Checkliste

Verbotene Praktik Nr. 8
Biometrische Echtzeit-Fernidentifizierung
i.S.d. Art 5 Abs. 1 h.) KI-VO, ErwGr 32, 33

Praktische Relevanz	● ● ● ● ●
Technische Relevanz	● ● ○ ○ ○
Rechtliche Relevanz	● ● ● ● ●
Orga.Relevanz	● ○ ○ ○ ○

Verortung im Prüfungsschema

I. Bereichsausnahmen
II. Anwendungsbereiche
III. Risikoeinordnung
- a. Risikoeinordnung – Verbotene Praktiken gem. Art. 1 Abs. 2 b.) i.V.m. Art. 5 KI-VO
  - i. Überblick Verbotene KI-Praktiken
  - ii. Verbotene KI-Praktiken im Einzelnen
    1. Unterschwelligen Beeinflussung und Manipulation Art 5 Abs. 1 a.) KI-VO, 29 ErwGr
    2. Ausnutzen von Vulnerabilität und Schutzbedürftigkeit Art. 5 Abs. 1 b.) KI-VO
    3. Soziale Bewertung oder Soziale Einstufung Art 5 Abs. 1 c.) KI-VO ErwGr 31
    4. Prädiktive Polizeiarbeit Art. 5 Abs. 1 d.) KI-VO
    5. Ungezielte Sammlung von Gesichtsbildern (Scapring) Art. 5 Abs. 1 e.) KI-VO
    6. Emotionserkennung Art. 5 Abs. 1 f.) KI-VO ErwGr 44
    7. Biometrische Kategorisierung Art. 5 Abs. 1 g.) KI-VO
    → **8. Biometrische Echtzeit-Fernidentifizierung Art. 5 Abs. 1 h.) KI-VO**

Beachte hierzu auch:

Orientierungshilfe Verbotene KI-Praktiken Überblick (Version 1.1.),
Orientierungshilfe Verbotene KI-Praktik Nr. 8 (Version 1.3.), Übersicht Verbotene KI-Praktiken (Version 1.4)

Einleitung

Das Verbot der biometrischen Echtzeit-Fernidentifizierung (Art. 5 Abs. 1 lit. h) geht auf die zunehmende Nutzung biometrischer Technologien zurück, die aufgrund ihrer Eingriffe in die Grundrechte hoch umstritten sind. Ursprünglich eingeführt, um die Grundrechte zu schützen und einer unverhältnismäßigen Überwachung vorzubeugen, adressiert die Verordnung das Risiko der ständigen Überwachung in öffentlich zugänglichen Räumen.

Der Einsatz solcher Systeme birgt erhebliche Gefahren für die Privatsphäre und die Versammlungsfreiheit und könnte diskriminierende Effekte nach sich ziehen, beispielsweise aufgrund von Ungenauigkeiten bei der Identifikation verschiedener Bevölkerungsgruppen. Praktisch bedeutet dies, dass biometrische Echtzeit-Fernidentifizierungssysteme grundsätzlich verboten sind, es sei denn, sie werden zur Rettung von Opfern, zur Abwehr schwerwiegender Gefahren oder zur Identifikation von Straftätern in definierten Ausnahmefällen eingesetzt. Die Verordnung setzt strenge Voraussetzungen wie Genehmigungspflichten, Verhältnismäßigkeitsprüfungen und die Durchführung von Folgenabschätzungen, um die rechtmäßige und kontrollierte Anwendung sicherzustellen.

Warum gibt es die Regelung

Das Verbot zielt darauf ab, die spezifischen Risiken und Missbrauchsmöglichkeiten der biometrischen Echtzeit-Fernidentifizierung einzudämmen. Solche Systeme ermöglichen die Identifizierung von Personen in öffentlich zugänglichen Räumen in Echtzeit, oft ohne ihr Wissen oder ihre Einwilligung. Dies birgt ein hohes Risiko für die Privatsphäre und kann zu einer ständigen Überwachung führen, die das Verhalten von Menschen in der Öffentlichkeit beeinflusst und die Versammlungsfreiheit einschränkt. Das Verbot solcher Systeme basiert auf der Erkenntnis, dass sie ohne enge Einschränkungen unweigerlich zu Diskriminierung und Ungleichbehandlung führen können. Ungenauigkeiten bei der Identifizierung treffen besonders oft ethnische Minderheiten und andere vulnerable Gruppen. Außerdem könnten solche Technologien dazu genutzt werden, Massenüberwachung und nicht autorisierte Überwachung durchzuführen, was den Grundprinzipien der Europäischen Union widerspricht. Die Regelung stellt sicher, dass biometrische Echtzeit-Fernidentifizierung nur in klar definierten Ausnahmefällen wie der Suche nach Entführungsopfern, der Abwendung unmittelbarer Gefahren oder der Identifizierung von schweren Straftätern angewendet werden darf.

Definition

Art. 5 Abs. 1 lit. h.) KI-VO beschreibt die Praktik folgendermaßen:

1. *die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken, außer wenn und insoweit dies im Hinblick auf eines der folgenden Ziele unbedingt erforderlich ist:*

    i. *gezielte Suche nach bestimmten Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung sowie die Suche nach vermissten Personen;*
    ii. *Abwenden einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder einer tatsächlichen und bestehenden oder tatsächlichen und vorhersehbaren Gefahr eines Terroranschlags;*
    iii. *Aufspüren oder Identifizieren einer Person, die der Begehung einer Straftat verdächtigt wird, zum Zwecke der Durchführung von strafrechtlichen Ermittlungen oder von Strafverfahren oder der Vollstreckung einer Strafe für die in **Anhang II** aufgeführten Straftaten, die in dem betreffenden Mitgliedstaat nach dessen Recht mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens vier Jahren bedroht ist.*

*Unterabsatz 1 Buchstabe h gilt unbeschadet des **Artikels 9** der Verordnung (EU) 2016/679 für die Verarbeitung biometrischer Daten zu anderen Zwecken als der Strafverfolgung*

Checkliste Verbotene KI-Praktik Biometrische Echtzeit-Fernidentifizierung i.S.d. Art. 5 Abs. 1 h.) KI-VO, ErwGr 23, 33

Zur besseren Orientierung und für ein formalisiertes Vorgehen wurde die folgende Checkliste entwickelt, um festzustellen, ob eine eine verbotene KI-Praktik nach Art. 5 Abs. 1 h) KI-VO, ErwGr 32, 33.

(1) Objektiver Tatbestand

(a) KI-Technologie

(i) KI-System (Art. 3 Nr. 1 KI-VO)

Prüfen, ob es sich um ein KI-System handelt, das nach Art. 3 Nr. 1 der KI-VO definiert ist.

(ii) Biometrische Fernidentifizierungssysteme (Art. 3 Nr. 41 KI-VO):

Ein biometrisches Fernidentifizierungssystem verarbeitet biometrische Daten wie Gesichtsbilder oder andere körperliche Merkmale, um eine Person zu identifizieren. Es handelt sich um Systeme, die ohne aktive Einbindung der betroffenen Person arbeiten. Abzugrenzen sind Systeme, die biometrische Daten lediglich zur Verifizierung verwenden.

(iii) Echtzeitbetrieb (Art. 3 Nr. 42 KI-VO):

Echtzeitbetrieb bedeutet, dass die Erfassung, Verarbeitung und Identifizierung ohne spürbare Verzögerung erfolgt. Systeme, die Ergebnisse mit minimalem Zeitverzug liefern, fallen ebenfalls unter diese Definition. Auch ein begrenzter kurzer Zeitverzug fällt unter diese Definition, sofern dadurch die Echtzeitwirkung nicht unterlaufen wird. Es ist entscheidend, dass die Technologie unmittelbar eine Reaktion ermöglicht.[1]

(b) Öffentlich zugängliche Räume (Art. 3 Nr. 44 KI-VO):

Auslegungshilfe: Öffentlich zugängliche Räume sind physische Orte, an denen sich eine unbestimmte Anzahl von Personen aufhalten kann. Dazu zählen Straßen, Parks und öffentliche Gebäude. Auch privat betriebene Orte, wie z. B. Konzertsäle, Kinos oder Einkaufszentren, gelten als öffentlich zugängliche Räume, sofern eine unbestimmte Anzahl von Personen Zutritt erhalten kann, unabhängig von etwaigen Zugangsbeschränkungen wie Ticketkauf oder Altersgrenzen. Ausgenommen sind Bereiche wie Grenzkontrollzonen, die einer besonderen Zugangsregelung unterliegen.[2]

(c) Handlungen

(i) Handlung I: Liegt eine der folgenden Handlungen vor?

1. Inverkehrbringen (Art. 3 Nr. 9 KI-VO)
   Auslegungshilfe: Bereitstellung eines Systems auf dem Markt, unabhängig davon, ob dies entgeltlich oder unentgeltlich geschieht.
2. Inbetriebnahme (Art. 3 Nr. 11 KI-VO)
   Auslegungshilfe: Bereitstellung eines Systems zum Eigengebrauch oder für Dritte im ersten Einsatz.
3. die Verwendung (Art. 3 Nr. 4 KI-VO)
   Auslegungshilfe: Aktiver Betrieb eines Systems durch einen Betreiber in einem spezifischen Kontext.

(ii) Handlung II: Zweck oder Ziel der Handlung

1. Gezielte Suche nach bestimmten Opfern (Art. 5 Abs. 1 lit. h Ziff. i)
2. Abwendung konkreter, erheblicher und unmittelbarer Gefahren (Art. 5 Abs. 1 lit. h Ziff. ii)
3. Identifizierung mutmaßlicher Straftäter bei schweren Verbrechen (Art. 5 Abs. 1 lit. h Ziff. iii)

   Der Einsatz zu Strafverfolgungszwecken unterliegt der Voraussetzung, dass er durch nationales Recht gestattet und reguliert ist. Ohne entsprechende nationale Regelung darf ein KI-System zu diesem Zweck nicht verwendet werden.[3]

[1] Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), S. 100, Abs. 310
[2] Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), S. 101, Abs. 314
[3] Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), S. 96, Abs. 290

(iii) Datenverarbeitung

Auslegungshilfe: Die Verarbeitung biometrischer Daten umfasst jede Art der Erfassung, Speicherung, Analyse und des Abgleichs solcher Daten, sofern sie zur Identifikation dient. Maßgeblich ist, ob die Datenverarbeitung mit der DS-GVO (Art. 9) konform ist.

(2) Verbotene Praktik

(a) Eingriff in Grundrechte:
Bewerten, ob ein unverhältnismäßiger Eingriff in die Rechte der betroffenen Personen vorliegt, insbesondere in die Privatsphäre und den Datenschutz.

(b) Schutz vor Diskriminierung:

Auslegungshilfe: Diskriminierungspotenziale ergeben sich aus technischen Ungenauigkeiten bei der Erkennung bestimmter Bevölkerungsgruppen, insbesondere aufgrund von ethnischen Merkmalen, Geschlecht oder Alter. Der Betreiber muss sicherstellen, dass das System keine systematischen Benachteiligungen erzeugt.[4]

(3) Zulässige Ausnahme (Art. 5 Abs. 1 lit. h KI-VO)

(a) Gezielte Suche nach bestimmten Opfern:
Diese Ausnahme umfasst Opfer von Entführung, Menschenhandel oder sexueller Ausbeutung. Der Einsatz muss zwingend erforderlich sein, um das Opfer zu retten. Weniger eingreifende Maßnahmen müssen nachweislich unwirksam sein.[5]
Diese Ausnahme umfasst auch die gezielte Suche nach vermissten Personen, insbesondere bei Gefährdungslagen oder bei Kindern. Dabei ist zu berücksichtigen, dass Erwachsene das Recht haben, freiwillig zu verschwinden, sodass der Einsatz von Echtzeit-RBI in solchen Fällen nur bei begründeter Besorgnis zulässig ist (z. B. Suizidgefahr, medizinische Gründe, Abhängigkeit). Die Suche muss einem polizeilichen Zweck dienen; rein administrative Verfahren sind nicht erfasst.[6]

(b) Abwendung konkreter, erheblicher und unmittelbarer Gefahren:

Die Gefahr muss objektiv konkret, erheblich und unmittelbar sein. Beispiele sind terroristische Bedrohungen oder Situationen, in denen ohne den Einsatz des Systems eine hohe Wahrscheinlichkeit für Todesfälle oder schwere Verletzungen besteht. Abstrakte Gefahren oder allgemeine Risiken genügen nicht.[7]

(c) Identifizierung mutmaßlicher Straftäter:

Diese Ausnahme gilt nur für Straftaten, die im Anhang II der KI-VO aufgeführt sind, wie Terrorismus, Menschenhandel oder Mord. Die Straftat muss nach nationalem Recht mit mindestens vier Jahren Freiheitsstrafe bedroht sein. Der Einsatz muss auf spezifische Verdächtige begrenzt sein.[8]

(4) Verfahren und Schutzvorkehrungen

(a) Genehmigungspflicht:
Der Einsatz erfordert eine Genehmigung durch eine unabhängige Justiz- oder Verwaltungsbehörde. In dringenden Fällen darf der Einsatz vorläufig beginnen, wenn die Genehmigung innerhalb von 24 Stunden nachträglich eingeholt wird. Die Ermächtigung zur Nutzung eines Echtzeit-BI-Systems muss in einem nationalen Gesetz verankert sein.[9] Ohne Genehmigung ist der Einsatz unzulässig.

(b) Verhältnismäßigkeitsprüfung:

Zu prüfen ist, ob der Nutzen des Einsatzes die möglichen Beeinträchtigungen der Grundrechte rechtfertigt. Geografische, zeitliche und personenbezogene Beschränkungen müssen eingehalten werden, um den Eingriff zu minimieren.

[4] Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), S. 96, Abs. 293
[5] Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), S. 106, Abs. 332
[6] Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), S. 106, Abs. 333 - 336
[7] Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), S. 107, Abs. 339
[8] Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), S. 109, Abs. 349
[9] Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), S. 104, Abs. 326

(c) Grundrechtsfolgenabschätzung und Registrierung

Bewerten, ob ein unverhältnismäßiger Eingriff in die Rechte der betroffenen Personen vorliegt, insbesondere in die Privatsphäre und den Datenschutz.

(i) Wurde eine Folgenabschätzung im Hinblick auf die Grundrechte durchgeführt? (Art. 27 KI-VO)
Vor der Nutzung ist eine umfassende Folgenabschätzung durchzuführen, die mögliche Risiken für die Rechte der Betroffenen und geeignete Schutzmaßnahmen dokumentiert.

(ii) Ist das System in der EU-Datenbank für Hochrisiko-KI-Systeme registriert? (Art. 49 KI-VO)
Das System muss zudem in der EU-Datenbank für Hochrisiko-KI-Systeme registriert werden, um Transparenz zu gewährleisten.