An den Grossen Rat **26.5151.02**

JSD/P265151

Basel, 1. Juli 2026

Regierungsratsbeschluss vom 30. Juni 2026

Schriftliche Anfrage Christoph Hochuli betreffend «der Kantonspolizei und der Staatsanwaltschaft die Bildfahndung mit KI-Tools ermöglichen»

Das Büro des Grossen Rates hat die nachstehende Schriftliche Anfrage Christoph Hochuli betreffend «der Kantonspolizei und der Staatsanwaltschaft die Bildfahndung mit KI-Tools ermöglichen» dem Regierungsrat zur Beantwortung überwiesen:

> «Im Rahmen der unbewilligten Demonstration vom 11.10.2025 wurden in der Stadt Bern zahlreiche Straftaten (Brandstiftung, Sachbeschädigungen, Angriffe gegen Polizistinnen und Polizisten) begangen. Dabei wurden 18 Polizistinnen und Polizisten verletzt. Der Sachschaden, der zur Anzeige gebracht wurde, beläuft sich gemäss damaligen Kenntnissen auf über 600'000 Franken.
>
> Bei den Auswertungen von Videoaufnahmen konnten 101 Straftäterinnen oder Straftäter eindeutig bezeichnet und identifiziert werden. Weiteren 32 Personen konnten anhand von Bildmaterial eindeutig bestimmte Straftaten nachgewiesen werden. Nachdem sich die mutmasslichen Täterinnen und Täter auch nach der Ankündigung der Öffentlichkeitsfahndung nicht bei der Polizei gemeldet hatten und deren Identität nach wie vor nicht geklärt war, hatte die Staatsanwaltschaft Bern-Mittelland die Publikation der verdeckten Bilder verfügt. Die Publikation der verdeckten Bilder auf der Website der Kantonspolizei Bern erfolgte am 20.03.2026. Bilder von Tatverdächtigen, die sich innert einer Frist bei der Kantonspolizei meldeten oder die identifiziert werden konnten, wurden von der Website entfernt.
>
> Nach Ablauf der Frist veröffentlichte die Kantonspolizei Bern am 30.03.2026 unverdeckte Bilder von 31 nicht identifizierten Personen, welche dringend verdächtigt werden, Straftaten an dieser Demonstration begangen zu haben[1]. Die Kantonspolizei bat die Bevölkerung um Hinweise zur Identität der gesuchten Personen. Wenn sich die gesuchten Personen melden oder aufgrund von Hinweisen identifiziert werden, entfernt die Polizei die Bilder von ihrer Website.
>
> Gemäss einem Artikel der Basler Zeitung[2] gelang es einer Privatperson mit einer Recherche mittels KI-Tool (wie Pimeyes.com, Clearview.ai oder Lenso.ai) zwei der gesuchten Personen mit ihren Namen zu identifizieren. Nutzerinnen und Nutzer können Bilder von Personen in diese KI-Tools hochladen und die KI gleicht diese mit Bildern im Internet (Social Media-Plattformen, Unternehmens-Webseiten etc.) ab. Laut einem Schreiben des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten ist die ungefragte Beschaffung von Gesichtsdaten im Internet persönlichkeitsverletzend[3].
>
> Die Strafverfolgungsbehörden dürfen öffentliche KI-Plattformen für die Bildfahndung nicht verwenden. Im Fall der Berner Öffentlichkeitsfahndung wäre es jedoch verhältnismässiger gewesen, hätte die Polizei KI-Tools genutzt statt die Bilder ins Internet zu stellen. Der fehlende Einsatz von KI-Tools verletzte die Persönlichkeitsrechte in diesem Fall viel stärker als die Veröffentlichung der unverdeckten Bilder der mutmasslichen Täterinnen und Täter. Deshalb wäre es sinnvoll, wenn auch die Kantonspolizei und die Staatsanwaltschaft unter bestimmten Voraussetzungen KI-Tools für die Bildfahndung verwenden

darf. Zusätzlich oder alternativ könnte für die Kantonspolizei und die Staatsanwaltschaft eine Gesichtserkennungs-Software angeschafft werde, wie sie einige Polizeikorps verwenden. Die Kantonspolizei St. Gallen nutzt beispielsweise «Griffeye», die Kantonspolizei Aargau «Better Tomorrow». Diese polizeiinternen Programme sind nicht mit dem Internet verbunden und greifen nur auf eigenes Bildmaterial der Kantonspolizei resp. Staatsanwaltschaft zurück.

In diesem Zusammenhang bittet der Unterzeichnende den Regierungsrat um Beantwortung der folgenden Fragen:

1. Wie sieht der Regierungsrat die rechtliche Zulässigkeit der Verwendung von öffentlich zugänglichen KI-Tools für Privatpersonen zur Personensuche im Internet mittels Hochladen von Fotos von Personen ohne deren Zustimmung?
2. Kann der Kantonspolizei und Staatsanwaltschaft die Bildfahndung mit öffentlich zugänglichen KI-Tools ermöglicht werden?
3. Wie müsste dazu – unter Einhaltung der bundesrechtlichen Vorschriften – die kantonale Gesetzgebung angepasst werden?
4. Falls die Benutzung von öffentlich zugänglichen KI-Tools für die Kantonspolizei und Staatsanwaltschaft rechtlich nicht möglich ist: Könnte der Kantonspolizei und der Staatsanwaltschaft alternativ eine KI-Gesichtserkennungs-Software zur Verfügung gestellt werden, um mit internen Fotobeständen Bildfahndung zu betreiben?
5. Bei welchen Delikten und unter welchen Voraussetzungen sollen künftig öffentlich zugängliche resp. interne KI-Tools für die Bildfahndung erlaubt werden?

[1] https://www.police.be.ch/de/start.html?newsID=673af34c-a30c-4f7d-a199-aa8c5c43c9c9

[2] https://www.bazonline.ch/bern-kantonspolizei-fahndet-nach-31-palaestina-demo-teilnehmern-347191096177

[3] https://www.edoeb.admin.ch/de/11022020-ungefragte-beschaffung-von-gesichtsdaten-ist-persoenlichkeitsverletzend

Christoph Hochuli»

Wir beantworten diese Schriftliche Anfrage wie folgt:

1. Vorbemerkungen

Wie in verschiedenen Lebensbereichen sorgen auch im Bereich der Strafverfolgung neue Technologien laufend für neue Möglichkeiten, aber auch gesteigerte Herausforderungen. Eine erste Herausforderung besteht darin, die im vorliegenden Fall auf Algorithmen beruhenden Techniken soweit zu verstehen, dass die Beurteilung der rechtlichen Zulässigkeit überhaupt möglich ist.

Bei der rechtlichen Beurteilung der schriftlichen Anfrage ist alsdann zwischen unterschiedlichen Arten von KI- bzw. Bildsuchdiensten zu unterscheiden. Die in der Anfrage genannten Dienste PimEyes.com, Clearview.ai und Lenso.ai verfolgen zwar alle das Ziel, anhand eines hochgeladenen Bildes ähnliche oder übereinstimmende Gesichtsbilder im Internet oder in Datenbeständen aufzufinden; sie beruhen jedoch nicht zwingend auf denselben technischen und damit auch datenschutzrechtlichen Voraussetzungen. So ist insbesondere zwischen Diensten zu unterscheiden, die *eigene* umfangreiche Datenbanken mit Gesichtsbildern bzw. biometrischen Daten aufbauen, und solchen, die *primär als internetbasierte* Bild- bzw. Gesichtssuchmaschinen auftreten.

Insbesondere Clearview.ai ist in diesem Zusammenhang problematisch, weil das Unternehmen (gemäss öffentlich bekannten Informationen) Gesichtsbilder aus dem Internet gesammelt und daraus eine eigene biometrische Suchdatenbank erstellt hat. Der EDÖB hat bereits 2020 ausgeführt, er gehe davon aus, dass die Anbieter von Clearview bei der Beschaffung von Gesichtsdaten die Persönlichkeit betroffener Personen in der Schweiz verletzen, und riet Privaten sowie Behörden in der Schweiz davon ab, durch Clearview beschaffte Daten zu bearbeiten (siehe Mitteilung des EDÖB vom 11. Februar 2020, einsehbar auf www.edoeb.admin.ch unter Mitteilungen 2020 11.02).

Demgegenüber bezeichnen sich Dienste wie PimEyes und Lenso.ai als Gesichtssuch- bzw. Reverse-Image-Search-Dienste, die anhand eines hochgeladenen Bildes im öffentlich zugänglichen Internet nach Bildern mit gleichen oder ähnlichen Gesichtern suchen. Auch allgemeine Bildsuchdienste wie Google Lens bzw. die Google-Bildersuche ermöglichen eine Suche anhand hochgeladener Gesichtsbilder. Daraus folgt, dass nicht jede Suche mit einem hochgeladenen Gesichtsbild automatisch mit einer spezialisierten biometrischen Identifikationsdatenbank gleichgesetzt werden kann. Gleichwohl kann bereits das Hochladen eines erkennbaren Gesichtsbildes in einen externen Dienst – je nach Funktionsweise des Dienstes – datenschutz- und persönlichkeitsrechtlich problematisch sein.

2. Zu den einzelnen Fragen

1. Wie sieht der Regierungsrat die rechtliche Zulässigkeit der Verwendung von öffentlich zugänglichen KI-Tools für Privatpersonen zur Personensuche im Internet mittels Hochladen von Fotos von Personen ohne deren Zustimmung?

Die rechtliche Zulässigkeit der Verwendung von KI-Tools durch Privatpersonen ist im Einzelfall durch die rechtsanwendenden (Strafverfolgungs-)Behörden und die Gerichte zu beurteilen und kann vom Regierungsrat nicht abschliessend beurteilt werden. Aufgrund der nachstehenden Erwägungen geht der Regierungsrat aber davon aus, dass die Rechtfertigung einer solchen Datenbearbeitung zur Verhinderung oder Aufklärung von Straftaten oder anderer rechtswidriger Handlungen nur sehr zurückhaltend anzunehmen wäre. Damit wäre der Vorgang in den meisten Fällen als rechtlich unzulässig einzustufen.

a. Gegenstand der Datenbearbeitung

Die Zulässigkeit der Bearbeitung von Personendaten natürlicher Personen durch Private richtet sich grundsätzlich nach dem Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG; SR 235.1). Ausgenommen vom Geltungsbereich des DSG sind Datenbearbeitungen durch Privatpersonen, die ausschliesslich persönlichen Zwecken dienen (vgl. dazu nachfolgender Bst. d). Als Datenbearbeitung gilt jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten (Art. 5 lit. d DSG).

Werden öffentlich zugängliche KI-Tools zur Personensuche verwendet, indem Fotografien einer Person hochgeladen werden, liegen regelmässig mehrere Datenbearbeitungsvorgänge vor, die es rechtlich zu beurteilen gilt. Erfasst sind insbesondere das Hochladen des Bildes, dessen technische Analyse zur Bestimmung personenbezogener Merkmale, deren Abgleich mit Datenbanken oder sonstigen Bildbeständen sowie gegebenenfalls die Bekanntgabe von Personendaten an den Anbieter des KI-Tools.

Dabei stellt sich zunächst die Frage, ob die aus den Fotografien gewonnenen Daten als biometrische Daten im Sinne von Art. 5 lit. c Ziff. 4 DSG zu qualifizieren sind. Biometrische Daten gelten als besonders schützenswerte Personendaten, da sie eine natürliche Person eindeutig identifizieren. Fotografien sowie andere Bild- oder Videoaufnahmen fallen nicht per se unter den Begriff der biometrischen Daten. Sie werden jedoch erfasst, wenn sie mittels spezifischer technischer Mittel oder Verfahren so bearbeitet werden, dass sie die eindeutige Identifizierung oder Authentisierung einer Person ermöglichen[1]. Die Bekanntgabe von besonders schützenswerten Personendaten an Dritte gilt als Persönlichkeitsverletzung (Art. 30 Abs. 2 lit. c DSG).

[1] BLECHTA/DAL MOLIN/WESIAK-SCHMIDT, in: Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, 4. Aufl. 2024, N. 75 zu Art. 5 DSG

Die Kombination der beschriebenen Bearbeitungsprozesse – das Hochladen eines Bildes in ein zur Personensuche entwickeltes KI-Tool, die Bestimmung personenbezogener Merkmale und deren Abgleich mit Datenbanken oder Bildbeständen – ist typischerweise darauf ausgerichtet, die abgebildete Person eindeutig zu identifizieren. In solchen Fällen spricht daher viel dafür, die bearbeiteten Daten als biometrische Daten und damit als besonders schützenswerte Personendaten im Sinne von Art. 5 lit. c Ziff. 4 DSG zu qualifizieren, womit deren Bekanntgabe an Dritte die Persönlichkeitsrechte verletzt.

b. Art und Weise der Datenbearbeitung

Nach Art. 6 Abs. 3 DSG dürfen Personendaten generell nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden; sie dürfen zudem nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist. Die Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein (Art. 6 Abs. 2 DSG). Erkennbarkeit setzt voraus, dass die betroffene Person aus den konkreten Umständen mit der Datenbeschaffung und dem Zweck der Bearbeitung rechnen musste oder entsprechend informiert wurde[2]. Art. 8 DSG verlangt zudem, dass Personendaten durch angemessene technische und organisatorische Massnahmen vor unbefugter Bearbeitung geschützt werden. Eine Verletzung der Bearbeitungsgrundsätze stellt – wie die Bekanntgabe von besonders schützenswerten Personendaten an Dritte – eine Persönlichkeitsverletzung dar (vgl. Art. 30 Abs. 2 lit. a DSG).

Das Hochladen eines Fotos in ein KI-Tool zur internetweiten Personensuche ist für die betroffene Person regelmässig nicht erkennbar. Dies gilt insbesondere dann, wenn sie weder über die Verwendung des Bildes noch über den Zweck des Abgleichs informiert wird. Handelt es sich zudem um besonders schützenswerte biometrische Daten (siehe oben), kann die Datenbearbeitung einen erheblichen Eingriff in die informationelle Selbstbestimmung darstellen. Dies gilt umso mehr, wenn die Daten Dritten bekanntgegeben werden. Findet darüber hinaus eine «umfangreiche» Datenbearbeitung statt, ist eine Datenschutz-Folgenabschätzung gemäss Art. 22 Abs. 2 lit. a DSG erforderlich. Die Verhältnismässigkeit eines solchen Eingriffs lässt sich zwar nicht losgelöst vom dadurch verfolgten Zweck beurteilen, doch ist zumindest davon auszugehen, dass die Grundsätze der Transparenz und der Datensicherheit durch die private Personensuche mittels Gesichtsbildern über öffentlich zugängliche KI-Tools im Internet verletzt werden, womit auch diesbezüglich eine Persönlichkeitsverletzung gegeben wäre.

c. Widerrechtlichkeit der Datenbearbeitung

Eine Persönlichkeitsverletzung ist widerrechtlich, sofern sie nicht durch Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist (Art. 31 Abs. 1 DSG). Ob eine persönlichkeitsverletzende Datenbearbeitung durch überwiegende private Interessen gerechtfertigt ist, ist durch Abwägung der privaten Interessen an der Datenbearbeitung und dem Datenschutzinteresse der betroffenen Person zu ermitteln. Insbesondere bei Verstössen gegen grundlegende Bearbeitungsgrundsätze sind Rechtfertigungsgründe nach der bundesgerichtlichen Rechtsprechung nur mit Zurückhaltung anzunehmen. Hierzu sind die Umstände des Einzelfalls zu berücksichtigen, zu denen der Umfang der bearbeiteten Daten, der systematische und unbestimmte Charakter der Bearbeitung und der Personenkreis, der auf die Daten zugreifen kann, gehören. Als überwiegende Bearbeitungsinteressen kommen in erster Linie die Interessen der bearbeitenden Person, aber auch solche von Dritten in Frage. Ob der Bearbeiter ein schützenswertes Interesse verfolgt, hängt vom Zweck der Datenbearbeitung ab. Die Bearbeitung von Daten zur eigenen Sicherheit oder zur Verhinderung oder Aufklärung von Straftaten kann ein schützenswertes Interesse darstellen. Als Sicherheitszweck kommt insbesondere der Schutz von Personen und/oder Sachen in Betracht[3]. So hat die bundesgerichtliche Rechtsprechung die Verwertung einer privaten Videoaufnahme in einem Strafverfahren zugelassen, auf welcher das Fahrzeug des Beschwerdeführers in unmittelbarer Nähe eines Bancomaten ersichtlich war, weil

[2] vgl. Urteil 7B_797/2023 vom 18. September 2024 E. 3.2
[3] vgl. Urteil 7B_797/2023 vom 18. September 2024 E. 3.3 und 3.4

die Aufnahme aus Sicherheitsgründen erstellt worden war und der Verhinderung bzw. Aufklärung rechtswidriger Handlungen diente[4].

Bei der hier zur Diskussion stehenden Verwendung öffentlich zugänglicher KI-Tools zur Personensuche ohne Zustimmung der betroffenen Person ist im Einzelfall zu prüfen, ob ein überwiegendes Interesse an der Datenbearbeitung besteht. Je schwerer der Grundrechtseingriff wiegt, desto gewichtiger müsste das verfolgte öffentliche Interesse sein, damit der Eingriff gerechtfertigt wäre. In allgemeiner Weise lässt sich einzig festhalten, dass im Unterschied zu einer örtlich begrenzten Videoüberwachung der Einsatz öffentlich zugänglicher KI-Tools zur Aufklärung von rechtswidrigen Handlungen mit einer wesentlich höheren Eingriffsintensität verbunden ist. Dies ergibt sich namentlich aus der Qualität der bearbeiteten besonders schützenswerten biometrischen Daten, dem Abgleich mit umfangreichen und häufig intransparenten Datenbeständen, dem systematischen und teils unbestimmten Charakter der Suche sowie dem gegebenenfalls weiten Kreis zugriffsberechtigter Personen auf den Datenbestand und der potenziellen Bekanntgabe dieser Daten an den Toolanbieter. Die Rechtfertigung einer solchen Datenbearbeitung zur Verhinderung oder Aufklärung von Straftaten oder anderer rechtswidriger Handlungen wäre daher nur sehr zurückhaltend anzunehmen.

d. Ausnahme: Bildersuche zu persönlichen Zwecken

Zwar dürfte sich die vorliegende Anfrage aufgrund des geschilderten Kontexts primär auf das Vorgehen einer Person beziehen, die von Anfang an beabsichtigt, zuhanden der Strafverfolgungsbehörden eine «private» Bildfahndung durchzuführen. Die Frage ist jedoch offen formuliert worden, weshalb der Vollständigkeit halber auch auf die Ausnahmebestimmung von Art. 2 Abs. 2 Bst. a DSG einzugehen ist.

Das DSG findet ausdrücklich keine Anwendung auf Datenbearbeitungen durch Privatpersonen, die ausschliesslich persönlichen Zwecken dienen. Daher fällt das private Hochladen eines Fotos einer Person in ein öffentlich zugängliches KI-Tool mit der Absicht, dies nur für persönliche Zwecke zu tun, grundsätzlich nicht in den Anwendungsbereich des DSG und stellt folglich keine widerrechtliche Persönlichkeitsverletzung im Sinne von Art. 30 DSG dar. Damit unterscheidet sich diese Konstellation von derjenigen im Zusammenhang mit der geschilderten medialen Berichterstattung, denn dort bestand offenbar von Anfang an die Absicht, die Strafverfolgungsbehörden zu unterstützen. Die abschliessende rechtliche Beurteilung obliegt jedoch auch hier den Gerichten.

2. Kann der Kantonspolizei und Staatsanwaltschaft die Bildfahndung mit öffentlich zugänglichen KI-Tools ermöglicht werden?

Das Legalitätsprinzip verlangt, dass sich jedes staatliche Handeln auf eine gesetzliche Grundlage stützt. Daher ist die Frage nach der Ermöglichung einer Bildfahndung durch die kantonalen Strafverfolgungsbehörden mit öffentlich zugänglichen KI-Tools darauf gerichtet, ob eine hinreichende gesetzliche Grundlage dafür besteht oder eine solche durch den kantonalen Gesetzgeber geschaffen werden kann. Auf Basis der nachfolgenden Ausführungen schliesst der Regierungsrat, dass derzeit keine hinreichende gesetzliche Grundlage besteht für die Bildfahndung mit öffentlich zugänglichen KI-Tools durch die Kantonspolizei oder die Staatsanwaltschaft. Auf kantonaler Ebene kann eine solche Grundlage nicht geschaffen werden.

Der Erlass des Straf- und Strafprozessrechts liegt in der Zuständigkeit des Bundes (Art. 123 Abs. 1 Bundesverfassung; BV; SR 101). Der Bund hat deshalb das Strafgesetzbuch (StGB; SR 311.0) und die Strafprozessordnung (StPO; SR 312.0) erlassen. Art. 354 StGB regelt die Speicherung und den Abgleich bereits erhobener biometrischer Daten (z. B. Fingerabdrücke, Gesichtsbilder) durch das zuständige Departement (EJPD), dient also der Identifikation gesuchter oder unbekannter Personen. Das bestehende automatische Fingerabdruck-Identifikationssystem (AFIS) wird im Projekt AFIS2026 erweitert, u. a. um einen Gesichtsbildabgleich. Dieser

[4] BGer Urteil 7B_797/2023 vom 18. September 2024 E. 3.4 und E. 4

erfolgt algorithmisch und liefert keine Echtzeitüberwachung und kein Abgleich mit externen Quellen wie sozialen Medien oder Ausweisdatenbanken[5]. Art. 354 Abs. 4 StGB i.V.m. Art. 2 lit. c der Verordnung über die Bearbeitung biometrischer erkennungsdienstlicher Daten vom 6. Dezember 2013 (ED-Verordnung; SR 361.3) erlaubt allerdings einzig dem Fedpol, biometrische erkennungsdienstliche Daten einschliesslich Fotografien in diesem Sinne zu bearbeiten. Abgleiche von Gesichtsbildern, die nicht vom Fedpol, sondern von den kantonalen Polizeikorps durchgeführt werden, sind von diesen Rechtsgrundlagen nicht erfasst[6].

Fraglich ist daher, ob Abgleiche von Gesichtsbildern durch kantonale Strafverfolgungsbehörden gestützt auf eine andere Grundlage des Bundesrechts zulässig sind. Bei der durch kantonale Polizeikorps durchgeführten nachträglichen Gesichtserkennung mittels Systeme zum Abgleich von Bild- und Videoaufnahmen mit Referenzdaten als Ermittlungsmassnahme im Nachgang von Straftaten, liegt ein strafprozessualer Einsatz vor, der in den Anwendungsbereich der StPO fällt[7]. Im Rahmen der Beantwortung der Interpellation Marti 22.3993 «Rechtliche Grundlage für die automatisierte Gesichtserkennung in Strafverfahren» hat sich der Bundesrat auf den Standpunkt gestellt, dass insbesondere Art. 260 ff. der StPO betreffend die Verwendung erkennungsdienstlicher Daten in Strafverfahren als Gesetzesgrundlagen für ein Gesichtsbildabgleich zur Identifizierung von gesuchten oder unbekannten Personen einschlägig seien (Stellungnahme des Bundesrates vom 16. November 2022 zur Interpellation Nr. 22.3993). Dass die kantonalen Strafverfolgungsbehörden gestützt auf Art. 260 ff. StPO oder andere Bestimmungen der StPO einen Gesichtsbildabgleich mittels Systemen zum Abgleich von Bild- und Videoaufnahmen mit Referenzdaten durchführen dürfen, wird in der Lehre allerdings bestritten[8]. Unabhängig davon ist unbestritten, dass sich zurzeit keine Grundlage in der StPO findet, die den kantonalen Strafverfolgungsbehörden eine Bildfahndung mit öffentlich zugänglichen KI-Tools ermöglicht.

Nach dem Gesagten kommt dem Bund nicht nur die Kompetenz zum Erlass der Gesetzgebung im Zusammenhang mit der Bildfahndung zu, sondern dieser hat auch seine diesbezügliche Gesetzgebungskompetenz ausgeschöpft. Der Erlass einer weitergehenden Gesetzgebung auf kantonaler Ebene, die eine Bildfahndung mit öffentlich zugänglichen KI-Tools ermöglichen würde, wäre bundesrechtswidrig und würde keine Rechtswirkungen entfalten (vgl. Art. 49 Abs. 1 BV). Der Kantonspolizei und der Staatsanwaltschaft kann die Bildfahndung mit öffentlich zugänglichen KI-Tools auf kantonaler Ebene demnach nicht ermöglicht werden.

3. Wie müsste dazu – unter Einhaltung der bundesrechtlichen Vorschriften – die kantonale Gesetzgebung angepasst werden?

Hier kann auf die Beantwortung der Frage 2 verwiesen werden. Dadurch, dass die Gesetzgebung des Bundes in diesem Bereich abschliessend ist, können auf kantonaler Ebene keine diesbezüglichen Bestimmungen erlassen werden.

4. Falls die Benutzung von öffentlich zugänglichen KI-Tools für die Kantonspolizei und Staatsanwaltschaft rechtlich nicht möglich ist: Könnte der Kantonspolizei und der Staatsanwaltschaft alternativ eine KI-Gesichtserkennungs-Software zur Verfügung gestellt werden, um mit internen Fotobeständen Bildfahndung zu betreiben?

Unter nachträglicher Gesichtserkennung ist der Einsatz technischer Systeme zu verstehen, mit denen bereits vorhandene Foto- oder Videoaufnahmen ausgewertet werden, typischerweise nach der Begehung einer Straftat im Rahmen der Strafverfolgung. Nach der in der Literatur beschriebenen Praxis werden in der Schweiz vereinzelt Fahndungsbilder mit polizeilichen Datenbeständen abgeglichen; dabei können kantonale Datenbanken mit weiteren, etwa kantonsübergreifenden Beständen verglichen werden. Das zugrundeliegende Bildmaterial stammt häufig aus Überwachungs-

[5] vgl. dazu BAUMANN, Staatliche Gesichtserkennung: eine rechtliche Einordnung, in: Risiko & Recht, 2/2025, S. 60 ff., S. 65 und 68
[6] SIMMLER/CANOVA, Die Unrechtmässigkeit des Einsatzes automatisierter Gesichtserkennung im Strafverfahren – ein weiterer Beitrag zu einer anhaltenden Debatte, in: Zeitschrift für Schweizerisches Recht, 2023/3, S. 201 ff., S. 216
[7] SIMMLER/CANOVA, S. 206
[8] SIMMLER/CANOVA, S. 221

kameras privater Geschädigter, beispielsweise aus Verkaufsgeschäften nach einem Diebstahl. Trotz des technischen Abgleichs erfolgt die eigentliche Zuordnung zu einer verdächtigten Person weiterhin durch eine Polizeibeamtin oder einen Polizeibeamten und nicht durch die Software selbst. Die rechtlichen Fragen, die sich bei maschineller Gesichtserkennung stellen, bestehen allerdings unabhängig davon, welche konkrete Technologie verwendet wird und ob diese als künstliche Intelligenz bezeichnet wird. In der rechtswissenschaftlichen Literatur wird der Einsatz solcher Systeme insgesamt deutlich kritisch beurteilt[9].

Der Bundesrat vertritt die Auffassung, dass auf Grundlage der bestehenden gesetzlichen Bestimmungen biometrische Gesichtsdaten zur Identifizierung von Personen im Rahmen von Ermittlungen und Strafverfahren verwendet werden dürfen (Antwort des Bundesrats vom 27. September 2021 auf die parlamentarische Anfrage Nr. 21.7896). In diesem Zusammenhang stellt er insbesondere darauf ab, dass die Bestimmungen der Art. 260 ff. StPO über die erkennungsdienstliche Erfassung eine hinreichende gesetzliche Grundlage für den Gesichtsbildabgleich zur Identifizierung gesuchter oder unbekannter Personen darstellen. Diese Auffassung ist jedoch in der Lehre umstritten. Es wird teilweise bezweifelt, dass sich ein Gesichtsbildabgleich mittels automatisierter Systeme, die Bild- und Videoaufnahmen mit Referenzdaten abgleichen, ohne Weiteres auf Art. 260 ff. StPO oder andere Bestimmungen der Strafprozessordnung stützen lässt (siehe oben zu Frage 2).

Vor diesem Hintergrund stellt sich die Frage, ob die bestehenden Normen den Anforderungen an eine hinreichende gesetzliche Grundlage genügen. Liegt – wie im Zusammenhang mit biometrischer Gesichtserkennung anzunehmen – ein schwerer Eingriff in Grundrechte vor, insbesondere in das Recht auf informationelle Selbstbestimmung, sind im Zusammenhang mit dem Erfordernis der hinreichenden gesetzlichen Grundlage besonders hohe Anforderungen sowohl an die Normstufe als auch an die Normdichte zu stellen. Zwar handelt es sich bei der Strafprozessordnung unbestrittenermassen um ein formelles Gesetz. Entscheidend ist jedoch, ob die einschlägigen Bestimmungen hinreichend bestimmt sind.

Art. 261 StPO regelt die Verwendung erkennungsdienstlicher Unterlagen. Ob diese Bestimmung in ihrer heutigen Form den Anforderungen an das Bestimmtheitsgebot genügt, ist fraglich. Nach der bundesgerichtlichen Rechtsprechung kann eine Norm zwar in bestimmten Konstellationen offener formuliert sein, namentlich dann, wenn komplexe Interessenabwägungen erforderlich sind. Gleichwohl gilt, dass bei schweren Grundrechtseingriffen besonders strenge Anforderungen an die Bestimmtheit der gesetzlichen Grundlage zu stellen sind. Das Bundesgericht hat in Übereinstimmung mit der Rechtsprechung des EGMR wiederholt festgehalten, dass Eingriffe von erheblicher Intensität eine präzise und detaillierte gesetzliche Regelung voraussetzen. Als solche schwerwiegenden Eingriffe wurden etwa die automatische Fahrzeugfahndung und Verkehrsüberwachung qualifiziert. In diesen Fällen genügt es nicht, dass eine staatliche Massnahme lediglich auf einer formell gesetzlichen Grundlage beruht. Vielmehr ist erforderlich, dass zentrale Aspekte wie die Erhebung, Speicherung, Verwendung und Löschung der Daten sowie deren Umfang hinreichend konkret geregelt sind. Dies bedingt regelmässig ein umfassendes Schutzkonzept, das den Anforderungen des Bestimmtheitsgebots genügt und die wesentlichen Modalitäten der Datenbearbeitung verbindlich festlegt[10].

Diese Anforderungen gelten im Ergebnis auch für den Einsatz biometrischer Gesichtserkennungssysteme im Strafverfahren. Daher setzt die Beantwortung dieser Frage eine vertiefte Recherche voraus, die den Rahmen einer schriftlichen Anfrage sprengen würde.

[9] NADJA BRAUN BINDER / ELIANE KUNZ / LILIANE OBRECHT, Maschinelle Gesichtserkennung im öffentlichen Raum, sui generis 2022, S. 54 ff., insb. N. 7, 14 und 37

[10] AISHA PALOMA BRAUN, Die öffentliche Sittlichkeit im Kontext der Rechtsstaatlichkeit, Zürich 2024, N 199 ff. und 229 ff., insb. N 234

5. Bei welchen Delikten und unter welchen Voraussetzungen sollen künftig öffentlich zugängliche resp. interne KI-Tools für die Bildfahndung erlaubt werden?

Wie bereits ausgeführt ist für die Bildfahndung durch die Kantonspolizei oder die Staatsanwaltschaft mit öffentlich zugänglichen KI-Tools derzeit keine hinreichende gesetzliche Grundlage vorhanden und kann auf kantonaler Ebene auch nicht geschaffen werden (vgl. oben zu Frage 2). Der Einsatz interner KI-Tools für die Bildfahndung ist umstritten und komplex. Eine rechtliche Beurteilung würde eine vertiefte Recherche voraussetzen und den Rahmen einer schriftlichen Anfrage sprengen (vgl. oben zu Frage 4). Hierzu gehört insbesondere auch die Einschätzung, wie eine allfällige Regelung auszugestalten wäre; namentlich bei welchen Delikten und unter welchen Voraussetzungen Bildfahndung erlaubt sein könnte.

Im Namen des Regierungsrates des Kantons Basel-Stadt

Dr. Conradin Cramer
Regierungspräsident

Barbara Schüpbach-Guggenbühl
Staatsschreiberin