Gerichte sehr nah dran. Und deshalb würde ich wie Björn Ommer sagen: Wir müssen jetzt abwarten, wir haben das Gerüst, aber die Ausfüllung wie bei so einem Fachwerkhaus, das kommt alles jetzt erst noch. Und da kommt es ganz entscheidend auf die Qualität und auf die Schnelligkeit an, das muss eigentlich alles stehen, wenn der der AI Act in Kraft tritt.

Und wann tritt er in Kraft: Im Sommer wird er wahrscheinlich im Amtsblatt veröffentlicht werden. Dann sind es erst einmal sechs Monate, bis die Regeln zu den verbotenen Praktiken in Kraft treten, zwölf Monate, bis die Foundation Model Rules in Kraft treten, mit dieser Ausnahme 24 Monate, wenn die schon im Markt sind. 24 Monate bis zu den High-Risk-Regeln und zwar den High-Risk-Regeln, die in Annex III sind. Das sind also diese spezifischen Beschäftigungen, Credit Scoring, Migration und so weiter. Und 36 Monate für die, die spezifisch in Annex II stehen. Das sind die jetzt schon hoch regulierten Teile, zum Beispiel Medical und andere, die jetzt schon im Produktsicherheitsrecht sind. Also da ist schon noch ein bisschen Zeit vorgesehen, aber sechs Monate und zwölf Monate, das ist eine knappe Zeit. Das ist letztlich in weniger als anderthalb Jahren, da muss man schon auch wirklich dann Butter bei die Fische geben.

Björn Ommer [00:26:25]

Wenn ich das nur kurz anführen darf: Es ist natürlich jetzt eine Menge Dynamik drin, denn derjenige, der diese Ausführung als Erstes implementiert – ich denke, das hat die Rechtsvergangenheit gezeigt –, der hat natürlich eine gute Chance, dass sich das dann auch als solches festsetzt im allgemeinen Diskurs. Und da gibt es nicht diesen festen Zeitpunkt, weil viele Fragestellungen über das, was Phillip gerade gesagt hat, hinaus sich natürlich erst in der Ausführung hinten heraus zeigen werden. Und derjenige, der die als solcher als Erstes erkennt, einen plausiblen Vorschlag macht, der dann von anderen als solcher auch aufgegriffen wird, der wird bei allem Interpretationsspielraum, der sich dort ergibt, natürlich dann vermutlich auch die höchste Chance haben, dass seine Interpretation dann als solche angenommen wird.

Moderator [00:27:08]

Dazu muss es natürlich erst einmal dazu kommen, dass der AI Act jetzt doch verabschiedet wird. Und darum dreht sich die erste Frage, die wir hier von außen haben. Die stelle ich an Sie, Herr Hacker. Wie hoch sehen Sie die Wahrscheinlichkeit, dass der AI Act auf den letzten Metern doch noch scheitert? Gibt es bei den jüngsten Änderungen Punkte, die neuen Streit provozieren könnten? Und könnten Deutschland, Frankreich und Italien eine Sperrminorität organisieren?

Philipp Hacker [00:27:29]

Die letzte Frage ist leicht zu beantworten: Deutschland, Frankreich und Italien, wenn jedenfalls die Personen, mit denen ich gesprochen habe, richtig gerechnet haben, können das alleine nicht. Aber sie können sich natürlich mit anderen Staaten, die da skeptisch sind, zusammentun, vor allem Ungarn. Die haben schon angekündigt, dass sie das nicht wollen. Das zeigt aber zugleich, dass es sehr viel politisches Kapital verbrennen würde, wenn Deutschland tatsächlich sich an die Seite von Ungarn stellen würde, um gegen den AI Act zu stimmen oder sich zu enthalten. Das wäre schon ein massives Signal. Und da sehe ich jetzt momentan ehrlich gesagt nicht, dass die Bundesregierung sich dazu durchringt. Das wäre doch wirklich ein schwerer Affront gegen die übrigen europäischen Partner, obwohl es natürlich berechtigte Anliegen gibt. Das ist ganz klar. Wie gesagt, das ist ein politischer Kompromiss. Da kann man aus verschiedenen Perspektiven immer noch daran herumdoktern.

Ich glaube ehrlich gesagt trotzdem, dass es eine 85-prozentige Wahrscheinlichkeit gibt, dass das Ganze durchgehen wird. Es gibt eine kleine Wahrscheinlichkeit, dass Frankreich und vielleicht auch Deutschland darauf dringen werden, das Ganze zu verschieben noch einmal, um dann einzelne Nachbesserungen vorzunehmen, was ja per se auch nicht verkehrt wäre. Das hat aber dann wahrscheinlich zur Folge, dass es in die nächste Legislaturperiode rutscht, weil wir einfach in die Wahlen hineinkommen. Und da gilt das alte Brüsseler Sprichwort: Wer möchte, dass ein Akt später verabschiedet wird, möchte eigentlich, dass er gar nicht verabschiedet wird. Das könnte dann

durchaus auch die heimliche Intention sein. Ich glaube aber ehrlich gesagt nicht, dass es dazu kommt. [...] Alle wissen gewissermaßen, was die Stunde geschlagen hat. Wenn wir es jetzt nicht machen, ist es unklar, ob es überhaupt kommt. Und das wäre doch eine massive Blamage auch auf der globalen Bühne, wenn Europa das jetzt nicht schafft.

Björn Ommer [00:29:15]

Um das vielleicht noch kurz zu ergänzen. So eine Filibuster-Politik: Dagegen spricht, dass wir natürlich im Dezember uns schon zusammengerungen haben. Da hätte man es natürlich auch vertagen können, wenn es einem daran läge, den Sommertermin zu überschreiten. Diese Hürde ist nicht gerissen worden. Das spricht natürlich dafür, dass alle Akteure anscheinend die Kosten in der einen Richtung höher als in der anderen sehen.

Moderator [00:29:39]

Also Sie sind beide erst einmal verhalten optimistisch, dass es doch noch klappt. Hier gibt es noch eine Verständnisfrage, die geht auch an Sie, Herr Hacker, wenn ich das richtig deute. Das klingt nach einer juristischen Einschätzung, und zwar, dass mit dem AI Act im Kontext der EU ein Regelrahmen entwickelt wird, der wohl mehr auf Missbrauchsschutz durch staatliche Akteure abzielt oder große Firmen. Wie gilt das dann entsprechend für den Missbrauch durch Privatiers, die durch die KI natürlich auch mächtige Werkzeuge in die Hand bekommen haben?

Philipp Hacker [00:30:05]

Das ist eine gute Frage. Es ist in der Tat so, dass der AI Act wie auch – und das muss man immer betonen – das Parallelwerkzeug, nämlich die Überarbeitung der Produkthaftungsrichtlinie, die dann sagt, wer am Ende des Tages eigentlich zahlen muss, [nur sagt], wer was machen muss. Wer zahlen muss, wenn ein Schaden eintritt, das sagt die Produkthaftungsrichtlinie zusammen mit anderen nationalen Vorschriften, dass diese beiden Rechtsakte abzielen auf Hersteller, also letztlich Entwickler, und gewisse Akteure in der KI-Wertschöpfungskette, vor allem der AI Act. Was nicht wirklich erfasst ist, sind Endverbraucher, die tatsächlich privat handeln, also nicht im professionellen und nicht im geschäftlichen Kontext. Und da könnte man jetzt sagen, das ist ja irgendwie eine Schutzlücke. Das ist aber nicht so, denn die unterliegen natürlich dem ganz normalen Recht. Es gibt Strafrecht, es gibt das Deliktsrecht, das heißt, wenn ich jetzt KI verwende, um – was weiß ich – jemanden wüst zu beleidigen, dann bleibt das eine Beleidigung, unabhängig davon, dass ich KI verwendet habe. Wenn ich eine KI nutze, um Terroranschläge zu planen, dann kann ich genauso wegen Mitgliedschaft in einer terroristischen Vereinigung belangt werden. Da gibt das geltende Recht schon einiges her.

Was der AI Act versucht eigentlich, ist – und das ist vielleicht für das Verständnis auch wichtig, und das ist auch ein Kritikpunkt –, [...]diese bestehende Regulierung, die im Wesentlichen am Ergebnis anknüpft – das [...] passt vielleicht zu dem, was Björn gesagt hat –, wir wollen doch eigentlich wissen: Was darf man, was darf man nicht in unserer Gesellschaft, unabhängig davon, ob das jetzt mit KI gemacht wurde oder nicht. Das heißt, bisher gibt es Regeln, die sagen, man darf nicht diskriminieren, man darf andere nicht verletzen, unabhängig davon, wie man das technisch hinkriegt, ob mit der Faust oder mit dem KI-Werkzeug. Und da besteht die Befürchtung, dass das bei KI nicht reicht, weil das so komplex ist und weil die Leute dann irgendwie nicht verstehen, wie es zustande gekommen ist und so weiter. Und weil es gewisse Marktmechanismen gibt, die vielleicht zu Informationsasymmetrien führen, zu Konzentrationen im Markt und so weiter. Und deshalb versucht man die Regulierung gewissermaßen in die Prozedur, also in die Entwicklung, in die ML-Pipeline hineinzuholen, sodass man da sagt: Ihr müsst aber schon gewisse Datensätze verwenden, die hinreichend divers sind, damit am Ende keine Diskriminierung herauskommt, auch wenn die ja

verboten wäre. Und das kann man durchaus kritisch sehen, dass man sagt, brauchen wir das wirklich, wenn wir diese Endregulierung, diese Ergebnisregulierung ohnehin schon haben. Da kann man sich lange drüber unterhalten. Was aber Fakt ist, ist, dass das diese Ergebnisregulierung bleibt und die bleibt bestehen, eben für die privaten Akteure. Daran müssen die sich eben auch halten. Ich darf auch KI als Privater nicht nutzen, um andere zu diskriminieren. Das unterliegt dann eben dem Allgemeinen Gleichbehandlungsgesetz.

Björn Ommer [00:32:58]

Um da kurz anzuschließen, weil das genau den Punkt betrifft, den ich gerade als eine der kritischsten Stellen ausgeführt habe: Wir haben zwei Dinge. Das eine war immer bisher, dass der Akteur, der entsprechend sich nicht rechtskonform verhält, dass der entsprechend mit dem Recht dann belangt worden ist. Der AI Act selbst versucht das aber nach vorne zu verlagern, dass gesagt wird: Diejenigen, die die Möglichkeiten dafür schaffen, dass jemand anderes etwas machen kann, haben auch eine gewisse Haftung in diesem Fall, die sie eingehen müssen, einen gewissen Haftungskodex, der vorn eingeführt wird. Das ist natürlich schwierig bei einer Technologie, die sehr breit gestreut wird, zu sagen, das möchten wir nicht, weil es das erlaubt, oder das andere ist wiederum in Ordnung. Wir sehen das zum Beispiel bei der Größe der Modelle, bei denen dann gesagt wird, ein Modell ab einer gewissen Größe ist potenziell immer ein kritischer Faktor, der sich dabei einstellt. Dass das Modell nachher in seiner Anwendung potenziell kritisch sein könnte, das hätten wir jetzt schon geregelt. Jetzt gibt es andere Fragestellungen: Wie sieht es aus mit einer Firma, die beispielsweise von einer anderen Firma, die diese Technologie einsetzt, [etwas] anwendet, ohne zu wissen, was darunter [liegt], dieses Basis- oder Foundation Model beispielsweise, was das potenziell an weiteren kritischen Dingen mit sich bringt. Wer haftet in diesem Fall? Und das sind alles Dinge, die jetzt natürlich nach vorne verlagert werden in diesem Diskurs, bei dem es auch gut ist, darüber zu reden, aber die natürlich sehr schwierig trennscharf zu klären sind. Und daraus resultieren jetzt sicherlich einige Probleme, mit denen wir uns in der Zukunft auseinandersetzen werden.

Moderator [00:34:30]

Ich habe hier noch einige Fragen. Eine kurze Nachfrage an Sie, Herr Hacker, wenn Sie kurz darauf eingehen könnten. Wenn mit KI Menschenrechte und Bürgerrechte verletzt werden durch Akteure außerhalb der EU: Wie können sich dann Betroffene hier wehren?

Philipp Hacker [00:34:44]

Erst einmal ist es so, dass wenn KI eingesetzt wird in der EU, dann gilt der AI Act. Es ist nicht so, dass weil KI außerhalb von Europa entwickelt wird und dann aber in Europa eingesetzt [wird], dass das deshalb nicht gilt. Es ist ähnlich wie bei der DSGVO, da ist es ja auch so, wenn ich in Amerika ein Unternehmen bin und Daten verarbeite von EU-Bürgern usw., dann geht das trotzdem. Die zweite Frage ist: Was kann ich denn jetzt machen als [Betroffener]? Und da sind tatsächlich zwei Sachen hinzugekommen noch einmal, die aber auch schon im politischen Kompromiss vom 8. Dezember angedeutet waren. Und zwar erstens gibt es ein Beschwerderecht und zweitens gibt es ein Recht auf Erklärung. Dieses Recht auf Erklärung ist allerdings relativ bescheiden formuliert. Es ist eigentlich ein komplett zahnloser Tiger. Da geht selbst die DSGVO weiter, so wie sie jetzt in der Rechtsprechung mittlerweile interpretiert wird. Da können wir gerne auch noch etwas zu sagen: SCHUFA-Fall, und es gibt es einen spannenden Fall, Uber und Ola in Amsterdam, der da schon deutlich weitergeht. Was man sonst machen kann, ist natürlich gewissermaßen beschränkt, wie immer, wenn ausländische Akteure aktiv sind. Man kann natürlich versuchen zu klagen. Das muss man dann je nach Prozessregelung eventuell in dem Drittstaat machen. Das ist natürlich nicht ganz einfach. Was aber möglich ist, ist eben: Man kann versuchen, darauf hinzuwirken, dass die nationalen

Aufsichtsbehörden tätig werden. Das ist wahrscheinlich das schärfste Schwert. […] Wenn man beispielsweise jetzt in Deutschland ist, dass die deutsche Aufsichtsbehörde sich dieses Unternehmen vorknöpft gewissermaßen und dann versucht, mit den Werkzeugen, die der AI Act an die Hand gibt, also mit Überprüfung, mit Audits und so weiter, mit Vorlagen, dem Herr zu werden. Und wenn die das nicht machen, dann können da Geldbußen entstehen und kann letztlich auch […] der Ausschluss vom EU-Markt kommen.

Moderator [00:36:38]

Okay, also es gibt schon Möglichkeiten. Eine Frage an Sie, Herr Ommer, als einer der oder der Erfinder der Bildgenerierungs-KI Stable Diffusion. Wie sind Sie denn jetzt eigentlich von der Regulierung betroffen, oder Stable Diffusion? Und gibt Ihnen das dann Nachteile gegenüber anderen Bildgenerierungs-KIs wie Midjourney oder Dall-E?

Björn Ommer [00:36:59]

Der aktuelle Text sieht dezidiert für die Forschung – ich bin Lehrstuhlinhaber einer deutschen Universität – sieht für die Forschung im universitären Bereich, aber auch im Firmenbereich Ausnahmen vor, [wodurch das, was wir machen,] gedeckt ist. Das ist natürlich ein Teil, den ich begrüße, da haben die Trilog-Partner direkt gesehen, dass Forschung in die Zukunft natürlich ein Investment in die Zukunft ist und hier entsprechende Steine in den Weg natürlich sehr kritisch wären. Der zweite Punkt [ist], und das hätte es auch anderweitig sehr, sehr schwierig gemacht: Wir haben natürlich eine Forschungsfreiheit, die bei uns grundgesetzlich verankert wäre. Und wenn man gewisse Dinge dort per definitionem aufgrund von irgendwelchen Modellgrößen oder Ähnlichem ausgeschlossen hätte, hätte man damit schon alleine grundgesetzlich relativ große Probleme bekommen, weil es so eine Multi-Purpose-Technologie ist, die in unterschiedliche Richtungen entwickelt wird.

Eine andere Frage stellt sich für – Sie haben jetzt gerade Stable Diffusion erwähnt – für Firmen, die natürlich basierend auf unserer Technologie dann Geld verdienen möchten und das umsetzen möchten. Da kommt man natürlich genau in so einen Bereich herein, das dann das Auditing und ähnliche Dinge eine Rolle spielen. Und auch hier wird es wieder diese Bifurkation geben, dass es sehr große Firmen gibt, die sowieso entsprechende Compliance-Abteilungen, Rechtsabteilungen haben und so weiter, für die das ein weiterer Punkt ist, ein weiteres Kästchen auf ihrer Liste, was dann auch noch abgearbeitet wird. [Für] kleinere Start-ups […] – und das war ja unser Punkt, diese Technologie zu demokratisieren, damit auch kleinere Firmen im Bereich der generativen KI die umsetzen können und wir hier gerade auch im deutschen und europäischen Bereich entsprechendes Wirtschaftswachstum in diesem Bereich erleben werden – für die bedeutet das natürlich jetzt zuerst einmal ein Risiko, weil es neue Rechtsfragen mit sich bringt und leider nicht überall die erwünschte Trennschärfe mit sich gebracht hat. Das werden die Ausführungsbestimmungen jetzt am Ende dann regeln müssen, dass auch für die wieder Rechtssicherheit geklärt wird.

Moderator [00:39:05]

Ja, danke. Eine Frage erst an Sie, Herr Hacker, aber Sie können gerne was hinzufügen, Herr Ommer, weil es dann auch ein bisschen über die KI-Forschung geht. Ist nicht das Problem eigentlich, dass ein Anwender bei generativer KI oft keine Kontrolle darüber hat, ob die KI diskriminiert oder nicht und das gegebenenfalls auch gar nicht bemerkt, also gewissermaßen, dass die KI von sich selbst aus diskriminiert, weil sie es in den Trainingsdaten gelernt hat?

Philipp Hacker [00:39:27]

Ja, das ist eines der Probleme, die da auftreten können. Ob man das jetzt nicht merkt, wenn die KI diskriminiert? Es kommt jetzt sehr darauf an, was man damit macht. Tatsächlich, wenn ich jetzt als Anwender einfach irgendwie unbesehen ein Modell nehme und davon zum Beispiel Jobkandidaten ranken lasse und da gar nicht mehr weiter darauf schaue, ja. Aber so sollte man es auch nicht machen. Das macht ja auch kaum jemand. Man muss dann schon schauen, welche Performance Metrics hat denn dieses Modell? Das ist genau Hintergrund des AI Acts auch, dass genau diese Parameter und diese Metriken offengelegt werden müssen. Es muss auch offengelegt werden, welche Probleme mit Bias bestehen. Das muss man sich dann anschauen als Anwender oder Anwenderin. Und tatsächlich, wenn ich das einsetze und dadurch auch ungewollt diskriminiere, dann kann man mich trotzdem haftbar machen. Und da ist kein Verschulden erforderlich nach dem Allgemeinen Gleichbehandlungsgesetz. Das Problem kann ich natürlich als Anwender nur schwer beheben. Das ist schon richtig. Da gibt es allerdings auch so Postprocessing-Möglichkeiten, wo man versuchen kann, die Ergebnisse dann noch einmal durch einen Filter laufen zu lassen und die dann etwas weniger diskriminierend zu gestalten. Da gibt es einen größeren Forschungsanteil, viele Forschungsarbeiten dazu, da gibt es durchaus Möglichkeiten.

Richtig ist: Wenn die Trainingsdaten schwer einseitig sind, dann ist es relativ wahrscheinlich, dass am Ende, wenn man nicht gut aufpasst als Entwickler, da auch etwas Diskriminierendes [bei] herauskommt. Und genau deshalb hat ja der AI Act jetzt in Artikel 10 ein Data Governance Regime aufgestellt, wo eben versucht wird zu sagen: Die Trainingsdaten müssen ausbalanciert sein in gewisser Weise. Die müssen vor allem auch repräsentativ sein für die Bevölkerungsgruppen, auf [die] dann das Modell später angewandt werden soll. [...] Und das soll es weniger wahrscheinlich machen, dass solche Probleme auftreten.

Aber es ist klar: Wir haben immer dieses Problem der Informationsweitergabe in dieser AI Value Chain. Wir haben immer das Problem, dass es ein gewisses Informationsgefälle gibt, dass gewissermaßen Informationsasymmetrien zwischen den Entwicklern und den Anwendern bestehen. Aber deshalb gibt es jetzt auch Auskunftsansprüche oder wird es eben nach Artikel 28 [geben], nach den Vorschriften über die AI Value Chain, wo genau die Anwender sagen können: Ich brauche diese oder jene Auskünfte jetzt noch, um letztlich compliant, um rechtssicher dieses Modell anwenden zu können. Da gibt es dann wieder neue Probleme mit Geschäftsgeheimnissen und IP-Rechten und so, aber da gibt es auch bewährte Verfahren im Recht, um das letztlich in geordnete Bahnen zu lenken.

Björn Ommer [00:42:11]

Eine sehr spannende Frage, um da direkt anzuknüpfen. Eine sehr spannende Frage, nämlich gerade aus der technischen Seite heraus. Artikel 28 ist jetzt gerade erwähnt worden, auf den hätte ich auch referenziert. Aber es gibt hier, denke ich, zwei Gruppen, die man auseinanderhalten sollte. Das eine sind die privaten Anwender. Hier ist natürlich eine gewisse AI Literacy in Zukunft enorm wichtig, was den Bildungsbereich natürlich noch mehr und immer mehr treffen wird, wenn solche Modelle angewendet werden, dass man als privater Nutzer und Nutzerin natürlich darüber nachdenkt, was man damit macht, wo die Grenzen von dieser Technologie sind und nicht alles für bare Münze nimmt.

Das andere betrifft aber Firmen als Anwender von den Produkten von anderen Firmen. Und hier muss man sich vorstellen, dass man ein Produkt kauft, was man als solches weiterverwendet oder einsetzt und potenziell natürlich haftbar gemacht werden kann für das, was dann die eigene Software, die gewissermaßen auf den Schultern von Giganten schon steht, was die dann hier in diesem Fall produziert. Hier kann man sich vorstellen, dass natürlich durch diesen Rechtsrahmen und die entsprechenden Haftungsregelungen, die dort dargestellt werden, in beide Richtungen auf einmal Verantwortung verlagert [wird] beziehungsweise die dafür [sorgt] hoffentlich, dass diese Modelle dort drunter im eigenen Interesse der Firma, die diese Services bereitstellt, und der anderen, die

diese Services dann nutzen möchten, dass dadurch eine gewisse Absicherung sich einstellt, weil ansonsten man keine Kunden mehr bekommt, wenn die hinten heraus dann haftbar gemacht werden. Und umgekehrt als Kunde möchte man sich natürlich auch nicht den Ruf ruinieren.

Und da hoffe ich natürlich darauf, dass es allein aus marktwirtschaftlichen Gründen [...], ohne dass das jetzt vom Gesetz noch weiter ausdiskutiert werden muss, sich einpendelt, dass diese Modelle eine gewisse Transparenz, und das wäre hier das letzte Stichwort, [bekommen]. Und dort ist im Forschungsbereich gerade ein sehr großes, offenes Feld. Wie kann ich sehr mächtige Modelle bauen, die aber gleichzeitig einen gewissen Grad an Transparenz herstellen? Und ich denke, wir haben in anderen Wirtschaftsbereichen sehr wohl gesehen, dass sich beides nicht ausschließt, dass ich also gut Geld verdienen kann, aber dass ich gleichzeitig auch für gewisse Transparenzen sorgen kann. Wir sehen das im medizinischen Bereich beispielsweise, dass sie keine Pille oder Tablette schlucken, die nicht irgendwo offen war, also Regulierungsbehörden zumindest hineinschauen konnten. Und gleichzeitig kann die Pharmaindustrie natürlich sehr viel Geld damit verdienen.

Moderator [00:44:34]

Also Verpflichtungen auf Anwendungs- und auch auf Herstellungsseite. Ich habe noch eine Frage, die ich vielleicht vor der Abschlussfrage durchkriegen würde, Herr Hacker [...]. Es ist ja jetzt kürzlich der neue EU-Plan bekannt geworden, um Innovationen in KI-Start-ups zu fördern und durch finanzielle Unterstützung und den Zugang zu Supercomputern zu unterstützen. Was halten Sie davon? Vielleicht an Sie zuerst, Herr Ommer, die Frage und dann Herr Hacker kurz zur Ergänzung, bevor wir zur Abschlussfrage kommen.

Björn Ommer [00:45:04]

Ich habe gerade einen kurzen Glitch gehabt im Audio, können Sie sagen noch einmal, um welchen Teil es ging, den Großteil habe ich gehört, aber...

Moderator [00:45:09]

Neuer EU-Plan, um Innovation in Start-ups zu fördern durch finanzielle Unterstützung und Zugang zu Supercomputern.

Björn Ommer [00:45:16]

Richtig, genau. Wir müssen uns alle bewusst machen, dass Computing, Supercomputing haben Sie gesagt, aber eine sehr spezifische Art von Computing, dieses GPU Computing, auf dem die gesamte generative KI fußt, dass das die neue Commodity ist, die diese neue Basistechnologie ist, die für Künstliche Intelligenz so wichtig ist, wie es in der Vergangenheit Strom und Wasser und Ähnliches für unsere Industrie gewesen sind. Und aktuell leisten wir uns auf dem europäischen Kontinent eine sehr große Abhängigkeit von äußeren Akteuren, von äußeren Firmen, die unsere Firmen hier damit bedienen. Wir haben gesehen, wohin solche Abhängigkeiten führen. Wir haben gerade die ganze Zeit über Regulierung gesprochen und Dinge, die wir nicht machen möchten und Ähnliches. Bei Gas beispielsweise, bei Energie, haben wir im letzten Jahr gesehen, dass wir gewisse Dinge auch politisch regulieren möchten. Aber wenn es hier kalt und dunkel wird, dann hört man relativ schnell auf, über die Regulierung zu reden und muss dann doch gewisse Kompromisse eingehen. Und deswegen kann ich nur mahnen und unterstützen, wenn es Bestrebungen gibt, hier europäische Souveränität, was Computing-Infrastruktur angeht, herzustellen.

Wir diskutieren allerdings und werden auch noch eine Zeit diskutieren, auf welche Art und Weise das abläuft, weil es natürlich Bestrebungen gibt, das möglichst groß zu verankern. Aber da wissen

wir alle, dass das natürlich wiederum sehr, sehr lange dauert. Und hier ist der kritische Punkt bei allem Leapfrogging, was als solches avisiert wird: Diese Technologie ist da, Generative KI ist jetzt da. Jetzt sind die Firmen dort, die entsprechend ihre Plätze besetzen wollen und bei denen sich Stakeholder bilden. Und wenn wir das aktuell verschlafen und aktuell bedeutet am besten gestern, dann werden wir in der Zukunft auch diese Technologie verschlafen können. Wir haben jetzt die Chance, das, was wir bei IT hier oder da verloren haben, mit dieser neuen Technologie, die vieles zurück auf Los setzt, noch einmal aufzuholen. Aber wir können auch das verschlafen, wenn wir nicht schnell genug machen. Und deswegen begrüße ich Initiativen, die hier europäische Souveränität gerade im Bereich des Computes [herstellen], aber wohl wissentlich, dass bei ein paar Dingen [...] die EU in der Vergangenheit [nur]erzählt hat, dass Sachen gemacht werden. Aber wir brauchen sehr spezifisches Compute, was für KI sich auch eignet. Da ist nicht irgendwie ein beliebiges dafür nützlich.

Moderator [00:47:34]

Also eine grundsätzlich begrüßenswerte Initiative, aber die Details bleiben abzuwarten. Herr Hacker, noch kurz dazu und dann die Abschlussfrage.

Philipp Hacker [00:47:41]

Ich kann mich nur anschließen. Ich glaube, das ist wirklich nicht zu überschätzen in der Wichtigkeit. Der Zug ist fast schon abgefahren, er ist vielleicht sogar schon abgefahren. Wir sind mal wieder in Europa extrem spät dran. Dank Björn und seinem Team gibt es doch noch gewisse Möglichkeiten, in einzelnen Feldern aufzuschließen. Wir haben natürlich auch ein paar Firmen, die gute Sachen machen, aber insgesamt ist es schon frappierend. Im Jahr 2022 kam ja so eine Studie heraus [...]: 73 Prozent der Modelle in den USA, 15 Prozent aus China, damit bleibt rechnerisch – weil ja noch ein paar in Südostasien und sonst wo sind – weniger als zehn Prozent in der EU. Das sind die großen KI-Modelle. Das ist seitdem nicht besser geworden. Und das ist, genau wie Björn sagt, eine extreme Abhängigkeit. Ich meine, China ist momentan einfach kein verlässlicher Partner. Und wenn wir an Trump 2025 denken, die USA leider auch nur in begrenzter Weise. Und wir laufen jetzt tatsächlich in eine neue Abhängigkeit hinein, wie wir sie gerade bei Öl und Gas gesehen haben. Das ist schierer Wahnsinn eigentlich. Und da kommt diese Initiative wahrscheinlich schon zu spät. Aber es ist trotzdem sehr richtig, genau an diesem Bottleneck einzugreifen.

Aber was mir immer wieder Leute sagen, es gibt ja auch jetzt schon Förderinitiativen in Deutschland. Deutschland legt zum Beispiel ja einen mit einer Milliarde Euro ausgestatteten Fonds für Deep Tech und Climate auf, auch das sehr sinnvoll. Aber häufig sind diese Förderrichtlinien dann an solch schwierige bürokratische Prozesse geknüpft, dass gerade für Start-ups es fast unmöglich ist, diese Dinger einzuwerben. Denn das Geld, das sie einwerben, das müssen Sie direkt in eine Kraft stecken, die das Ding einfach verwaltet. Und das kann halt nicht sein. Es muss wirklich einfacher, unbürokratischer Zugang zu genau dem sein, was wir jetzt für High Quality Compute in dem Bereich brauchen. Ob das wirklich kommt? Da habe ich so ein bisschen meine Zweifel, gerade was das Unbürokratische anbelangt, denn das ist immerhin die EU. Aber es ist auf jeden Fall ein Schritt in die richtige Richtung Und es ist ein Signal, da noch viel mehr zu tun. Und besser gestern als heute.

Moderator [00:49:38]

Vielen Dank. Und wir kommen noch zur Abschlussfrage. Wir fangen mit Ihnen an, Herr Ommer. Die allgemeine Frage: Was ist denn Ihrer Meinung nach jetzt momentan im AI Act und in der aktuellen Debatte um den AI Act der wichtigste Aspekt?

Björn Ommer [00:49:51]

Ich begrüße es, dass wir auf europäischer Ebene uns um Transparenz bemühen. Dass wir dafür sorgen, dass diese Technologie, die für alles fundamental werden wird, was wir wirtschaftlich und forschungsgesellschaftlich hier bei uns machen, dass diese Technologie mit den Menschen und für die Menschen entwickelt werden kann. Diesen Impetus begrüße ich. Ich würde mir wünschen, dass wir dabei aber mit einigermaßen großer, mit maximaler Trennschärfe operieren, damit alle Akteure am Ende wissen, wo sie denn stehen. Das muss jetzt in den Ausführungsbestimmungen geklärt werden, weil vieles im Vertraglichen nicht erfüllt ist.

Und ich hätte Sorge, dass wir uns hier oder da, um einfach überall Felder auch politisch besetzen zu können, zu sagen, wir haben uns darum gekümmert, zu viele Graubereiche leisten, die dann leider wieder dafür sorgen, dass auf europäischer Ebene, auf europäischem Boden Technologie, die für die Zukunft enorm wichtig ist, mit sehr, sehr großen Hürden entwickelt werden muss, die aber nicht gewisse negative Effekte, die wir leider haben, verhindern können, weil diese Technologie nämlich weltweit entwickelt wird. Und davor dürfen wir uns auch nicht verschließen. Und da wäre mir sehr daran gelegen, dass alle Akteure genau wissen, wo sie denn dran wären, was erlaubt ist und was nicht, und wir nicht zu große graue Felder haben, sodass nachher das Ganze doch wieder nur vor Gerichten entschieden werden kann.

Moderator [00:51:13]

Ja, vielen Dank, Herr Ommer, Und an Sie, Herr Hacker, die gleiche Frage, was Ihrer Meinung nach momentan beim AI Act und in der Debatte der wichtigste Aspekt ist.

Philipp Hacker [00:51:21]

Für mich wäre das Wichtigste, dass wir wirklich versuchen, uns auf die wenigen Aspekte zu konzentrieren, wo wirklich KI kritisch und gesellschaftlich relevant schädlich sein kann. Das sind dann wenige Einsatzbereiche, wo wir gucken auf Bioterrorismus, Chemieterrorismus und Ähnliches, letztlich auch auf Cybersecurity. Das ist ein extrem relevanter Bereich, der völlig unterbelichtet ist. Und wir wissen ja aus dem IoT-Bereich, dass da häufig Schwachstellen sind, die dann ausgenutzt werden können von bösartigen Akteuren staatlicher wie auch nichtstaatlicher Natur. [...] Diesen ganzen Cybersecurity-Aspekt, [...] den müsste man noch schärfen. Das ist ja beispielsweise bei den Foundation Models so, was man sich vorstellen kann, wenn da mal so eine Backdoor ist, das ist sehr ungünstig. Die verteilt sich dann durch das ganze Ökosystem nach unten. Das sind Teile, wo man wirklich das Augenmerk darauf haben kann.

Und der Rest, da wäre es mir eigentlich lieb, wenn man viel mehr auf diese Endregulierung schaut, die wir schon haben, also die Ergebnisregulierung: Nichtdiskriminierungsrecht, Haftungsrecht und so weiter, und da etwas zurückhaltender ist dahingehend, den Entwicklern jetzt wirklich jeden einzelnen Schritt vorzugeben und da ein bisschen mehr darauf vertraut, dass da auch gute Industriepraktiken bestehen, die ja dann am Ende des Tages aus marktwirtschaftlichen Gesichtspunkten ohnehin viele einhalten müssen. Vielleicht das Ganze ein bisschen schlanker denken, ein bisschen mehr auf die Enderegulierung vertrauen und das Ganze paaren, so wie wir das jetzt gesehen haben, mit einer massiven Investmentoffensive. Wir brauchen da Milliarden, die wirklich hineingehen, um mithalten zu können mit den USA, mit China, letztlich auch mit UK. Und selbst Norwegen hat gerade 1 Milliarde Kronen dafür locker gemacht. Das müssen wir matchen, um hier letztlich unsere Zukunft sowohl in ökonomischer wie in sozialer Hinsicht sicherzustellen.

Moderator [00:53:11]

Gut, dann haben wir 13 Uhr jetzt auch schon durch. Erst einmal vielen Dank an Sie, Herr Hacker und Herr Ommer, dass Sie sich die Zeit genommen haben. Und vielen Dank auch an die Journalistinnen und Journalisten für Ihre Aufmerksamkeit und die Fragen. Heute werden wir so schnell wie möglich die Aufzeichnung auch auf unserer Homepage online stellen. Voraussichtlich morgen wird da auch das Transkript veröffentlicht werden. Falls Sie die Audioaufzeichnungen, die Videodatei oder heute schon das maschinell erstellte Transkript haben wollen, finden Sie den Link dazu in der Reminder-Mail heute Morgen. Vielen Dank für Ihre Zeit. Ich wünsche Ihnen noch einen schönen Tag und auf Wiedersehen.

Ansprechpartner in der Redaktion

Bastian Zimmermann
Redakteur 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