Druckversion Dienstag, 4.02.2025, 11:14 Uhr

LTO Legal Tribune Online

https://www.lto.de//recht/hintergruende/h/ai-act-ki-verordnung-eu-sicherheit-risiko-teil-1

AI Act tritt in Kraft: Was das neue Gesetz für Künstliche Intelligenz in Europa bedeutet

von Dr. Jasper Siems und Nico Kuhlmann 01.08.2024

Der AI Act der EU tritt am 1. August 2024 in Kraft. Den risikobasierten Ansatz und warum der EU-Gesetzgeber das Regelungskonzept des Produktsicherheitsrechts gewählt hat, erklären *Jasper Siems* und *Nico Kuhlmann*.

Vom Chatbot zum selbstfahrenden Auto – Künstliche Intelligenz (KI oder auf Englisch: Artificial Intelligence, AI) ist längst nicht mehr nur Science Fiction, sondern Teil des Alltags geworden. Die Art und Weise, wie wir nun mit KI interagieren, wird die Welt umfassend prägen, in der wir in Zukunft leben werden.

Dieses Veränderungspotenzial hat auch die EU erkannt und für die 2020er-Jahre das digitale Jahrzehnt ausgerufen. In einer Mitteilung vom März 2021 mit dem Titel "Digitaler Kompass 2030: Der europäische Weg in die digitale Dekade" hat sie ihre Zielvorstellungen für den digitalen Wandel bis 2030 dargelegt. Grundlegendes Anliegen ist die Regulierung des digitalen Raums durch zahlreiche neue EU-Gesetze.

Neben wirtschaftlich-gesellschaftlichen Themen wie der Plattformökonomie (Digital Services Act; DSA), der Marktmacht großer Digitalkonzerne (Digital Markets Act; DMA) und der besseren Wertschöpfung aus Daten intelligenter Produkte (Data Act) ist KI die zentrale Technologie, deren bessere Regulierung sich die EU im Rahmen der Digitalen Dekade auf die Fahnen geschrieben hat. Denn die EU befürchtet, dass das bestehende Recht zahlreiche blinde Flecken gegenüber den Besonderheiten und Risiken von KI-Systemen aufweist.

Was der AI Act von Spielzeug und Medizinprodukten lernt

So ist KI als Technologie in der Lage, autonomer zu agieren als herkömmliche regelbasierte Software. Gleichzeitig ist ein KI-System oft deutlich komplexer und zugleich weniger transparent. All diesen und weiteren Risiken von KI-Systemen wollte die Europäische Kommission mit ihrem Vorschlag für einen AI Act vom April 2021 begegnen. Nach drei Jahren intensiver Beratungen stimmten das Europäische Parlament und der Rat im März 2024 dem AI Act zu, der am 1. August 2024 formell in Kraft tritt. Die einzelnen Regelungen haben dann jeweils eine eigene Übergangsfrist.

Der AI Act ist eine EU-Verordnung. Dennoch spricht der EU-Gesetzgeber, wie schon beim Digital Services Act und dem Digital Markets Act, nicht von einer "AI Regulation", sondern vom "AI Act". Dieser Trend, insbesondere bei EU-Regelwerken im Digitalbereich, die Bezeichnung "Act" zu wählen, mag mehrere Hintergründe haben. Besonders relevant dürfte sein, dass "Act" im anglo-amerikanischen Sprachraum besonders anschlussfähig ist.

Der zentrale Regelungsansatz des AI Act ist dem Produktsicherheitsrecht entnommen. Dabei orientiert sich der AI Act am sogenannten New Legislative Framework der EU (NLF). Hierbei handelt es sich um einen im Jahr 2008 eingeführten Regelungsrahmen, der – bestehend aus zahlreichen Maßnahmen und Rechtsakten – die Grundlage für die Herstellung und den Vertrieb von Produkten innerhalb der EU bildet. Beispielsweise wird das NLF für die Marktzulassung von Produkten wie Spielzeug, Medizinprodukte oder Haushaltsgeräte verwendet. Produkte aus diesen sehr unterschiedlichen Kategorien dürfen nach Konzeption des NLF alle nur mit der CE-Kennzeichnung auf den europäischen Markt. Mit der CE-Kennzeichnung erklären die Hersteller dieser Produkte, dass den jeweils einschlägigen Sicherheitsanforderungen entsprochen wird.

Produktsicherheitsrecht und KI-Regulierung weisen eine ganz wesentliche Gemeinsamkeit auf: So schützt das Produktsicherheitsrecht immer die Gesundheit und Sicherheit von Menschen – und genau in diesem Bereich möchte der EU-Gesetzgeber mit der Regulierung von KI-Systemen ein hohes Schutzniveau erreichen.

Produktsicherheit trifft Grundrechtsschutz

Die zweite Säule des AI Act ist der Schutz der Grundrechte aus der EU-Grundrechtecharta. Denn die EU sieht es als zwingende Voraussetzung, dass KI eine menschenzentrierte Technologie ist.

So verlangt der AI Act etwa in bestimmten Konstellationen von Anbietern und Betreibern von KI-Systemen, dass sie die Auswirkungen auf die Grundrechte der Nutzer darlegen. Je nach Einsatzgebiet des KI-Systems sind die möglichen Auswirkungen zum Beispiel auf die Meinungsfreiheit oder Berufsfreiheit der Nutzer abzuschätzen. Diese Auswirkungen sind in Grundrecht-Folgenabschätzungen detailliert darzulegen, vergleichbar mit den Datenschutz-Folgenabschätzungen. Als Kombination von Grundrechtsschutz und Produktsicherheitsrechts betritt der AI Act damit auch strukturell-regulatorisch neues Terrain. Insbesondere gibt es im Produktsicherheitsrecht noch keine Erfahrungen oder

gar technische Standards im Hinblick auf die Berücksichtigung von Grundrechten bei der Produktsicherheit.

Übergeordnetes Ziel des AI Act ist es, einen einheitlichen Rechtsrahmen für die Entwicklung, das Inverkehrbringen, die Inbetriebnahme und die Verwendung von KI-Systemen in der Union zu schaffen. Dieses Ziel spiegelt sich im weiten Anwendungsbereich des AI Act wider: Zunächst ist der Begriff des KI-Systems sehr weit gefasst: Gemäß Art. 3 Abs. 1 AI Act ist ein KI-System "ein maschinengestütztes System, das für einen […] autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann". Das System wird mit Eingaben bestimmter Ziele gefüttert, seine "Intelligenz" besteht darin, dass es aus diesen Eingaben "Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen" ableitet.

Ebenso weit ist der Anwendungsbereich in räumlicher und sachlicher Hinsicht: Verkürzt gesagt ist der AI Act anwendbar, sobald der KI-Output in der Union genutzt wird. Damit haben es nicht der Hersteller und Anbieter, sondern die Nutzer in der Hand, ob die KI den EU-Regeln unterfällt. Hierbei gilt der AI Act über Sektorengrenzen hinweg und richtet sich sowohl an öffentliche als auch an private Akteure. Die Vorgaben des AI Act finden also für nahezu alle Einsatzbereiche Anwendung von lustigen Chatbots über smarte Staubsauger bis hin zu medizinischen Robotern.

Der risikobasierte Ansatz des AI Act

Als Produktsicherheitsgesetz legt der AI Act in erster Linie Pflichten für die Anbieter von KI-Systemen fest. Ein Anbieter ist jeder, der ein KI-System entwickelt hat oder entwickeln lässt und dieses in Verkehr bringt oder in Betrieb nimmt. Es ist dabei irrelevant, ob dies entgeltlich oder unentgeltlich geschieht.

Der sichtbarste Ausdruck des AI Act als Regelungschimäre aus Produktsicherheitsrecht und Grundrechtsschutz ist der risikobasierte Ansatz. Der AI Act gibt vor, dass KI-Systeme basierend auf ihren potenziellen Risiken für die Sicherheit, Grundrechte und Gesundheit von EU-Bürgern in verschiedene Risikokategorien eingeordnet werden. Je nach Risikokategorie treffen den Anbieter umfangreiche Pflichten.

Der AI Act kennt insgesamt vier Risikokategorien: die verbotenen Systeme, Hoch-Risiko Systeme, bestimmte KI-Systeme und KI-Systeme mit minimalem Risiko.

In Art. 5 benennt der AI Act bestimmte Praktiken, die im KI-Bereich innerhalb der EU generell verboten sind. Diese KI-Systeme dürfen weder entwickelt noch genutzt werden. Verboten sind beispielsweise KI-Systeme, die ein Social Scoring von Menschen ermöglichen. Nicht möglich wäre damit ein Sozialkredit-System auf Basis von KI wie es teilweise in China genutzt wird.

Vom Chatbot zum Hochrisiko System

Hochrisiko-Systeme im Sinne des Art. 6 AI Act lassen sich in zwei Unterkategorien aufteilen: Zum einen sind KI-Systeme erfasst, die in Produkten verwendet werden, die unter die in Anhang I aufgeführten Produktsicherheitsvorschriften der EU fallen. Hierunter kann man sich etwa ein KI-System vorstellen, das Teil eines größeren medizinischen Operationsroboters ist. Zum anderen zählen zu den Hochrisiko-KI-Systemen alle Systeme, die den in Anhang III aufgeführten Bereichen angehören und keiner der eng gefassten Ausnahmen unterliegen. Dazu zählen KI-Systeme in der kritischen Infrastruktur. Das sind etwa Komponenten, die den sicheren Betrieb von Software im Straßenverkehr oder bei der Versorgung mit Wasser, Gas, Wärme oder Strom gewährleisten sollen.

Anbieter von KI-Systemen mit einem begrenzten Risiko treffen gemäß Art. 50 AI Act demgegenüber in erster Linie nur Transparenzpflichten. Sie müssen insbesondere dem Nutzer deutlich machen, dass er mit KI interagiert. Ein klassisches Beispiel für ein derartiges KI-System ist der Chatbot.

Anbieter von KI-Systemen mit minimalem Risiko wie beispielsweise Spam-Filtern bei E-Mail-Programmen unterliegen grundsätzlich keinerlei Pflichten unter dem AI Act.

Insbesondere die Regulierung von Hochrisiko-Systemen basiert stark auf klassischem Produktsicherheitsrecht. So setzt der AI Act genauso auf die CE-Kennzeichnung: Anbieter von Hochrisiko-Systemen eine sogenannte Konformitätsbewertung durchführen, bevor das KI-System in der EU auf den Markt kommt. Hierbei müssen zahlreiche Vorgaben erfüllt werden. Das betrifft unter anderem die Bereiche Daten-Governance, also die möglichst diskriminierungsfreie und datenschutzfreundliche Auswahl der Trainingsdaten, das Risikomanagement sowie Transparenz und Dokumentation. Eine erfolgreiche Konformitätsbewertung endet – wie auch im klassischen Produktsicherheitsrecht – stets mit dem CE-Kennzeichen.

Aufgrund der umfangreichen Regelungen des AI Act – und weil diese Regulierung spürbare Auswirkungen auf viele wirtschaftlich und gesellschaftlich relevante Bereiche haben wird – ist die praktische Bedeutung des AI Act für die nächsten Jahre und Jahrzehnte kaum zu überschätzen.

Dieser Beitrag ist Teil einer Miniserie zum Inkrafttreten des AI Act. Im nächsten Beitrag, der nun hier verfügbar ist, geht es im Detail um die verbotenen KI-Praktiken und Regelungen für KI-Modelle mit allgemeinem Verwendungszweck.

Die Autoren arbeiten als Rechtsanwälte bei Hogan Lovells International LLP in der Praxisgruppe Intellectual Property, Media & Technology in Hamburg.

Zitiervorschlag

AI Act tritt in Kraft: . In: Legal Tribune Online, 01.08.2024 , *https://www.lto.de/persistent/a_id/55127* (abgerufen am: 04.02.2025)

- Mehr zum Thema
  - Europa- und Völkerrecht
  - Digitalisierung
  - Künstliche Intelligenz
  - Produkthaftung