

## Die Zukunft der Regulierung von KI-Systemen in Europa

### Der „erste Aufschlag“ der Europäischen Kommission – Zum Anwendungsbereich des EU-Artificial-Intelligence-Act

Bereits vor dem insgesamt sechsten Wimbledon Sieg am letzten Sonntag von Novak Djokovic, hat die Europäische Kommission am 21. April 2021 ihren ersten „Regulierungs-Aufschlag“ für europaweit einheitliche Regeln im Bereich intelligenter Softwaresysteme ausgeführt. Auch im Tennis ist der Aufschlag erst der Beginn eines Ballwechsels, aber das Thema der Regulierung von KI-Systemen („AI systems“) ist für den Wirtschaftsstandort Europa zu wichtig, um nicht frühzeitig den Ball zu retournieren und in die Diskussion einzusteigen. Nach dem ersten hier veröffentlichten Überblick über die Regulierungswerkzeuge der KI-Verordnung wird in diesem Beitrag näher auf den Anwendungsbereich der KI-Verordnung eingegangen.

#### Der große Aufschrei ist ausgeblieben

Zwar ist ein Raunen durch die Wirtschaft gegangen, weil der Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zu harmonisierten Regeln im Bereich Künstlicher Intelligenz (im Folgenden: KI-Verordnung) einen allgemeinverbindlichen, sektorenübergreifenden Harmonisierungsstandard setzen will, aber der große Aufschrei ist bislang (zu Recht) ausgeblieben. Denn die Erfahrungen im Gesetzgebungsprozess der Datenschutzgrundverordnung haben gezeigt, dass es im Laufe des Konsultationsprozesses mit dem Europäischen Parlament und dem Rat der Europäischen Union und deren „Returnspiel“ zahlreiche Änderungen geben wird.

#### In Kürze: Für wen werden die Regeln der KI-Verordnung relevant?

Auf eine Faustformel gebracht, findet die KI-Verordnung in allen europäischen privaten und öffentlichen (Wirtschafts-)Bereichen Anwendung, in denen Anbieter („Provider“) KI-Systeme entwickeln, Importeure KI-Systeme importieren („Importer“), Verkäufer („Distributor“) KI-Systeme anbieten und sonstige Unternehmen („User“) KI-Systeme zu nicht-privaten Zwecken anbieten und verwenden. Bestimmte Wirtschaftsbereiche fallen allerdings unter Bereichsausnahmen (Art. 2 Ziff. 2–4 KI-Verordnung). Dies betrifft z. B. bislang die Typengenehmigung für Kraftfahrzeuge und damit die Automobilbranche (vgl. Art. 2 Ziff. f u. h KI-Verordnung), die die Regeln damit



zukünftig – Stand April 2021 – nicht beachten muss. In allen anderen Bereichen reicht ein wirtschaftlicher Bezug zum Europäischen Wirtschaftsraum aus, um in den Anwendungsbereich zu fallen, wenn sie ein KI-System nutzen.

### **Sachlicher Anwendungsbereich: KI-Systeme**

Die weite Definition des Begriffs KI-System ist im Kontext der Anwendungsszenarien zu lesen. Denn die KI-Verordnung definiert die Anwendungsszenarien („Verboten“ / „Hohes Risiko“ / „Mittleres Risiko“ / „Geringes (kein) Risiko“) vergleichsweise sehr spezifisch, wodurch z. B. Amazon's Empfehlungsalgorithmen oder Google's Suchmaschinen-Algorithmen im Ergebnis zwar KI-Systeme darstellen, aber nicht in das Regelungsregime für High-Risk-Systeme fallen und auch nicht als „prohibited AI-System“ verboten werden.

### **Im Einzelnen:**

Art. 3(1) KI-Verordnung definiert KI-Systeme als Software, die mit einer oder mehr der in Annex 1 genannten Programmieretechniken entwickelt wurde, die für ein oder mehrere von einem Menschen definierte Ziele „Output“ generiert, wie Vorhersagen, Empfehlungen oder Entscheidungen treffen, die das Umfeld beeinflussen, in dem die Software eingesetzt wird.

*„software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with“*

Der Schwerpunkt der Definition liegt klar auf den eingesetzten Techniken, die in Annex 1 der KI-Verordnung für den jeweiligen Geltungszeitpunkt abschließend definiert sind. Die Europäische Kommission behält sich vor, diesen Katalog anzupassen (Art. 4 KI-Verordnung).

Im Verordnungsvorschlag der EU-Kommission sind folgende Techniken in Annex 1 berücksichtigt:

- Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;
- Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;
- Statistical approaches, Bayesian estimation, search and optimization methods.



Damit kann im Ausgangspunkt zwar nicht jede Software unter den Anwendungsbereich der Verordnung fallen, aber – da die Methoden des maschinellen Lernens in nahezu jedem Lebensbereich angewendet werden (können) und zudem oft das größte Optimierungspotential bieten – fallen viele Softwareanwendungen unter die Begriffsdefinition der KI-Verordnung. Ob es ausreicht, dass im Rahmen der Prüfung der Quellcodes statistische Verfahren angewendet werden, soll an dieser Stelle offen bleiben, denn der Begriff der Software ist stets im Verwendungskontext zu lesen, weil nicht jeder Anwendungszweck mit für die KI-Verordnung erheblichen Risiken behaftet ist:

Nicht jede Software wird in einem Hochrisiko-Bereich eingesetzt (Art. 6 KI-Verordnung), auch die „verbotene Software“ (Art. 5 KI-Verordnung) sowie sonstige KI-Systeme (Art. 52 KI-Verordnung) wurden von der EU-Kommission eng definiert. Dies wird insbesondere in der Medienethik in Bezug auf Art. 5 Ziff. 1 lit. a) KI-Verordnung anders gesehen. Nach dieser Vorschrift sind KI-Systeme verboten, die unterschwellige Techniken außerhalb des Bewusstseins einer Person einsetzen, um das Verhalten einer Person in einer Weise zu beeinflussen, die dieser Person oder einer anderen Person physischen oder psychischen Schaden zufügt oder zufügen kann. Zu weit geht es allerdings, den

gesamten Bereich personalisierter Werbung und die Empfehlungsalgorithmen der Sozialen Medien darunter zu fassen (so aber Heesen, Leiterin des Forschungsschwerpunkts Medienethik und Informationstechnik, Internationales Zentrum für Ethik in den Wissenschaften, Eberhard Karls Universität Tübingen, Stellungnahme ist hier abrufbar). Angesichts der breiten Diskussion in der Öffentlichkeit sowie der Aufklärungsmaßnahmen der Plattformbetreiber und der Möglichkeit, diese Funktionen abzustellen, kann nicht davon ausgegangen werden, dass Nutzer keine Kenntnis und kein Bewusstsein für durch Algorithmen kuratierte Werbung oder „Facebook“-News haben. Vielmehr kennt das allgemeine Wettbewerbsrecht das Verbot „sublimier Techniken“ bereits; mangels ausreichenden Belegen zur Wirksamkeit solcher Techniken, wird die Technik nicht genutzt und die Nachweisführung würde herausfordernd sein (vgl. § 22 Abs. 1 S. 2 MedienStV).

### **Personeller Anwendungsbereich: Alle? Gemeinsam?**

Wie es der Rechtsanwender von europäischen Rechtsvorschriften gewohnt ist, enthält auch die KI-Verordnung Legaldefinitionen für die Adressaten der Regelung. Zu unterscheiden ist zwischen dem „Provider“, dem „Importeur“, dem „Distributor“ und dem „User“, die zusammengefasst als „Operator bezeichnet



sind. Im Mittelpunkt steht freilich der „Provider“, der Entwickler des AI-Systems, den wesentliche Pflichten bei der Entwicklung und Überwachung des KI-Systems treffen (vgl. Art. 16 KI-Verordnung):

*„Provider means a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge.“*

„Provider“, die ein KI-System entwerfen, programmieren und es auf dem Markt platzieren, sei es unter ihrer eigenen Marke, kostenlos oder gegen Entgelt, sind von zahlreichen Regeln der KI-Verordnung betroffen. Irrelevant ist, ob der „Provider“ seine Software an Verbraucher oder Unternehmer vermarktet.

„Importeure“, die das AI-System von einem Provider, der in einem Drittstaat sitzt, in den europäischen Wirtschaftsraum importieren, sind ebenfalls in gewissem Rahmen verpflichtet, für die Anwendungssicherheit des AI-Systems zu sorgen (z. B. kontrollieren, ob eine hinreichende Konformitätserklärung vorliegt).

„User“ meint gemäß Art. 3 IV „any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is

used in the course of a personal non-professional activity“. Es kommt nicht darauf an, mit welcher Hardware ein AI-System betrieben wird, sondern wer die Software kontrolliert. In der deutschen Rechtswissenschaft wird die Frage aufgeworfen, ob Software-as-a-Service-Nutzer „User“ im Sinne dieser Vorschrift seien oder ob nur der Softwareanbieter „User“ ist (Bomhard/Merkle, RDI 2021, 276). Da der Softwareanbieter in diesem Fall auch „Provider“ der Software ist, und die eigene Software nicht selbst nutzt, sondern einem Dritten überlässt, ist diese Frage zu verneinen. Es ist ausreichend, dass der „User“ im Rahmen der vom Provider gegebenen Möglichkeiten, die Software kontrolliert (und sei es, dass er die Software lediglich aktivieren und deaktivieren kann). Denn andernfalls würde der Begriff „User“ zu einem großen Teil leerlaufen, weil er keinen relevanten Anwendungsbereich hätte.

Es sei darauf hingewiesen, dass jeder „User“, „Importeur“, „Distributor“ zu einem „Provider“ werden kann, wenn (1) er das AI-System selbst erstmalig im Europäischen Wirtschaftsraum unter eigenem Namen zugänglich macht oder (2) der Anwendungszweck des AI-Systems verändert wird, das bereits auf den Markt platziert ist oder (3) das AI-System substantiell modifiziert wird (Art. 28 KI-Verordnung). Während die Auslegung der Varianten (1) und (2) keine Probleme



keine Probleme bereitet, ist fraglich, wann die Schwelle einer substantiellen Modifizierung eines KI-Systems erreicht wird.

### **Räumlicher Anwendungsbereich: EU und darüber hinaus?**

Nicht relevant ist der Sitz des Unternehmens oder der Standort der Server, wenn KI-Systeme im Europäischen Wirtschaftsraum vermarktet oder zur Nutzung (auch kostenfrei) angeboten werden. Unklar ist, wie die Anwendungsregel zu verstehen ist, dass auch Unternehmen („Provider“, „User“) mit Sitz in einem Drittland unter den Anwendungsbereich fallen, wenn der „Output“ des Systems in der Union genutzt („used“) wird (Art. 2 Nr. 1 c) KI-Verordnung). Die bloße „Abrufbarkeit“ und „Nutzbarkeit“ eines KI-Systems durch einen in der EU ansässigen Verbraucher dürfte als solche nicht ausreichen, denn nach dem Wortlaut der entsprechenden Norm muss das im Drittland ansässige Unternehmen den „Output“ in der Europäischen Union nutzen (Bomhard/Merkle, RDI 2021, 276, 278). Ein Nutzungswille muss aber positiv festgestellt werden, sodass z. B. für den südamerikanischen Markt ausgerichtete Angebote auch in Europa abrufbar sind. Im Übrigen ist für die Frage des räumlichen Anwendungsbereichs offen, ob die Generierung / Nutzung von Output in einem Drittland ausreicht, der aber über ein

Produkt, z. B. einen Roboter, den europäischen Wirtschaftsraum erreicht („mittelbarer Output“).

### **Ausblick**

Der erste Regulierungsaufschlag der EU-Kommission, KI-Systeme in einen neuen Regulierungsrahmen zu implementieren, ist kein „Ass“. Wie kraftvoll der „Return“ des Europäischen Rates und im Besonderen des Europäischen Parlaments ausfällt, wird gerade von der jetzt stattfindenden Willensbildung der Abgeordneten abhängen, die wiederum von Verbänden und Wirtschaftsvertretern beeinflusst wird. Im Ergebnis ist – anders als im Tennis – nicht entscheidend, wer von den (mehr als zwei) Spielern als Sieger hervorgeht, sondern ob durch die KI-Verordnung der Innovationsstandort Europa gestärkt wird.

Die KI-Verordnung tritt frühestens im Jahr 2025 in Kraft.

### **Kontakt**



**Dr. Dominic Habel**  
Rechtsanwalt, Associate

T +49 40 55436 4114

E [dominic.habel@osborneclarke.com](mailto:dominic.habel@osborneclarke.com)

