Checkliste

Verbotene Praktik Nr. 5
Erstellung und Erweiterung von Gesichtsdatenbanken i.S.d. Art. 5 Abs. 1 e.) KI-VO, ErwGr 43

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
    4. Prädiktive Polizeiarbeit Art. 5 Abs. 1 d.) KI-VO
    → **5. Ungezielte Sammlung von Gesichtsbildern Art. 5 Abs. 1 e.) KI-VO**

Beachte hierzu auch:

Orientierungshilfe Verbotene KI-Praktiken Überblick (Version 1.1.),
Orientierungshilfe Verbotene KI-Praktik Nr. 5 (Version 1.3.), Übersicht Verbotene KI-Praktiken (Version 1.4)

Einleitung

Im Folgenden befassen wir uns mit der verbotenen Praktik der Erstellung und Erweiterung von Gesichtsdatenbanken durch KI-Systeme, wie sie in der EU-KI-Verordnung geregelt ist. Diese Praktik umfasst die automatisierte Erfassung und Verarbeitung von Gesichtsbildern aus Quellen wie dem Internet oder Überwachungsaufnahmen, um Datenbanken zur Gesichtserkennung zu erstellen oder zu erweitern. Dabei liegt der Fokus auf ungezielten Methoden, bei denen Personen unabhängig von einem konkreten Anlass erfasst werden, was unter anderem grundlegende rechtliche und ethische Fragen aufwirft.

Dieses Verbot soll nicht nur die willkürliche oder missbräuchliche Verwendung solcher Technologien verhindern, sondern stellt sicher, dass bereits bei der Entwicklung dieser Systeme klare Grenzen gezogen werden. Folgend werden wir detailliert darauf eingehen, welche Handlungen durch diese Regelung untersagt sind, welche Technologien konkret betroffen sind und welche rechtlichen Rahmenbedingungen die Nutzung von KI-Systemen in diesem Bereich bestimmen.

Warum gibt es die Regelung

Gesichtsdatenbanken basieren auf biometrischen Daten, die als besonders sensibel gelten, da sie einzigartige physische Merkmale einer Person erfassen und eine eindeutige Identifizierung ermöglichen. Die automatisierte Erstellung solcher Datenbanken, insbesondere durch ungezieltes Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen, birgt erhebliche Risiken für das Recht auf Privatsphäre, den Schutz personenbezogener Daten und die Menschenwürde.

Eine unregulierte Nutzung von KI-Systemen welche solche Datenbanken Erstellen oder Erweitern kann das Gefühl der Massenüberwachung in der Gesellschaft verstärken und zu Missbrauch führen, etwa durch unrechtmäßige Überwachung oder Diskriminierung bestimmter Gruppen. So können Gesichtserkennungssysteme ohne klare rechtliche und ethische Grenzen dazu verwendet werden, Bewegungsprofile von Personen zu erstellen oder diese ohne deren Wissen und Zustimmung zu überwachen. Die öffentliche Debatte und Vorfälle, wie die Praktiken des Unternehmens Clearview AI, bei denen Gesichtsdatenbanken durch unrechtmäßiges Auslesen von Bildern aus sozialen Medien erstellt wurden, haben verdeutlicht, wie schwerwiegend die Folgen solcher Technologien für die Gesellschaft sein können.

Ein weiteres Problem liegt darin, dass das ungezielte Auslesen von Gesichtsbildern oft gegen Datenschutzrecht verstößt. Selbst wenn Bilder öffentlich zugänglich sind, bedeutet dies nicht, dass biometrische Daten daraus rechtmäßig verarbeitet werden dürfen. Die Datenschutz-Grundverordnung (DS-GVO) schreibt vor, dass die Verarbeitung biometrischer Daten nur unter strengen Bedingungen zulässig ist, etwa wenn sie unbedingt erforderlich und verhältnismäßig ist.

Das Verbot stellt sicher, dass Technologien zur Gesichtserkennung nicht ohne strikte gesetzliche Kontrolle entwickelt und eingesetzt werden dürfen. Sie schützt somit nicht nur Einzelpersonen vor unzulässigen Eingriffen in ihre Privatsphäre, sondern wahrt auch die gesellschaftliche Integrität und das Vertrauen in digitale Technologien.

Definition

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

> *(…) 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;*

Checkliste Verbotene KI-Praktik Nr. 5 i.S.d. Art. 5 Abs. 1 e.) KI-VO, ErwGr 43

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 f) KI-VO, ErwGr 43 vorliegt.

(1) Objektiver Tatbestand

(a) KI-Technologie

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

(b) Zielgruppe

(i) Betroffene Personen

1. Die Sammlung betrifft natürliche Personen, deren Gesichtsbilder ohne vorherige Einwilligung oder rechtliche Grundlage extrahiert und verarbeitet werden.

(ii) Quellen der Gesichtsbilder

a. Internet

Auslegungshilfe: Der Begriff „Internet" umfasst alle online verfügbaren Inhalte, einschließlich sozialer Medien, Websites und Plattformen mit eingeschränktem Zugang (z. B. durch Passwörter oder Benutzeranmeldungen).[1]

b. Überwachungsaufnahmen

Auslegungshilfe: Bilder aus Videoüberwachungssystemen, die ursprünglich für andere Zwecke wie Sicherheit, Verkehrskontrolle oder Zugangsbeschränkungen aufgenommen wurden, gelten als Quelle. Auch Aufnahmen aus privat betriebenen Kameras, wenn sie auf öffentlichen oder halböffentlichen Räumen zugreifen, fallen darunter.

(c) Handlungen

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

1. Inverkehrbringen (Art. 3 Nr. 9 KI-VO)
2. Inbetriebnahme (Art. 3 Nr. 11 KI-VO) oder
3. Verwendung (Art. 3 Nr. 4 KI-VO)

(ii) Handlung II: Liegt eine der verbotenen Praktiken vor?

1. Ungezielte Sammlung von Gesichtsbildern

Auslegungshilfe: Die Sammlung ist „ungezielt", wenn sie ohne konkreten Anlass oder spezifischen Zweck erfolgt, z. B. durch massenhafte Extraktion von Bildern aus sozialen Medien oder Überwachungsaufnahmen. Dabei ist es unerheblich, ob technische Protokolle (z. B. „robots.txt") respektiert werden – die wahllose, massenhafte Extraktion bleibt unzulässig. Es liegt keine sachliche Begrenzung der Zielgruppe vor, und die Sammlung erfolgt unabhängig davon, ob die Daten für einen bestimmten rechtlichen oder operativen Zweck benötigt werden.[2]

2. Erstellung oder Erweiterung von Datenbanken

Auslegungshilfe: Die Erstellung umfasst die erstmalige Zusammenführung von Gesichtsbildern, die zur biometrischen Identifikation geeignet sind. Die Erweiterung einer bestehenden Datenbank umfasst das Hinzufügen neuer biometrischer Profile, unabhängig von deren Quelle. Entscheidend ist, dass die Datenbank objektiv geeignet ist, Personen in zukünftigen Anwendungen zu identifizieren oder zu verifizieren – eine tatsächliche Verwendung zu diesem Zweck ist nicht erforderlich. Die Datenbank kann dabei auch dezentral organisiert oder nur temporär vorhanden sein.[3]

[1] Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), S. 79, Abs. 232
[2] Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), S. 78, Abs. 228
[3] Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), S. 78, Abs. 226

(2) Ausnahmen

a. Gesetzlich vorgesehene Verwendung
Auslegungshilfe: Die Sammlung und Verarbeitung biometrischer Daten ist zulässig, wenn sie durch spezifische Rechtsakte der EU oder nationale Gesetze ausdrücklich erlaubt wird. Allgemeine Ermächtigungen oder rein technische Möglichkeiten reichen nicht aus.[4] Beispiele sind Anwendungen in der Strafverfolgung oder Grenzkontrolle, die in entsprechenden Rechtsvorschriften klar geregelt sind.

b. Notwendige Sicherheitsmaßnahmen
Auslegungshilfe: Die Nutzung von KI-Systemen zur Sammlung von Gesichtsbildern ist nur in Ausnahmefällen erlaubt, wenn sie zwingend erforderlich ist, um unmittelbare und erhebliche Gefahren für die öffentliche Sicherheit zu verhindern. Beispiele sind die Abwehr von Terroranschlägen oder die Suche nach vermissten Personen. Die Maßnahme muss verhältnismäßig sein und darf nicht übermäßig in die Rechte der Betroffenen eingreifen.

c. Wissenschaftliche Forschung
Auslegungshilfe: Die Nutzung ist zulässig, wenn sie ausschließlich wissenschaftlichen Zwecken dient und unter strikter Einhaltung datenschutzrechtlicher Bestimmungen erfolgt. Die Forschung muss in einem kontrollierten Umfeld stattfinden, ohne dass die Daten für kommerzielle Zwecke oder außerhalb des Forschungskontexts verwendet werden. Betroffene Personen müssen, sofern möglich, anonymisiert werden, und eine Datenschutz-Folgenabschätzung ist durchzuführen. Forschungsprojekte dürfen nicht dazu führen, dass gesammelte Daten in späteren operativen KI-Systemen zur Identifikation realer Personen verwendet werden.[5]

[4] Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), S. 80, Abs.238
[5] Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), S. 79, Abs. 234