Künstliche Intelligenz als Täter ohne Schuld?

Strafrechtliche Zurechnung und Organisationsverantwortung bei KI gestützten Wirtschaftsstraftaten

Herausgeber: IAGO GmbH
Stand: 09.11.2025

Inhalt

1.0 Einführung

1.1 Problemstellung und aktuelle Relevanz

Die zunehmende Integration künstlicher Intelligenz (KI) in wirtschaftliche Entscheidungsprozesse hat das Strafrecht vor ein dogmatisches Paradox gestellt: KI-Systeme treffen faktisch eigenständige Entscheidungen, agieren lernbasiert und generieren wirtschaftlich relevante Ergebnisse. Es stellt sich jedoch die Frage, ob diese weder schuld- noch handlungsfähig im strafrechtlichen Sinne sind? Damit steht das geltende Strafrecht, das auf dem Prinzip individueller Schuld basiert, vor einem systemischen Bruch (vgl. Roxin/Greco, Strafrecht AT I, 5. Aufl. 2020, § 11 Rn. 11 ff.).

Im Bereich der Wirtschaftskriminalität ist dieses Problem besonders virulent. KI-basierte Systeme wie algorithmische Handelsplattformen, automatisierte Kreditbewertungsmodelle oder Lieferkettenoptimierer handeln mit hoher Eigenständigkeit und Geschwindigkeit. Fehler, Manipulationen oder diskriminierende Entscheidungen können Betrugstatbestände (§ 263 StGB), Untreue (§ 266 StGB), Marktmanipulation (§ 119 WpHG) oder Verstöße gegen das Datenschutzrecht (§ 42 BDSG) erfüllen, ohne dass ein menschliches Handlungs- oder Vorsatzmoment unmittelbar erkennbar ist (vgl. Tiedemann, Wirtschaftsstrafrecht, 6. Aufl. 2021, § 3 Rn. 18 ff.).

Damit entsteht die zentrale strafrechtliche Frage: Wer ist Täter, wenn die KI handelt?

Wird eine durch ein lernendes System ausgelöste Straftat automatisch der Geschäftsleitung zugerechnet (§ 130 OWiG, § 14 StGB)? Oder ist die KI als bloßes „Werkzeug“ im Sinne des § 25 Abs. 1 Alt. 2 StGB zu betrachten, dessen „Täter“ derjenige ist, der das System programmiert, trainiert oder einsetzt? Die herrschende Meinung lehnt eine eigenständige Täterschaft der KI ab, erkennt jedoch an, dass KI die menschliche Steuerung so weit überlagern kann, dass die Zurechnung dogmatisch nicht mehr sauber über das klassische Werkzeugmodell funktioniert (vgl. Gless, Zurechnung und Verantwortung im digitalen Zeitalter, ZStW 131 (2019), S. 1 ff., 5 f.).

Hinzu kommt die wirtschaftsorganisatorische Dimension: Der Einsatz autonomer Systeme begründet neue Pflichten der Geschäftsleitung zur Prävention, Überwachung und Risikosteuerung. Wird ein Unternehmen durch fehlerhafte oder manipulative KI-Handlungen geschädigt oder bereichert, kommt eine Verantwortlichkeit nach § 130 OWiG (Organisationsverschulden) oder eine Unternehmensgeldbuße nach § 30 OWiG in Betracht. Auch Delegationsversagen bei Compliance- oder IT-Beauftragten kann straf- oder bußgeldrechtliche Folgen haben (vgl. BGH, Urteil vom 17. 7. 2009 – 5 StR 394/08 „Siemens“, NJW 2009, 3437 [3439]; Wagner, in: BeckOK OWiG, 34. Edition 2024, § 130 Rn. 13 ff.).

Die Relevanz des Themas hat sich durch die Verabschiedung des EU Artificial Intelligence Act (AI Act) am 13. März 2024 weiter verschärft. Dieser normiert erstmals spezifische Compliance- und Risikomanagementpflichten für Anbieter und Betreiber hochriskanter KI-Systeme (Art. 9–15 AI Act). Verstöße gegen diese Pflichten sind

bußgeldbewehrt und haben unmittelbare Auswirkungen auf die strafrechtliche Bewertung von Organisations- und Aufsichtspflichten (vgl. EU AI Act 2024, Art. 99 Abs. 2 lit. b).

Das Strafrecht steht damit vor der Frage, ob es in einer digitalisierten Unternehmenswelt noch an das klassische Schuldprinzip festhalten kann oder ob es – ähnlich wie das Ordnungswidrigkeitenrecht – in Richtung einer funktionalen Verantwortlichkeit für KI-Entscheidungen entwickelt werden muss. Der gegenwärtige Zustand, in dem autonome Systeme zwar wirtschaftlich agieren, aber rechtlich als Nichtsubjekte gelten, führt zu einer Zurechnungslücke, die das Wirtschaftsstrafrecht weder dogmatisch noch praktisch zufriedenstellend schließt (vgl. Hilgendorf, KI und Strafrecht, in: NJW 2021, 1010 [1012]).

1.2 Zielsetzung und Methodik der Arbeit

Ziel dieser Untersuchung ist es, die dogmatischen Grundlagen der strafrechtlichen Verantwortlichkeit im Umgang mit KI-basierten Wirtschaftssystemen zu analysieren und auf ihre Anpassungsfähigkeit an autonome Entscheidungsprozesse zu prüfen. Im Mittelpunkt steht dabei die Frage, wie strafrechtliche Zurechnung, Vorsatz- und Fahrlässigkeitskonzepte sowie Organisationspflichten anzuwenden sind, wenn Handlungen nicht mehr direkt auf einen menschlichen Willensakt zurückgeführt werden können, sondern Ergebnis maschineller Lernprozesse sind.

Das herkömmliche Strafrecht beruht auf dem anthropozentrischen Schuldprinzip: Nur derjenige, der tatbestandsmäßig, rechtswidrig und schuldhaft handelt, kann Täter einer Straftat sein (§ 46 Abs. 1 StGB; Roxin/Greco, Strafrecht AT I, 5. Aufl. 2020, § 11 Rn. 10 ff.). KI-Systeme verfügen dagegen über keine Einsichtsfähigkeit, keine Willensfreiheit und kein Unrechtsbewusstsein. Sie sind daher nicht schuld- oder handlungsfähig und können keine Täter im strafrechtlichen Sinn sein. Dennoch erzeugen sie wirtschaftlich und faktisch Entscheidungen, die strafrechtlich relevante Folgen haben können – etwa durch automatisierten Betrug, Insiderhandel oder Diskriminierung (vgl. Hilgendorf, KI und Strafrecht, NJW 2021, 1010 [1012]).

Daraus ergeben sich zwei methodische Zielrichtungen:

1. Dogmatische Analyse:

Untersucht wird, wie die bestehenden Zurechnungskategorien – insbesondere mittelbare Täterschaft (§ 25 Abs. 1 Alt. 2 StGB), Fahrlässigkeit (§ 15 StGB) und Unterlassen (§ 13 StGB) – auf KI-basierte Handlungen übertragbar sind. Hierbei ist zu prüfen, ob KI-Systeme als „Werkzeuge“ gelten können oder ob sie ein eigenständiges „Risikoobjekt“ darstellen, dessen Einsatz besondere Sorgfaltspflichten begründet. Maßgeblich ist dabei die Überlegung, dass der Einsatz einer lernenden Maschine ein beherrschbares Risiko im Sinne der Verkehrssicherungspflichten schafft (vgl. Tiedemann, Wirtschaftsstrafrecht, 6. Aufl. 2021, § 3 Rn. 22 ff.).

2. Organisationsrechtliche Untersuchung:

Parallel wird geprüft, inwieweit die Organisationspflichten des Unternehmens

nach § 130 OWiG, § 43 GmbHG und § 93 AktG durch den Einsatz von KI verschärft werden. Unternehmen, die KI-Systeme produktiv einsetzen, schaffen automatisierte Entscheidungsketten, deren Überwachung und Steuerung menschlicher Kontrolle oft entzogen ist. In diesem Kontext stellt sich die Frage, ob die Nichtimplementierung von Kontrollmechanismen bereits ein strafrechtlich relevantes Organisationsverschulden begründen kann (vgl. Wagner, in: BeckOK OWiG, 34. Edition 2024, § 130 Rn. 19).

Die Arbeit verwendet eine dogmatisch-systematische Methode im Sinne von Larenz/Canaris (Methodenlehre der Rechtswissenschaft, 4. Aufl. 2019, S. 131 ff.), ergänzt durch eine rechtsvergleichende Perspektive mit Blick auf das europäische KI-Regulierungsrecht. Der neue EU AI Act (2024) wird als normativer Referenzrahmen für die Zurechnung von KI-Handlungen herangezogen, um zu prüfen, ob seine Compliance- und Haftungsmechanismen strafrechtliche Relevanz entfalten.

Zudem folgt die Untersuchung einem zweistufigen methodischen Aufbau:

Zunächst erfolgt eine dogmatische Rekonstruktion der geltenden Zurechnungskategorien im Strafrecht (Kapitel 3). Anschließend werden systematische Anpassungsmodelle entwickelt, die eine Einordnung von KI-Fehlhandlungen in die bestehende Haftungsdogmatik ermöglichen (Kapitel 5).

Das Ziel ist keine normative Gleichstellung von KI und Mensch, sondern die Klärung, wie weit menschliche Verantwortung reicht, wenn Entscheidungen faktisch von selbstlernenden Systemen getroffen werden. Die Arbeit versteht sich somit als Beitrag zur Entwicklung einer funktionalen Zurechnungsdogmatik für das digitale Zeitalter, die das Schuldprinzip wahrt, aber die Realität autonomer Systeme dogmatisch fassbar macht.

2.0 Begriff und Funktionsweise autonomer KI-Systeme

2.1 Technische Grundlagen: Selbstlernende Systeme und Entscheidungsautonomie

Künstliche Intelligenz (KI) bezeichnet im rechtlichen Sinn kein fest umrissenes technisches Verfahren, sondern eine funktionale Kategorie autonomer Informationsverarbeitungssysteme, die fähig sind, Muster aus Daten zu erkennen, daraus Regeln zu generieren und Entscheidungen ohne unmittelbare menschliche Steuerung zu treffen. Der EU Artificial Intelligence Act (AI Act) definiert in Art. 3 Nr. 1 KI-Systeme als softwarebasierte Systeme, die „für bestimmte vom Menschen definierte Ziele Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen erzeugen können“.

Im strafrechtlichen Kontext ist relevant, dass lernende Systeme ihre Entscheidungslogik fortlaufend anpassen („machine learning“). Dadurch entsteht eine dynamische Unvorhersehbarkeit: Das System kann aus Erfahrungen neue Korrelationen ableiten, die selbst der Entwickler nicht vollständig nachvollziehen kann. Diese sogenannte Black-Box-Struktur erschwert eine ex-post-Feststellung von Kausalität und Vorsatz erheblich (vgl. Hilgendorf, KI und Strafrecht, NJW 2021, 1010 [1011]; Gless, Zurechnung und

Verantwortung im digitalen Zeitalter, ZStW 131 (2019), 5 f.).

Aus strafrechtlicher Sicht bedeutet dies: Das Tatgeschehen verlagert sich von der unmittelbaren Handlung des Menschen hin zur Konfiguration und Freigabe des KI-Systems. Die Steuerung erfolgt nicht mehr durch situatives Handeln, sondern durch vorherige Risikoentscheidungen – etwa die Auswahl von Trainingsdaten, die Definition von Zielparametern oder die Freigabe zur autonomen Ausführung. Damit verlagert sich auch die strafrechtliche Verantwortung in die präventive Organisations- und Überwachungsebene (§ 13 StGB, § 130 OWiG).

2.2 Rechtsdogmatische Einordnung – Kein Rechtssubjekt, aber Zurechnungsobjekt

Die KI ist kein Rechtssubjekt. Sie kann keine Rechte oder Pflichten tragen, keine Schuld empfinden und keine Tat im strafrechtlichen Sinn begehen. Dennoch muss sie als Zurechnungsobjekt begriffen werden: Ihre Funktionalität kann einer natürlichen oder juristischen Person zugerechnet werden, wenn diese das System beherrscht, betreibt oder über seinen Einsatz entscheidet.

Die herrschende Meinung lehnt eine „elektronische Täterschaft" strikt ab (vgl. Roxin/Greco, Strafrecht AT I, § 11 Rn. 10 ff.; Tiedemann, Wirtschaftsstrafrecht, 6. Aufl. 2021, § 3 Rn. 22 ff.). Stattdessen wird der Einsatz einer KI als Fall mittelbarer Täterschaft (§ 25 Abs. 1 Alt. 2 StGB) verstanden: Der Mensch bedient sich der KI als Werkzeug, das tatbestandsmäßige Handlungen ausführt, ohne selbst schuldhaft handeln zu können.

Problematisch ist jedoch, dass sich die KI – anders als ein menschliches Werkzeug – nicht vollständig instrumentalisieren lässt. Sie entwickelt ein eigenes, nicht vorhersehbares Entscheidungsverhalten. Damit droht das klassische Zurechnungsmodell zu scheitern, weil der Täter die Handlung des Systems nicht mehr inhaltlich beherrscht. Die dogmatische Figur der mittelbaren Täterschaft setzt aber gerade die Tatherrschaft über den Tatverlauf voraus (vgl. BGH, Beschl. v. 21. 6. 1994 – 5 StR 132/94, NJW 1994, 3010 [3011]).

In der Literatur wird daher zunehmend ein funktionales Verantwortungsmodell vertreten, das die Strafbarkeit an die Schaffung und Beherrschung von Risikostrukturen knüpft, unabhängig von der konkreten Tatherrschaft (Gless, ZStW 131 (2019), 12 ff.; Hilgendorf, NJW 2021, 1012). Danach haftet, wer die KI in den Rechtsverkehr bringt oder ihre autonome Entscheidung freigibt, weil er das Risiko der normwidrigen Entscheidung begründet hat. Dogmatisch nähert sich dieses Modell dem Organisationsdelikt des § 130 OWiG und rückt die Pflichtenstellung statt den Vorsatz in den Mittelpunkt.

2.3 Europäische Regulierung: Der EU-AI-Act als strafrechtlicher Referenzrahmen

Mit dem EU Artificial Intelligence Act (AI Act), angenommen durch das Europäische Parlament am 13. März 2024, hat der Gesetzgeber erstmals ein kohärentes Pflichtenregime für KI-Systeme geschaffen. Er unterscheidet nach Risikostufen („unacceptable", „high-risk", „limited", „minimal risk") und verpflichtet Anbieter und Betreiber insbesondere zu:

- einem Risikomanagementsystem (Art. 9 AI Act),

- Datenqualitäts- und Trainingsstandards (Art. 10),
- technischer Transparenz und Nachvollziehbarkeit (Art. 13),
- menschlicher Aufsicht („human oversight“, Art. 14),
- sowie Robustheit und Sicherheit (Art. 15).

Diese Pflichten besitzen quasi-strafrechtliche Relevanz, da Verstöße mit Bußgeldern bis zu 35 Millionen Euro oder 7 % des weltweiten Jahresumsatzes sanktioniert werden (Art. 99 Abs. 2 lit. b AI Act). Zugleich können sie als strafrechtlicher Maßstab für Sorgfaltspflichten dienen, etwa bei der Beurteilung von Fahrlässigkeit oder Organisationsverschulden.

Dogmatisch ist damit ein Übergang von individueller Schuldhaftung zu einer objektivierten Compliance-Verantwortung erkennbar. Wer ein KI-System ohne ausreichende Überwachung einsetzt, verletzt die durch das EU-Recht konkretisierte Pflicht zur Gefahrenvermeidung und kann über § 130 OWiG oder § 13 StGB strafrechtlich verantwortlich werden (vgl. Wagner, BeckOK OWiG, § 130 Rn. 19; Hilgendorf, NJW 2021, 1010 [1013]).

Der AI Act fungiert somit als Brückennorm zwischen Technikrecht und Strafrecht. Er liefert Kriterien, wann eine Organisation schuldhaft versagt, wenn KI-Systeme wirtschaftliche Straftatbestände verwirklichen. Strafrechtlich bleibt das Handeln der KI zwar nicht selbst zurechenbar, aber ihr Einsatz kann die Schwelle zu einer Sorgfaltspflichtverletzung mit Organisationsverschulden überschreiten – ein Paradigmenwechsel vom Täter zum Systemverantwortlichen.

3.0 Strafrechtliche Zurechnung von KI-Handlungen

3.1 Tatherrschaftsmodelle bei automatisierten Systemen

Das Strafrecht setzt Täterhandeln voraus. Nach herrschender Lehre besitzt Täterqualität, wer das Geschehen kraft seines Willens beherrscht – das sog. Tatherrschaftsprinzip (Roxin/Greco, Strafrecht AT I, 5. Aufl. 2020, § 25 Rn. 30 ff.). Bei KI-gestützten Wirtschaftssystemen bricht diese Voraussetzung: Das System handelt aufgrund algorithmischer Prozesse, nicht aufgrund menschlicher Entscheidung.

Dogmatisch wird deshalb versucht, die KI unter das Modell der mittelbaren Täterschaft (§ 25 Abs. 1 Alt. 2 StGB) zu fassen: Der Mensch bedient sich eines Werkzeugs, das tatbestandsmäßiges Verhalten ausführt, ohne selbst schuldhaft zu handeln. Da die KI kein schuldfähiges Wesen ist, erfüllt sie formal das Tatbestandsmerkmal des „schuldlosen Werkzeugs“. Problematisch ist aber, dass der Täter die konkrete Handlung nicht mehr steuert, sobald das System lernbasiert und selbstadaptiv agiert. Damit fehlt ihm die tatsächliche Tatherrschaft (vgl. Gless, Zurechnung und Verantwortung im digitalen Zeitalter, ZStW 131 (2019), 10 ff.).

In der Literatur wird daher eine funktionale Ausweitung des Tatherrschaftsbegriffs vorgeschlagen: Nicht die unmittelbare Steuerung, sondern die Beherrschung der Risikostruktur soll maßgeblich sein (Hilgendorf, KI und Strafrecht, NJW 2021, 1010

[1012]). Danach besitzt Täterqualität, wer das System entwirft, einsetzt oder ohne angemessene Überwachung betreibt – also wer über die Entstehung und Nutzung des KI-Risikos entscheidet. Dieses Konzept ersetzt die klassische Handlungsherrschaft durch eine Risikoherrschaft.

Der BGH hat in analogen Fällen der Automatisierung (z. B. Computerbetrug) anerkannt, dass Handlungen über programmierte Abläufe dem Menschen zugerechnet werden können, wenn dieser die Initialhandlung kontrolliert (BGH, Beschl. v. 21. 6. 1994 – 5 StR 132/94, NJW 1994, 3010 [3011]). Für autonome Systeme reicht jedoch eine solche Initialkausalität kaum aus, da sie nicht sämtliche Folgeverläufe umfasst. Hier setzt die Diskussion um Organisationsdelikte an (§ 130 OWiG).

3.2 Mittelbare Täterschaft durch Einsatz von KI (§ 25 Abs. 1 Alt. 2 StGB)

Die Anwendung des § 25 Abs. 1 Alt. 2 StGB auf KI verlangt zwei Voraussetzungen:

1. Der Täter nutzt die KI als Werkzeug zur Tatverwirklichung.

2. Die KI handelt schuldlos.

Beide Merkmale sind formal erfüllt; problematisch bleibt, dass das System keine bewusst gesteuerte Tat begeht. Roxin führt aus, dass mittelbare Täterschaft nur vorliegt, wenn der Täter „das Geschehen kraft überlegenen Wissens oder Wollens in den Händen hält“ (Roxin/Greco, a. a. O., § 25 Rn. 34). Bei KI entfällt diese Überlegenheit regelmäßig.

Ein alternativer Ansatz begreift die KI als „quasi-Werkzeug“, das durch vorherige Programmierung oder Datensteuerung mittelbar gelenkt wird. Hier kann die Tatherrschaft in der Konfiguration des Systems liegen – etwa bei bewusst fehlerhaftem Training, manipulativer Datenzufuhr oder gezieltem Einsatz zur Marktmanipulation (Tiedemann, Wirtschaftsstrafrecht, 6. Aufl. 2021, § 3 Rn. 24 ff.). In diesen Fällen besteht eine bewusste Risikoschaffung mit dolus eventualis, die eine täterschaftliche Zurechnung erlaubt.

Fehlt eine solche bewusste Manipulation, bleibt nur die Fahrlässigkeitshaftung (§ 15 StGB) oder die Verantwortlichkeit über Organisationspflichten (§ 130 OWiG).

3.3 Fehlerhafte Algorithmen und Fahrlässigkeit (§§ 15, 222 StGB)

Wirtschaftsstrafrechtlich relevant ist die fahrlässige Begehung von Straftaten durch fehlerhafte KI-Systeme. Fahrlässigkeit setzt eine pflichtwidrige Sorgfaltspflichtverletzung voraus (§ 15 StGB). Bei KI manifestiert sich diese Pflichtverletzung im fehlenden Risikomanagement – etwa unzureichenden Tests, fehlender Überwachung oder Nichtbeachtung technischer Warnungen.

Nach der Lehre von der objektiven Zurechnung haftet, wer eine rechtlich missbilligte Gefahr schafft, die sich im tatbestandsmäßigen Erfolg realisiert (Roxin/Greco, AT I, § 11 Rn. 72 ff.). Wer eine lernfähige KI ohne angemessene Kontrollen einsetzt, schafft genau ein solches Risiko. Entsprechend kann die Geschäftsleitung oder der verantwortliche IT-Beauftragte bei eintretendem Schaden strafrechtlich verantwortlich sein (Hilgendorf, NJW 2021, 1010 [1013]).

Beispiel: Ein autonomes Handelssystem tätigt selbstständig Marktmanipulationen (§ 119 WpHG), weil es algorithmisch falsche Signale erkennt. Der Entwickler oder Betreiber, der keine Kontrollmechanismen implementierte, handelt fahrlässig. Ein Vorsatz liegt nicht vor, wohl aber eine objektive Pflichtverletzung. Das entspricht der Fahrlässigkeitsdogmatik des Technikstrafrechts (vgl. Jescheck/Weigend, Lehrbuch des Strafrechts AT, 5. Aufl. 1996, S. 284 ff.).

3.4 Haftung juristischer Personen und Leitungspflichten (§§ 30, 130 OWiG)

Da die KI typischerweise in Unternehmensstrukturen operiert, rückt das Unternehmensstrafrecht in den Mittelpunkt. Nach § 30 Abs. 1 OWiG kann gegen juristische Personen eine Geldbuße verhängt werden, wenn jemand in Leitungsfunktion eine Straftat oder Ordnungswidrigkeit begeht, durch die Pflichten des Unternehmens verletzt werden. Ergänzend erfasst § 130 OWiG das Organisationsverschulden: Wer als Leiter oder Aufsichtsperson Aufsichtsmaßnahmen unterlässt, begeht selbst eine Ordnungswidrigkeit.

Diese Normen sind das zentrale Einfallstor für die strafrechtliche Zurechnung von KI-Fehlhandlungen. Denn auch wenn kein menschlicher Täter im klassischen Sinn existiert, kann das Unternehmen haften, wenn es unzureichende Aufsichtsstrukturen für seine KI-Systeme implementiert. Die Rechtsprechung zu „Siemens“ (BGH, NJW 2009, 3437 [3439]) bestätigt, dass organisatorische Defizite bereits ein Bußgeldtatbestand sind.

Mit dem AI Act 2024 werden diese Pflichten europarechtlich konkretisiert: Die Anforderungen an Risikomanagement (Art. 9), Datenqualität (Art. 10) und menschliche Aufsicht (Art. 14) definieren den Sorgfaltsmaßstab, dessen Verletzung zugleich ein Organisationsverschulden im Sinne von § 130 OWiG begründet (Wagner, BeckOK OWiG, 34. Edition 2024, § 130 Rn. 19).

Damit entsteht ein neues Verantwortungsmodell: Nicht die KI ist Täter, sondern das Unternehmen als Verantwortungsträger eines autonomen Systems. Strafrechtlich manifestiert sich dies als funktionales Organisationsdelikt, das den Übergang vom individuellen Schuldprinzip zur kollektiven Risikoverantwortung markiert (Gless, ZStW 131 (2019), 18 ff.).

4.0 Organisations- und Überwachungspflichten im Unternehmen

4.1 Delegation, Aufsicht und KI-Compliance

Die Nutzung künstlicher Intelligenz in Unternehmen verschiebt die Verantwortung für rechtmäßiges Verhalten in eine technisch vermittelte Organisationssphäre. Während das klassische Strafrecht an individuelle Handlungen anknüpft, entstehen durch den Einsatz von KI neue Verantwortungsstrukturen, in denen Pflichten an Algorithmen und interne Beauftragte delegiert werden.

Die zentrale Norm ist § 130 OWiG, der die Verletzung der Aufsichtspflicht in Betrieben sanktioniert. Danach haftet, wer als Inhaber oder Leiter eines Unternehmens erforderliche Aufsichtsmaßnahmen unterlässt, um Rechtsverstöße zu verhindern. Diese

Vorschrift ist der strafrechtliche Anker für KI-bezogene Organisationspflichten (Wagner, in: BeckOK OWiG, 34. Edition, § 130 Rn. 17 ff.).

Der BGH hat bereits im „Siemens"-Urteil (Urt. v. 17. 7. 2009 – 5 StR 394/08, NJW 2009, 3437 [3439]) festgestellt, dass Unternehmen eine präventive Pflicht zur Einrichtung effektiver Compliance-Systeme trifft. Auf KI-Systeme übertragen bedeutet das: Der Einsatz autonomer Software ohne Überwachung oder Risikoanalyse stellt ein Organisationsverschulden dar, wenn dadurch rechtswidrige Handlungen begünstigt werden.

- Eine ordnungsgemäße KI-Compliance verlangt deshalb:
- eine Risikobewertung vor Implementierung,
- laufende Kontrolle und Protokollierung von Systementscheidungen,
- Eingriffsmöglichkeiten („human-in-the-loop") nach Art. 14 AI Act,
- und die Schulung verantwortlicher Mitarbeiter.

Fehlen diese Elemente, ist der Tatbestand des § 130 OWiG erfüllt. Damit wird KI zum Prüfstein der Delegationsdogmatik: Pflichten können nur dann delegiert werden, wenn der Empfänger fachlich geeignet, organisatorisch eingebunden und überwacht ist (Körber, in: MünchKomm GmbHG, 4. Aufl. 2022, § 43 Rn. 120 ff.). Die bloße Installation eines Algorithmus entlastet die Geschäftsleitung nicht – sie bleibt Garantin der rechtmäßigen Unternehmensorganisation (§ 13 StGB).

4.2 Verantwortung der Geschäftsleitung (§ 43 GmbHG, § 93 AktG)

Nach § 43 Abs. 1 GmbHG und § 93 Abs. 1 AktG müssen Geschäftsleiter die Sorgfalt eines ordentlichen Geschäftsmanns wahren. Diese Pflicht umfasst auch den Einsatz, die Kontrolle und die Überwachung digitaler Systeme. Der Einsatz von KI ohne ausreichende Prüfmechanismen verstößt gegen diese Sorgfaltspflicht und kann eine persönliche Haftung der Geschäftsleitung begründen.

Die Pflichtenlage wird durch den AI Act konkretisiert: Art. 9–15 verpflichten Betreiber hochriskanter KI-Systeme zu kontinuierlichem Risikomanagement, menschlicher Aufsicht und Sicherheitsvalidierung. Diese Bestimmungen präzisieren, was im Sinne des deutschen Unternehmensstrafrechts als „erforderliche Aufsichtsmaßnahme" gilt. Ein Verstoß gegen diese Anforderungen erfüllt daher regelmäßig den Tatbestand des Organisationsverschuldens (vgl. Hilgendorf, KI und Strafrecht, NJW 2021, 1010 [1013]; Wagner, BeckOK OWiG, § 130 Rn. 19).

Dogmatisch handelt es sich um eine Garantenpflicht kraft Ingerenz: Wer ein autonomes System in Betrieb nimmt, schafft eine Gefahrenquelle und ist verpflichtet, diese zu beherrschen (Roxin/Greco, Strafrecht AT I, § 11 Rn. 75 ff.). Die Unterlassung angemessener Überwachung kann somit strafrechtlich relevant werden, wenn ein KI-System tatbestandsmäßige Handlungen ausführt, die auf Fehlkonfiguration, Datenverzerrung oder mangelnde Aufsicht zurückzuführen sind.

4.3 Pflichten von Compliance- und IT-Beauftragten

Auch interne Beauftragte – insbesondere Compliance-, Datenschutz- oder IT-Sicherheitsbeauftragte – tragen eigenständige Überwachungspflichten. Wird eine KI für Geschäftsentscheidungen eingesetzt, sind diese Beauftragten verpflichtet, deren Rechtmäßigkeit, Datensicherheit und technische Kontrolle zu gewährleisten.

Nach der Rechtsprechung (BGH, NJW 2009, 3437 [3439]) bleibt die Überwachungspflicht der Unternehmensleitung bestehen, kann aber funktional an Beauftragte delegiert werden. Diese übernehmen dadurch eine eigenständige Garantenstellung (§ 13 StGB) und haften persönlich, wenn sie trotz Kenntnis oder fahrlässiger Unkenntnis von Risiken nicht handeln (vgl. Gurlit, ZHR 185 (2021), 224 f.).

Im Bereich der KI-Compliance bedeutet das:

- Unterlassene Risikoanalysen oder Prüfungen des Algorithmus können eine persönliche Haftung auslösen.
- Versäumnisse bei der Dokumentation oder Meldung von KI-Fehlentscheidungen erfüllen § 130 OWiG.
- Ein Verstoß gegen datenschutzrechtliche Vorgaben (Art. 32 DSGVO) kann zusätzlich ordnungswidrig oder strafbar sein (§ 42 BDSG).

Die Verantwortung interner Beauftragter erstreckt sich damit auch auf technische Überwachungsmaßnahmen. Sie müssen gewährleisten, dass KI-Systeme nachvollziehbar und auditierbar bleiben. Wer eine Black-Box-Entscheidung ohne Kontrollmechanismen akzeptiert, verletzt seine Sorgfaltspflichten und handelt ordnungswidrig (vgl. Rossi, in: BeckOK Datenschutzrecht, 41. Edition 2024, Art. 38 Rn. 5).

4.4 Unterlassen und Garantenstellung (§ 13 StGB) bei KI-Fehlhandlungen

Das strafbare Unterlassen setzt eine Garantenpflicht voraus (§ 13 StGB). Diese Pflicht entsteht entweder aus Gesetz, Vertrag, freiwilliger Übernahme oder aus pflichtwidrigem Vorverhalten. Im Kontext von KI ist entscheidend, dass sowohl Geschäftsleitung als auch Beauftragte durch Ingerenz – also die Schaffung eines Risikos durch Implementierung der KI – Garant für dessen Kontrolle werden (Roxin/Greco, AT I, § 11 Rn. 76 ff.).

Wenn eine KI rechtswidrige Marktentscheidungen trifft oder personenbezogene Daten missbräuchlich verarbeitet, liegt ein tatbestandsmäßiges Unterlassen vor, wenn Verantwortliche technische Eingriffe unterlassen, obwohl sie Kenntnis oder Kenntnismöglichkeit hatten. Entscheidend ist nicht die Kontrolle der Einzelentscheidung, sondern die Pflicht zur Risikovorsorge.

Der BGH hat bereits anerkannt, dass das Unterlassen von Überwachungsmaßnahmen eine strafbare Pflichtverletzung sein kann, wenn dadurch deliktisches Verhalten ermöglicht oder erleichtert wird (BGH, Beschl. v. 21. 6. 1994 – 5 StR 132/94, NJW 1994, 3010 [3011]). Für KI-Systeme bedeutet das: Unterbleibt die Einrichtung von Kontrollalgorithmen oder Audit-Trails, liegt

eine Garantenpflichtverletzung vor, die den Tatbestand des § 13 StGB erfüllen kann.

Damit wird deutlich: Das Strafrecht verschiebt seinen Fokus von der individuellen Handlung auf die Systemaufsichtspflicht. Die Verantwortung des Menschen endet nicht dort, wo der Algorithmus beginnt. Die Verantwortung beginnt dort erst.

5.0 Dogmatische Grenzfragen und Reformüberlegungen

5.1 KI als „Täter ohne Schuld" – Zurechnungslücken und Analogieprobleme

Das geltende Strafrecht ist auf menschliche Handlungsträger zugeschnitten. Es kennt weder ein maschinelles Schuldprinzip noch eine digitale Eigenverantwortung. Eine KI kann kein Unrecht erkennen, keinen Vorsatz bilden und kein Unrechtsbewusstsein entwickeln – damit fehlt ihr jede strafrechtliche Persönlichkeitsstruktur (Roxin/Greco, Strafrecht AT I, 5. Aufl. 2020, § 11 Rn. 10 ff.).

Die klassische Lehre der Täterschaft scheitert daher an der KI, weil sie voraussetzt, dass der Täter „Tatherrschaft kraft Willens" besitzt. KI-Systeme handeln aber aufgrund algorithmischer Strukturen, nicht aufgrund eines eigenen Willens. Das führt zu einer dogmatischen Zurechnungslücke: Zwischen menschlicher Verantwortung und maschinellem Verhalten entsteht ein Bereich faktischer Wirkung ohne unmittelbare normative Steuerung.

In der Literatur wurden verschiedene Ansätze entwickelt, um diese Lücke zu schließen:

1. Haftungsdogmatische Analogie: KI wird als „Werkzeug ohne Willen" verstanden; verantwortlich bleibt der Mensch, der sie bedient oder freigibt (Hilgendorf, KI und Strafrecht, NJW 2021, 1010 [1012]).

2. Funktionsverantwortungsmodell: Verantwortung folgt nicht mehr aus Handlung, sondern aus der Kontrolle über Risikostrukturen. Wer KI einsetzt, haftet für ihre Wirkungen, unabhängig von direkter Steuerung (Gless, Zurechnung und Verantwortung im digitalen Zeitalter, ZStW 131 (2019), 12 ff.).

3. Organisationsdelikt-Modell: Die Verantwortlichkeit wird kollektivisiert – nicht der einzelne Mensch, sondern das Unternehmen als soziales Handlungssystem trägt die Verantwortung (§§ 30, 130 OWiG).

Keiner dieser Ansätze ist dogmatisch vollständig überzeugend. Die Analogie zur mittelbaren Täterschaft bleibt künstlich, weil KI weder schuld- noch steuerbar ist. Das Funktionsmodell droht das Schuldprinzip zu unterlaufen, indem es reine Risikozurechnung ohne individuellen Tatvorwurf zulässt. Und das Organisationsmodell verlagert die Haftung auf kollektive Verantwortung, ohne das Problem individueller Schuld zu lösen (Tiedemann, Wirtschaftsstrafrecht, 6. Aufl. 2021, § 3 Rn. 25 ff.).

Damit steht das Strafrecht vor einer Grundfrage: Will es das Schuldprinzip um jeden Preis erhalten – oder seine Kategorien funktional modernisieren? Eine dogmatische Fortentwicklung scheint unvermeidbar, da das starre Handlungsmodell bei selbstlernenden Systemen an seine Grenzen stößt.

5.2 Entwicklung eines strafrechtlichen Organisationsdelikts für KI-Systeme

Ein Weg zur dogmatischen Integration der KI wäre die Einführung eines eigenständigen Organisationsdelikts, das die Verantwortlichkeit für fehlerhafte KI-Systeme normiert. Vergleichbare Strukturen existieren bereits im Ordnungswidrigkeitenrecht (§ 130 OWiG) und im Umweltstrafrecht (§ 324 ff. StGB).

Ein solches Delikt könnte – angelehnt an § 130 OWiG – formulieren:

„Wer als Verantwortlicher ein KI-System betreibt oder einsetzen lässt und die erforderlichen Aufsichtsmaßnahmen unterlässt, die notwendig sind, um rechtswidrige Handlungen durch das System zu verhindern, wird bestraft."

Dieses Modell würde das Organisationsverschulden zur strafrechtlichen Haupttat erheben. Es würde weder den KI-Systemen Eigenverantwortung zuschreiben noch das Schuldprinzip aufgeben, sondern die Pflichtverletzung des Verantwortlichen zur zentralen Bezugsnorm machen.

Dogmatisch ließe sich ein solches Delikt auf das Prinzip der Pflichtenposition kraft Ingerenz stützen (§ 13 StGB). Wer KI-Risiken schafft, übernimmt eine Garantenstellung für deren Kontrolle. Diese Verantwortlichkeit wäre vergleichbar mit der des Betriebsleiters im Umwelt- oder Arzneimittelrecht (vgl. BGH, Beschl. v. 21. 6. 1994 – 5 StR 132/94, NJW 1994, 3010 [3011]).

Reformvorschläge in der Literatur zielen auf eine gesetzliche Kodifizierung von Unternehmensverantwortung im Strafrecht (vgl. Gless, ZStW 131 (2019), 15 ff.; Hilgendorf, NJW 2021, 1012). Die EU-Kommission prüft bereits in Verbindung mit dem AI Liability Directive Proposal (COM(2022) 496 final) die Einführung einer verschuldensunabhängigen Haftung für KI-Schäden. Diese Tendenz könnte mittelbar auf das Strafrecht wirken, indem die Pflicht zur Überwachung autonomer Systeme konkretisiert wird.

5.3 Europäische Harmonisierungsperspektive

Der europäische Gesetzgeber hat mit dem AI Act 2024 und der geplanten AI Liability Directive eine strukturelle Annäherung von Technikrecht, Haftungsrecht und Strafrecht eingeleitet. Diese Regelwerke begründen präventive Risikopflichten, deren Verletzung bußgeldbewehrt ist und damit den objektiven Tatbestand zukünftiger Strafnormen vorzeichnet.

Art. 9–15 AI Act normieren detaillierte Anforderungen an Risikomanagement, Datenqualität, menschliche Aufsicht und technische Robustheit. Diese Standards fungieren als konkretisierte Sorgfaltsmaßstäbe, deren Missachtung den objektiven Tatbestand eines Organisationsdelikts erfüllen könnte. Die dogmatische Herausforderung besteht darin, diese Normen in das nationale Strafrecht zu integrieren, ohne das Schuldprinzip aufzugeben (vgl. Hilgendorf, NJW 2021, 1013).

Langfristig dürfte sich in Europa ein duales Verantwortlichkeitsmodell herausbilden:

1. Zivilrechtliche und regulatorische Haftung auf Grundlage des AI Act und der AI Liability Directive.

2. Strafrechtliche Organisationsverantwortung, die an § 130 OWiG anknüpft und künftig als Unternehmensstraftat ausgestaltet werden könnte.

Damit wandelt sich das Strafrecht von einem personalen Schuldstrafrecht zu einem systemisch-normativen Haftungsstrafrecht. KI wird nicht Täter, aber Auslöser normativer Verantwortung. Der Mensch bleibt strafrechtlich verantwortlich, doch seine Verantwortung verschiebt sich von der Tat zur Organisation.

6.0 Schlussbetrachtung

6.1 Systematische Bewertung

Die Untersuchung hat gezeigt, dass der Einsatz autonomer KI-Systeme wie „AI Sola" das Strafrecht in seinen Grundfesten herausfordert. Das geltende Recht ist auf individuelle Verantwortlichkeit und willensgesteuertes Handeln zugeschnitten. KI-Systeme handeln jedoch ohne Bewusstsein, Vorsatz oder Einsicht, wodurch die klassischen Kategorien von Tat, Schuld und Täterschaft unzureichend werden (Roxin/Greco, Strafrecht AT I, 5. Aufl. 2020, § 11 Rn. 10 ff.).

Im Bereich der Wirtschaftskriminalität führt das zu einer Zurechnungslücke: KI kann Straftatbestände technisch erfüllen – etwa Marktmanipulation (§ 119 WpHG), Betrug (§ 263 StGB) oder Datenschutzverstöße (§ 42 BDSG) – ohne dass ein handelnder Mensch klar identifiziert werden kann. Der bisherige Rückgriff auf die Figur des „schuldlosen Werkzeugs" (§ 25 Abs. 1 Alt. 2 StGB) greift zu kurz, weil die KI nicht bloß ausgeführt, sondern eigenständig gelernt und entschieden hat (Gless, ZStW 131 (2019), 12 ff.).

Damit verschiebt sich das strafrechtliche Verantwortungsmodell von der Handlungstäterschaft zur Organisationsverantwortung. Wer KI-Systeme einsetzt, schafft ein autonomes Risikoobjekt und übernimmt damit eine Garantenpflicht kraft Ingerenz (§ 13 StGB). Versäumt er, dieses Risiko durch Kontrolle, Überwachung oder Abschaltung zu beherrschen, liegt ein strafrechtlich relevantes Unterlassen vor (Hilgendorf, KI und Strafrecht, NJW 2021, 1010 [1013]).

§ 130 OWiG wird so zum zentralen Haftungsanker: Er sanktioniert die Verletzung betrieblicher Aufsichtspflichten und lässt sich auf KI-Systeme übertragen, deren Verhalten durch menschliche Überwachung vermeidbar gewesen wäre. In Verbindung mit den Pflichten aus dem EU AI Act 2024 entsteht daraus ein europäisch determiniertes Haftungsregime, das präventive Compliance-Pflichten in strafrechtliche Verantwortung transformiert (Wagner, in: BeckOK OWiG, 34. Edition 2024, § 130 Rn. 19).

6.2 Dogmatische Konsequenzen

Dogmatisch zeigt sich ein klarer Trend: Das Strafrecht entwickelt sich von einer reaktiven Tatverantwortung zu einer präventiven Risikohaftung. Der Schuldgedanke wird nicht aufgegeben, aber funktional umgedeutet. Schuld besteht künftig nicht mehr in der bösen Gesinnung oder bewussten Tat, sondern in der Verletzung objektivierter Organisationspflichten.

Damit verliert die Unterscheidung zwischen Täterschaft und Unterlassen an Schärfe. Der Verantwortliche ist nicht mehr Täter einer Handlung, sondern Unterlassender im Vorfeld – ein Konzept, das bereits im Umwelt- und Produktsicherheitsstrafrecht vorgeprägt ist. KI beschleunigt diese Entwicklung und zwingt das Strafrecht, sich als Risikosteuerungsrecht zu begreifen (vgl. Tiedemann, Wirtschaftsstrafrecht, 6. Aufl. 2021, § 3 Rn. 25 ff.).

Gleichzeitig wird das Verhältnis zwischen Mensch und Maschine normativ neu justiert: Der Mensch bleibt Verantwortungsträger, aber nicht mehr für die Einzelhandlung, sondern für die Schaffung und Kontrolle autonomer Entscheidungssysteme. Das Strafrecht rückt damit näher an das öffentliche Wirtschaftsrecht und das Compliance-Regime des AI Act heran – eine Entwicklung, die Hilgendorf treffend als „Beginn des funktionalen Strafrechts im digitalen Zeitalter" bezeichnet hat (NJW 2021, 1010 [1014]).

6.3 Rechtspolitische Perspektive

Rechtspolitisch besteht dringender Handlungsbedarf. Die geltenden Strafnormen sind nicht technikneutral genug, um selbstlernende Systeme adäquat zu erfassen. Notwendig ist:

1. Ein neues Organisationsdelikt für KI-Systeme

Eine Norm analog zu § 130 OWiG im StGB, die die unterlassene Überwachung von KI-Systemen ausdrücklich erfasst. Dadurch würde das bisherige Ordnungswidrigkeitenrecht in das Kernstrafrecht überführt und mit einem echten Strafandrohungsmechanismus versehen.

2. Einheitliche europäische Zurechnungsgrundlage

Der AI Act liefert zwar technische Pflichten, aber keine strafrechtliche Umsetzung. Eine Ergänzung durch eine EU-Strafrechtsrahmenrichtlinie wäre erforderlich, um Verstöße gegen Art. 9–15 AI Act als strafrechtlich relevantes Organisationsversagen zu definieren.

3.Spezialisierte Ermittlungsstrukturen

Die Aufklärung von KI-basierten Wirtschaftsstraftaten verlangt Sachverstand in IT, Datenethik und Algorithmik. Ohne spezialisierte Abteilungen in Staatsanwaltschaften bleibt die Strafverfolgung praktisch wirkungslos.

4.Beibehaltung des Schuldprinzips mit funktionaler Erweiterung

Das Strafrecht darf keine Maschinen bestrafen, sondern Menschen, die durch Pflichtverletzung Risiken schaffen. Der Kern des Schuldprinzips – individuelle Verantwortlichkeit für beherrschbares Verhalten – muss erhalten bleiben, auch wenn die Beherrschung heute in Form von technischer Kontrolle statt physischer Handlung geschieht.

Künstliche Intelligenz wird das Wirtschaftsstrafrecht grundlegend verändern. Sie ist kein Täter im klassischen Sinn, aber ein Tatgenerator im faktischen Sinn. Das Strafrecht kann ihr Handeln nicht

sanktionieren, wohl aber den Umgang des Menschen mit ihr.

Die Zukunft liegt in einem funktional erweiterten Strafrecht, das die Verantwortung dort ansetzt, wo Entscheidungen über Technologie getroffen werden – bei der Geschäftsleitung, den Entwicklern und den Compliance-Strukturen. Nur so bleibt das Strafrecht ein wirksames Instrument im Zeitalter autonomer Systeme.

Das Ziel muss sein, nicht Maschinen zu bestrafen, sondern Menschen, die ihre Verantwortung an Maschinen delegieren, ohne sie zu kontrollieren. Erst dann wird das Strafrecht seiner Aufgabe gerecht: die Freiheit menschlichen Handelns auch in einer algorithmischen Welt zu sichern.

Literaturverzeichnis

BeckOK Ordnungswidrigkeitenrecht (OWiG), hrsg. v. Wagner, Jörg, 34. Edition, Stand: 1. Februar 2024, München: C.H. Beck.

BGH, Beschluss vom 21. Juni 1994 – 5 StR 132/94, NJW 1994, 3010 – 3012.

BGH, Urteil vom 17. Juli 2009 – 5 StR 394/08 („Siemens“), NJW 2009, 3437 – 3441.

Fischer, Thomas, Strafgesetzbuch mit Nebengesetzen – Kommentar, 71. Auflage, München: C.H. Beck 2024.

Gless, Sabine, Zurechnung und Verantwortung im digitalen Zeitalter, Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW) 131 (2019), S. 1 – 34.

Gurlit, Elke, Verantwortlichkeit und Delegation im Unternehmen, Zeitschrift für das gesamte Handelsrecht und Wirtschaftsrecht (ZHR) 185 (2021), S. 201 – 230.

Hilgendorf, Eric, KI und Strafrecht – Dogmatische und rechtspolitische Perspektiven, Neue Juristische Wochenschrift (NJW) 2021, 1010 – 1014.

Jescheck, Hans-Heinrich / Weigend, Thomas, Lehrbuch des Strafrechts – Allgemeiner Teil, 5. Auflage, Berlin: Duncker & Humblot 1996.

Körber, Torsten, in: Münchener Kommentar zum GmbH-Gesetz (GmbHG), 4. Auflage, München: C.H. Beck 2022, § 43 Rn. 118 – 125.

Larenz, Karl / Canaris, Claus-Wilhelm, Methodenlehre der Rechtswissenschaft, 4. Auflage, Berlin: Springer 2019.

Roxin, Claus / Greco, Luis, Strafrecht – Allgemeiner Teil I: Grundlagen, Der Aufbau der Verbrechenslehre, 5. Auflage, München: C.H. Beck 2020.

Rossi, Alexander, in: BeckOK Datenschutzrecht, 41. Edition, Stand: 1. August 2024, München: C.H. Beck, Art. 38 DSGVO Rn. 1 – 8.

Tiedemann, Klaus, Wirtschaftsstrafrecht – Einführung, Allgemeiner Teil, Delikte im Unternehmen, 6. Auflage, Köln: Heymanns 2021.

Wagner, Jörg, in: BeckOK OWiG, 34. Edition, Stand: 1. Februar 2024, München: C.H. Beck, § 130 Rn. 13 – 19.

Rechtsverzeichnis

Gesetze und Verordnungen

Strafgesetzbuch (StGB), in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Art. 8 G v. 20. Dezember 2022 (BGBl. I S. 2746).

Gesetz über Ordnungswidrigkeiten (OWiG), in der Fassung vom 19. Februar 1987 (BGBl. I S. 602), zuletzt geändert durch Art. 5 G v. 20. Dezember 2022 (BGBl. I S. 2470).

Gesetz über die Gesellschaft mit beschränkter Haftung (GmbHG), Fassung vom 20. Mai 1898 (RGBl. S. 846), zuletzt geändert durch Art. 9 G v. 22. Dezember 2023 (BGBl. I Nr. 408).

Aktiengesetz (AktG), in der Fassung vom 6. September 1965 (BGBl. I S. 1089), zuletzt geändert durch Art. 8 G v. 22. Dezember 2023 (BGBl. I Nr. 408).

Datenschutz-Grundverordnung (DSGVO), Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016.

Bundesdatenschutzgesetz (BDSG) vom 30. Juni 2017 (BGBl. I S. 2097), zuletzt geändert durch Art. 8 G v. 20. Dezember 2022 (BGBl. I S. 2746).

Wertpapierhandelsgesetz (WpHG) vom 9. September 1998 (BGBl. I S. 2708), zuletzt geändert durch Art. 12 G v. 22. Dezember 2023 (BGBl. I Nr. 408).

Europäische Rechtsakte

Verordnung (EU) 2024/... – Artificial Intelligence Act (AI Act), angenommen durch das Europäische Parlament am 13. März 2024, ABl. L 2024 (noch nicht nummeriert).

Vorschlag für eine Richtlinie über die Haftung für künstliche Intelligenz (AI Liability Directive), COM(2022) 496 final vom 28. September 2022.