

Unkontrollierte Nutzung Künstlicher Intelligenz durch Polizeibehörden? Fragmentierte Accountability- und Compliance-Vorkehrungen

Hartmut Aden und Steven Kleemann

Zusammenfassung

Dieser Beitrag betrachtet die *Accountability*- und *Compliance*-Vorkehrungen für die Kontrolle der Nutzung Künstlicher Intelligenz (KI) durch Polizeibehörden, mit denen sichergestellt werden soll, dass auftretende Risiken möglichst frühzeitig erkannt und minimiert werden. Die Kontrollstrukturen der 2024 verabschiedeten KI-Verordnung der Europäischen Union sind grundsätzlich auch auf Strafverfolgungsbehörden anwendbar. Allerdings relativieren zahlreiche „Hintertüren“ in Form von Sonderregelungen und Ausnahmen diesen integrierten Regelungsansatz. Dieser Beitrag zeigt, dass die EU-KI-VO eine Reihe von *Accountability*- und *Compliance*-Strukturen auf EU-Ebene und in den Mitgliedstaaten vorsieht. Im Mittelpunkt stehen prozedurale *Accountability*-Vorkehrungen, u. a. Pflichten zur Einführung eines Risikomanagementsystems und bei staatlichen Stellen zur Durchführung einer Grundrechte-Folgenabschätzung. Allerdings sind auch diese Vorgaben aufgrund zahlreicher Sonderregelungen für die Strafverfolgung nur eingeschränkt anwendbar.

1. Einleitung¹

Die KI-Verordnung der Europäischen Union (englisch *Artificial Intelligence Act*, im Folgenden: EU-KI-VO) wurde 2021 von der Europäischen Kommission vorgeschlagen und 2024 nach kontroversen Diskussionen als Ver-

1 Dieser Beitrag basiert zu Teilen auf Erkenntnissen des Verbundforschungsprojekt *VIKING (Vertrauenswürdige Künstliche Intelligenz für polizeiliche Anwendungen)*, 2022 bis 2025, gefördert vom Bundesministerium für Bildung und Forschung (seit 2025: Bundesministerium für Forschung, Technologie und Raumfahrt), Förder-Kennzeichen 13N16241.

ordnung (EU) 2024/1689 verabschiedet.² Die Vorschriften treten in einem mehrstufigen, gestreckten Zeitrahmen in Kraft (vgl. Art. 113 EU-KI-VO in der durch Verordnung (EU) 2026/1744 geänderten Fassung). Die EU-KI-VO schafft einen allgemeinen Rahmen für die KI-Nutzung und die Bewertung der von ihr ausgehenden Risiken.

Anders als die EU-Datenschutz-Grundverordnung (DSGVO) gilt die EU-KI-VO auch für die strafrechtliche Ermittlung – nach ihrem Art. 3 Abs. 3 nicht aber für Nachrichtendienste, auf die sich die Gesetzgebungszuständigkeit der EU bislang nicht erstreckt. Eingriffsbefugnisse für die tatsächliche Einführung und Nutzung von KI-Systemen durch staatliche Behörden wie die Polizei müssen indes die Mitgliedstaaten im Rahmen ihrer Gesetzgebung etablieren. Vor dem Hintergrund der Intensität möglicher Folgen für die Grundrechte der Betroffenen und der Rechtsprechung des Europäischen Gerichtshofs, des Europäischen Gerichtshofs für Menschenrechte sowie in Deutschland auch des Bundesverfassungsgerichts sind spezialgesetzliche Regelungen erforderlich, soweit die staatliche Nutzung von KI-Systemen zu Grundrechtseingriffen führt. Bund und Länder sind daher bestrebt, mehr spezialgesetzliche Eingriffsbefugnisse für die KI-Nutzung durch Strafverfolgungsbehörden zu schaffen. Gesetzgebungsvorschläge für das Ermöglichen polizeilicher KI-Nutzung sind daher bereits Teil der rechtspolitischen Agenda, u. a. für die Polizeigesetze (vgl. Martini/Botta 2025, S. 1038ff.).

Vor Verabschiedung der EU-KI-VO unterlagen KI-Systeme nur den Anforderungen des Datenschutzrechts und weiteren, nicht KI-spezifischen rechtlichen Regelungen. Auch wenn es sich bei der EU-KI-VO um eine nach Art. 288 AEUV unmittelbar geltende Verordnung handelt, bedürfen die *Accountability*-Anforderungen der EU-KI-VO in vielerlei Hinsicht noch der Konkretisierung, auch durch die Mitgliedstaaten. Der Aufbau der institutionellen Strukturen steht erst am Anfang. Die EU-KI-VO nutzt in mancherlei Hinsicht den Ansatz „regulierter Selbstregulierung“ – die kontrollierten Akteure haben daher erhebliche Spielräume bei der Ausgestaltung der Kontrollstrukturen.

Bereits im Hinblick auf die Privatwirtschaft erscheint dies im Ausgangspunkt problematisch, da die Kontrolle unabhängig und der Einfluss der

2 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz).

Kontrollierten auf die Kontrolle begrenzt sein sollte. Im Folgenden wird gezeigt, wie diese Problematik bei Strafverfolgungsbehörden durch ihre weitreichenden Befugnisse zur KI-Nutzung und die zahlreichen, speziell für sie geschaffenen Ausnahmetatbestände oder „Hintertüren“ in der EU-KI-VO verschärft wird. Ausnahmen für die Strafverfolgung gibt es z. B. für die biometrische Fernidentifizierung (Art. 5 Abs. 1 lit. h EU-KI-VO für die eigentlich verbotenen Systeme und Anhang III Nr. 1 lit. a, Art. 26 Abs. 10 EU-KI-VO für Hochrisiko-Anwendungen), für Tests unter Realbedingungen (Art. 60 Abs. 4 lit. i EU-KI-VO) oder durch Verweise auf die neu eingeführte und dem Datenschutzrecht unbekannte Kategorie „sensible operative Daten“ (Art. 3 Nr. 38 EU-KI-VO), deren Kontrolle Einschränkungen und Sonderregelungen unterliegt (vgl. Kleemann/Aden 2025). Hinzu kommt die unübersichtliche Vielzahl von *Compliance*- und *Accountability*-Vorkehrungen der EU-KI-VO, die im Endeffekt zu einer „*Accountability*-Falle“ werden können, wenn sie unkoordiniert und intransparent bleiben – und somit ein ganzheitlicher *Accountability*-Ansatz fehlt. Daher erscheint es fraglich, ob die Regelungen der EU-KI-VO ausreichen, um die polizeiliche KI-Nutzung im Hinblick auf die Grundrechte Betroffener wirksam zu kontrollieren und zu begrenzen. Die mitgliedstaatliche Gesetzgebung könnte zwar trotz der unzulänglichen Regelungen der EU-KI-VO diese Aufgabe übernehmen. Angesichts des Trends zu sicherheitsorientierter Gesetzgebung (vgl. Aden/Fährmann 2021) ist dies allerdings kaum zu erwarten.

Dieser Beitrag untersucht Kriterien für die Beurteilung der Effektivität von *Accountability*- und *Compliance*-Vorkehrungen für die KI-Nutzung im Allgemeinen sowie deren Möglichkeiten und Grenzen im Kontext der polizeilichen KI-Nutzung auf der Basis der EU-KI-VO. Zudem nimmt er die (begrenzten) Einflussmöglichkeiten etablierter *Accountability*-Foren (Europäischer Datenschutzbeauftragter, Europäischer Datenschutzausschuss, mitgliedstaatliche Datenschutzaufsicht, mitgliedstaatliche Menschenrechtseinstitutionen, Europäische Bürgerbeauftragte usw.) auf die Kontrolle der KI-Nutzung durch Strafverfolgungsbehörden in den Blick. Der Beitrag verfolgt das Ziel, die *Accountability*- und *Compliance*-Vorkehrungen für die KI-Entwicklung und -Nutzung aus einer ganzheitlichen Perspektive zu untersuchen, die technische Eigenschaften, den rechtlichen Rahmen und den sozio-technischen Kontext von KI sowie deren Wechselwirkungen einbezieht. Zur exemplarischen Illustration werden die KI-gestützte

Objektdetektion und die Sprechendenerkennung verwendet.³ Während bei der Sprechendenerkennung der Eingriff in die Telekommunikationsfreiheit im Fokus steht, ist die Objektdetektion ein relevantes Beispiel für die polizeiliche Auswertung großer Datenmengen. Der Einsatz von KI-Systemen zur automatisierten Detektion von Objekten in großen Video- und Bilddatenbeständen (z. B. im Rahmen einer Rasterfahndung oder der Auswertung sichergestellter Speichermedien) und zur KI-gestützten Sprechendenerkennung bei der Telekommunikationsüberwachung erfordert eigenständige spezialgesetzliche Grundlagen, da sie unmittelbar in Grundrechte – insbesondere das Recht auf informationelle Selbstbestimmung und den Schutz des Fernmeldegeheimnisses – eingreifen.

2. Die Relevanz von Accountability- und Compliance-Vorkehrungen für polizeiliche KI-Anwendungen

Das Ziel, umfängliche KI-*Accountability* zu gewährleisten, umfasst die Komponenten *Compliance*, Berichterstattung, unabhängige Aufsicht und Durchsetzung (Novelli u. a. 2024). Eine effektive Kontrolle der polizeilichen KI-Nutzung ist vor dem Hintergrund potenziell weitreichender Auswirkungen auf die Grundrechte Betroffener von hoher Relevanz. Die EU-KI-VO etabliert hierfür eine Reihe von Instrumenten, die als *Accountability*-Foren fungieren. Ein *Accountability-Forum* verbindet nach Bovens (2007, S. 450) einen Akteur, der für ein Handeln Verantwortung trägt, und eine Kontrollinstanz, z. B. ein Aufsichtsgremium. Der rechenschaftspflichtige Akteur, hier die Polizei, ist verpflichtet, Verhalten und Handlungen gegenüber dem Forum zu rechtfertigen. Das Forum kann nachfragen, das Verhalten beurteilen und in einigen Fällen auch Sanktionen verhängen. In Rechtsstaaten sind staatliche Behörden wie die Polizei typischerweise gegenüber mehreren *Accountability*-Foren rechenschaftspflichtig (Bovens u. a. 2014), insbesondere gegenüber vorgesetzten Behörden, speziellen Aufsichtsbehörden wie den Datenschutzbeauftragten und den Rechnungshöfen, den Parlamenten, den Gerichten und einer breiteren Öffentlichkeit. *Accountability* nimmt somit eine umfassendere Perspektive ein als *Compliance*, die in erster Linie Regelkonformität in den Blick nimmt. Die *Compliance* kann zumeist mit Checklisten überprüft werden, wohingegen *Accountability* die Kontrollstrukturen und ihren Kontext betrachtet.

3 Anknüpfend an das Forschungsprojekt VIKING, näher hierzu Fischer u. a. 2025.

In der EU-KI-VO werden beide Konzepte unterschiedlich aufgegriffen. Je nach Risikokategorie, in die ein KI-System einzuordnen ist, müssen unterschiedliche *Compliance*- und Informationspflichten erfüllt werden. Die *Accountability*-Ebene geht darüber hinaus und enthält beispielsweise Anforderungen an ein Qualitätsmanagementsystem (Art. 17 EU-KI-VO), menschliche Aufsicht (Art. 14 EU-KI-VO), technische Dokumentations- und Protokollierungspflichten (z. B. Art. 11, 12, 18, 19 EU-KI-VO), aber auch erst noch im Detail auszugestaltende Instrumente wie die Grundrechte-Folgenabschätzung (Art. 27 EU-KI-VO) oder die Etablierung der verschiedenen Aufsichtsgremien auf europäischer und nationaler Ebene (z. B. Art. 64, 65, 70 EU-KI-VO).

Künstliche Intelligenz wird von vielen Autor:innen als *Black Box* eingestuft, weil die genutzten KI-Systeme und ihre Ergebnisse nur begrenzt transparent und erklärbar sind. Bei der polizeilichen KI-Nutzung kommt ein institutioneller *Black Box*-Effekt hinzu, da die organisatorischen Prozesse und die konkrete Nutzung von KI-Systemen aufgrund von Geheimhaltungsbedürfnissen in Sicherheitsbehörden tendenziell in weiten Teilen intransparent sind (vgl. Fährmann u. a. 2022; Kleemann/Aden 2026; Martinez u. a. 2026).

Dieser doppelte *Black Box*-Effekt verstärkt Risiken für die Grundrechte derjenigen, deren Daten in polizeilichen KI-Systemen verarbeitet werden. Fehler, die polizeiliche KI-Systeme erzeugen, können unmittelbare und im Vergleich zu privaten Nutzungen ungleich intensivere Auswirkungen auf die Grundrechte der Betroffenen haben – von diskriminierenden Entscheidungen bis zu irrtümlichen Festnahmen. Da Polizeibehörden zumeist KI-Systeme nutzen, die von externen Firmen entwickelt wurden, sind auch diese externen KI-Anbietenden in die Betrachtung einzubeziehen.

Bei der Objektdetektion und der Sprechendenerkennung in der Telekommunikationsüberwachung führt dieser doppelte *Black Box*-Effekt dazu, dass in der Regel weder die Betroffenen noch externe Kontrollinstanzen wissen, welche Algorithmen die erkannten Objekte oder Stimmen bestimmten Personen zuordnen. Auch das Ausmaß der Fehleranfälligkeit des Systems und die Integration von Treffern in polizeiliche Entscheidungsprozesse – etwa für eine Durchsuchung oder Festnahme – sind für Betroffene und Kontrollinstanzen kaum nachvollziehbar.

Wie lässt sich die Effektivität von *Accountability*-Vorkehrungen für die KI-Nutzung allgemein und speziell für die polizeiliche KI-Nutzung bewerten? Von Relevanz sind hier insbesondere die institutionelle Unabhängigkeit des *Accountability*-Forums gegenüber der Polizeibehörde, die KI-An-

wendungen (weiter-)entwickelt und nutzt, sowie die Reichweite der Kontrollbefugnisse. Die Unabhängigkeit von *Accountability*-Foren gegenüber den Akteur:innen, die KI-Anwendungen entwickeln oder nutzen, reduziert das Risiko, dass kontrollierende Akteure ihre eigenen Interessen verfolgen. Dies gilt in besonderem Maße für KI im polizeilichen Kontext, in dem die Rollen der KI-Entwickelnden und -Betreibenden mit der Macht des staatlichen Gewaltmonopols zusammenfallen können. Ein sich selbst regulierender Markt, der sich bei Versagen der Technologie in Teilen selbst regulieren könnte, fehlt hier, da der Staat der „Markt“ selbst ist und Sicherheitsbehörden dazu noch Geheimhaltungsinteressen haben. Unabhängige *Accountability*-Foren können dies durch ihre Kontrolltätigkeit jedenfalls ein Stück weit kompensieren.

3. Normativ-inhaltliche Anknüpfungspunkte der KI-Accountability und -Compliance

Vor dem Inkrafttreten der EU-KI-VO stammten die normativen Anforderungen an KI-Accountability vorwiegend aus der Ethik-Diskussion zu den Grenzen dessen, was mit KI-Unterstützung möglich sein sollte. Die Zielsetzungen der EU-KI-VO sind ambitioniert und zugleich so breit angelegt, dass Zielkonflikte unvermeidbar sind. Die EU-KI-VO soll dazu beitragen,

„das Funktionieren des Binnenmarkts zu verbessern und die Einführung einer auf den Menschen ausgerichteten und vertrauenswürdigen künstlichen Intelligenz (KI) zu fördern und gleichzeitig ein hohes Schutzniveau in Bezug auf Gesundheit, Sicherheit und die in der Charta verankerten Grundrechte, einschließlich Demokratie, Rechtsstaatlichkeit und Umweltschutz, vor schädlichen Auswirkungen von KI-Systemen in der Union zu gewährleisten und die Innovation zu unterstützen“ (Art. 1 Abs. 1).

Eine zentrale normative Frage war und ist eng mit *Accountability*-Fragen verknüpft: Wie kann KI so ausgestaltet werden, dass sie sich gegenüber menschlichen Entscheidungen nicht verselbständigt? Auch für die polizeiliche KI-Nutzung, deren Ergebnisse zu weitreichenden Grundrechtseingriffen führen können, ist dieses Thema von höchster Relevanz. Die Nutzung komplexer, nicht ohne Weiteres nachvollziehbarer KI-Systeme kann die Handlungsautonomie und den Ermessensgebrauch der nutzenden Polizeibeamt:innen faktisch einschränken, wenn sie sich auf die Ergebnisse des

Systems verlassen (müssen), was wiederum Auswirkungen auf die Grundrechte Betroffener haben kann. In der EU-KI-VO spiegelt sich dieses Anliegen insbesondere in den Regelungen zur menschlichen Aufsicht (Art. 14) sowie zur Genauigkeit, Robustheit und Cybersicherheit (Art. 15) wider, die für Hochrisiko-KI-Systeme und damit auch für weite Teile der polizeilichen KI-Nutzung gelten (vgl. Kleemann/Aden 2025). Was z. B. menschliche Aufsicht, Genauigkeit, Robustheit und Cybersicherheit bei einer KI-gestützten Objektdetektion über tausende Video-Frames bedeutet, ob es als menschliche Aufsicht ausreicht, dass Beamt:innen die vom System markierten Treffer nachträglich sichten oder ob bei der KI-Sprechendenerkennung die Einordnung eines Datensatzes durch Analyst:innen als hinreichende menschliche Kontrolle gilt, bleibt in der EU-KI-VO offen und wird weiter zu konkretisieren sein, u. a. durch Rechtsprechung. Die Kommission soll zudem die „Entwicklung von Benchmarks und Messmethoden“ für Genauigkeit, Robustheit und Cybersicherheit von KI-Systemen fördern (Art. 15 Abs. 2).

Die Pflicht zur Gewährleistung menschlicher Aufsicht „auch mit geeigneten Instrumenten einer Mensch-Maschine-Schnittstelle“ (Art. 14 Abs. 1 EU-KI-VO) schlägt zugleich den Bogen zu zentralen normativen Elementen des Schutzzwecks: „Risiken für Gesundheit, Sicherheit und Grundrechte“ sollen minimiert werden (Art. 14 Abs. 2). Allerdings bleiben die normativen Anforderungen der EU-KI-VO an den Schutz der Grundrechte allgemein. Die Grundrechtsanforderungen für die Minimierung von KI-Risiken werden ebenso wenig konkretisiert wie die Auflösung möglicher Zielkonflikte zwischen sicherer und grundrechtsschützender KI-Nutzung. Die Konkretisierung der Anforderungen und die Bewertung der Risiken werden damit weitgehend den Anbietenden und Betreibenden von KI-Systemen sowie den *Accountability*-Foren überantwortet. Weitere einzelfallübergreifende Konkretisierungen werden erforderlich sein, auch im Polizei- und Datenschutzrecht, um sicherzustellen, dass Risiken frühzeitig erkannt und wirksam bewältigt werden.

4. Institutionalisierte Aufsichtsstrukturen nach der EU-KI-Verordnung

Die EU-KI-VO sieht institutionalisierte Aufsichtsstrukturen sowohl auf EU-Ebene (4.1) als auch in den Mitgliedstaaten vor (4.2), die mit Einschränkungen auch für die polizeiliche KI-Nutzung zuständig sind bzw. sein werden. Allerdings handelt es sich nicht um *Accountability*-Foren mit um-

fassenden Kontrollaufgaben. Allenfalls die Marktüberwachungsbehörden, die auf mitgliedstaatlicher Ebene für Hochrisiko-KI-Systeme einzurichten sind (Art. 70 EU-KI-VO), kommen im Hinblick auf ihre institutionelle Positionierung, ihre Aufgaben und Befugnisse einem unabhängigen *Accountability*-Forum nahe. Die Relevanz dieser Kontrollstrukturen für polizeiliche KI-Systeme wurde indes im Laufe des Gesetzgebungsverfahrens signifikant dadurch reduziert, dass weniger KI-Anwendungsfelder der Hochrisiko-Kategorie zugeordnet wurden als durch den Verordnungsentwurf der Europäischen Kommission zunächst beabsichtigt (vgl. Kleemann/Aden 2025, S. 20f.).

4.1 Institutionelle Strukturen auf EU-Ebene

Die EU-KI-VO etabliert zentrale Governance-Strukturen für KI-Fragen auf EU-Ebene. Wichtige Funktionen übernimmt dabei das *Büro für Künstliche Intelligenz* (englisch *Artificial Intelligence Office*), das gemäß Art. 64 EU-KI-VO der Europäischen Kommission zugeordnet ist, die damit zentrale Aufgaben bei der KI-Entwicklung und -Nutzung wahrnimmt. Bereits vor Inkrafttreten der EU-KI-VO richtete die Kommission das Büro per Beschluss ein (C(2024) 390 final vom 24.1.2024). Die EU-KI-VO und der Einrichtungsbeschluss weisen dem Büro umfangreiche Aufgaben bei der Umsetzung der EU-KI-VO zu, u. a. bei der Durchführung von Überwachungsmaßnahmen (Art. 89). Die Kommission kann gemäß Art. 101 EU-KI-VO Geldbußen für Verstöße gegen die Verordnung durch Anbietende von KI-Modellen mit allgemeinem Verwendungszweck (*General Purpose AI*) verhängen. Das KI-Büro ist in diesen Prozess eingebunden und wurde daher bereits als *AI Police* bezeichnet (Krahn 2024, S. 122). Aufgrund der Höhe der möglichen Bußgelder – bis zu 3 % des Jahresumsatzes bzw. 15 Mio. € (Art. 99 Abs. 3 EU-KI-VO) – kann die Kompetenz des KI-Büros jedenfalls in Bezug auf Sanktionsmöglichkeiten als „scharfes Schwert“ angesehen werden. Somit übernimmt das KI-Büro gewisse *Accountability*-Aufgaben; ihm mangelt es aber aufgrund der Einbindung in die Verwaltungsstrukturen der Kommission an institutioneller Unabhängigkeit.

Im KI-Gremium (englisch *Artificial Intelligence Board*) ist – entsprechend der üblichen Logik des EU-Mehrebenensystems (vgl. Novelli u. a. 2025) – jeder Mitgliedstaat vertreten; der Europäische Datenschutzbeauftragte nimmt nur als Beobachter teil (Art. 65 Abs. 2 und 3 EU-KI-VO). Das Gremium „berät und unterstützt die Kommission und die Mitglied-

staaten, um die einheitliche und wirksame Anwendung dieser Verordnung zu erleichtern“ (Art. 66 EU-KI-VO). Eigene Kontrollbefugnisse hat das KI-Gremium allerdings nicht. Allenfalls im Rahmen von Empfehlungen und Stellungnahmen kann es zum Schutz der von der KI-Nutzung Betroffenen beitragen (so insbesondere gemäß Art. 66 lit. e, n und o EU-KI-VO). Vor dem Hintergrund, dass die mitgliedstaatlichen Regierungen und deren Interessen in dem Gremium repräsentiert sind, dürften hier kaum substantielle Vorgaben für die polizeiliche KI-Nutzung zu erwarten sein.

Noch weniger Kontrollbefugnisse hat das Beratungsforum, das gemäß Art. 67 EU-KI-VO die Europäische Kommission berät und bei dessen Zusammensetzung „auf ein ausgewogenes Verhältnis zwischen wirtschaftlichen und nicht-wirtschaftlichen Interessen“ geachtet werden soll. Die Mitglieder sollen „Industrie, Start-up-Unternehmen, KMU, die Zivilgesellschaft und die Wissenschaft“ vertreten (Abs. 2). Die Kommission übt u. a. durch ihre Befugnis, die Mitglieder auszuwählen, erheblichen Einfluss auf das Forum aus (Abs. 3). Deutlich wurde dies auch im Rahmen der Besetzung, bei der große Tech-Firmen, wirtschaftliche Akteure und deren Interessenvertretungen überproportional vertreten sind, wohingegen zivilgesellschaftliche Akteure wenig und nationale Menschenrechtsinstitutionen gar nicht ausgewählt wurden (ECNL 2026).

Das wissenschaftliche Gremium unabhängiger Sachverständiger, das gemäß Art. 68 EU-KI-VO eingerichtet wird, unterstützt auch „Durchsetzungstätigkeiten“ (Abs. 1). Seine konkreten Aufgaben sind beratend und unterstützend (Abs. 3), so dass es sich ebenfalls nicht um ein voll ausgeprägtes *Accountability*-Forum mit effektiven Kontrollrechten handelt. Immerhin kann das Gremium aber Warnungen vor systemischen Risiken aussprechen, die von KI-Modellen mit allgemeinem Verwendungszweck ausgehen (Art. 90 EU-KI-VO).

Im Ergebnis wurde keine der nach der EU-KI-VO neu eingerichteten institutionellen Strukturen auf EU-Ebene als unabhängiges *Accountability*-Forum mit umfassenden Kontrollfunktionen ausgestattet. Für die verantwortliche KI-Nutzung im Allgemeinen und die speziellen Grundrechtsrisiken der polizeilichen KI-Nutzung bleiben die bestehenden *Accountability*-Foren daher von großer Bedeutung, insbesondere der Europäische Datenschutzbeauftragte, die EU-Bürgerbeauftragte, die EU-Grundrechteagentur und der Europäische Gerichtshof (EuGH) (s. auch Abschnitt 6).

4.2. Institutionelle Strukturen in den Mitgliedstaaten

Die EU-KI-VO schreibt die Einrichtung weiterer institutioneller Strukturen für die administrative Implementation der KI-Verordnung in den Mitgliedstaaten vor. Jeder Mitgliedstaat muss mindestens eine Marktüberwachungsbehörde und eine notifizierende Behörde einrichten, die ihre Befugnisse unabhängig ausüben sollen (Art. 70 Abs. 1 EU-KI-VO). Die konkretere Ausgestaltung ist den Mitgliedstaaten überlassen, insbesondere auch die Frage, ob diese Aufgaben bestehenden Aufsichtsbehörden übertragen werden und ggf. welchen. Für Hochrisiko-KI-Systeme, die für Strafverfolgung, Grenzmanagement sowie „Justiz und Demokratie“ eingesetzt werden, müssen die Mitgliedstaaten indes die nach der DSGVO oder der Richtlinie (EU) 2016/680 (JI-Richtlinie) bereits etablierten Datenschutzaufsichtsbehörden als Marktüberwachungsbehörden benennen oder vergleichbar unabhängige Aufsichtsbehörden für die Marktüberwachung schaffen. Marktüberwachungstätigkeiten dürfen hier „in keiner Weise die Unabhängigkeit von Justizbehörden beeinträchtigen [...]“ (Art. 74 Abs. 8 EU-KI-VO).

Die Marktüberwachungsbehörden nehmen einige typische *Accountability*-Aufgaben wahr. So üben sie Überwachungsaufgaben für Hochrisiko-KI-Systeme aus (Art. 74 EU-KI-VO) und bearbeiten Meldungen schwerwiegender Vorfälle bei der Nutzung solcher Systeme (Art. 73 EU-KI-VO). Sie haben im Rahmen ihrer Aufsichtstätigkeit weitreichende Rechte auf Zugang zu Informationen über Hochrisiko-Systeme (Art. 73 Abs. 12 und 13 EU-KI-VO).

Die Mitgliedstaaten haben zudem notifizierende Behörden als Teil eines Konformitätsbewertungssystems einzurichten. Hierzu zählt mindestens eine notifizierende Behörde pro Mitgliedstaat, die die Konformitätsbewertungsstellen (Art. 31 EU-KI-VO) notifiziert und überwacht. Mit den Anforderungen an „Objektivität und Unparteilichkeit“ (Art. 28 Abs. 3 EU-KI-VO) weisen diese Behörden ebenfalls Merkmale von *Accountability-Foren* auf. Die von ihnen überwachten Konformitätsbewertungsstellen bewerten die Konformität von Hochrisiko-KI-Systemen mit der EU-KI-VO (Art. 43). Sie sind ein weiterer Baustein in der *Accountability*-Kaskade der EU-KI-VO. Gegenüber den Anbietenden des jeweiligen Hochrisiko-KI-Systems und „allen anderen Akteuren, die ein wirtschaftliches Interesse an den zu bewertenden Hochrisiko-KI-Systemen haben“, müssen sie unabhängig sein. Bei Hochrisiko-Systemen für Strafverfolgungsbehörden gilt erneut eine abweichende Zuständigkeit, nämlich der Aufsichtsbehörden, die ge-

mäß Art. 74 Abs. 8 EU-KI-VO die Aufgaben der Marktüberwachung mit übernehmen (Art. 43 Abs. 1 Satz 3 EU-KI-VO).

Zudem ermöglicht Art. 77 EU-KI-VO, andere mitgliedstaatliche „Behörden oder öffentliche Stellen“ einzubinden, „die die Einhaltung des Unionsrechts zum Schutz der Grundrechte einschließlich des Rechts auf Nichtdiskriminierung [...] beaufsichtigen oder durchsetzen“ (Abs. 1 Satz 1), die sogenannten *Artikel 77-Stellen*. Allerdings beschränken sich die formalen Befugnisse dieser Stellen auf den Zugang zu Dokumentationen, die über Hochrisiko-KI-Systeme zu führen sind (Abs. 1). Mit der durch Verordnung (EU) 2026/1744 geänderten Fassung wurden diese Stellen dahingehend geschwächt, dass die Informationsanforderung nur noch über die Marktüberwachungsbehörden möglich ist und nicht mehr direkt bei Anbietenden und Betreibenden. Sind diese Informationen nicht ausreichend, können *Artikel 77-Stellen* bei der Marktüberwachungsbehörde die Durchführung eines technischen Tests des Hochrisiko-Systems beantragen (Abs. 3).

Diese im Ausgangspunkt schwachen *Accountability*-Befugnisse werden indes ergänzt durch Kontrollrechte der jeweiligen Stelle aufgrund anderer Rechtsvorschriften, z. B. der Datenschutz- und Antidiskriminierungs-Gesetzgebung. Für Deutschland benannte das Bundeswirtschaftsministerium die Datenschutzbeauftragten des Bundes und der Länder, die Antidiskriminierungsstelle des Bundes sowie die Ombudsstelle für Gleichbehandlung und gegen Diskriminierung nach dem Landes-Antidiskriminierungsgesetz Berlin.⁴ Nicht benannt wurden bisher die unabhängigen Polizeibeauftragten, die seit 2014 in einer Reihe von Bundesländern und 2024 auch auf Bundesebene etabliert worden sind (hierzu Töpfer u. a. 2023; Aden 2025), sowie das Deutsche Institut für Menschenrechte als unabhängige nationale Menschenrechtsinstitution Deutschlands.

Im Ergebnis schreibt die EU-KI-VO somit fragmentierte *Accountability*-Strukturen vor, deren Zuständigkeit sich im Wesentlichen auf Hochrisiko-KI-Systeme beschränkt. Polizeiliche KI-Systeme fallen in die Zuständigkeit dieser Strukturen, allerdings mit einigen abweichenden Regelungen für die Zuständigkeit und die Reichweite der Kontrollbefugnisse (vgl. Kleemann/Aden 2025).

4 Liste nach Art. 77 Abs. 2 EU-KI-VO (Stand 19. Dezember 2024). https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Downloads/J-L/liste-nach-art-77-abs-2-ki-verordnung.pdf?__blob=publicationFile&v=8

5. Prozedurale Accountability- und Compliance-Vorkehrungen der EU-KI-Verordnung

Für Hochrisiko-KI-Systeme etabliert die EU-KI-VO eine Reihe von prozeduralen *Accountability*- und *Compliance*-Vorkehrungen. Spezielle Verfahren sollen sicherstellen, dass Risiken für die Grundrechte, die Sicherheit und die Gesundheit frühzeitig erkannt und minimiert werden. Die inhaltlichen Anforderungen werden dagegen in der EU-KI-VO nur mit allgemeinen Postulaten konkretisiert (s. Abschnitt 3). Den Anbietenden und Betreibenden von KI-Systemen verbleiben damit weitreichende Spielräume, die allerdings durch die Aufsichtsstrukturen (s. Abschnitt 4) und die Rechtsprechung konkretisiert werden dürften. Für Polizeibehörden gelten indes auch hier Ausnahmen.

Polizeibehörden, die KI-Software privater Firmen einkaufen und in eigenen bzw. öffentlichen Strukturen (wie etwa HessenDATA oder VeRA) mit speziell zugeschnittenen Funktionen weiterentwickeln und verwenden, könnten gem. Art. 25 Abs. 1 lit. a und b EU-KI-VO Quasi-Anbietende sein und müssen dann sowohl die Anforderungen an Betreibende als auch die an Anbietende einhalten (vgl. Martini/Botta 2025, S. 1037, a. A. Bosman 2025, Art. 25, Rn. 37ff.).

5.1 Risikomanagement

Die Etablierung von Risikomanagementsystemen gehört heute zum Standardinstrumentarium des EU-Rechts, wobei ausgehend vom Umweltrecht weitreichende rechtliche Instrumente zur Durchsetzung des Vorsorgeprinzips (*precautionary principle*) für den Umgang mit Risiken entwickelt wurden (Guerra 2019). Nach der EU-KI-VO haben die Anbietenden von Hochrisiko-KI-Systemen ein solches System einzurichten, das als „kontinuierlicher iterativer Prozess [...] während des gesamten Lebenszyklus“ des Systems angelegt sein soll (Art. 9 Abs. 2 EU-KI-VO). Wer in die Anbietenden-Kategorie fällt, ist in Art. 25 EU-KI-VO geregelt.

Normativer Anknüpfungspunkt für die Risikoermittlung sind hier nach Art. 9 Abs. 2 lit. a wiederum „Gesundheit, Sicherheit oder Grundrechte“ ohne nähere Spezifizierung. Trotz des zentralen Stellenwerts der Risikokategorisierung in der EU-KI-VO bleiben hier also weite Interpretationsspielräume, die der Konkretisierung bedürfen (Schuett 2024). Dies liegt zunächst in der Verantwortung der Anbietenden und Betreibenden und

kann durch die zuständigen Gremien, Behörden und Gerichte überprüft werden. Nicht vorgeschrieben ist, wer für die Durchführung zuständig ist, so dass Anbietende das Risikomanagementsystem „mit Bordmitteln“ betreiben könnten, was zu Interessenkonflikten führen kann. Gerade hierfür bedarf es folglich einer effektiven Aufsicht. Dies gilt auch und besonders für Anbietende von KI-Systemen für polizeiliche Nutzungszwecke.

So könnte etwa ein privates Unternehmen, das ein KI-System zur Objektdetektion oder Sprechendenerkennung für Polizeibehörden entwickelt und betreibt, das Risikomanagementsystem eigenverantwortlich gestalten. Die Folge könnte sein, dass Informationen über systemische Fehler (z. B. erhöhte Falsch-Positiv-Raten bei bestimmten Bevölkerungsgruppen) intern bleiben und von keiner unabhängigen Stelle für den Hochrisikoeinsatz ausreichend überprüft werden, bevor das System durch die Polizei genutzt wird.

5.2 Grundrechte-Folgenabschätzung

Für Einrichtungen, die öffentliche Dienste erbringen, schreibt die EU-KI-VO zudem eine Grundrechte-Folgenabschätzung (GRFA) vor – ein zusätzliches prozedurales Element zur Sicherung des Grundrechtsschutzes bei Hochrisiko-KI-Systemen, das auf Initiative des Europäischen Parlaments und zivilgesellschaftlicher Akteure erst in der Aushandlungsphase der EU-KI-VO zusätzlich eingefügt wurde. Die GRFA ist somit auch für polizeiliche KI-Systeme vorgeschrieben, die in die Hochrisiko-Kategorie fallen. Sie ist vor Inbetriebnahme des Systems durchzuführen und bei Änderungen zu aktualisieren (Abs. 2). Die Inhalte der GRFA werden durch die EU-KI-VO vorstrukturiert (Art. 27 Abs. 1), nicht aber die normativen Anforderungen an das zu erreichende Schutzniveau für die Grundrechte.

Die Inhalte der GRFA überschneiden sich mit denen des Risikomanagementsystems nach Art. 9 EU-KI-VO. Allerdings sind für die GRFA die Betreibenden, für das Risikomanagementsystem dagegen die Anbietenden eines Hochrisiko-KI-Systems zuständig (vgl. Kleemann/Aden 2026). Inhalte einer zuvor durchgeführten Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO oder Art. 27 JI-Richtlinie können bereits Bestandteile des Pflichtprogramms der GRFA erfüllen und entsprechend übernommen werden. Die GRFA ergänzt dann die DSFA (Art. 27 Abs. 4 EU-KI-VO; vgl. Thomaidou/Limniotis 2025; Garcia-Godinez 2025) – und umgekehrt,

falls für neue KI-Systeme zuerst eine GRFA und erst danach eine DSFA durchgeführt wird.

Die Ergebnisse der GRFA werden an die zuständige Marktüberwachungsbehörde übermittelt. Die Pflichten zur Veröffentlichung der GRFA-Ergebnisse gelten für die Strafverfolgung nur mit erheblichen Einschränkungen (vgl. Kleemann/Aden 2026). Denn Betreibende müssen Hochrisiko-Systeme gem. Art. 49 Abs. 1 EU-KI-VO in einer EU-Datenbank (Art. 71 EU-KI-VO) registrieren. Behörden haben gem. Art. 49 Abs. 3 i. V. m. Anhang VIII Abschnitt C Nr. 4 EU-KI-VO grundsätzlich eine Ergebniszusammenfassung der GRFA zu veröffentlichen. Für KI-Systeme der Strafverfolgung (Anhang III Nr. 6 EU-KI-VO) entfällt dies gem. Art. 49 Abs. 4 EU-KI-VO. Diese Informationen werden lediglich in einem nicht-öffentlichen Teil der EU-Datenbank gespeichert. Zugriff haben nur die Europäische Kommission und die nationalen Marktüberwachungsbehörden (Art. 49 Abs. 4 UAbs. 2, Art. 74 Abs. 8 EU-KI-VO), und dies auch nur beschränkt auf Informationen gem. Anhang VIII Abschnitt C Nr. 1–3 (Art. 49 Abs. 4 lit. c EU-KI-VO), wobei die GRFA und DSFA dort in Nr. 4 und 5 genannt und somit gar nicht umfasst sind. Die Transparenz- und Dokumentationspflichten in besonders sensiblen Bereichen (Anhang III Nr. 1, 6 und 7) werden somit erheblich untergraben.

Das kann mit Blick auf unser Beispiel bedeuten, dass eine GRFA, die etwa die Fehlerquoten eines Systems zur automatisierten Sprechendererkennung bei der Überwachung von Telekommunikationsverbindungen oder einer KI-gestützten Objektdetektion in sichergestellten Datensätzen (inklusive möglicher diskriminierender Wirkungen für bestimmte Sprach- oder Bevölkerungsgruppen) enthält, für Betroffene, Zivilgesellschaft und unabhängige Forschung nicht einsehbar ist. *Accountability* im Sinne von Rechenschaft, Verantwortlichkeit und Nachweisbarkeit ist damit erheblich eingeschränkt. In einem effektiven *Accountability*-Forum ist die regelkonforme Nutzung nicht einfach anzunehmen, sondern muss auch nachgewiesen werden. Diese Anforderung trägt dazu bei, dass Verantwortung und die Konsequenzen getragen werden müssen, wenn etwas schief läuft.

5.3 Beschwerdeverfahren und Recht auf Erläuterung der Entscheidungsfindung

Die EU-KI-VO sieht ausdrücklich ein Beschwerderecht jeder natürlichen oder juristischen Person bei der zuständigen Marktüberwachungsbehörde

vor, wenn jemand „Grund zu der Annahme hat, dass gegen die Bestimmungen dieser Verordnung verstoßen wurde“ (Art. 85 EU-KI-VO). Dies mag zunächst selbstverständlich erscheinen, stärkt aber die Funktion der Marktüberwachungsbehörden als *Accountability*-Foren und erfordert die Einrichtung einer institutionalisierten Beschwerdebearbeitung. Diese Regelung ähnelt zwar dem Recht auf Beschwerde bei einer Aufsichtsbehörde bei Datenschutzverstößen gem. Art. 77 DSGVO, setzt aber keine persönliche Betroffenheit oder Verletzung einer natürlichen Person voraus (vgl. Hartmann 2026, Art. 85 Rn. 2ff.). Ein Verstoß durch ein Hochrisiko-KI-System ist ebenso wenig Voraussetzung für das Erheben einer solchen Beschwerde wie ein konkret entstandener Schaden. Es reicht die Annahme, dass ein Verstoß gegen die EU-KI-VO vorliegt.

Die Marktüberwachungsbehörde muss sich auf Basis der Marktüberwachungs- und Produktkonformitätsverordnung (VO (EU) 2019/1020, MÜ-VO) mit der Beschwerde auseinandersetzen. Konkretisierende Standards speziell für Beschwerden nach der EU-KI-VO fehlen allerdings, so dass der auf diesem Wege erreichbare Schutz zwischen den zuständigen Behörden variieren kann, solange keine vereinheitlichenden Standards erlassen werden. Das Beschwerdeverfahren ersetzt – selbstverständlich – ausdrücklich nicht andere Rechtsbehelfe und Klageverfahren und ist auch für Strafverfolgungsbehörden anwendbar.

Das Recht auf Erläuterung der Entscheidungsfindung im Einzelfall besteht gegenüber den Betreibenden von Hochrisiko-Systemen (Art. 86 EU-KI-VO). Es gilt ebenfalls für Strafverfolgungsbehörden; Geheimhaltungsinteressen sollten hier restriktiv gehandhabt werden. Im Gegensatz zu Art. 85 EU-KI-VO setzt dieses Recht allerdings eine Betroffenheit von der Entscheidung voraus.

5.4 Recht auf Anfechtung KI-basierter Entscheidungen (*right to contest*)

Das Recht auf Anfechtung umfasst die Möglichkeit, gegen Entscheidungen von Systemen Einspruch zu erheben oder sich effektiv zu beschweren, was angesichts von strukturellen Machtasymmetrien für die Gewährleistung von Handlungsfähigkeit und Fairness in digitalen Umgebungen von hoher Relevanz ist (vgl. Hirsbrunner u. a. 2025; Kleemann/Tahraoui 2026). Eine KI-basierte Entscheidung anzufechten, ist ein Recht, das in gemeinsamen Grundsätzen wie Transparenz, Zugänglichkeit und Autonomie verankert ist. Wenn die Anfechtbarkeit in das Design von Entscheidungssystemen

eingebettet ist, kann sie als Brücke zwischen Nutzenden, Betroffenen und Systemen dienen und Einzelpersonen Möglichkeiten bieten, sich aktiv mit Entscheidungen, die ihr Leben betreffen, auseinanderzusetzen und diese zu beeinflussen (Collins u. a. 2024, S. 96ff.). Wenn ein *right to contest* so verstanden und umgesetzt wird, kann es zu einem höheren Maß an Fairness, Gerechtigkeit und Rechtsstaatlichkeit beitragen, indem Fehler korrigiert, ungerechte Ergebnisse verhindert oder nachträglich geändert werden (Kaminski/Urban 2021, S. 1974f.).

Ein allgemeines, über den gerichtlichen Rechtsschutz im mitgliedstaatlichen Strafprozess- und Verwaltungsprozessrecht (z. B. Anfechtungsklage oder Beschwerde) hinausgehendes Recht auf Anfechtung KI-basierter Entscheidungen ergibt sich nicht explizit aus der EU-KI-VO. Es kann aber aus dem Grundrecht auf Privatsphäre (Art. 7 und 8 EU-GRCh) und auch aus Rechtsprechung des EuGH abgeleitet werden. Im Hinblick auf die staatliche KI-Nutzung in Deutschland ergänzt ein solches Recht die Rechtsschutzgarantie des Grundgesetzes (Art. 19 Abs. 4 GG). Auch die DSGVO respektive JI-Richtlinie lässt sich hierfür argumentativ heranziehen.

Datenschutzrechtlich bestimmt Art. 22 Abs. 1 DSGVO, dass Personen nicht einer ausschließlich automatisierten Entscheidung unterworfen werden dürfen und Verantwortliche „angemessene Maßnahmen [treffen müssen], um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf *Anfechtung der Entscheidung* gehört“ (Abs. 3). Parallel dazu schreibt Art. 11 JI-Richtlinie für die Strafverfolgung vor, „dass eine ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidung — einschließlich Profiling —, [...] verboten ist [...]“. Dazu heißt es in Erwägungsgrund 38 JI-Richtlinie konkretisierend: „In jedem Fall sollte eine solche Verarbeitung mit geeigneten Garantien verbunden sein, einschließlich [...] des Rechts [...] auf *Anfechtung der Entscheidung*.“ Ein Recht auf Anfechtung existiert demnach für gewisse Formen der Verarbeitung personenbezogener Daten, insbesondere für vollautomatisierte Verarbeitungsformen. Das dürfte auf einen erheblichen Teil KI-basierter Entscheidungen zutreffen, welche Einzelpersonen auf individueller Ebene betreffen.

Damit ein solches Recht effektiv ist, muss es zudem über ein bloßes Recht auf Berichtigung hinausgehen und zumindest die Verpflichtung umfassen, die Begründetheit der Beschwerde zu prüfen und die Entscheidung zu begründen. Die für die Datenverarbeitung Verantwortlichen müssen

dazu verpflichtet werden, die automatisierten Entscheidungen wirksam anfechtbar zu machen oder die Nutzung des algorithmischen Entscheidungssystems gänzlich einzustellen (Bayamhoğlu 2022, S. 1063).

Auch der EuGH hat in einer Entscheidung aus dem Februar 2025 ein „Recht auf Erklärung“ im Zusammenhang mit automatisierten Entscheidungen bestätigt.⁵ Das Urteil stellte klar, dass Gerichte und zuständige Behörden Zugang zu Informationen haben müssen, die durch Geschäftsgeheimnisse geschützt sind, wenn dies erforderlich ist, um diesen Schutz mit den Grundrechten der betroffenen Personen in Einklang zu bringen. Damit wird das Recht auf Anfechtung auch für KI-Systeme gegenüber gegenläufigen privatwirtschaftlichen Interessen gestärkt.

Eine Person, die z. B. aufgrund eines Treffers in einem KI-gestützten Objektdetektionssystem oder einer KI-basierten Sprechenderkennung in das Visier der Strafverfolgung geraten ist, wird in der Praxis kaum Kenntnis davon erlangen, dass dieses System zur Ermittlung gegen sie beigetragen hat, geschweige denn, welche Parameter und Trainingsdaten dem Ergebnis zugrunde lagen. Das Recht auf Anfechtung kann hier Gefahr laufen, strukturell leer zu bleiben, solange keine Offenlegungspflichten gegenüber Betroffenen bestehen.

5.5 Weitere prozedurale *Accountability*-Vorkehrungen

Darüber hinaus enthält die EU-KI-VO weitere prozedurale *Accountability*-Vorkehrungen in unterschiedlicher Zuständigkeit, so die Pflicht der Anbietenden von Hochrisiko-KI-Systemen, ein Qualitätsmanagementsystem einzurichten (Art. 17 EU-KI-VO) und die in der Zuständigkeit des KI-Büros liegenden Überwachungsmaßnahmen gegenüber Anbietenden von KI-Modellen mit allgemeinem Verwendungszweck (Art. 89 EU-KI-VO). Auch die Pflicht der Anbietenden zur Beobachtung ihrer Systeme nach dem Inverkehrbringen (Art. 72 EU-KI-VO) sei hier erwähnt. Sie umfasst auch die Pflicht zur Erhebung und Dokumentation relevanter Daten über das jeweilige KI-System während seiner gesamten Lebensdauer (Abs. 2).

Die freiwillig zu befolgenden Verhaltenskodizes für KI-Systeme, die nicht in die Hochrisiko-Kategorie fallen, sind schließlich einer der wenigen, allerdings schwach ausgeprägten Beiträge zu *Accountability*-Vorkehrungen außerhalb des Hochrisiko-Bereichs.

5 EuGH, Urteil vom 27.2.2025, Rechtssache C-203/22, CK gg. Magistrat der Stadt Wien (Dun & Bradstreet Austria).

5.6 Einbindung Externer als *Accountability*-Foren?

Die Möglichkeit einer Überprüfung KI-basierter Entscheidungen durch Dritte kann auch durch weitere Überwachungsmechanismen wie *Audits* erleichtert werden, die darauf ausgelegt sind, Fehler oder Schäden durch KI-Systeme zu vermeiden. An vielen Stellen überlässt die EU-KI-VO Anbietenden und Betreibenden Spielräume bei der Frage, wie sie die ihnen obliegenden laufenden Kontrollaufgaben für ihre KI-Systeme wahrnehmen. Hier kommt die Einbindung externer Expertise, etwa zertifizierter Auditor:innen, in Betracht. Auch notifizierte Stellen (Art. 3 Nr. 22 EU-KI-VO) könnten hier vor dem Hintergrund ihrer Aufgaben und Informationspflichten (Art. 31 und 45 EU-KI-VO) eingebunden werden. Weiteren Stellen, z. B. staatlichen Behörden und zivilgesellschaftlichen Organisationen, könnten Überwachungsaufgaben übertragen werden, soweit sie über den erforderlichen Sachverstand verfügen. Beispielsweise schreibt Art. 14 Abs. 1 EU-KI-VO eine menschliche Aufsicht für risikoreiche Systeme vor und verlangt darüber hinaus gründliche Untersuchungen von Vorfällen, um die Behebung von Fehlern oder entstandenen Schäden zu gewährleisten (vgl. Laux 2024, S. 2857). Diese Aufgaben könnten im Interesse der Qualitätssicherung von neutralen Dritten wahrgenommen werden. Dabei sind allerdings Interessenkonflikte zu vermeiden, etwa die Vereinnahmung der Auditor:innen durch Industrieinteressen. Als bewährte Gegenmaßnahmen sehen viele *Accountability*-Foren z. B. eine Rotation der Auditor:innen und Prüfer:innen vor (vgl. Laux 2024, S. 2861).

Die Wahrnehmung dieser Aufgaben erfordert interdisziplinäre Expertise, da bei der Prüfung von KI-Systemen oftmals technische, rechtliche und oft auch sozialwissenschaftliche Fragen eng miteinander verknüpft sind. Forschende, zivilgesellschaftliche Akteur:innen und unabhängige Expert:innen können an solchen Audits beteiligt sein, um einen umfassenden, vielfältigen und letztlich effektiven Rechenschaftsrahmen zu etablieren. Das Risiko eines sogenannten *Audit Washing* besteht immer dann, wenn interne Audits oder Konformitätsbewertungen lediglich von den Entwickelnden und Anbietenden von KI-Systemen durchgeführt werden (Hartmann u. a. 2025).

6. *Accountability*- und *Compliance*-Vorkehrungen im Kontext bestehender *Accountability*-Foren in der EU und den Mitgliedstaaten

Wie gezeigt, hat die EU-KI-VO zusätzliche, stark fragmentierte *Accountability*- und *Compliance*-Vorkehrungen institutioneller und vor allem pro-

zeduraler Art etabliert, deren Anwendungsfeld weitgehend auf Hochrisiko-KI-Systeme beschränkt bleibt. Keine der KI-Behörden fungiert indes als durchsetzungsstarkes *Accountability*-Forum. Die bestehenden *Accountability*-Foren bleiben daher von großer Bedeutung, auch für die Kontrolle der KI-Nutzung, insbesondere der Europäische Datenschutzbeauftragte, die EU-Bürgerbeauftragte, die EU-Grundrechteagentur, der EuGH sowie die mitgliedstaatlichen Aufsichtsbehörden und Gerichte.

KI-Anwendungen benötigen große Mengen an Daten für das Training und Testen. Viele KI-Anwendungen verarbeiten auch für ihre Kernzwecke personenbezogene Daten, so dass auch insofern die Datenschutzaufsicht zuständig ist. Vor diesem Hintergrund ist es bemerkenswert, dass die Datenschutzaufsicht trotz ihrer einschlägigen Kompetenz und Erfahrungen in der EU-KI-VO nur am Rande vorkommt. Dies gilt in besonderem Maße für Mitgliedstaaten wie Deutschland, in denen die Funktion der KI-Marktüberwachungsbehörde entgegen Art. 74 Abs. 8 EU-KI-VO nicht bei den Datenschutzbehörden angesiedelt wurde. Die EU-KI-VO ermöglicht zwar, bestimmte Kontrollaufgaben an die Datenschutzaufsicht zu übertragen, insbesondere mit Blick auf die KI-Nutzung durch Strafverfolgungsbehörden, jedoch haben die Mitgliedstaaten dabei erhebliche Entscheidungsspielräume.

Der Europäische Datenschutzbeauftragte (*European Data Protection Supervisor*, EDPS) übernimmt die Funktion der Aufsichtsbehörde für die KI-Nutzung durch Organe, Einrichtungen und sonstige Stellen der EU (Art. 70 Abs. 9 und Art. 74 Abs. 9 EU-KI-VO). Hierunter fallen auch die für die Polizei- und Justizzusammenarbeit zuständigen EU-Agenturen, insbesondere Europol, Eurojust und eu-LISA. An dem KI-Gremium, das auf der Basis von Art. 65 EU-KI-VO eingerichtet wird, ist der EDPS allerdings nur mit Beobachterstatus beteiligt.

Andere EU- und mitgliedstaatliche *Accountability*-Foren wie die Ombudsinstitutionen und die Rechnungshöfe finden in der EU-KI-VO keine Erwähnung, können aber im Rahmen ihrer allgemeinen Zuständigkeit Kontrollaufgaben auch bezüglich der behördlichen KI-Nutzung wahrnehmen. Dies führt zur Notwendigkeit einer engen Abstimmung und Koordination zwischen den diversen *Accountability*-Foren, damit es nicht zu einer *Accountability*-Diffusion, Fragmentierung und Kompetenzgerangel kommt und Rechtssicherheit erreicht werden kann. Für die mitgliedstaatlichen Gerichte und den EuGH dürfte sich die Auslegung der EU-KI-VO ebenfalls zu einem neuen Arbeitsfeld entwickeln, sobald einschlägige Fälle dorthin gelangen.

7. Schlussfolgerungen und Ausblick

Dieser Beitrag hat gezeigt, dass die EU-KI-VO fragmentierte Mehrebenen-*Accountability*- und *Compliance*-Strukturen vorsieht, deren Anwendungsbereich sich weitgehend auf Hochrisiko-KI-Systeme beschränkt und die mit einigen Einschränkungen auch für die polizeiliche KI-Nutzung anwendbar sind.

Damit wird die Risikoklassifizierung eines KI-Systems zur entscheidenden Weichenstellung für die Intensität der prozeduralen Anforderungen und der Aufsichtsbefugnisse gegenüber der KI-Nutzung. Während der Aushandlung der EU-KI-VO kam es zu signifikanten Einschränkungen der Hochrisiko-Kategorie für Strafverfolgungsbehörden (vgl. Kleemann/Aden 2025) und damit auch zu einer Reduzierung der *Accountability*-Vorkehrungen für die polizeiliche KI-Nutzung. Bestrebungen im Rahmen des sogenannten *Digital Omnibus* (Europäische Kommission 2025), die EU-KI-VO und weitere Digitalgesetze (u. a. auch die DSGVO) zugunsten von Interessen an vereinfachten Verfahren zu ändern, berühren auch die Regeln für die Strafverfolgung. Allerdings fehlt es an Evidenz für die Notwendigkeit der Änderungen eines so neuen Rechtsakts wie der EU-KI-VO, dessen Anwendungspraxis noch begrenzt ist (zur Kritik vgl. Leufer 2025, Dachwitz 2025). Die Übergangsphase bis zur vollen Geltung der Hochrisiko-Anforderungen wurde schließlich verlängert (Art. 113 EU-KI-VO in der durch Verordnung (EU) 2026/1744 geänderten Fassung). Während die Europäische Kommission unter dem Druck von Interessengruppen und einiger mitgliedstaatlicher Regierungen versuchte, das Schutzniveau zu senken, schlug sie mit dem *Digital Omnibus* zugleich die Stärkung des KI-Büros und damit einer kommissionseigenen Dienststelle vor und setzte sich damit weitgehend durch (Art. 75a, 75b und 75c EU-KI-VO in der durch Verordnung (EU) 2026/1744 geänderten Fassung). Eine solche Zentralisierung auch im Bereich der Strafverfolgung wurde von einigen mitgliedstaatlichen Regierungen als zu starker Eingriff in ihre Kompetenzen kritisiert, weswegen sie eine Ausnahme von dem Aufgabenzuwachs für das KI-Büro befürworten (Bertuzzi 2026a). Dies wurde in Art. 75 in der durch Verordnung (EU) 2026/1744 geänderten Fassung festgeschrieben. Zudem schlossen sich 23 der 27 Mitgliedsstaaten einem Brief an, mit dem sie Einfluss auf die Leitlinien zur Einstufung von Hochrisiko-KI fordern, um zu einer möglichst engen Auslegung des Anwendungsbereichs der Hochrisiko-Anforderungen zu kommen; insbesondere der Bereich Strafverfolgung bedürfe „besonderer Überlegungen“, damit die Fähigkeiten von Strafverfolgungsbehörden nicht

untergraben würden (Bertuzzi 2026b). In einem Bereich, der ohnehin von Ausnahmen und „Hintertüren“ (siehe oben, Abschnitt 1) geprägt ist, sollte hier allerdings das Schutzniveau eher gesteigert als abgeschwächt werden.

Effektive *Accountability*- und *Compliance*-Vorkehrungen für die KI-Entwicklung und -Nutzung zeichnen sich durch eine ganzheitliche Perspektive auf technische Eigenschaften und den rechtlichen Rahmen sowie auf ihre Wechselwirkungen aus. Aufgrund der Fragmentierung der institutionellen Strukturen und der Aufsichtskompetenzen fehlt eine solche ganzheitliche Perspektive bisher. Wichtige Funktionen werden in diesem Kontext sogar den Anbietenden und Betreibenden von KI-Systemen überlassen, andere Aufsichtsfunktionen sind abhängigen Behörden wie dem KI-Büro in der Europäischen Kommission und Marktüberwachungsbehörden in den Mitgliedstaaten zugewiesen. Die EU-KI-VO gewährleistet daher aus sich heraus weder eine effektive Kontrolle der KI-Entwicklung und -Nutzung im Allgemeinen noch speziell der polizeilichen KI-Nutzung.

Absehbar ist die EU-KI-VO erst der Anfang der KI-Regulierung in Europa. Für die Rechtsprechung sowie für Empfehlungen und Entscheidungen der in der Verordnung vorgesehenen Behörden und Gremien verbleibt dabei ein großer Konkretisierungsbedarf, insbesondere zur Sicherung des in der EU-KI-VO an vielen Stellen geforderten hohen Schutzniveaus für „Grundrechte, Gesundheit und Sicherheit“, gerade in grundrechtssensiblen Bereichen wie der Strafverfolgung. Manches bleibt durch zukünftige weitere Gesetzgebung zu konkretisieren. Weiterer interdisziplinärer Forschungsbedarf besteht dabei unter anderem für die Übersetzung abstrakter Begriffe in handhabbare. In der EU-KI-VO, der KI-Rahmenkonvention des Europarats (CETS No. 225) und auch in *soft-law*-Instrumenten wie den OECD-Empfehlungen zu KI (OECD/LEGAL/0449) oder den UNESCO Empfehlungen zur Ethik von KI (SHS/BIO/PI/2021/1) wurden grundlegende Prinzipien für die KI-Entwicklung und -Nutzung definiert. Diese bedürfen der Konkretisierung hinsichtlich der Operationalisierung von Grundrechtsschutz in Form messbarer Indikatoren für Grundrechtseingriffe durch KI-Systeme, auch im Rahmen von Strafverfolgung.

Für KI-Systeme zur Objektdetektion oder Sprechendenerkennung in der Strafverfolgung könnte dies etwa bedeuten: Welche Fehlerquoten (hier insbesondere *False-Positive*-Raten) sind mit dem Verhältnismäßigkeitsgrundsatz noch vereinbar, auch unter Berücksichtigung der Intensität des jeweiligen Grundrechtseingriffs? Welche Mindestanforderungen an Trainingsdaten gelten, um diskriminierende Outputs zu vermeiden? Und ab welchem

Automatisierungsgrad ist eine menschliche Letztentscheidung zwingend erforderlich, bevor ein KI-Treffer zu einer operativen Maßnahme führt?

Für einzelne KI-Systeme könnte dies im Rahmen einer umfassend verstandenen Grundrechte-Folgenabschätzung geschehen. Konzepte von menschlicher Aufsicht und Intervention bedürfen weiterer Konkretisierung hinsichtlich einheitlicher Definitionen, Handhabung oder Umsetzung. Dazu zählen z. B. Art. 22 DSGVO, Art. 14 EU-KI-VO und weitere Ausformungen im mitgliedstaatlichen Recht. Offene Fragen verbleiben auch für die Haftung bei Fehlentscheidungen, im polizeilichen Kontext auch für die Rechenschaftspflicht für unrechtmäßige Polizeimaßnahmen, die auf KI-Entscheidungen zurückgehen.

Ein maßgeblicher Ansatzpunkt für effektive *Accountability*-Strukturen ist das Zusammenspiel aller beteiligten Akteur:innen im KI-Lebenszyklus. Technischen KI-Entscheidungen folgen echte soziale und rechtliche Auswirkungen. Sozio-technische Systeme müssen daher auch als solche behandelt werden. Ein Zurückziehen auf reine technische (Un-)Möglichkeiten oder rechtliche Vorgaben kann hier nicht funktionieren.

Literatur

- Aden, Hartmut (2025): Dilemmata der Polizeibeauftragten, *vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik*, Heft 249 (= 64(1)), S. 3–14.
- Aden, Hartmut und Fährmann, Jan (2021): Argumente für einen besseren Musterentwurf für einheitlichere Polizeigesetze. Kritische Analyse von Entwicklungen im Polizeirecht aus rechtsstaatlicher und bürgerrechtlicher Perspektive. In: Martin H. W. Möllers und Robert Chr. van Ooyen (Hrsg.): *Jahrbuch Öffentliche Sicherheit 2020/2021*, Baden-Baden: Nomos und Frankfurt/Main: Verlag für Polizeiwissenschaft, S. 580–615.
- Bayamlioglu, Emre (2022): The right to contest automated decisions under the General Data Protection Regulation: Beyond the so-called “right to explanation”. *Regulation & Governance*, 16(4), S. 1058–1078. <https://doi.org/10.1111/rego.12391>.
- Bertuzzi, Luca (2026a): Can EU plans to centralize AI law enforcement endure pushback by member states? *MLex* vom 30.01.2026, URL: <https://www.mlex.com/mlex/articles/2435744/can-eu-plans-to-centralize-ai-law-enforcement-endure-pushback-by-member-states-> (besucht am 13.05.2026).
- Bertuzzi, Luca (2026b): EU countries press for law enforcement considerations in AI law guidelines. *MLex* vom 28.01.2026, URL: <https://www.mlex.com/mlex/articles/2434470/eu-countries-press-for-law-enforcement-considerations-in-ai-law-guidelines> (besucht am 13.05.2026).

- Bosman, Timo (2025): Kommentierung zu Art. 25 EU-KI-VO. In: Schefzig, Jens und Kilian, Robert (Hrsg.): BeckOK KI-Recht, 5. Edition
Stand: 01.11.2025, München: C.H. Beck.
- Bovens, Mark (2007): Analysing and assessing accountability: A conceptual framework. *European Law Journal*, 13(4), S. 447–468.
- Bovens, Mark; Goodin, Robert E. und Schillemans, Thomas (2014): Public Accountability. In: Mark Bovens, Thomas Schillemans und Robert E. Goodin (Hrsg.): *The Oxford Handbook of Public Accountability*. Oxford: Oxford University Press, S. 1–20.
- Collins, Robert Patrick; Redström, Johan und Rozendaal, Marco (2024): The Right to Contestation: Towards Repairing Our Interactions with Algorithmic Decision Systems, *International Journal of Design*, 18, S. 95–106.
- Dachwitz, Ingo (2025): „Größter Rückschritt für digitale Grundrechte in der Geschichte der EU“. *Netzpolitik* vom 13.11.2025, URL: <https://netzpolitik.org/2025/digitaler-omnibus-groesster-rueckschritt-fuer-digitale-grundrechte-in-der-geschichte-der-eu/> (besucht am 08.02.2026).
- Europäische Kommission (2025): Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnungen (EU) 2024/1689 und (EU) 2018/1139 im Hinblick auf die Vereinfachung der Umsetzung harmonisierter Vorschriften für künstliche Intelligenz (Digital-Omnibus-Verordnung zur KI), COM(2025) 836 final 2025/0359 (COD). URL: <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A52025PC0836> (besucht am 20.07.2026).
- European Center for Not-for-Profit Law (ECNL) (2026): Four things to know about the EU AI Act Advisory Forum. URL: <https://ecnl.org/news/four-things-know-about-eu-ai-act-advisory-forum> (besucht am 20.07.2026).
- Fährmann, Jan; Aden, Hartmut und Arzt, Clemens (2022): Transparenz der polizeilichen Datenverarbeitung: Defizite und technische Lösungsansätze: In: Michael Friedewald, Michael Kreutzer und Marit Hansen (Hrsg.): *Selbstbestimmung, Privatheit und Datenschutz - Gestaltungsoptionen für einen europäischen Weg*, Wiesbaden: Springer, S. 303–326.
- Fischer, Maximilian T.; Schlegel, Udo; Keim, Daniel A.; Altmann, Stefan; Grothe, Claudia; Reuter, Paul; Coleman, Graham; Geierhos, Manuela; Maoro, Falk; Kluin, Marco; Weinbuch, Monika; Aden, Hartmut; Kleemann, Steven; Tahraoui, Milan; Louban, Anna; Arndt, Maximilian; Schönrock, Sabrina; Brandner, Lou T.; Hirsbrunner, Simon D.; Loh, Wulf und Yilmaz, Yusuf (2025): *DIN SPEC 91517:2025–05. Anforderungen an vertrauenswürdige KI-Methoden in polizeilichen Anwendungen*. Berlin: DIN Media GmbH, <https://doi.org/10.31030/3612025>.
- Garcia-Godinez, Miguel (2025): A default framework for fundamental rights impact assessment. *AI Ethics*, 5, S. 5149–5163, <https://doi.org/10.1007/s43681-025-00761-1>.
- Guerra, Georgia (2019): An Interdisciplinary Approach for Comparative Lawyers: Insights from the Fast-Moving Field of Law and Technology. *German Law Journal*, 19(3), S. 579–601, <https://doi.org/10.1017/S2071832200022793>.
- Hartmann, David; Laranjeira de Pereira, José Renato; Streitbürger, Chiara und Berendt, Bettina (2025): Addressing the regulatory gap: moving towards an EU AI audit ecosystem beyond the AI Act by including civil society. *AI Ethics*, 5, S. 3617–3638.

- Hartmann, Sarah (2026): Kommentierung zu Art. 85 EU-KI-VO. In: Martini, Mario und Wendehorst, Christiane (Hrsg.): KI-VO: Verordnung über künstliche Intelligenz, Kommentar. 2. Auflage, München: C.H. Beck.
- Hirsbrunner, Simon; Kleemann, Steven und Tahraoui, Milan (2025): Contestation in artificial intelligence as a practice: from a system-centered perspective of contestability towards normative contextualization, situative critique and organizational culture. *Frontiers in Communication* 10. <https://doi.org/10.3389/fcomm.2025.1638257>.
- Kaminski, Margot E. und Urban, Jennifer M. (2021): The Right to Contest AI, in: *Columbia Law Review*, 121, S. 1957–2048.
- Kleemann, Steven und Aden, Hartmut (2025): Die Nutzung Künstlicher Intelligenz durch Strafverfolgungsbehörden – „Hintertüren“ der Verordnung der Europäischen Union über Künstliche Intelligenz. In: Wilfried Honekamp, Stefanie Kemme und Jens Struck (Hrsg.): *Auswirkungen von Künstlicher Intelligenz auf die zukünftige Polizeiarbeit. Technologische Potenziale, rechtliche Rahmenbedingungen, kriminologisch-sozialwissenschaftliche Erkenntnisse*, Wiesbaden: Springer, S. 3–30.
- Kleemann, Steven und Aden, Hartmut (2026): Die Grundrechte-Folgenabschätzung nach dem Artificial Intelligence Act der Europäischen Union – Chancen einer qualitativen Konkretisierung für die polizeiliche KI-Nutzung. *Die Polizei*, 117(4a) (Sonderheft), S. 226–230.
- Kleemann, Steven und Tahraoui, Milan (2026): Responsibility and Accountability for the use of AI in Law Enforcement in the European Union: Lost in Negotiations?. *MenschenRechtsMagazin*, 30(2), S. 117–143. <https://doi.org/10.60935/mrm2025.30.28>.
- Krahn, Noelle V. (2024): The European Union’s Artificial Intelligence Act – A Status Report, *Transatlantic Law Journal (TLJ)*, 3, S. 120–125.
- Laux, Johann (2024): Institutionalised distrust and human oversight of artificial intelligence: Towards a democratic design of AI governance under the European Union AI Act. *AI & Society*, 39(6), S. 2853–2866.
- Leufer, Daniel (2025): Digital Rights Are on the Chopping Block in the European Commission’s Omnibus. *Tech Policy Press* vom 19.11.2025, URL: <https://www.techpolicy.press/digital-rights-are-on-the-chopping-block-in-the-european-commissions-omnibus/> (besucht am 13.05.2026).
- Martini, Mario und Botta, Jonas (2025): Polizeiliche Datenanalyse mittels KI – Unions-, verfassungs- und polizeirechtliche Leitplanken für Palantir & Co. *Die Öffentliche Verwaltung (DÖV)*, 78(24), S. 1033–1044.
- Martinez Demarco, Sol; Tahraoui, Milan und Kleemann, Steven (2026): The siloed logic and the implementation of the Artificial Intelligence Act in the law enforcement context: legal and ethical analysis of the applicability of accountability and responsibility to high-risk AI systems. In: Marie Eneman, Diana Miranda, Jan Ljungberg und William Webster (Hrsg.): *AI Surveillance and the Future of Policing: Opportunities, Threats, Perspectives and Cases*. London: Routledge, i.E.
- Novelli, Claudio; Taddeo, Mariarosaria und Floridi, Luciano (2024): Accountability in artificial intelligence: What it is and how it works. *AI & Society*, 39, S. 1871–1882.

- Novelli, Claudio; Hacker, Philipp; Morley, Jessica; Trondal, Jarle und Floridi, Luciano (2025): A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities. *European Journal of Risk Regulation*. 16(2), S. 566–590. <https://doi.org/10.1017/err.2024.57>.
- Schuett, Jonas (2024): Risk Management in the Artificial Intelligence Act. *European Journal of Risk Regulation*, 15(2), S. 367–385. <https://doi.org/10.1017/err.2023.1>.
- Thomaidou, Anna und Limniotis, Konstantinos (2025): Navigating Through Human Rights in AI: Exploring the Interplay Between GDPR and Fundamental Rights Impact Assessment. *Journal of Cybersecurity and Privacy*, 5(1), 7, <https://doi.org/10.3390/jcp5010007>.
- Töpfer, Eric; John, Sonja und Aden, Hartmut (2023): *Parlamentarische Polizeibeauftragte: Menschenrechtliche Empfehlungen für die Stellen in Bund und Länder*. Berlin: Deutsches Institut für Menschenrechte und Forschungsinstitut für Öffentliche und Private Sicherheit, <https://doi.org/10.4393/opushwr-4265>

