**Fachbereiche EU 6 und WD 5**

# Biometrischer Abgleich mit Bildern aus dem Internet

Technische Umsetzung und Vereinbarkeit mit der KI-Verordnung



EU 6 - 3000 - 074/25; WD 5 - 3000 - 105/25

**Biometrischer Abgleich mit Bildern aus dem Internet**
Technische Umsetzung und Vereinbarkeit mit der KI-Verordnung

| | |
|---|---|
| Aktenzeichen: | EU 6 - 3000 - 074/25; WD 5 - 3000 - 105/25 |
| Abschluss der Arbeit: | 22. Januar 2026 |
| Fachbereich: | EU 6: Fachbereich Europa; WD 5: Wirtschaft, Energie und Klima |

## Inhaltsverzeichnis

## 1. Einleitung

Der Einsatz von Künstlicher Intelligenz (KI) zum Zweck der Gesichtserkennung wird kontrovers diskutiert. Schon seit einiger Zeit sammeln private Unternehmen wie *PimEyes* und *Clearwiev AI* in großem Umfang öffentlich zugängliche Fotos aus dem Internet und bieten Privatpersonen an, biometrische Abgleiche durchzuführen.[1] Diese – von europäischen Datenschutzbehörden als rechtswidrig eingestufte[2] – Praxis der Privatwirtschaft steht in Kontrast zu den Befugnissen der Ermittlungsbehörden. Bislang darf die Polizei Fahndungsfotos nur mit polizeiinternen Datenbanken abgleichen, etwa mit Bildern aus der erkennungsdienstlichen Behandlung.[3]

Die derzeitige Koalition hat es sich – wie zuvor bereits die Ampel-Koalition[4] – zum Ziel gesetzt, die digitalen Ermittlungsbefugnisse der Sicherheitsbehörden auszudehnen. So sieht der Koalitionsvertrag vor, dass Sicherheitsbehörden für bestimmte Zwecke „den nachträglichen biometrischen Abgleich mit öffentlich zugänglichen Internetdaten, auch mittels Künstlicher Intelligenz, vornehmen können“ sollen.[5] Im Jahr 2025 sind zwei Referentenentwürfe des Bundesinnenministeriums „zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit“ bekannt geworden,[6] die neue Befugnisse für den biometrischen Abgleich mit Bildern aus dem Internet vorsehen. Die Entwürfe befinden sich derzeit in Abstimmung zwischen den Ministerien.

Der biometrische Abgleich mit Bildern aus dem Internet ist – nicht zuletzt angesichts exponentieller Fortschritte von KI-Systemen – technisch wie rechtlich umstritten.[7] So erschien im September 2025 im Auftrag der Nicht-Regierungsorganisation „AlgorithmWatch“ ein Gutachten über die technische Realisierung des biometrischen Abgleichs mit im Internet verfügbaren Bildern.[8] Das Gutachten kommt zu dem Ergebnis, dass ein biometrischer Abgleich von Gesichtern, die staatli-

---

1 Näher dazu: *Ogorek*, Staatliche Gesichtserkennung durch biometrischen Abgleich mit Online-Daten, LTZ 2024, 274 (274 f.).

2 Gegen *Clearview AI* wurden bereits Löschungs- und Bußgeldanordnungen durch mitgliedstaatliche Datenschutzbehörden erlassen.

3 Zur Funktionsweise der polizeiinternen Datenbank INPOL siehe: *Ogorek*, Staatliche Gesichtserkennung durch biometrischen Abgleich mit Online-Daten, LTZ 2024, 274 (275).

4 Ein ähnliches Gesetzgebungsvorhaben der Ampel-Koalition war im Bundesrat gescheitert, siehe Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung, Drucks. 20/12806 und 20/13413 Buchstabe b.; *Rath*, Kopflos in die Gesichtserkennung, Beitrag im Anwaltsblatt v. 29. Oktober 2024.

5 Verantwortung für Deutschland, Koalitionsvertrag zwischen CDU, CSU und SPD, 21. Legislaturperiode, 5. Mai 2025, S. 82 Rn. 2629 ff.

6 Entwürfe eines ersten und zweiten Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit 26. Juni 2025, veröffentlicht durch Netzpolitik.org am 23. Juli 2025.

7 Offener Brief mehrerer zivilgesellschaftlicher Organisationen an Bundeskanzler Merz, Vizekanzler Klingbeil, Bundesminister Dobrindt und Bundesministerin Hubig vom 8. August 2025.

8 *Lewandowski*, Braucht die Polizei eine Datenbank zum biometrischen Abgleich? Das Durchsuchen von Internetbildern zur Gesichtserkennung, Technisches Gutachten im Auftrag von AlgorithmWatch, September 2025.

chen Behörden in Form von Fotos vorliegen, mit öffentlich zugänglichen Bildern aus dem Internet nicht umsetzbar ist, ohne hierfür eine Datenbank zu erstellen, was – so das Gutachten – die Verordnung über Künstliche Intelligenz (KI-VO) „ausnahmslos […] verbiete“.[9]

Unter Bezugnahme auf dieses Gutachten wurden die Wissenschaftlichen Dienste und der Fachbereich Europa des Deutschen Bundestages mit der Prüfung beauftragt,

– ob es *technische* Möglichkeiten gebe, um derzeit oder in absehbarer Zukunft frei verfügbare Bilder aus dem Internet für einen biometrischen Abgleich praktikabel automatisiert durchsuchbar zu machen, ohne eine zuvor angelegte Datenbank mit entsprechenden Bildern aus dem Internet zu nutzen;

– wie demzufolge *rechtlich* mit Blick auf die Vorgaben der KI-Verordnung nationale Bestrebungen wie das neue Sicherheitspaket zu bewerten seien, die einen biometrischen Abgleich mit Bildern aus dem Internet vorsehen.

Auftragsgemäß verfolgt das Gutachten einen zweiteiligen Aufbau: In einer ersten technischen Analyse wird untersucht, ob – und wenn ja, unter welchen Voraussetzungen – ein biometrischer Abgleich mit im Internet verfügbaren Bildern ohne die vorherige Erstellung einer Datenbank möglich ist. Ziel ist es, die zugrunde liegenden Annahmen transparent zu machen, zentrale Abgrenzungen herauszuarbeiten und dem Leser eine belastbare Orientierung in einer komplexen und vielfach verkürzten Debatte zu bieten (Ziff. 2). In einer zweiten, rechtlichen Analyse wird – aufbauend auf den Ergebnissen der technischen Analyse – geprüft, ob ein automatisierter biometrischer Abgleich mit öffentlich zugänglichen Bildern aus dem Internet, wie ihn das Sicherheitspaket des Bundesinnenministeriums vorsieht, mit der KI-Verordnung (KI-VO)[10] vereinbar wäre (Ziff. 3).

Gegenstand der rechtlichen Analyse sind dabei lediglich die Vorgaben der KI-VO.[11] Es wird darauf hingewiesen, dass der biometrische Abgleich mit Bildern aus dem Internet auch eine datenschutzrechtliche und eine grundrechtliche Komponente hat.[12]

---

9 *Lewandowski*, Braucht die Polizei eine Datenbank zum biometrischen Abgleich? Das Durchsuchen von Internetbildern zur Gesichtserkennung, Technisches Gutachten im Auftrag von AlgorithmWatch, September 2025.

10 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, ABl. L 2024/1689, 12. Juli 2024.

11 Die Darstellung beschränkt sich auf die KI-VO in der am 1. August 2024 in Kraft getretenen Fassung, unabhängig vom Geltungsbeginn einzelner Bestimmungen gemäß Art. 111, 113 KI-VO.

12 Vgl. überblicksartig *Rückert*, Gesichtserkennung durch KI im Strafverfahren, Die Technik ist da, das Recht (noch) nicht, Legal Tribune Online vom 25. April 2025; KOM, Leitlinien zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689, Rn. 238.

## 2. Technische Analyse

### 2.1. Der Ausgangspunkt: Das technische Gutachten im Auftrag von AlgorithmWatch

In einem technischen Gutachten der Hochschule für Angewandte Wissenschaften Hamburg im Auftrag der Nicht-Regierungsorganisation AlgorithmWatch[13] untersucht der Autor die technischen Möglichkeiten, ob ein biometrischer Abgleich von Gesichtern, die staatlichen Behörden in Form von Fotos vorliegen, mit öffentlich zugänglichen Bildern aus dem Internet möglich ist, ohne hierfür eine Datenbank zu erstellen. Ausgangspunkt ist ein Szenario, in dem der abgleichenden Stelle ein Bild einer Person sowie ein daraus erzeugtes biometrisches Gesichtstemplate zur Verfügung stehen. Weitere biometrische Merkmale, etwa Stimmproben, werden ausgeschlossen. Die Analyse konzentriert sich auf den technischen Kern der Fragestellung.

#### 2.1.1. Technische Grundannahmen und Begriffsverständnis

Zentral für die Argumentation des Gutachtens ist ein präzises und weiter gefasstes Verständnis des Begriffs „Datenbank“. Als Datenbank gelte jede strukturierte Sammlung von Datensätzen, die mithilfe eines Datenbankverwaltungssystems durchsucht werden kann. Dabei sei es unerheblich, ob die Daten dauerhaft oder nur temporär gespeichert werden und ob sie aus internen oder externen Quellen stammen. Bereits die Anlage einzelner Datensätze – bestehend aus Metadaten wie URLs oder Templates und gegebenenfalls den zugehörigen Bildern – begründet nach dieser Definition das Vorliegen einer Datenbank.

Für eine praktikable Durchsuchbarkeit sei zudem eine Vorverarbeitung der Daten erforderlich, insbesondere in Form von Indexstrukturen. Solche Indexe gelten als Verzeichnisse, die eine effiziente Suche ermöglichen, stellen technisch jedoch selbst wiederum Datenbanken dar. Dieses weite Begriffsverständnis ist entscheidend, da es verhindert, dass funktional notwendige Zwischenspeicher, temporäre Sammlungen oder Indexmechanismen fälschlich als „datenbankfrei“ eingeordnet werden könnten.

#### 2.1.2. Grundsätzliche Grenzen eines Abgleichs ohne Datenbank

Vor diesem Hintergrund diskutiert das Gutachten, dass ohne eine Datenbank kein One-to-Many-Abgleich, wie er im angegebenen Szenario bei z. B. klassischen Bildersuchmaschinen dargestellt ist, möglich sei. Ein solcher Abgleich, bei dem ein Referenzbild systematisch mit einer Vielzahl potenzieller Vergleichsbilder im Internet abgeglichen wird, setze eine (vor-)strukturierte Sammlung dieser Vergleichsbilder voraus. Ohne eine entsprechende Datenbasis bleibt technisch lediglich ein One-to-One-Vergleich möglich, bei dem jeweils zwei Bilder daraufhin geprüft werden, ob sie dieselbe Person zeigen.

Laut Gutachten ließe sich ein One-to-Many-Abgleich theoretisch simulieren, indem das Referenzbild sukzessive mit einer großen Zahl einzelner Bilder verglichen wird. Sobald diese Bilder je-

13 *Lewandowski*, Braucht die Polizei eine Datenbank zum biometrischen Abgleich? Das Durchsuchen von Internetbildern zur Gesichtserkennung, Technisches Gutachten im Auftrag von AlgorithmWatch, September 2025.

doch vorab systematisch erfasst, vorverarbeitet oder auch nur kurzfristig gesammelt werden, entstehe dabei funktional eine Datenbank. Daher sei es nach gängigen Ansätzen der Internetbildersuche nicht möglich, Suchen ohne Datenbanken durchzuführen.

Allerdings werden im Gutachten auch theoretische Alternativansätze diskutiert, auf eine Datenbank zu verzichten, dies führe jedoch zu Lösungen, die ineffizient, ressourcenintensiv, nicht skalierbar und damit nicht praktikabel wären – vorausgesetzt, man legt als „praktikabel“ einen Maßstab an, der den Erwartungen einer regulären Websuche entspricht.

#### 2.1.3. Prüfung theoretischer Alternativen ohne expliziten Datenbankaufbau

Das Gutachten untersucht verschiedene theoretische Ansätze, die einen biometrischen Abgleich ohne expliziten Aufbau einer Datenbank ermöglichen könnten, und bewertet diese anhand der Einschätzung auf praktische Umsetzbarkeit.

Ein erster Ansatz ist eine sogenannte „Live-Suche“ im Internet. Dabei würde erst zum Zeitpunkt der Suchanfrage mit der Erfassung von Webinhalten begonnen. Ein Crawler würde Webseiten systematisch durchsuchen, Bilder herunterladen, aus diesen biometrische Templates erzeugen, diese mit dem Referenztemplate vergleichen und die Bilder anschließend wieder löschen. Ein solches Vorgehen wäre zwar theoretisch denkbar, erweise sich jedoch als praktisch nicht durchführbar. Angesichts der Größe und Dynamik des gesamten Internets wäre der erforderliche Zeitaufwand so hoch, dass Ergebnisse erst nach Monaten oder Jahren vorlägen. Zudem würde sich der zugrunde liegende Datenbestand währenddessen so stark verändern oder aktualisieren, dass der Suchprozess faktisch nie abgeschlossen werden könnte. Hinzu kommen erhebliche technische Belastungen der abgefragten Server sowie die hohe Wahrscheinlichkeit, dass ein derartiges Crawling durch Serveranbieter unterbunden werden würde.

Als Variante dieser Live-Suche wird das sogenannte Focused Crawling betrachtet, bei dem das Crawling auf bestimmte Websites oder Themenbereiche beschränkt wird. Zwar reduziert eine solche Einschränkung den Umfang der zu verarbeitenden Daten, sie geht jedoch zwangsläufig mit einer deutlichen Verschlechterung der Ergebnisqualität einher. Selbst einzelne relevante Plattformen enthalten Milliarden von Bildern, sodass auch unter diesen Bedingungen keine praktikable Lösung entsteht.

Ein weiterer theoretischer Ansatz ist der Zugriff über Programmierschnittstellen (APIs) einzelner Anbieter. Auch dieser Ansatz scheitert nach Auffassung des Gutachtens an praktischen Beschränkungen. APIs stehen nur für wenige Plattformen zur Verfügung, unterliegen strikten Nutzungs- und Zugriffsbeschränkungen und erlauben keinen umfassenden Zugriff auf den gesamten Bildbestand des Internets. Selbst unter idealisierten Annahmen bliebe der Abgleich stets auf einzelne Anbieter begrenzt und würde damit das Ziel eines umfassenden Abgleichs verfehlen.

Schließlich wird das Scraping bestehender Bildersuchmaschinen diskutiert. Dabei würde eine automatisierte Nutzung von Bildersuchdiensten erfolgen, um von deren bereits aufgebautem Datenbestand zu profitieren, ohne selbst eine Datenbank anzulegen. Das Gutachten zeigt jedoch, dass die hierfür notwendigen Suchanfragen – ob textbasiert, bildbasiert oder in Kombination – keine hinreichend zuverlässige Vorauswahl relevanter Bilder ermöglichen. Die Treffer beruhen

entweder auf trivialen textuellen Übereinstimmungen oder auf oberflächlichen visuellen Ähnlichkeiten, die für einen biometrischen Abgleich ungeeignet sind. Auch bei einer großen Zahl abgefragter Ergebnisse bleibe die Erfolgswahrscheinlichkeit verschwindend gering.

#### 2.1.4. Technisches Gesamtergebnis

Auf Basis dieser Analyse kommt das Gutachten zu folgendem Ergebnis: Bilder aus dem Internet lassen sich ohne die Erstellung einer Datenbank nicht sinnvoll und praktikabel durchsuchbar machen. Alle untersuchten theoretischen Ansätze erweisen sich laut Gutachten in der praktischen Umsetzung entweder als technisch ungeeignet oder als nicht realisierbar. Ein automatisierter biometrischer Abgleich mit öffentlich zugänglichen Bildern setzt demnach zwingend den Aufbau einer Datenbasis voraus, die eine strukturierte Vorverarbeitung und effiziente Suche ermöglicht. Ohne eine solche Datenbasis ist ein systematischer und zuverlässiger biometrischer Abgleich technisch nicht möglich.

### 2.2. Einordnung durch weitere Expertinnen und Experten

#### 2.2.1. Übereinstimmung in allen wesentlichen Punkten

Im Folgenden wurden weitere Experteneinschätzungen in Bezug auf die Leitfrage eingeholt.[14] Über alle Einschätzungen hinweg besteht ein klarer Konsens, dass ein automatisierter biometrischer Abgleich frei zugänglicher Web-Bilder ohne eine Form persistenter Datenhaltung praktisch derzeit unter den getroffenen Annahmen nicht realisierbar sei.

Besonders hervorgehoben wird in diesem Zusammenhang die technische Notwendigkeit eines Indexes. Für jede Form einer effizienten Suche sei eine Vorverarbeitung der Daten erforderlich, die Suchanfragen gegen strukturierte Repräsentationen erlaubt. Ohne diese Vorverarbeitung müsste bei jeder Anfrage der gesamte relevante Datenbestand erneut analysiert werden, was technisch nicht praktikabel ist. Es wird daher übereinstimmend festgestellt, dass vollständig „on-the-fly“ arbeitende Verfahren für das gesamte Internet weder skalierbar noch hinreichend präzise umsetzbar sind. Die hierfür erforderlichen Verarbeitungsschritte für ein effizientes Vorgehen – Erfassung, Analyse, Vergleich und Wiederverwendung von Bildinformationen – könnten zu Speicher- und Vorverarbeitungsmechanismen führen, die funktional einer Datenbank entsprächen. Diese Argumentation deckt sich unmittelbar mit dem technischen Gesamtergebnis des vorliegenden Gutachtens.

#### 2.2.2. Vertiefende und ergänzende Punkte der Expertinnen und Experten

Eine inhaltliche Erweiterung gegenüber dem Gutachten besteht in der Diskussion möglicher Umgehungsszenarien.

So wird der im Gutachten zugrunde gelegte Datenbankbegriff zwar von den Experten geteilt, jedoch wird auf implizite Speicherformen hingewiesen, die etwa in Form von Vektorrepräsentationen oder Modellgewichten neuronaler Netze vorliegen und funktional die Rolle einer Datenbasis

---

14 Es wurden drei Expertinnen und Experten von Forschungseinrichtungen und aus dem kommerziellen Bereich um eine fachliche Einschätzung gebeten.

übernehmen könnten. Im klassischen Sinne sind dies jedoch keine persistenten Datenbanken, da sie anders funktionieren.

Darüber hinaus wird auf die Nutzung bestehender Bildsuchdienste, Programmierschnittstellen oder fortgeschrittener Vektorsuchverfahren verwiesen. Konzeptionell ließe sich ein Vorgehen denken, das nicht auf ein ungezieltes Massen-Crawling abzielt, sondern auf einen gezielten, möglicherweise wiederholenden Zugriff auf bestimmte externe Systeme oder verengte Bereiche, um Bilder mit bestimmten biometrischen Mustern zu identifizieren.

In diesem Zusammenhang wird auch eine begriffliche Verschiebung vom „ungezielten Auslesen“ hin zum „gezielten Auslesen“ diskutiert. Technisch setzt ein solches Vorgehen jedoch voraus, dass externe Bilder vektorisiert, mit Referenzdaten verglichen und effizient durchsucht werden können. Der Verzicht auf eine eigene Bilddatenbank führe somit nicht zu einer Aufhebung der technischen Anforderungen. Vielmehr verlagern sich die Speicher- und Indexfunktionen auf andere Systemebenen oder Akteure.

Allerdings wird wiederholend betont, dass diese Ansätze eher theoretischer Natur sind. Selbst bei gezieltem Zugriff bleiben die infrastrukturellen Anforderungen hoch, die Abdeckung begrenzt und die zeitliche Verzögerung erheblich. Die Expertenmeinungen erweitern daher das konzeptionelle Verständnis, stellen jedoch keinen Widerspruch zu den im Gutachten analysierten Verfahren dar.

Ergänzend wird darauf hingewiesen, dass biometrische Verfahren zur Verifikation einer Person auf zwei unterschiedlichen Bildern heute technisch zuverlässig ohne Datenbank im Sinne eines One-to-One-Abgleichs eingesetzt werden können. Diese Feststellung steht jedoch nicht im Widerspruch zu den Kernaussagen des Gutachtens. Sie verdeutlicht vielmehr die technische Abgrenzung zwischen Bildabgleichsszenarien.

### 2.2.3. Synthese

Als Befund lässt sich festhalten, dass ein systematischer biometrischer Abgleich im Sinne eines One-to-Many-Abgleichs ohne eine Form persistenter Datenhaltung derzeit und in naher Zukunft technisch nicht praktikabel sei. Sowohl das Gutachten als auch die herangezogenen Experteneinschätzungen kommen übereinstimmend zu dem Ergebnis, dass eine effiziente, skalierbare und hinreichend präzise Suche nach Personen in großen, offenen Bildbeständen zwingend auf Vorverarbeitung, Indexierung und dauerhaft verfügbare Repräsentationen angewiesen ist.

Ein vollständig „on-the-fly“ arbeitendes System, das bei jeder Anfrage das Internet erneut vollständig erfasst und analysiert, sei angesichts der Datenmengen, der Dynamik des Internets und der erforderlichen Rechenressourcen jedoch technisch heute nicht umsetzbar.

Erweitert wird die Diskussion um den Begriff der Datenbank. Datenbanken sollten nicht auf klassische Bildsammlungen oder deren Zusatzinformationen verengt werden. Rein abstrakt-funktional könnten auch temporäre Speicher, Vektorindizes oder implizite Repräsentationen in KI-Basismodellen die Rolle einer Datenbank erfüllen, sofern sie es ermöglichen, Suchanfragen effizient in einen großen Datenbestand auszuführen.

Die diskutierten theoretischen Umgehungsszenarien, etwa der gezielte Zugriff auf bestehende Bildsuchdienste, APIs oder fokussierte Crawling-Ansätze, ändern an diesem Befund nichts. Zwar lässt sich argumentieren, dass ein gezieltes Auslesen biometrisch relevanter Bilder von einem ungezielten Massencrawling zu unterscheiden ist. Technisch erfordere jedoch auch ein solches Vorgehen die Vektorisierung externer Bilder, deren Vergleich mit Referenzdaten sowie Mechanismen zur effizienten Suche und Wiederverwendung bereits analysierter Informationen. Damit verschiebt sich der Ort der Datenhaltung, ohne dass auf eine datenbankartige Struktur verzichtet werden kann.

Daher bleibt die praktische Leistungsfähigkeit solcher Ansätze begrenzt. Selbst bei einer starken Fokussierung auf einzelne Plattformen oder Anbieter seien die Zeitverzögerungen erheblich, die Abdeckung unvollständig und die Abhängigkeit eines tolerierten Zugriffs auf externe Systeme hoch.

### 2.3. Ergänzende Einordnung zur technischen Betrachtung: Praktikabilität unter Ermittlungsbedingungen

Vom Gutachter und von allen Expertinnen und Experten wurde eine rein technische Einschätzung erbeten. Sie bewerteten die technische Praktikabilität datenbankfreier biometrischer Abgleichsverfahren primär anhand von Kriterien wie Effizienz, Skalierbarkeit, zeitnaher Ergebnisverfügbarkeit und vertretbarem Ressourceneinsatz. Diese Maßstäbe sind für allgemeine Informationssysteme, insbesondere für Suchmaschinen oder kommerzielle Plattformen, sachgerecht und nachvollziehbar. Diese Bewertung basiert jedoch implizit auf einer Nutzungsperspektive, die eher einer Konsumenten- oder Providerlogik entspricht als der operativen Logik strafverfolgungsbehördlicher Ermittlungen, wie sie im Titel des Gutachtens genannt wird.

In Ermittlungszusammenhängen der Polizei kann sich der Maßstab der Praktikabilität und der Effizienz verschieben.[15] Strafverfolgungsbehörden stehen unter hohem Erfolgs- und Zeitdruck, insbesondere in Fällen mit erheblicher Gefahrenlage oder hoher politischer und gesellschaftlicher Relevanz. Gleichzeitig stehen nicht in allen Fällen alternative Ermittlungsansätze zur Verfügung, die schneller, zuverlässiger oder weniger ressourcenintensiv wären. Unter solchen Bedingungen kann auch ein technisch aufwendiges, langsames oder nur partiell wirksames Verfahren als unterstützend betrachtet werden, sofern es einen potenziellen Erkenntnisgewinn verspricht und es keine andere Möglichkeit gibt.

Vor diesem Hintergrund ist Praktikabilität nicht als absolute Eigenschaft eines technischen Systems zu verstehen, sondern als Kompromisslösung der verfügbaren Alternativen, der bereitstellbaren personellen und technischen Ressourcen, der zeitlichen Restriktionen sowie der erwarteten Relevanz möglicher Ergebnisse. Verfahren, die unter allgemeinen Effizienzmaßstäben als nicht praktikabel gelten, können unter Ermittlungsbedingungen dennoch eingesetzt werden.

Hinzu kommt, dass der biometrische Bilderabgleich in Ermittlungsprozessen in der Regel nicht als eigenständiges Suchinstrument eingesetzt wird. Vielmehr ist er häufig ein Teil eines mehrstu-

15 Vgl. *Hofmann*, Effektivität, Effizienz und Pragmatismus: Eine rechtsvergleichende Analyse staatsanwaltlicher Strafverfolgung in den Niederlanden und in Deutschland, in Kriminalpolitische Zeitschrift 1, 2020, S. 38 ff.

figen Ermittlungsprozesses. Zusätzliche Hinweise, wie zeitliche, räumliche, soziale oder kontextuelle Anhaltspunkte, können den Suchraum erheblich verengen. In solchen Konstellationen kann der biometrische Abgleich dazu dienen, bestehende Hypothesen zu verdichten oder einzelne Verdachtsmomente zu überprüfen. Dies ist auch dann möglich, wenn die zugrunde liegenden technischen Verfahren isoliert betrachtet als ineffizient oder unvollständig gelten.

Bei dieser Einordnung handelt es sich jedoch um konzeptionelle Überlegungen. In die vorliegende Stellungnahme wurden keine praktischen Erfahrungen oder Einschätzungen von Expertinnen und Experten aus den Bereichen Sicherheits- oder Strafverfolgungsbehörden einbezogen. Daher können keine Aussagen zur tatsächlichen Einsatzpraxis, zur organisatorischen Umsetzbarkeit oder zur Akzeptanz solcher Verfahren getroffen werden. Der vorgeschlagene Perspektivwechsel dient ausschließlich dazu, die in dieser Arbeit getroffenen technischen Aussagen zu kontextualisieren und nicht den zentralen Befund infrage zu stellen.

## 3. Rechtliche Analyse

Die vorangegangene *technische* Analyse hat gezeigt, dass Bilder aus dem Internet ohne die Erstellung einer Datenbank nicht sinnvoll und praktikabel durchsuchbar gemacht werden können. In der nun folgenden *rechtlichen* Analyse wird geprüft, ob daraus eine Verletzung der KI-VO, insbesondere von Art. 5 Abs. 1 Buchst. e KI-VO, folgt.

Das dem Auftrag zugrunde liegende Gutachten stellt insofern fest:

> „Die KI-Verordnung der EU **verbietet es ausnahmslos**, durch ein anlassloses Scraping von Gesichter-Aufnahmen Datenbanken zur Gesichtserkennung aufzubauen. Insofern würden nationale Gesetzesvorhaben, die einen biometrischen Abgleich mit Bildern aus dem Internet vorsehen, geltendem EU-Recht zuwiderlaufen, falls dieser Abgleich nur mithilfe von Datenbanken stattfinden kann.“[16]

Die Annahme greift – jedenfalls in dieser Pauschalität – zu kurz. Sie bedarf einer differenzierten Betrachtung, die im Folgenden erfolgen soll. Zunächst wird knapp der Regelungsgehalt des Sicherheitspakets dargestellt (Ziff. 3.1). Sodann wird untersucht, ob der Anwendungsbereich der KI-Verordnung eröffnet ist (Ziff. 3.2). Im Zentrum der rechtlichen Analyse steht die Frage, ob der biometrische Abgleich mit im Internet verfügbaren Bildern als verbotene Praxis im Sinne des Art. 5 Abs. 1 Buchst. e KI-VO einzuordnen ist (Ziff. 3.3). Schließlich werden knapp die Anforderungen an Hochrisiko-KI-Systeme, insbesondere jene zur nachträglichen biometrischen Fernidentifizierung dargestellt (Ziff. 3.4).

16 *Lewandowski*, Braucht die Polizei eine Datenbank zum biometrischen Abgleich? Das Durchsuchen von Internetbildern zur Gesichtserkennung, Technisches Gutachten im Auftrag von AlgorithmWatch, September 2025, S. 3.

### 3.1. Sicherheitspaket zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit

Das Sicherheitspaket „zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit“[17] befindet sich im Entwurfsstadium. Es besteht aus **zwei Referentenentwürfen** des Bundesinnenministeriums vom 26. Juni 2025, die derzeit zwischen den Ministerien abgestimmt werden. Hintergrund der Aufteilung in zwei Gesetze ist die Zustimmungspflicht des Bundesrates für bestimmte Regelungsbereiche: Das erste Gesetz enthält die zustimmungsfreien Bestandteile des Pakets, für das zweite Gesetz ist die Zustimmung des Bundesrates notwendig.

Durch das Sicherheitspaket sollen vier Gesetze um **neue digitale Ermittlungsbefugnisse** ergänzt werden, namentlich das Bundeskriminalamtgesetz (BKAG), das Bundespolizeigesetz (BPolG), die Strafprozessordnung (StPO)[18] und das Asylgesetz (AsylG). Künftig sollen Strafverfolgungsbehörden unter bestimmten Voraussetzungen Daten „mit öffentlich zugänglichen personenbezogenen Daten aus dem Internet mittels einer automatisierten Anwendung zur Datenverarbeitung biometrisch abgleichen“ können. Die Behörde soll so in die Lage versetzt werden, Personen zu „identifizieren, lokalisieren sowie Tat-Täter Zusammenhänge zu erschließen“. Beispielsweise erlaubt es die Befugnisnorm, ein aufgenommenes Foto einer gesuchten Person mit beliebigen Fotos aus dem Internet abzugleichen, um diese Person aufzufinden. Dabei ist ein Echtzeitabgleich explizit ausgeschlossen – die neue Befugnis bezieht sich also nur auf den *nachträglichen* Abgleich.[19]

Die wesentliche Änderung ist die Referenzdatenbank: Bislang beschränkt sich der Abgleich auf Lichtbilder, die in der polizeiinternen Datenbank INPOL gespeichert sind.[20] Künftig soll ein Abgleich mit allen öffentlich zugänglichen personenbezogenen Daten im Internet möglich sein, was die Reichweite der Ermittlungen enorm erweitert.

### 3.2. Anwendungsbereich (Art. 2 KI-VO)

Zunächst ist zu klären, ob der Anwendungsbereich der KI-VO überhaupt eröffnet ist.

---

17 Entwürfe eines ersten und zweiten Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit 26. Juni 2025, veröffentlicht durch Netzpolitik.org am 23. Juli 2025.

18 Die vorgesehenen Änderungen der Strafprozessordnung sind in der veröffentlichten Version der Gesetzentwürfe nicht abgebildet.

19 Die KI-VO differenziert zwischen der Fernidentifizierung in **Echtzeit** (Art. 3 Nr. 42 KI-VO) und der **nachträglichen** Fernidentifizierung (Art. 3 Nr. 43 KI-VO), auch: asynchrone oder retrograde Fernidentifizierung. Entscheidend ist, ob die biometrischen Informationen sofort oder erst zeitversetzt mit einer Referenzdatenbank verglichen werden. Erfolgt der Abgleich ohne nennenswerte Verzögerung, handelt es sich um eine Echtzeit-Fernidentifizierung. Wird der Abgleich hingegen erst nachgelagert durchgeführt, also nachdem zwischenzeitlich eine Unterbrechung eingetreten ist, spricht man von einer nachträglichen Fernidentifizierung, vgl. *Coombe*, Die Fehlbewertung der nachträglichen biometrischen Fernidentifizierung in der KI-VO, GSZ 2024, 262 (263 f.).

20 Zur Funktionsweise von INPOL siehe näher: *Ogorek*, Staatliche Gesichtserkennung durch biometrischen Abgleich mit Online-Daten, LTZ 2024, 274 (274 f.).

### 3.2.1. Anbieter oder Betreiber von KI-Systemen (Art. 2 Abs. 1 KI-VO)

Gemäß Art. 2 Abs. 1 Buchst. a und b KI-VO gilt die Verordnung für Anbieter und Betreiber von KI-Systemen.

**Anbieter** ist gemäß Art. 3 Nr. 3 KI-VO jede „natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich“. **Betreiber** ist gemäß Art. 3 Nr. 4 KI-VO jede „natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet“.

Dabei ist zu beachten, dass der KI-VO ein horizontaler Regelungsansatz zugrunde liegt, weshalb sich die Regelungen gleichermaßen auf private und staatliche Akteure beziehen.[21] **Behörden** können also sowohl Anbieter i. S. v. Art. 3 Nr. 3 KI-VO als auch Betreiber i. S. v. Art. 3 Nr. 4 KI-VO von KI-Systemen sein und fallen damit grundsätzlich in den Anwendungsbereich der KI-VO.[22]

Der Entwurf des Sicherheitspakets betont, dass in der Gefahrenabwehr und der Strafverfolgung künftig neue technologische Instrumente – „auch Künstliche Intelligenz“ – zum Einsatz kommen soll. Je nachdem, ob die einzusetzenden KI-Systeme von der Behörde selbst entwickelt oder von externen Dritten eingekauft werden sollen, kann es sich also bei den Gefahrenabwehr- und Strafverfolgungsbehörden also um Anbieter oder Betreiber von KI-Systemen handeln, die grundsätzlich dem Anwendungsbereich der KI-VO unterfallen.

### 3.2.2. Ausnahme für nationale Sicherheit (Art. 2 Abs. 3 KI-VO)

Allerdings normiert Art. 2 Abs. 3 UAbs. 2 KI-VO folgende Ausnahme vom Anwendungsbereich der KI-VO:

> „Diese Verordnung gilt nicht für KI-Systeme, wenn und soweit sie **ausschließlich** für militärische Zwecke, Verteidigungszwecke oder Zwecke der **nationalen Sicherheit** in Verkehr gebracht, in Betrieb genommen oder, mit oder ohne Änderungen, verwendet werden, unabhängig von der Art der Einrichtung, die diese Tätigkeiten ausübt.“

Die Ausnahme soll sicherstellen, dass die Mitgliedstaaten ihre Verteidigungsfähigkeit und Sicherheit wahren können. In militärischen Konflikten, bei hybriden Bedrohungen oder in der nachrichtendienstlichen Aufklärung lassen sich die Vorgaben der KI-Verordnung oft nicht praktisch umsetzen. Außerdem könnten die vorgeschriebenen Transparenzpflichten den verteidigungspolitischen Interessen widersprechen. Zudem soll – auch in systematischer Zusammenschau mit UAbs. 1 – die **Regelungszuständigkeit der Mitgliedstaaten** für die nationale Sicherheit

---

21 *Guckelberger*, Hochrisiko-KI-Systeme in der Verwaltung, DÖV 2025, S. 45 (46).

22 Für eine vertiefte Behandlung der rechtlichen Vorgaben der KI-VO für Behörden siehe Deutscher Bundestag, Fachbereich Europa, Infobrief, Zu rechtlichen Vorgaben der Verordnung über Künstliche Intelligenz für den Einsatz von KI in Behörden der EU-Mitgliedstaaten, EU 6 - 3010 - 032/25 vom 7. Juli 2025.

gewahrt bleiben. Erwägungsgrund (ErwG) 24 S. 3 KI-VO verweist insoweit ausdrücklich auf Art. 4 Abs. 2 S. 3 EUV, der die nationale Sicherheit den Mitgliedstaaten vorbehält. [23]

Zur Auslegung des Begriffs der nationalen Sicherheit in Art. 2 Abs. 3 UAbs. 2 KI-VO ist bislang noch keine unionsgerichtliche Rechtsprechung ergangen. Der Begriff taucht aber auch in anderen Unionsrechtsakten auf, etwa in Art. 4 Abs. 2 S. 3 EUV, mittelbar auch in Art. 2 Abs. 2 Buchst. a DSGVO. Auf die dazu ergangene Rechtsprechung des Europäischen Gerichtshofs (EuGH) kann für die Auslegung zurückgegriffen werden.

Nach der inzwischen gefestigten Rechtsprechung des EuGH ist die Ausnahme der nationalen Sicherheit **eng auszulegen**.[24] Sie beinhaltet im Wesentlichen die Abwehr äußerer Angriffe und innerer Attacken auf die staatliche Ordnung. Die nationale Sicherheit bezieht sich auf das Anliegen, „die wesentlichen Funktionen des Staates und die grundlegenden Interessen der Gesellschaft zu schützen, und umfasst die Verhütung und Repression von Tätigkeiten, die geeignet sind, die tragenden Strukturen eines Landes im Bereich der Verfassung, Politik oder Wirtschaft oder im sozialen Bereich in schwerwiegender Weise zu destabilisieren und insbesondere die Gesellschaft, die Bevölkerung oder den Staat als solchen unmittelbar zu bedrohen, wie insbesondere terroristische Aktivitäten.“[25]

Die Abwehr von Terrorismus würde demnach in den Bereich der nationalen Sicherheit fallen. Wird eine Technologie also *ausschließlich* zur Bekämpfung von Terrorismus[26] eingesetzt, ist die Anwendung der KI-VO nach Art. 2 Abs. 3 UAbs. 2 KI-VO gesperrt. Allerdings betont ErwG 24 S. 4 KI-VO, dass der Anwendungsbereich der KI-VO wiederum eröffnet bleibt, solange die Technologie vorübergehend oder ständig für andere Zwecke, etwa „für Zwecke der Strafverfolgung oder öffentlichen Sicherheit“, eingesetzt wird. Daraus ergibt sich im Gegenschluss, dass die bloße Strafverfolgung und öffentliche Sicherheit gerade nicht zur nationalen Sicherheit zählen und damit in den Anwendungsbereich der KI-VO fallen.[27] Insofern übersteigt eine Bedrohung für die nationale Sicherheit in ihrer Art und Schwere sowie der sie begründenden besonderen Umstände die Gefahr, welche von Störungen der öffentlichen Sicherheit oder schweren Straftaten ausgehen kann.[28]

Die Zielsetzung der neuen Befugnis zum biometrischen Abgleich ist nicht eindeutig: Die Referentenentwürfe nehmen durchaus Bezug auf „eine hohe abstrakte Bedrohungslage für die Sicherheit

---

23 *Wendehorst*, in: Martini/Wendehorst, KI-VO, 2. Aufl. 2026, Art. 2 Rn. 58 f.

24 *Wendehorst*, in: Martini/Wendehorst, KI-VO, 2. Aufl. 2026, Art. 2 Rn. 66.

25 EuGH, Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u.a., Rn. 135 ; Urteil vom 21. Juni 2022, Ligue des droits humains gegen Conseil des ministres, C-817/19, Rn. 170 ; *Wendehorst*, in: Martini/Wendehorst, KI-VO, 2. Aufl. 2026, Art. 2 Rn. 65.

26 Zur grundsätzlichen Schwierigkeit, den Begriff „Terrorismus“ zu definieren, siehe *Greene*, Defining Terrorism: One Size fits all?, ICLQ vol. 66, April 2017. S. 411.

27 Vgl. EuGH, Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 62 f.

28 EuGH, Urteil vom 5. April 2022, Rs. C-140/20, Commissioner of An Garda Síochána, Rn. 62; Urteil vom 6. Oktober 2020, verb. Rs. C-511/18, C-512/18 und C-520/18, La Quadrature du Net u.a., Rn. 136.

in Deutschland – auch durch den internationalen Terrorismus“. Die Rede ist aber auch von einer „Bedrohung durch terroristische und kriminelle Strukturen“ sowie von der Notwendigkeit des Einsatzes von KI „in der Gefahrenabwehr und der Strafverfolgung“. Dabei geht es nicht nur um die Ermittlung von Tatverdächtigen, sondern auch um die Identifizierung und Aufenthaltsermittlung anderer Personen, „beispielsweise von Kontaktpersonen, Opfern und Zeugen“. Mehr noch: Auch die Bilder von Asylsuchenden, die keinerlei Bezug zu einer Straftat aufweisen, sollen „zur Feststellung der Identität oder Staatsangehörigkeit“ abgeglichen werden dürfen.

Daraus muss geschlossen werden, dass die neue Befugnis nicht *nur* zur Bekämpfung von Terrorismus gelten soll, sondern dass es um eine **breite Ermächtigung** für verschiedene Tätigkeiten geht, die in den Aufgabenbereich der jeweiligen Behörde fallen.[29] Damit ist die Ausnahme der nationalen Sicherheit jedenfalls insoweit nicht einschlägig und der Anwendungsbereich der KI-VO eröffnet.

### 3.3. Verbotene Praktiken (Art. 5 Abs. 1 Buchst. e KI-VO)

Die KI-VO enthält in Art. 5 KI-VO einen Katalog mit verbotenen Praktiken. Bei dem im Sicherheitspaket vorgesehenen biometrischen Abgleich mit öffentlich zugänglichen personenbezogenen Daten könnte es sich um eine verbotene Praktik i. S. d. Art. 5 Abs. 1 Buchst. e KI-VO handeln. Verboten ist danach

> „das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von **KI-Systemen**, die **Datenbanken zur Gesichtserkennung** durch das **ungezielte Auslesen** von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen **erstellen** oder erweitern“.

Der Zweck dieses Verbots besteht ausweislich ErwG 43 darin, das ungezielte Auslesen von Gesichtsbildern mittels KI zu verhindern, da es die Privatsphäre und den Datenschutz der Betroffenen erheblich beeinträchtigt und das Gefühl ständiger Überwachung erzeugt. Zudem wird das Verbot mit der Gefahr schwerer Grundrechtsverletzungen, insbesondere des Rechts auf Privatsphäre, begründet.[30]

Damit das Verbot gilt, müssen mehrere kumulative Bedingungen erfüllt sein, namentlich das Erstellen oder Erweitern einer Datenbank zur Gesichtserkennung (Ziff. 3.3.1), das ungezielte Auslesen von Gesichtsbildern aus dem Internet (Ziff. 3.3.2) und nicht zuletzt der Einsatz eines KI-Systems zu diesem Zweck (Ziff. 3.3.3).

---

29 Der Offene Brief an Bundeskanzler Merz, Vizekanzler Klingbeil, Bundesminister Dobrindt und Bundesministerin Hubig vom 8. August 2025 spicht insofern sogar von einer „Standardmaßnahme“.

30 KOM, Leitlinien zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689, Rn. 223.

#### 3.3.1. Erstellen oder Erweitern einer Datenbank zur Gesichtserkennung

Art. 5 Abs. 1 Buchst. e KI-VO setzt zunächst voraus, dass eine „**Datenbank zur Gesichtserkennung**“ erstellt oder erweitert wird. Dieses Tatbestandsmerkmal wird in den Leitlinien der Europäischen Kommission (KOM) zu verbotenen Praktiken wie folgt definiert:

> „Unter ‚Datenbank‘ ist in diesem Zusammenhang jede Sammlung von Daten oder Informationen zu verstehen, die speziell für eine schnelle Suche und Abfrage durch einen Computer aufgebaut ist. Eine Datenbank zur Gesichtserkennung ist in der Lage, ein menschliches Gesicht von einem digitalen Bild oder einer Videoaufnahme mit einer Datenbank für Gesichter abzugleichen, es mit Bildern in der Datenbank zu vergleichen und festzustellen, ob zwischen beiden Gesichtern eine Übereinstimmung wahrscheinlich ist. Eine solche Datenbank zur Gesichtserkennung kann temporär, zentral oder dezentral sein.“[31]

Daraus folgt, dass die Datenbank „zur Gesichtserkennung“ erstellt werden, also dem Zweck der Identifizierung von Personen dienen muss.[32] Dafür sollte sie eine Mindestanzahl an Profilen und biometrische Daten i. S. d. Art. 3 Nr. 34 KI-VO enthalten.[33] Diese Daten müssen für eine biometrische Identifizierung oder Verifizierung geeignet sein, also ein gewisses Maß an **Vorverarbeitung** erreichen. Eine bloße Sammlung von Fotografien ist dagegen nicht ausreichend.[34]

Für die Anwendung dieser Maßstäbe auf den biometrischen Abgleich mit Bildern aus dem Internet kann auf die vorstehende technische Analyse verwiesen werden. Sie kommt in Ziff. 2.2.3 zu dem Ergebnis, dass ein automatisierter biometrischer Abgleich mit öffentlich zugänglichen Bildern – wie ihn das Sicherheitspaket vorsieht – zwingend den Aufbau einer Datenbank voraussetzt, die eine strukturierte Vorverarbeitung und effiziente Suche ermöglicht. Ein systematischer biometrischer Abgleich im Sinne eines One-to-Many-Abgleichs ohne eine Form persistenter Datenhaltung sei dagegen derzeit und in naher Zukunft technisch nicht praktikabel. Ein vollständig „on-the-fly“ arbeitendes System, das bei jeder Anfrage das Internet erneut vollständig erfasst und analysiert, sei angesichts der Datenmengen, der Dynamik des Internets und der erforderlichen Rechenressourcen heute technisch nicht umsetzbar. Vor diesem Hintergrund ist davon auszugehen, dass das Sicherheitspaket das Tatbestandsmerkmal des Erstellens bzw. Erweiterns einer Datenbank zur Gesichtserkennung erfüllen würde.

#### 3.3.2. Durch ungezieltes Auslesen von Gesichtsbildern aus dem Internet

Art. 5 Abs. 1 Buchst. e KI-VO setzt weiter voraus, dass die Datenbanken „durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet“ erstellt oder erweitert werden.

---

31 KOM, Leitlinien zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689, Rn. 226.

32 Vgl. *Böning/Schindler*, in: Geminn/Johannes, Europäisches Datenrecht, 1. Aufl. 2026, § 28 Rn. 72.

33 *Wendehorst*, in: Martini/Wendehorst, KI-VO, 2. Aufl. 2026, Art. 5 Rn. 146.

34 *Wendehorst*, in: Martini/Wendehorst, KI-VO, 2. Aufl. 2026, Art. 5 Rn. 148.

Das Merkmal „**Gesichtsbilder**“ stellt klar, dass das Verbot aus Art. 5 Abs. 1 Buchst. e KI-VO nur für Gesichtsbilder und nicht für andere biometrische Daten, etwa Proben menschlicher Stimmen, gilt.[35]

„**Auslesen**“ meint die Verwendung bestimmter Software zur automatischen Extrahierung von Daten oder Inhalten aus verschiedenen Quellen, insbesondere Websites oder sozialen Medien.[36]

Dieses Auslesen muss „**ungezielt**“ erfolgen. Das ist dann der Fall, wenn kein Bezug zu einem speziellen Anlass – etwa der Aufklärung einer Straftat – vorliegt, sondern einzelne Profile ausschließlich zu dem Zweck ausgelesen werden, der Datenbank weitere Profile hinzuzufügen.[37] Wie eng dieses Merkmal auszulegen ist, ist umstritten. Laut den Leitlinien der KOM bezieht sich „ungezielt“ auf

> „eine Technik, die wie ein „Staubsauger“ funktioniert und so viele Daten und Informationen wie möglich aufnimmt, ohne auf speziell und individuell bestimmte Subjekte für das Auslesen abzuzielen. Durch das Auslesen werden Daten oder Inhalte wahllos „geerntet“. Somit bedeutet der Begriff „ungezielt“, dass kein besonderer Schwerpunkt auf bestimmte Einzelpersonen oder eine bestimmte Gruppe von Einzelpersonen gelegt wird.“[38]

Dementsprechend legt die KOM das Merkmal „ungezielt“ eng und den erforderlichen Anlass weit aus. Die Definition der Leitlinien legt es nahe, nur dann von ungezielt zu sprechen, wenn unterschiedslos alle im Internet aufzufindenden Personen gesammelt werden. Sobald das Auslesen auf eine vordefinierte Gruppe von Personen beschränkt wird, geht die KOM von einem gezielten Auslesen aus, das nicht unter das Verbot fällt.[39] Zugleich weist sie auf die Gefahr hin, dass das Verbot – wohl durch zu weite Eingrenzungen einer Gruppe – umgangen werden könnte.[40] Aus diesem Grund wird im Schrifttum vertreten, dass das Auslesen einer Gruppe von Personen durchaus ungezielt sein könne, wenn die betroffene Personengruppe so groß und unspezifisch ist.[41]

---

35 KOM, Leitlinien zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689, Rn. 234.

36 Dabei ist in dem Einstellen von eigenen Bildern auf eine Social Media Plattform **keine Einwilligung** in die Aufnahme dieser Bilder in eine Gesichtserkennungsdatenbank zu sehen, siehe KOM, Leitlinien zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689, Rn. 227, 232.

37 Hilgendorf/Härtlein, KI-VO, 1. Aufl. 2025, Art. 5 KI-VO, Rn. 47.

38 KOM, Leitlinien zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689, Rn. 228.

39 KOM, Leitlinien zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689, Rn. 229 f.

40 KOM, Leitlinien zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689, Rn. 230.

41 *Wendehorst*, in: Martini/Wendehorst, KI-VO, 2. Aufl. 2026, Art. 5 Rn. 150.

Bezogen auf das Sicherheitspaket ist zu klären, ob das für einen biometrischen Abgleich erforderliche Auslesen von Bildern aus dem Internet ungezielt erfolgt, also einen hinreichenden Anlass hat. Dem Wortlaut der entsprechenden Normen (bspw. § 10b BKAG) zufolge steht der Abgleich unter strengen Voraussetzungen, insbesondere dem auf Tatsachen begründetem Verdacht einer konkreten Straftat. Diese Voraussetzungen betreffen aber nur den *Abgleich* mit Daten aus der Datenbank. Wie das technische Gutachten gezeigt hat, ist diesem Abgleich aber notwendigerweise das *Erstellen* einer Datenbank durch Auslesen von Bildern aus dem Internet vorgeschaltet.

Hier kommt es auf die konkrete Ausgestaltung des Erstellens der Datenbank an: Würde die Datenbank – mit den Worten der KOM – „wie ein Staubsauger", also ungefiltert, befüllt, dann läge es nahe, dass dem anlassbezogenen Abgleich ein „ungezieltes" Auslesen vorgeschaltet wäre. Würde dagegen für jeden Straftatverdacht eine neue, spezifische Datenbank erstellt, die auf eine bestimmte Personengruppe zugeschnitten ist, wäre das Auslesen als gezielt anzusehen und fiele damit nicht unter Art. 5 Abs. 1 Buchst. e KI-VO.[42]

### 3.3.3. Einsatz eines KI-Systems

Schließlich kommt es darauf an, dass ein KI-System zum Einsatz kommt. Denn gemäß Art. 5 Abs. 1 Buchst. e KI-VO ist nur das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von **KI-Systemen** verboten, die Datenbanken durch Auslesen von Gesichtsbildern aus dem Internet erstellen oder erweitern. Das Verbot also greift nur dann, wenn die in Rede stehenden Datenbanken auch mit KI-Systemen erstellt werden. Umgekehrt gilt das Verbot nicht, wenn an der Auslesung keine KI-Systeme beteiligt sind.[43]

Dies entspricht nicht nur dem klaren Wortlaut der Verordnung, sondern auch ihrem Sinn und Zweck: Wie der Name der Verordnung bereits nahelegt, reguliert die KI-VO den Einsatz von KI-Systemen. Ohne den Einsatz eines KI-Systems kann daher kein Verbot gemäß dieser Verordnung greifen. Für die Beurteilung von Art. 5 Abs. 1 Buchst. e KI-VO ist es deshalb nicht nur maßgeblich, ob überhaupt Datenbanken erforderlich sind, sondern vor allem, ob diese Datenbanken mittels KI-Systemen aufgebaut werden.

Nach Art. 3 Nr. 1 KI-VO handelt es sich bei einem **KI-System** um ein „maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb angelegt ist, nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben Ausgaben für explizite oder implizite Ziele ableitet, wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen, die physische oder virtuelle Umgebungen beeinflussen können". Diese Merkmale dienen gemäß ErwG 12 S. 2 KI-VO der Abgrenzung zu herkömmlichen Softwaresystemen und Programmierungsansätzen. Systeme, die auf ausschließlich von natürlichen Personen definierten

---

42 Ob dieser gezielte Ansatz für Sicherheitsbehörden praktikabel ist, erscheint indes zweifelhaft, vgl. Ziff. 2.2.3 und Ziff. 2.3). Das einzelfallbezogene Erstellen von Datenbanken würde einen erheblichen Zusatzaufwand bedeuten und zu Verzögerungen führen. Zudem liefe es möglicherweise dem Sinn und Zweck des Sicherheitspakts zuwider, die Ermittlungserfolge gerade durch eine Ausweitung des Ermittlungsradius auf eine große Zahl von Personen zu verbessern.

43 KOM, Leitlinien zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689, Rn. 234.

Regeln für das automatische Ausführen von Operationen beruhen, sind nach ErwG 12 S. 2 KI-VO keine KI-Systeme.[44]

Bit Blick auf diese Definition stellt sich also die Kernfrage, ob – und wenn ja, wann – bei dem biometrischen Abgleich mit Bildern aus dem Internet KI ins Spiel kommt.

Die technischen Gutachten sind insoweit offen. Auch aus den Gesetzesentwürfen ergibt sich kein klarer Befund. Von KI ist nur in den allgemeinen Ausführungen zur Problemstellung, Zielsetzung und Begründung die Rede, nicht aber im Gesetzeswortlaut selbst. Die Bezugnahmen lauten wie folgt:

> „Die Bedrohung durch terroristische und kriminelle Strukturen erfordert den Einsatz technologischer Instrumente – **auch Künstlicher Intelligenz** – in der Gefahrenabwehr und der Strafverfolgung“;
>
> „IT-Produkte sind elementarer Bestandteil einer modernen polizeilichen Arbeit. Der Gesetzentwurf enthält eine Befugnis für das Testen und Trainieren von IT-Produkten. Dies umfasst auch **selbstlernende Systeme**.“[45]

Die Referentenentwürfe bekräftigen, dass KI grundsätzlich zum Einsatz kommen soll. Ob sie aber speziell für das Auslesen von Bildern aus dem Internet eingesetzt werden soll, ist unklar. In den konkreten Befugnisnormen für den biometrischen Abgleich mit Bildern aus dem Internet ist lediglich von einer „automatisierten Anwendung zur Datenverarbeitung“ die Rede. Eine automatisierte Anwendung muss aber nicht notwendigerweise KI beinhalten. Der Begriff „automatisiert“ bezieht sich allgemein auf Prozesse, die ohne menschliche Eingriffe ablaufen, was sowohl mit als auch ohne den Einsatz von KI möglich ist.

Insbesondere können Datenbanken von Bildern aus dem Internet auch ohne KI erstellt werden. Das Erstellen solcher Datenbanken erfordert nicht zwangsläufig den Einsatz von KI. So können Web-Scraping-Techniken verwendet werden, um Bilder automatisch von Websites zu extrahieren. Dabei werden standardisierte Methoden zum Herunterladen von Bildern aus dem Internet eingesetzt, ohne dass KI eingesetzt wird. Die Bilder werden dann in einer Datenbank gespeichert, oft mit den zugehörigen Metadaten, die ebenfalls automatisch erfasst werden (z.B. Bildgröße, URL, Dateiname).

KI *kann* relevant werden, wenn es darum geht, die Inhalte der Bilder zu analysieren und zu kategorisieren. In diesem Fall würde man auf Bildklassifikation, Objekterkennung oder Texterkennung zurückgreifen, die durch maschinelles Lernen realisiert werden. Beispielsweise könnte ein KI-Algorithmus in der Lage sein, automatisch Bilder zu kategorisieren oder Objekte auf den Bildern zu erkennen. Andererseits kann die für eine Datenbank erforderliche Vorverarbeitung

---

44 Die Kommission hat (nicht rechtsverbindliche) Leitlinien zur Definition von KI-Systemen veröffentlicht, die die einzelnen Begriffsmerkmale der Definition näher erläutern, s. Kommission, Approval of the content of the draft Communication from the Commission - Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), KOM(2025) 924 endg., 6. Februar 2025.

45 Entwürfe eines ersten und zweiten Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit 26. Juni 2025, veröffentlicht durch Netzpolitik.org am 23. Juli 2025.

(siehe Ziff. 2.1.1 und 3.3.1) auch ohne KI stattfinden, etwa um biometrische Daten wie Gesichtserkennungsmerkmale oder Gesichtsmessungen zu extrahieren. Es gibt auch klassische Algorithmen zur Extraktion biometrischer Merkmale aus Gesichtern, die keine KI erfordern.

Der Einsatz von KI ist also **nicht zwingend erforderlich**, um einen biometrischen Abgleich mit Bildern aus dem Internet durchzuführen. Dies bringt *Rückert* wie folgt auf den Punkt:

> „Und auch eine weitere Schutzmaßnahme entfaltet nicht die erhoffte Wirkung: So dürfen Datenbanken zwar nicht durch ungezieltes Auslesen von Gesichtsbildern aus dem Internet oder Überwachungskameras erstellt oder erweitert werden. Aber eben nur, wenn es sich dabei um KI handelt, die Software also anpassungsfähig sein kann. Tatsächlich werden derartige Datenbanken durch sogenannte Crawler aufgebaut, die automatisiert das öffentlich zugängliche Internet nach Bildern durchsuchen. Dafür braucht es aber gerade keine KI. Vielmehr kann diese Leistung auch durch ‚klassische' Programme erreicht werden, welche dann nicht unter das Verbot fallen."[46]

Festzuhalten bleibt: Für den Verbotstatbestand aus Art. 5 Abs. 1 Buchst. e KI-VO kommt es auf die konkrete Ausgestaltung und technische Umsetzung des in den Gesetzesentwürfen vorgesehenen biometrischen Abgleichs an. Sollte der biometrische Abgleich mit einem KI-gestützten Verfahren erfolgten, spricht vieles dafür, dass das Verbot aus Art. 5 Abs. 1 Buchst. e KI-VO greift. Sollte hingegen auf eine klassische Software zurückgegriffen werden, steht dem jedenfalls die KI-VO nicht entgegen.

### 3.4. Hochrisiko-KI-Systeme (Art. 6 Abs. 2, 26 Abs. 10 KI-VO)

Sollte das Verbot aus Art. 5 Abs. 1 Buchst. e KI-VO als nicht einschlägig erachtet werden, greifen subsidiär die Regelungen zur Hochrisiko-KI-Systemen (HRKS).

Sofern dabei KI zum Einsatz kommt, ist der biometrische Abgleich mit Bildern aus dem Internet als Hochrisiko-KI-System einzuordnen. Dies ergibt sich aus Art. 6 Abs. 2 KI-VO i. V. m. Anhang III Nr. 1, der KI-Systeme zur biometrischen Fernidentifizierung und biometrischen Kategorisierung zu HRKS erklärt und Nr. 6, wonach KI-Anwendungsfälle in der Strafverfolgung, die in die Grundrechte der Menschen eingreifen können, als HRKS einzustufen sind. Daraus folgen umfassende Anbieter- und Betreiberpflichten, die sich im Einzelnen aus Kapitel 5 der KI-VO ergeben.[47]

Spezielle Pflichten ergeben sich hier aus Art. 26 Abs. 10 KI-VO, der für Betreiber eines **Hochrisiko-KI-Systems zur nachträglichen biometrischen Fernidentifizierung** gilt. Die Vorschrift soll sicherstellen, dass die Nutzung von KI-Systemen zur biometrischen Fernidentifizierung streng kontrolliert, dokumentiert und auf das notwendige Maß begrenzt bleibt.

---

46 Vgl. *Rückert*, Gesichtserkennung durch KI im Strafverfahren, Die Technik ist da, das Recht (noch) nicht, Legal Tribune Online vom 25. April 2025.

47 Siehe dazu umfassend: *Guckelberger*, Hochrisiko-KI-Systeme in der Verwaltung, DÖV 2025, S. 45 sowie Deutscher Bundestag, Fachbereich Europa, Infobrief, Zu rechtlichen Vorgaben der Verordnung über Künstliche Intelligenz für den Einsatz von KI in Behörden der EU-Mitgliedstaaten, EU 6 - 3010 - 032/25 vom 7. Juli 2025.

Art. 26 Abs. 10 KI-VO enthält eine Genehmigungspflicht (UAbs. 1) für HRKS zur nachträglichen biometrischen Fernfernidentifizierung. Diese gilt allerdings nicht, wenn das System zur erstmaligen Identifizierung einer Person eingesetzt wird, die einer Straftat verdächtig ist. Bei Ablehnung der Genehmigung muss das System sofort gestoppt und alle mit der Nutzung verbundenen personenbezogenen Daten gelöscht werden. Zudem ist jede Nutzung auf das unbedingt notwendige Maß zu beschränken.

UAbs. 2 soll sicherstellen, dass das System nicht für allgemeine, nicht zielgerichtete Strafverfolgung oder ohne Zusammenhang zu einer Straftat verwendet wird. Ferner dürfen Strafverfolgungsbehörden keine Entscheidungen treffen, die nachteilige rechtliche Folgen für eine Person haben, wenn diese ausschließlich auf den Ergebnissen des KI-Systems zur biometrischen Fernidentifizierung basieren. Schließlich legen UAbs. 3 und 4 Dokumentations-, Informations- und Berichtspflichten fest. Beispielsweise müssen die zuständigen Marktüberwachungsbehörden und Datenschutzbehörden auf Antrag über die Nutzung informiert werden.

An dieser Stelle sei erneut darauf hingewiesen, dass die datenschutzrechtliche Zulässigkeit der Datenverarbeitung auch im Bereich von Art. 26 Abs. 10 KI-VO gesondert zu beurteilen ist. Die Voraussetzungen der KI-VO sind zusätzlich einzuhalten, ersetzen aber nicht die datenschutzrechtliche Prüfung.[48]

### 3.5. Fazit und Ausblick

Abschließend ist festzuhalten, dass es für die rechtliche Beurteilung nach der KI-VO entscheidend auf die **konkrete technische Ausgestaltung** des im Sicherheitspaket vorgesehenen biometrischen Abgleichs mit Bildern aus dem Internet ankommt: Nur wenn für das Auslesen der Bilder aus dem Internet und Erstellen einer Datenbank ein KI-System zum Einsatz kommt, können das Verbot aus Art. 5 Abs. 1 Buchst. e KI-VO und subsidiär die besonderen Pflichten für HRKS aus Art. 6 Abs. 2, 26 Abs. 10 KI-VO greifen. Hinsichtlich der einzusetzenden Technologie für den Abgleich biometrischer Daten sind die Referentenentwürfe aber bislang zu vage, um sie im Detail am Maßstab der KI-VO überprüfen zu können.

Es wird darauf hingewiesen, dass die in der KI-VO vorgesehene Konkretisierung durch Normen europäischer Normungsorganisationen, Durchführungsrechtsakte der KOM, Praxisleitfäden und Leitlinien sowie nationale Rechtsakte nicht abgeschlossen ist. Zudem ist es möglich, dass sich die KI-VO, die sich derzeit in einem Evaluationsprozess befindet, noch einmal ändern könnte.[49] Schließlich liegt, soweit ersichtlich, noch keine Rechtsprechung der Unionsgerichte zur Auslegung und Anwendung der KI-VO vor. Eine abschließende Entscheidung über die Auslegung von Art. 5 Abs. 1 Buchst. e KI-VO obliegt dem EuGH.

---

48 *Eisenberger/Binder*, in: Martini/Wendehorst, KI-VO, 2. Aufl. 2026, Art. 26 Rn 13.

49 Vgl. zu potenziellen Vereinfachungen der Anforderungen: *Gkristsi/Haeck*, EU Commission opens door for 'targeted changes' to AI Act, Politico, 13. Mai 2025; *Kafsack*, EU-Kommission will KI-Gesetz vereinfachen, FAZ, 10. April 2025, S. 16; Kommission, Aktionsplan für den KI-Kontinent – Q&A. Vgl. zudem den Draghi-Report, Teil B, Abschnitt 1, Kapitel 3, S. 79, wonach die Komplexität und das Risiko von Unstimmigkeiten zwischen der KI-VO und der DSGVO die KI-Entwicklung durch europäische Akteure untergraben könne.

Fachbereich Europa