

# KI-REGELN FÜR FAIRNESS UND VERBRAUCHERVERTRAUEN

Zusammenfassung der Stellungnahme des Verbraucherzentrale Bundesverbands (vzbv) zum Vorschlag der Europäischen Kommission für den Artificial Intelligence Act (AIA)

## GENERELLE BEWERTUNG

Aus Verbrauchersicht ist es zu begrüßen, dass die Europäische Kommission mit dem Artificial Intelligence Act (AIA)<sup>1</sup> einen Verordnungsvorschlag für Künstliche Intelligenz (KI) vorlegt. Um die Entwicklung "vertrauenswürdiger KI" zu fördern, empfiehlt der vzbv, Verbraucherinnen und Verbrauchern<sup>2</sup> stärker in den Fokus des AIA zu rücken sowie den zu engen Anwendungsbereich des AIA auszuweiten. Eine zentrale Herausforderung ist die Intransparenz von KI-Systemen und daraus resultierende verdeckte Diskriminierung und ungerechtfertigte Behandlung von Verbrauchern. Deshalb sollte der Gesetzgeber mehr Möglichkeiten für unabhängige Bewertungen risikoreicher KI-Systeme vorsehen und mehr Transparenz für Verbraucher schaffen.

### ❖ Weite Definition von KI beibehalten

Die schnelle Weiterentwicklung von KI-Techniken in der Vergangenheit<sup>3</sup> zeigt, dass der europäische Gesetzgeber die weit gefasste Definition von KI-Systemen in Artikel 3 Absatz 1 und Anhang I beibehalten sollte. Die weite Definition spiegelt das breite Spektrum algorithmenbasierter Entscheidungssysteme wieder, die wichtige Entscheidungen über Verbraucher vorbereiten oder „treffen“. Die vorgeschlagene weite Definition stellt sicher, dass der AIA zukunftsfest ist. Eine engere Definition von KI-Systemen, etwa mit dem Fokus auf heute aktuelle Ausprägungen des maschinellen Lernens, birgt die Gefahr, dass der AIA wirkungslos wird, sobald neue KI-Technologien und -Methoden an Bedeutung gewinnen.

### ❖ Verbraucher müssen individuelle Erklärungen erhalten

KI-Systeme müssen gegenüber Verbrauchern transparent und nachvollziehbar sein, damit sie souveräne Entscheidungen treffen können. Leider sieht der AIA-Entwurf lediglich eine Kennzeichnungspflicht für drei Anwendungsbereiche von KI-Systemen vor (Art. 52: KI-Systeme, die mit Personen interagieren, Systeme zur

<sup>1</sup> Europäische Kommission: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union (COM(2021) 206 final) (2021), URL: <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021PC0206&from=EN> [Zugriff: 10.08.2021].

<sup>2</sup> Die im weiteren Text gewählte männliche Form bezieht sich immer zugleich auf Personen aller Geschlechter. Wir bitten um Verständnis für den weitgehenden Verzicht auf Mehrfachbezeichnungen zugunsten einer besseren Lesbarkeit des Textes.

<sup>3</sup> Vgl. etwa: Pitchford, Daniel. Forbes: A Decade Of Advancements As We Enter A New Age Of AI (2019), URL: <https://www.forbes.com/sites/danielpitchford/2020/12/31/a-decade-of-advancements-as-we-enter-a-new-age-of-ai/?sh=5c65d3cb4055> [Zugriff: 19.07.2021].

Emotionserkennung, Deep Fake Videos/Audios). Darüber hinaus sind keine Transparenzverpflichtungen gegenüber Verbrauchern vorgesehen.

Der AIA muss Anbieter und berufliche Nutzer<sup>4</sup> risikoreicher KI-Systeme verpflichten, Verbraucher nicht nur über den Einsatz von KI-Systemen zu informieren, sondern auf Verlangen des Verbrauchers auch das Ergebnis eines KI-Systems im Einzelfall nachvollziehbar, sachgerecht und konkret zu erläutern. Solche Betroffenenrechte sind die Voraussetzung dafür, dass Verbraucher Entscheidungen über sie, die durch KI-Systeme vorbereitet oder de facto „getroffen“ werden, nachvollziehen und individuell überprüfen können. Nur dann können sie ihre Rechte wahrnehmen und gegen ungerechtfertigte Behandlung oder Diskriminierung vorgehen.

Zur Erklärung, die Anbieter oder berufliche Nutzer auf Anfrage abgeben müssen, zählen etwa Informationen über die Eingabedaten, auf deren Grundlage ein KI-System eine Entscheidung über die Person „trifft“/vorbereitet, die Logik des Modells, die Kriterien, anhand derer das KI-System optimiert, aussagekräftige Kennzahlen für Fairness/Bias, Robustheit und Genauigkeit sowie der Einsatzzweck des KI-Systems.

### ❖ Informationen für die Öffentlichkeit bereitstellen

Um Vertrauen in KI-Systeme zu schaffen, die breite gesellschaftliche Auswirkungen haben können, bedarf es einer informierten, öffentlichen Debatte in der die Risiken und Chancen dieser Systeme diskutiert werden. Um diesen Diskurs zu ermöglichen, müssen die Anbieter risikoreicher KI-Systeme der Öffentlichkeit alle Informationen zur Verfügung stellen, die für eine fundierte Bewertung und das Verständnis der Systeme benötigt werden. Dazu gehören zum Beispiel Informationen über die Eigenschaften, Fähigkeiten und Leistungsgrenzen des Systems (wie Datengrundlage, Robustheit und Bias) sowie Informationen über die menschliche Aufsicht der Anwendung. Diese entsprechen weitgehend den Informationspflichten gegenüber beruflichen Nutzern (Art. 13).

### ❖ Ergänzung der Liste risikoreicher KI-Systeme

Die Regeln des AIA-Vorschlags für hochriskante KI-Systeme beschränken sich vor allem auf Systeme in den Bereichen (Produkt-)Sicherheit, Gesundheit und Grundrechte. Bei der Schadens- und Risikobetrachtung vernachlässigt der Vorschlag Verstöße gegen Verbraucherrechte (etwa Irreführung) oder dass KI-Systeme einzelne Verbraucher oder Gruppen erhebliche wirtschaftliche/finanzielle Schäden zufügen können.

Die Liste hochriskanter KI-Anwendungen in Anhang III sollte um Anwendungsgebiete ergänzt werden, in denen KI-Systeme Verbrauchern erheblichen wirtschaftlichen/finanziellen Schaden zufügen beziehungsweise Verbraucherrechte schwer

---

<sup>4</sup> Unter Art. 3 (3) definiert der AIA „Nutzer“ von KI Systemen als natürliche oder juristische Personen, Behörden, Einrichtungen oder sonstige Stellen, die ein KI-System im Rahmen ihrer beruflichen, professionellen Tätigkeit verwenden. „Nutzer“ im Sinne von Verbrauchern oder Bürgern werden nicht definiert.

verletzen können. Dies umfasst beispielsweise KI-Systeme, die im Versicherungsbereich eingesetzt werden (etwa als vermeintliche Lügendetektoren<sup>5</sup> oder zur Bestimmung individueller Risiken<sup>6</sup> und Boni<sup>7</sup>), verbrauchernahe KI-Anwendungen für Finanzanlagen und Portfoliomanagement (etwa „Roboadvisors“<sup>8</sup>) sowie KI-Systeme im Bereich Zahlungsverkehr und Inkasso. Ebenso als potenziell hochriskant zu deklarieren sind KI-Systeme, die zur Bewertung und Erstellung von Verbraucherprofilen („Scoring“) eingesetzt werden, wenn diese den Zugang der Verbraucher zu Dienstleistungen oder Märkten bestimmen.

### ❖ **Künftige risikoreiche Anwendungen: Verbraucherrechte und wirtschaftliche Risiken berücksichtigen**

Um den AIA zukunftsfest zu machen, muss der Gesetzgeber in der Lage sein, neue risikoreiche KI-Systeme aus anderen Anwendungsbereichen als den bereits in Anhang III aufgeführten hinzuzufügen. Bei der Aktualisierung der Liste der risikobehafteten KI-Systeme in Anhang III kann der Gesetzgeber nur solche KI-Systeme hinzufügen, die "das Risiko einer Beeinträchtigung der Gesundheit und Sicherheit oder das Risiko einer Beeinträchtigung der Grundrechte mit sich bringen" (Art. 7 Abs. 1. 1. (b)). Um die Zukunftssicherheit des AIA zu gewährleisten, muss der Gesetzgeber die Möglichkeit haben, ein KI-System als risikoreich einzustufen, wenn es erhebliche Risiken in Bezug auf die Verletzung von Verbraucherrechten sowie soziale und wirtschaftliche Schäden für Einzelpersonen und (soziale) Gruppen birgt.

### ❖ **Verbot von Dark Patterns und der Ausnutzung von Schwächen**

Mit Art. 5 Abs. 1 (a) sollte der AIA generell verbieten, dass KI-Systeme so genannte "Dark Patterns"<sup>9</sup> einsetzen, um auf unfaire Art und Weise die Autonomie, Entscheidungsfindung oder Wahlmöglichkeiten der Verbraucher im kommerziellen Interesse der Anbieter zu untergraben oder zu beeinträchtigen. Dark Patterns manipulieren Nutzer etwa durch eine nicht-neutrale Gestaltung der Struktur, Funktion oder der Art und Weise der Bedienung einer Benutzeroberfläche oder eines Teils davon. Taktiken, die auf Dark Patterns basieren, sind gut dokumentiert und wer-

---

<sup>5</sup> Quach, Katyanna: Insurance startup backtracks on running videos of claimants through AI lie detector (2021), URL: [https://www.theregister.com/2021/05/26/ai\\_insurance\\_lemonade/](https://www.theregister.com/2021/05/26/ai_insurance_lemonade/) [Zugriff: 23.07.2021].

<sup>6</sup> Taulli, Tom: Lemonade IPO Shows The Power Of AI (Artificial Intelligence) (2020), URL: <https://www.forbes.com/sites/tomtaulli/2020/07/03/lemonade-ipo-shows-the-power-of-ai-artificial-intelligence/?sh=152fd0f83aeb> [Zugriff: 23.07.2021].

<sup>7</sup> Generali Vitality GmbH: Generali Vitality (2021), URL: <https://www.generalivitality.com/about-our-program/> [Zugriff: 20.07.2021].

<sup>8</sup> Frankenfield, Jake: What Is a Robo-Advisor? in: Investopedia (2021), URL: <https://www.investopedia.com/terms/r/roboadvisor-roboadviser.asp> [Zugriff: 20.07.2021].

<sup>9</sup> „Techniken der unterschweligen Beeinflussung außerhalb des Bewusstseins einer Person“ (Art. 5 Abs. 1 (a))

den etwa eingesetzt, um Nutzer zur Einwilligung in die Datenerfassung und -verarbeitung zu drängen,<sup>10</sup> sie bewusst davon abzuhalten, sich von Diensten abzumelden<sup>11</sup>, oder sie zum Kauf zusätzlicher Dienste zu bewegen<sup>12</sup>.

Art. 5 Abs. 1 (b) sollte verbieten, dass KI-Systeme persönliche Schwächen oder die Schutzbedürftigkeit von Verbrauchern zu deren Nachteil ausnutzen. Bisher schützt der AIA in dieser Hinsicht nur alte und behinderte Menschen. Dieses Verbot sollte aber alle Verbraucher einschließen, denn jeder Mensch kann sich, wenn auch zeitweise, in einer sehr verletzbaren, schutzbedürftigen Lage befinden. Individuelle Verletzlichkeit kann etwa durch emotionale oder traumatische Erfahrungen, Erschöpfung, Müdigkeit, Trauer, Spielsucht<sup>13</sup>, körperliche Schmerzen oder den Einfluss von Medikamenten bedingt sein. KI-Systeme dürfen solche Schwächen nicht ausnutzen, und schon gar nicht im kommerziellen Interesse eines Anbieters.

Eine Voraussetzung für das bisher im AIA vorgesehene Verbot von Dark Patterns oder der Ausnutzung von verletzlichen Verbrauchern ist, dass dies zu psychischen oder körperlichen Schäden auf Seiten der Betroffenen führt, und dass der Anbieter dies intendiert. Es wird jedoch weitgehend unmöglich sein, zu beweisen, dass ein Anbieter von KI-Systemen die Herbeiführung solcher Schäden beabsichtigte. Deshalb muss der Gesetzgeber diese Intentionalität streichen. Außerdem sollte sich der Schadensbegriff in Art 5 Abs. 1 (a) und (b) nicht nur auf physische oder psychische Schäden beschränken. Vielmehr sollten der Schadensbegriff auch ökonomische Wohlfahrtsverluste, Verletzungen von Grundrechten (zum Beispiel Diskriminierung) und Verbraucherrechten (zum Beispiel Täuschung) erfassen.

### ❖ **Verbot des allgemeinen Sozial-Scorings durch private Stellen**

Art. 5 Abs. 1 (c) verbietet das allgemeine Sozial-Scoring durch öffentliche Stellen unter bestimmten Umständen. Ein allgemeines Sozial-Scoring durch private Stellen kann ebenfalls erhebliche negative Folgen für Einzelpersonen oder soziale Gruppen haben. Ungerechtfertigte oder diskriminierendes Sozial-Scoring kann zum Ausschluss von Verbrauchern von ganzen Märkten oder Dienstleistungen

---

<sup>10</sup> Peter Hense: The end of dark patterns in “cookie walls”: German court bans deceptive designs (2021), URL: <https://www.jdsupra.com/legalnews/the-end-of-dark-patterns-in-cookie-5786302/> [Zugriff: 01.02.2021].

<sup>11</sup> So zeigt beispielsweise der jüngste Bericht des Norwegischen Verbraucherrates, wie Amazon Nutzer, die sich von Amazon Prime abmelden wollen, offenbar gezielt dabei behindert werden: “In the process of unsubscribing from Amazon Prime, the company manipulates consumers to continue using the service in what seems like a deliberate attempt to confuse and frustrate customers.” Vgl. Forbrukerradet: Amazon manipulates customers to stay subscribed, URL: <https://www.forbrukerradet.no/news-in-english/amazon-manipulates-customers-to-stay-subscribed/> [Zugriff: 01.02.2021].

<sup>12</sup> Beispielsweise: “A [...] federal lawsuit asserts that Electronic Arts unlawfully increases its sports games’ difficulty in order to induce gamers into paying the video game publisher additional money.” Vgl. Sportico: Federal Law Suit: This Video Game is too Damn Hard (2020), URL: <https://www.sportico.com/law/analysis/2020/ea-sports-its-in-the-game-1234617287/> [Zugriff: 01.02.2021].

<sup>13</sup> So könnten KI-Systeme Spielsüchtige dazu verleiten, vermehrt sogenannte “in-Game” Käufe zu tätigen: “Systems also pair in-game purchase offers with known triggers for an individual player or known triggers for similar players.” Markle, Tracy; Kennedy, Brett: In-Game Purchases: How Video Games Turn Players into Payers. in: Digital Media Treatment (2021), URL: <https://digitalmediatreatment.com/in-game-purchases/> [Zugriff: 21.07.2021] Daniel L. King u. a.: Unfair play? Video games as exploitative monetized services: An examination of game patents from a consumer protection perspective 101 (2019), in: Computers in Human Behavior, p. 131–143, URL: <https://www.sciencedirect.com/science/article/pii/S0747563219302602> [Zugriff: 21.07.2021].

führen – mit erheblichen wirtschaftlichen und sozialen Schäden für Betroffene<sup>14</sup>. Der AIA muss deshalb auch privaten Stellen untersagen, allgemeines Sozial-Scoreing dafür einzusetzen, um die Vertrauenswürdigkeit von Verbrauchern, auf Grundlage ihres sozialen Verhaltens oder vermeintlicher Persönlichkeitseigenschaft vorherzusagen oder die Menschen danach zu klassifizieren.

### ❖ **Verbot der biometrischen Fernidentifizierung im öffentlichen Raum durch private Stellen**

Art. 5 Abs. 1 (d) untersagt (mit Einschränkungen) den Einsatz von Systemen zur biometrischen Fernidentifizierung in Echtzeit in öffentlich zugänglichen Räumen durch Behörden. Aber auch die Verwendung solcher Systeme durch private Stellen kann Verbrauchern erheblichen Schaden zufügen, etwa hinsichtlich ihrer Autonomie oder des Rechts auf Privatsphäre. Beispiele für potenzielle Anwendungen, die besonders problematisch sind, umfassen sogenannte „Smarte“ Brillen (etwa von Facebook<sup>15</sup>), Augmented-Reality-Anwendungen für Mobiltelefone, die Objekte im öffentlichen Raum identifizieren können<sup>16</sup> oder die Analyse von Aufnahmen von Überwachungskameras in Einkaufszentren. Der AIA muss den Einsatz solcher biometrischer Fernidentifizierungssysteme in öffentlich zugänglichen Räumen durch private Stellen verbieten. Das Verbot muss sowohl die biometrische Identifizierung in Echtzeit als auch die nachträgliche Identifizierung umfassen.

### ❖ **Verbot von Systemen zur Emotionserkennung durch private Stellen**

Der AIA schützt Verbraucher nicht wirksam vor dem Einsatz von Systemen zur Emotionserkennung und -auswertung durch private Stellen. Unternehmen können solche Systeme nutzen, um Verbraucher zu täuschen und zu manipulieren und dabei die Autonomie und Entscheidungsfindung der Menschen untergraben. Solche Systeme können menschliche Merkmale analysieren, etwa die Mimik, Stimme, Tastaturanschläge und Surfverhalten<sup>17</sup> oder andere biometrische oder verhaltensbezogene Signale. Diese können auch zum Nachteil der Verbraucher eingesetzt werden (etwa in Form vermeintlicher „Lügendetektoren<sup>18</sup>“) beziehungsweise genutzt werden, um Menschen individuell zu deren Nachteil zu beeinflussen (etwa im Marketing, um personalisierte Angebote auszuspielen<sup>19</sup>).

<sup>14</sup> So hält AirBnB ein Patent zur Ermittlung der Vertrauenswürdigkeit seiner Nutzer auf Basis von Informationen aus Sozialen Medien: Business Insider: Airbnb has patented software that digs through social media to root out people who display 'narcissism or psychopathy' (2020), URL: <https://www.businessinsider.de/international/airbnb-software-predicts-if-guests-are-psychopaths-patent-2020-1/?r=US&IR=T> [Zugriff: 12.05.2020]; Booker beware: Airbnb can scan your online life to see if you're a suitable guest (2020), URL: <https://www.standard.co.uk/tech/airbnb-software-scan-online-life-suitable-guest-a4325551.html>.

<sup>15</sup> Vgl. wearable.com: The best smartglasses and AR specs 2021: Snap, Amazon and more (2021), URL: <https://www.wearable.com/ar/the-best-smartglasses-google-glass-and-the-rest> [Zugriff: 20.07.2021].

<sup>16</sup> Etwa Anwendungen wie Google Lens oder Google Maps. Vgl. Google: Google Lens – search what you see (2021), URL: <https://lens.google/intl/en-GB/> [Zugriff: 20.07.2021]; Google: Augmented Reality (2021), URL: <https://arvr.google.com/ar/> [Zugriff: 20.07.2021].

<sup>17</sup> Prudsys: Price Optimization: Intelligent and Personalized Couponing (2021), URL: [https://prudsys.de/en/case/price-optimization\\_promotion-pricing/](https://prudsys.de/en/case/price-optimization_promotion-pricing/) [Zugriff: 22.07.2021].

<sup>18</sup> Bittle, Jake: Lie detectors have always been suspect. AI has made the problem worse., URL: <https://www.technologyreview.com/2020/03/13/905323/ai-lie-detectors-polygraph-silent-talker-iborderctrl-converus-neuroid/> [Zugriff: 21.07.2021].

<sup>19</sup> Prudsys (see FN. 17); Adriano, Lyle: Kanetix leverages AI technology to optimize consumer experience (2018), URL: <https://www.insurancebusinessmag.com/ca/news/digital-age/kanetix-leverages-ai-technology-to-optimize-consumer-experience-93703.aspx> [Zugriff: 21.07.2021]; Davenport, Thomas u. a.: How Artificial Intelligence Will

Art. 5 muss die Verwendung von KI-Systemen zur Emotionserkennung und -analyse von Verbrauchern durch private Einrichtungen untersagen. Ausnahmen von diesem Verbot sollten für spezifische Anwendungsfälle gewährt werden, wenn diese nachweislich zum Vorteil der Verbraucher sind (etwa für spezielle medizinische Anwendungen oder Forschungszwecke im öffentlichen Interesse).

Der vzbv schließt sich der Forderung des Europäischen Datenschutzausschusses (EDSA)<sup>20</sup> nach einem generellen Verbot für den Einsatz KI-basierter und automatischer Erkennung von menschlichen Merkmalen im öffentlich zugänglichen Raum an.

### ❖ **Unabhängige Konformitätsbewertung für alle KI-Systeme mit hohem Risiko**

Der AIA-Entwurf sieht vor, dass die Konformitätsbewertung von Hochrisiko-Anwendungen, mit wenigen Ausnahmen, nur vom Anbieter selbst durchgeführt werden muss. So sollen die Anbieter selber die Einhaltung von Standards und damit die Rechtskonformität ihrer Systeme überprüfen. Wenn der Gesetzgeber sein Ziel einer „vertrauenswürdigen KI“ wirklich erreichen möchte, darf der AIA die Konformitätsbewertung von Hochrisiko-Systemen nicht der Selbsteinschätzung der Anbieter überlassen. Nur unabhängige Überprüfungen können Vertrauen in intransparente KI-Systeme schaffen und die Akzeptanz von KI im Allgemeinen befördern<sup>21</sup>.

Bei ihrer Markteinführung sollten alle Hochrisiko-Anwendungen einer unabhängigen Konformitätsbewertung gemäß Anhang VII unterzogen werden. Zudem sollte der AIA eine unabhängige Konformitätsbewertung von Hochrisiko-Systemen vorsehen, wenn es begründete Hinweise darauf gibt, dass sie nicht mehr die Anforderungen des AIA erfüllen (etwa wenn ein System geändert wurde oder in einem anderen Kontext eingesetzt wird).

### ❖ **Ergänzung der Rechtsdurchsetzung durch unabhängige Audits auf Antrag von Organisationen der Zivilgesellschaft**

Die Marktüberwachung nur auf Behörden und öffentliche Stellen zu beschränken (Art. 64 Abs. 3), ist nicht ausreichend. Organisationen der Zivilgesellschaft müssen das Recht haben, Prüfungen von hochriskanten KI-Systemen durch notifizierte Stellen zu verlangen. Dieses Antragsrecht sollte greifen, wenn es begründete Hinweise darauf gibt, dass Hochrisiko-KI-Systeme gegen europäisches oder nationales Recht verstoßen (unter anderem gegen die Bestimmungen des AIA), erhebli-

---

Change the Future of Marketing 48 (2020), in: Journal of the Academy of Marketing Science, H. 1, p. 24–42, URL: <https://link.springer.com/content/pdf/10.1007/s11747-019-00696-0.pdf> [Zugriff: 08.07.2021].

<sup>20</sup> EDPB & EDPS: EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination | European Data Protection Board (2021), URL: [https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible\\_en](https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en) [Zugriff: 20.07.2021].

<sup>21</sup> Das Bedürfnis der Verbraucher nach unabhängiger Kontrolle intransparenter KI Systeme spiegelt sich klar in aktuellen Umfragen wider. Vgl. BEUC: Artificial Intelligence: what consumers say - Findings and policy recommendations of a multi-country survey on AI (2020), URL: <https://www.beuc.eu/publications/survey-consumers-see-potential-artificial-intelligence-raise-serious-concerns/html> [Zugriff: 20.07.2021]; TÜV-Verband: Verbraucher wollen Sicherheit und Transparenz bei Künstlicher Intelligenz (2020), URL: <https://www.tuev-verband.de/IG-NB/vdtuev-startseite/news/ki-studie?context=e3068ebc9b4940b0b56ad4576ca633bd> [Zugriff: 20.07.2021].

che negative Auswirkungen auf das soziale, wirtschaftliche, physische oder psychische Wohlergehen oder die Sicherheit von Personen oder gesellschaftliche Gruppen haben oder erhebliche Umweltrisiken bergen.

Der Gesetzgeber muss verbindliche Verfahren für Anbieter hochriskanter KI-Systemen etablieren, die sicherstellen, dass notifizierte Stellen auf Antrag von Organisationen der Zivilgesellschaft, unabhängige Prüfungen durchführen können. Dazu gehört die Verpflichtung der Anbieter, den Prüfern Zugang zu allen Daten, Unterlagen und Aufzeichnungen zu gewähren, die erforderlich sind, um die Risiken des KI-Systems zu bewerten. Die Risikobewertung sollte, je nach Anwendungskontext, unter anderem Risiken für das soziale, wirtschaftliche, physische oder psychische Wohlergehen und die Sicherheit von Personen oder Gruppen sowie potenzielle Umweltauswirkungen des KI-Systems umfassen. Die notifizierte Stelle muss die Ergebnisse des Audits in einem Bericht veröffentlichen.

### ❖ **Gewährleistung der privaten Durchsetzung des AIA**

Verbraucher profitieren erheblich, wenn Verbraucherschutzorganisationen, ergänzend zur Rechtsdurchsetzung durch zuständige Behörden und öffentliche Stellen, ihre Rechte vor Gericht durchsetzen<sup>22</sup>. Um sicherzustellen, dass Verbraucherschutzorganisationen die AIA-Bestimmungen vor Gericht durchsetzen können, muss der Gesetzgeber den AIA in Anhang I der Europäischen Richtlinie über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher ((EU) 2020/1828)<sup>23</sup> aufnehmen.

### ❖ **Handelsabkommen dürfen Transparenz und Überwachung von KI-Systemen nicht einschränken**

Die zurzeit in der Welthandelsorganisation (WHO) diskutierten Regeln zur Nichtoffenlegung von Software Quellcodes könnten die Möglichkeit der Europäischen Union einschränken, künftig Regeln zur Zertifizierung und unabhängigen Bewertungen/Audits von KI-Systeme zu erlassen. Die Europäische Union muss sicherstellen, dass Handelsverträge europäischen Regulierungsplänen zu KI nicht im Wege stehen und den Verbraucherschutz an dieser Stelle nicht aushebeln können<sup>24</sup>.

---

<sup>22</sup> Verbraucherzentrale Bundesverband: Mehr Sammelklage wagen - Kurzpapier des vzbv (2021), URL: <https://www.vzbv.de/pressemitteilungen/mehr-sammelklage-wagen> [Zugriff: 21.07.2021]; Verbraucherzentrale Bundesverband: vzbv-Klage gegen VW führt zu Deutschlands größtem Massenvergleich (2020), URL: <https://www.vzbv.de/urteile/vzbv-klage-gegen-vw-fuehrt-zu-deutschlands-groesstem-massenvergleich> [Zugriff: 21.07.2021].

<sup>23</sup> European Parliament: Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (2020), URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32020L1828> [Zugriff: 21.07.2021].

<sup>24</sup> Verbraucherzentrale Bundesverband: Handelsabkommen dürfen die Regulierung von Algorithmen nicht einschränken. vzbv veröffentlicht Gutachten zu Auswirkungen von Handelsregeln auf EU-Algorithmenregulierung, URL: <https://www.vzbv.de/publikationen/handelsabkommen-duerfen-die-regulierung-von-algorithmen-nicht-einschraenken> [Zugriff: 09.08.2021].

## **Kontakt**

*Verbraucherzentrale  
Bundesverband e.V.*

*Team  
Digitales und Medien*

*Rudi-Dutschke-Straße 17  
10969 Berlin*

*[digitales@vzbv.de](mailto:digitales@vzbv.de)*