

Rechtslücke: Haftung & KI-Systeme

Fünf Gründe, warum ein Opfer ohne Entschädigung enden könnte

VULNERABILITÄT



Häufige Aktualisierungen und permanente externe Interaktionen ermöglichen es Hackern (die oft unauffindbar oder mittellos sind), das KI-System zu modifizieren oder Fehlfunktionen auszulösen.

KONNEKTIVITÄT



Ein KI-System ist mit vielen anderen KI- und nicht-KI-Systemen in einem komplexen digitalen Ecosystem verbunden, was es sehr schwierig macht, das schädigende System ausfindig zu machen.

AUTONOMIE



Ein KI-System kann ohne Kontrolle operieren, indem es seinen ursprünglichen Algorithmus eigenständig ändert oder von den ursprünglichen Anweisungen abweicht, ohne für seine Handlungen verantwortlich gemacht werden zu können.

INTRANSPARENZ



Self- und deeplearning Prozesse des KI-Systems machen es schwierig oder sogar unmöglich, bestimmte menschliche Eingaben oder Entscheidungen im Design, die die schädliche Aktivität ausgelöst haben, zurückzuverfolgen.

ABHÄNGIGKEIT



Externe Informationen, ohne die das KI-System nicht funktionieren kann, könnten fehlerhaft sein oder fehlen, von eingebauten Sensoren falsch wahrgenommen oder von Datenquellen/Lieferanten falsch übermittelt werden.

Mögliche Haftungsansprüche

für die von einem KI-System verursachten Schäden



Vertragspartner

Vertragsrecht

Situation: Das Opfer erlitt einen Schaden, der durch ein KI-System verursacht wurde, welches Bestandteil eines Vertrages war.

Verfahren: Der Vertragspartner haftet dann, wenn ihn ein Verschulden trifft oder wenn der Vertrag eine verschuldens-unabhängige Haftung vorsieht.



Produzent

Produkthaftung

Situation: Das Opfer erlitt einen Schaden, der durch ein defektes KI-System verursacht wurde.

Verfahren: Der Hersteller muss haften, wenn er sich nicht entlasten kann und wenn das Opfer den Schaden, den Fehler im Produkt und den Kausalzusammenhang zwischen beidem nachweisen kann.

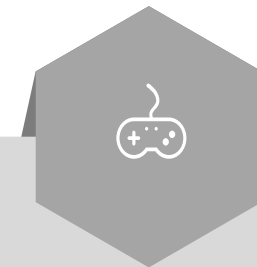


Drittpartei

Deliktsrecht

Situation: Das Opfer erlitt einen Schaden, der durch ein externen Eingriff verursacht wurde, welcher den Betrieb des KI-Systems beeinträchtigte.

Vorgehensweise: Der Störer (z.B. Hacker) unterliegt der verschuldensabhängigen Haftung, wenn der Eingriff den Schaden verursacht und er/sie die unerlaubte



Betreiber

Neue Verordnung

Situation: Das Opfer erlitt einen Schaden, der durch ein operierendes KI-System verursacht wurde.

Vorgehen: Der Betreiber unterliegt der verschuldens-unabhängigen Haftung, wenn das KI-System als „high-risk“ eingestuft wird. Ansonsten nur dann, wenn er/sie den Schaden zu verschulden hat.

Haftung des Betreibers

basierend auf einem risikobasierten Ansatz

Gefährdungshaftung

- Betreiber haftet für Schäden, die durch das high-risk KI-System verursacht werden, unabhängig vom Verschulden.
- Schäden bis zu einem Gesamtbetrag von max. 10 Mio. Euro (Tod/Gesundheit) oder 2 Mio. (Eigentum) zu ersetzen.
- Haftungsansprüche unterliegen je nach geschütztem Recht einer besonderen Verjährungsfrist von 10/30 Jahren.
- Keine Entlastungsmöglichkeit. Der Betreiber haftet nur nicht in Fällen höherer Gewalt.
- Eine Haftpflichtversicherung ist für jedes „high-risk“ KI-System obligatorisch.

Verschuldenshaftung

- Der Betreiber haftet für Schäden, die durch das KI-System verursacht werden, wenn ihn ein Verschulden trifft.
- Das Opfer eines Schadens profitiert von einer Verschuldens-vermutung gegen den Betreiber des KI-Systems.
- Haftungsbefreiung durch Nachweis, dass die Sorgfaltspflicht eingehalten wurde / Aktivierung ohne Wissen erfolgte.
- Betreiber haftet für Schäden, die durch Hacker verursacht wurden, wenn dieser unauffindbar oder mittellos ist.
- Nationale Gesetze über die Höhe/den Umfang der Entschädigung und die Verjährungsfristen gelten fort.

Einstufung eines KI-Systems als "high-risk"

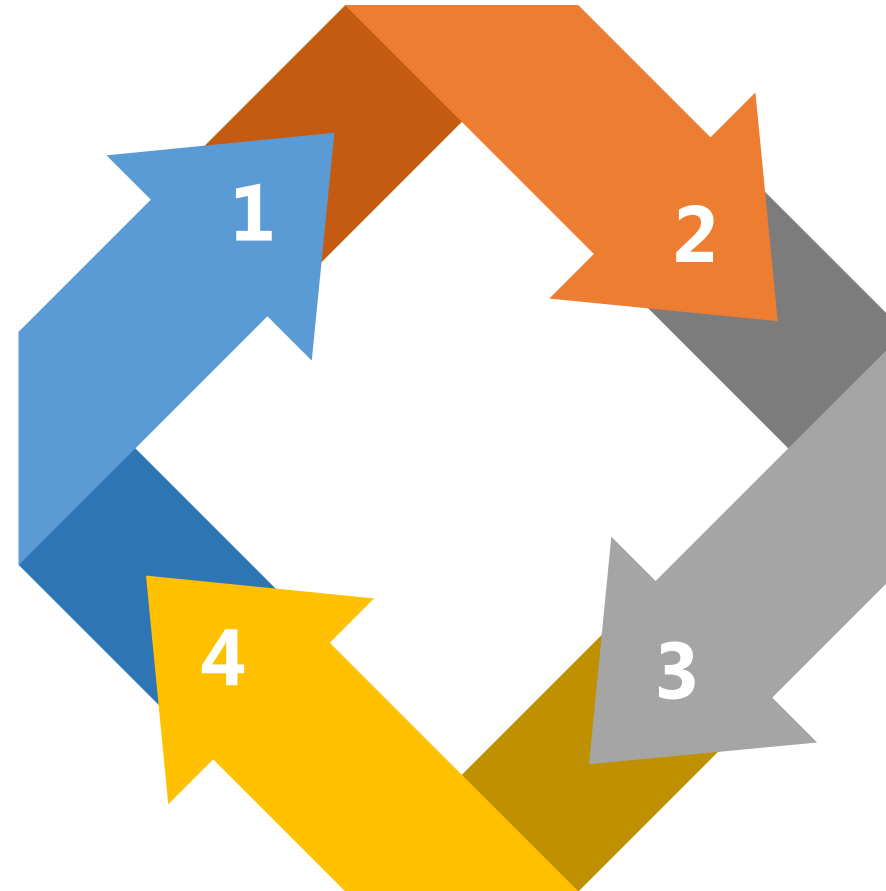
Legislatives Verfahren

Notifizierung

Zivilgesellschaft, Verbraucherorganisationen, Wissenschaftler, Unternehmen oder Mitgliedstaaten teilen der Kommission mit, dass ein neues KI-System als „high-risk“ eingestuft werden könnte.

Übergangsfrist

Delegierter Rechtsakt der Kommission klassifiziert das KI-System als „high-risk“ und tritt sechs Monate nach der Verabschiedung in Kraft



Überprüfung

Kommission + ständiger TCRAI-Ausschuss bewerten rechtlich/technisch, ob das KI-System den von der Verordnung festgelegten „high-risk“ Kriterien entspricht.

Widerspruch

Parlament und Rat (deren Experten auch an den vorherigen Überprüfungssitzungen teilnehmen können) haben zwei Monate Zeit, um gegen die Entscheidung der Kommission Einspruch zu erheben.