KONGRESS DER KSSD · BERN 2026

Überwachung mit biometrischer Gesichtserkennung

Anmerkungen aus grundrechtlicher Sicht

Dr. iur. Patrice Martin Zumsteg, Rechtsanwalt

ZHAW School of Management and Law · AAK Anwälte und Konsulenten AG

ÜBERBLICK

Worüber ich spreche

1 **Aktualität** Frankfurt, Berlin – und die Schweiz

2 **Neue Qualität** Warum das nicht Videoüberwachung 2.0 ist

3 **Drei Formen** Echtzeit, nachträglich, Internetabgleich

4 **Grundrechte** Privatsphäre, Versammlungs- und Meinungsfreiheit, Rechtsschutz

5 **Fehlerquellen** Diskriminierungsverbot und Geeignetheit

6 **EU-KI-Verordnung** Kein anwendbares Recht, aber Massstab

7 **Schweiz** Zuständigkeit und zehn Anforderungen an die Norm

8 **Fragen und Diskussion**

AKTUALITÄT I

Frankfurt am Main: Echtzeit im Bahnhofsviertel

Rechtsgrundlage

Novelle des HSOG im Dezember 2024. § 14 Abs. 9 HSOG erlaubt die «biometrische Echtzeit-Fernidentifizierung» – zur Terrorabwehr und zur Suche nach Vermissten und Opfern schwerer Delikte. Gerichtliche Anordnung nach Abs. 11.

Einsatz seit Juli 2025

Sechs KI-gestützte Kameras im Bahnhofsviertel. Erfassung und Abgleich aller Personen im Blickfeld – massenhafte Bearbeitung besonders schützenswerter Personendaten.

Zwischenbilanz

Niedrige zweistellige Anzahl gesuchter Personen bis Frühling 2026 – **ein** Erfolg. Klage vor dem Verwaltungsgericht Frankfurt hängig.

AKTUALITÄT II

Berlin: Abgleich mit Internetquellen

Anderer Weg als Hessen

ASOG-Revision 2025: keine Echtzeit-Identifizierung, dafür biometrischer Abgleich mit öffentlich zugänglichen Internetquellen – Instagram, TikTok, Facebook.

Flankierung

Rechtsgrundlage für kriminalitätsbelastete Orte und – immerhin – ein ausdrückliches Verbot des Racial Profiling.

Zirkularität der Datengrundlage

Festlegung nach polizeilichen Erfahrungswerten → anlasslose Kontrollen → Anfälligkeit für Stereotype → mehr registrierte Kriminalität → Bestätigung der Festlegung

AKTUALITÄT III

Die Schweiz: weiter als man denkt

fedpol – AFIS2026

Erweiterung des Fingerabdruck-Identifikationssystems um ein Modul für den Gesichtsbildabgleich. Live-Scan ist nicht vorgesehen.

Kantonspolizeien

Mindestens vier Korps (SG, AG, VD, NE) setzen Gesichtserkennungssoftware im Strafverfahren ein. Zulässigkeit umstritten.

Bundesverwaltungsgericht

April 2026: Erfassen biometrischer Merkmale und Abgleich sind je eigenständige Datenbearbeitungen; formell-gesetzliche Grundlage der entsprechenden Tätigkeit des NDB fraglich (A-4286/2022 vom 20. April 2026).

Private

Nach den Ausschreitungen in Bern identifizierten Privatpersonen Teilnehmende mit frei verfügbaren KI-Werkzeugen.

KERNTHESE

Keine Videoüberwachung 2.0

1

Aus Beobachtung wird Identifizierung

Nicht der Störer wird überprüft, sondern alle, damit der Störer identifiziert wird – die Umkehrung der polizeirechtlichen Grundfigur.

2

Die Daten sind anderer Natur

Besonders schützenswerte Personendaten (Art. 5 lit. c Ziff. 4 DSG). Sein Gesicht kann man nicht wechseln.

3

Eingriffsschwellen werden technologisch unterlaufen

Die begrenzte menschliche Auswertungsfähigkeit war die faktische Begrenzung. Der Schritt zur Identifizierung ist kein Bau-, sondern ein Softwareentscheid.

4

Die Einschränkung beginnt vor dem ersten Abgleich

Die Referenzdatenbank ist der Kern der Sache: über eine Million Gesichtsbilder aus rund 400’000 erkennungsdienstlichen Behandlungen bei AFIS.

SYSTEMATIK

Drei Formen – drei Regelungen

Echtzeit-Identifizierung

Anlasslos, maximale Streubreite. Für den Einzelnen kaum spürbar – bis ein Fehltreffer eintritt. Dann Polizeimassnahme ohne sachlichen Grund.

Nachträgliche Identifizierung

Anlassbezogen, wirkt gezielter. Greift aber auf dauerhafte Bestände zu, reicht zeitlich zurück, erlaubt Bewegungsprofile – und durchsucht potenziell ganze Demonstrationen.

Abgleich mit Internetquellen

Die eingriffsintensivste Variante: weitet die Referenzdatenbank faktisch auf die gesamte Bevölkerung aus. Scraping ist in der EU verboten (Art. 5 Abs. 1 lit. e KI-VO).

Getrennte Regelungen mit unterschiedlichen Schwellen. Eine Norm, die «biometrische Auswertung» pauschal erlaubt, erfüllt das Bestimmtheitsgebot nicht.

Welche Grundrechte tangiert sind

Privatsphäre und informationelle Selbstbestimmung

Art. 13 Abs. 2 BV · Art. 8 EMRK

BGE 151 I 137 E. 4.5.4: schwerer Eingriff – es bedarf einer ausdrücklichen Grundlage im formellen Gesetz. Die Norm darf die entscheidenden Fragen nicht dem Verordnungsgeber überlassen.

Versammlungs- und Meinungsfreiheit

Art. 22 i.V.m. Art. 16 BV · Art. 11 und 10 EMRK

Anonymität im öffentlichen Raum ist Voraussetzung dafür, dass Menschen von ihren Kommunikationsgrundrechten Gebrauch machen. Die Abschreckung wirkt unabhängig vom Abgleich im Einzelfall.

Verfahrensgarantien

Art. 29a BV · Art. 13 EMRK

Ohne Kenntnis kein Rechtsschutz. Mitteilungspflicht mit nachträglichem Rechtsschutz als Voraussetzung der Verfassungsmässigkeit – BGE 149 I 218 E. 6.3.2.

EGMR, GLUKHIN GEGEN RUSSLAND, NR. 11519/20, URTEIL VOM 4. JULI 2023

«The use of highly intrusive facial recognition technology in the context of the applicant's exercising his Convention right to freedom of expression is incompatible with the ideals and values of a democratic society governed by the rule of law.»

Rz. 90

- **Verletzung von Art. 8 und Art. 10 EMRK** einstimmig – Lokalisierung und Verhaftung nach einer friedlichen Einzeldemonstration in der Moskauer Metro.
- **Besonders schwere Datenbearbeitung** weil sie sich auf die Ausübung eines Konventionsrechts bezog und politische Meinungen offenbarte.
- **Fehlende Garantien** keine klar umrissenen Ermächtigungsgrundlagen, keine Verfahrensgarantien.

FEHLERQUELLEN

Diskriminierungsverbot – und die Geeignetheit

«Beide Fehlerquellen können die Geeignetheit der maschinellen Gesichtserkennung in Frage stellen.»

BGE 151 I 137 E. 4.5.4 – die Fehleranfälligkeit schlägt auf die erste Stufe der Verhältnismässigkeitsprüfung durch.

Das Basisratenproblem

100’000 Gesichter pro Tag, Falsch-Positiv-Rate von 0,1 % – hundert Fehltreffer täglich bei einer Handvoll gesuchter Personen. Laborgenauigkeit ist nicht Feldgenauigkeit.

Der Ort entscheidet, wen es trifft

Kameras stehen nicht zufällig. Erfasst werden systematisch vulnerable Gruppen. Ein Racial-Profiling-Verbot genügt nicht, wenn der Fehler in den Trainingsdaten angelegt ist.

Der «human in the loop»

Automation Bias ist belegt. Menschliche Kontrolle wirkt nur als unabhängige Verifikation vor jeder Massnahme – dokumentiert und nicht durch Zeitdruck aushebelbar.

EU-RECHT

Die KI-Verordnung als Massstab

Echtzeit-Fernidentifizierung

Grundsätzlich verboten – unannehmbares Risiko (Art. 5 Abs. 1 lit. h KI-VO), mit engen Ausnahmen. Die Verbote stehen in Kraft.

Nachträgliche Identifizierung

Hochrisiko-Anwendung (Anhang III Ziff. 1 lit. a KI-VO). Die Pflichten wurden durch den Digital Omnibus auf 2027 verschoben.

Der Pflichtenkatalog als fertige Regelungsvorlage

Qualifizierte menschliche Aufsicht (Art. 26 Abs. 2 KI-VO) · relevante und repräsentative Eingabedaten (Abs. 4) · vorgängige Genehmigung durch eine Justiz- oder unabhängige Verwaltungsbehörde (Abs. 10) · Registrierung (Abs. 8) · Information der Betroffenen (Abs. 11) · Grundrechte-Folgenabschätzung (Art. 27 KI-VO)

Aber: Die KI-VO ist kein Polizeigesetz. Sie ersetzt die nationale Ermächtigungsgrundlage nicht, sondern setzt sie voraus.

ZUSTÄNDIGKEIT

Die Städte können dieses Problem nicht selbst lösen

Strafverfolgung

Dient ein System in erster Linie der Strafverfolgung, braucht es eine Grundlage in der StPO. Dafür ist der Kanton nicht zuständig (Art. 123 Abs. 1 BV).

Prävention

Für den verbleibenden Bereich: Die Luzerner Norm war zu unbestimmt. Gerettet nur durch verfassungskonforme Auslegung auf «einfache» Systeme.

Kommunale Verbote

Zürich, St. Gallen und Lausanne sind rechtlich vor allem Moratorien.

Das Bundesgericht ist von seiner Rechtsprechung abgerückt, wonach im Polizeirecht herabgesetzte Anforderungen an die Normdichte bestehen, soweit das Grundrecht auf Privatsphäre tangiert ist.

Zehn Anforderungen an die gesetzliche Grundlage

1. **Legaldefinitionen und Trennung der Anwendungsfälle.** Je einzeln regeln oder je einzeln untersagen – kein Sammeltitel «Analysesysteme».

2. **Festlegung der Methode.** Selbstlernend oder nicht: Diese Weiche stellt der Gesetzgeber, nicht die Beschaffung.

3. **Die Datenbankseite als eigener Regelungsgegenstand.** Speicherzweck, Speicherschwelle, Speicherdauer. Keine Ausweisdatenbanken, keine Asylregister, kein Scraping.

4. **Abschliessender Delikts- und Zweckkatalog.** Bagatell- und Ordnungsdelikte ausgeschlossen; nach Glukhin auch Versammlungen und Demonstrationen.

5. **Echtzeit-Einsatz nur als eng umgrenzte Ausnahme.** Räumlich und zeitlich befristet, vorgängige gerichtliche Genehmigung.

Zehn Anforderungen an die gesetzliche Grundlage

6 **Genehmigungsvorbehalt auch nachträglich.** Staatsanwaltschaftliche Anordnung oder Vorlage an das Zwangsmassnahmengericht; Subsidiarität.

7 **Menschliche Letztentscheidung ausgestalten.** Ein Treffer ist ein Fahndungshinweis – nie ein hinreichender Grund für Freiheitsentzug.

8 **Qualität, Diskriminierung, Souveränität im Gesetz.** Mindestgenauigkeit, demografische Fehlerdifferenzen, unabhängige Audits, Offenlegung von System und Anbieter.

9 **Transparenz und Rechtsschutz.** Mitteilungspflicht, Beschwerdemöglichkeit, öffentliches Register, Berichterstattung ans Parlament, Folgenabschätzung.

10 **Befristung mit obligatorischer Evaluation.** Sunset-Mechanismus.

Querschnittsforderung: Denken Sie in einer Überwachungsgesamtrechnung – massgebend ist die kumulative Last an einem gewöhnlichen Tag.

FAZIT

1. Die biometrische Gesichtserkennung ist – höchstrichterlich festgestellt – eine schwerwiegende Grundrechtseinschränkung.

2. Sie ist nicht per se ausgeschlossen, bedarf aber einer ausdrücklichen formell-gesetzlichen Grundlage.

3. Für den Strafverfolgungsbereich kann diese Grundlage nur der Bund schaffen.

Der Gesetzgeber soll sich an die Arbeit machen, bevor die Technik da ist – nicht danach.

Fragen und Diskussion

Vielen Dank für Ihre Aufmerksamkeit.

ZUM NACHLESEN

Weiterführende Hinweise

RECHTSPRECHUNG

- EGMR, Glukhin gg. Russland, Nr. 11519/20, Urteil vom 4.7.2023
- BGE 151 I 137 (BGer 1C_63/2023 vom 17.10.2024)
- BVGer A-4286/2022 vom 20.4.2026

RECHTSGRUNDLAGEN UND PROJEKTE

- Verordnung (EU) 2024/1689 – KI-Verordnung
- ED-Verordnung (SR 361.3) und Art. 354 StGB
- fedpol, Projekt AFIS2026

LEHRE UND HINTERGRUND

- Braun Binder/Kunz/Obrecht, Maschinelle Gesichtserkennung im öffentlichen Raum, sui generis 2022, S. 53 ff.
- Simmler/Canova, Die Unrechtmässigkeit des Einsatzes automatisierter Gesichtserkennung im Strafverfahren, ZSR 142/2023 I, S. 201 ff.
- Sussner/Botta, Try harder hilft selten, Verfassungsblog 2026

KONTAKT

ZHAW School of Management and Law

Leiter Kompetenzbereich Sicherheits- und Innovationsrecht

zumg@zhaw.ch · 058 934 42 06

AAK Anwälte und Konsulenten AG

Öffentlicher Sektor und Regulierung in Wissenschaft und Praxis

zumsteg@aa-k.ch · 044 523 14 70



Patrice Martin Zumsteg

Dr. iur. Rechtsanwalt

LinkedIn-Profil