Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)493 K

Fachbereich Wirtschaftswissenschaften

Institut für Wirtschaftsrecht

Dr. Stephan Schindler

Universität Kassel – FB 07 – FG Öffentliches Recht, IT-Recht und Umweltrecht
Henschelstr. 4, D-34127 Kassel

Universität Kassel
Fachgebiet Öffentliches Recht,
IT-Recht und Umweltrecht
Henschelstr. 4
34127 Kassel

stephan.schindler@uni-kassel.de
fon +49-561 804-7925
fax +49-561 804-3621

Sekretariat: Lena Butterweck
fon +49-561 804-7924
lena.butterweck@uni-kassel.de

22.09.2024

Stellungnahme

zur öffentlichen Anhörung zu den Gesetzentwürfen der Fraktionen SPD, BÜNDNIS 90/DIE GRÜNEN und FDP „Entwurf eines Gesetzes zur Verbesserung der inneren Sicherheit und des Asylsystems“ (BT-Drs. 20/12805) und „Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung“ (BT-Drs. 20/12806) sowie dem Gesetzentwurf der Fraktion der CDU/CSU „Entwurf eines Gesetzes zur Begrenzung des illegalen Zustroms von Drittstaatsangehörigen nach Deutschland (Zustrombegrenzungsgesetz)“ (BT-Drs. 20/12804)

1 Vorbemerkung

Die Stellungnahme setzt sich – soweit dies in der Kürze der zur Verfügung stehenden Zeit möglich war – mit den Regelungen zum nachträglichen biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet und zur automatisierten Datenanalyse im „Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung“ auseinander.

2 Regelungen zum biometrischen Abgleich

Die §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E im „Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung“[1] sollen es dem BKA, der BPOL und den Strafverfolgungsbehörden erlauben, biometrische Daten zu Gesichtern und Stimmen mit öffentlich zugänglichen Daten aus dem Internet biometrisch abzugleichen. Dies soll es insbesondere möglich machen, „mutmaßliche Terroristen und Tatverdächtige zu identifizieren und lokalisieren“.[2]

[1] BT-Drs. 20/12806.

[2] BT-Drs. 20/12806, 2. Fragwürdig ist die dort aufzufindende Aussage, „dass die Strafverfolgungsbehörden zu Zwecken der Gefahrenabwehr“ handeln können.

Fraglich ist, ob diese Regelungen den einschlägigen verfassungs- und europarechtlichen Vorschriften genügen. Namentlich betrifft dies die Grundrechte sowie die Vorgaben der JI-Richtlinie und der KI-Verordnung.

2.1 Verfassungs- und grundrechtliche Erwägungen

2.1.1 Erheblicher Grundrechtseingriff

Die Regelungen in §§ 10b, 39a, 63b BKAG-E und § 34b BPolG-E sollen es den dort genannten Behörden erlauben, „biometrische Daten zu Gesichtern und Stimmen […] mit öffentlich zugänglichen personenbezogenen Daten aus dem Internet mittels einer automatisierten Anwendung zur Datenverarbeitung biometrisch ab[zu]gleichen". § 98d Abs. 1 StPO-E ist abweichend formuliert und spricht davon, dass „durch Erkennung des Gesichts und der Stimme […] biometrische Daten […] mit biometrischen Daten aus im Internet öffentlich zugänglichen Lichtbild- und Videodateien nachträglich mittels einer automatisierten Anwendung zur Datenverarbeitung abgeglichen werden" dürfen.

Bild- und Videoaufnahmen menschlicher Gesichter, die eine Identifikation der abgebildeten Person erlauben, sind personenbezogene Daten.[3] Das gilt auch für Stimmaufnahmen, wenn sie einer bestimmten Person zugeordnet werden können. Zudem handelt es sich bei den Daten, mit denen der Abgleich erfolgen darf, ausdrücklich um personenbezogene Daten. Somit erlauben die genannten Regelungen Eingriffe in das Grundrecht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG,[4] das Grundrecht auf Schutz personenbezogener Daten gem. Art. 7 und 8 GRCh[5] sowie das Recht auf Achtung des Privat und Familienlebens gem. Art. 8 EMRK[6]. Dabei bilden die Erhebung der Daten, der Datenabgleich und mögliche Speicherungen jeweils eigene Grundrechtseingriffe.[7]

Je nach Situation sind weitere Grundrechtseingriffe denkbar, etwa in die Versammlungsfreiheit (Art. 8 GG, Art. 12 GRCh, Art. 11 EMRK), wenn Bildaufnahmen in den Abgleich einbezogen werden, die während einer Versammlung entstanden sind. Hierauf wird im Folgenden nicht weiter eingegangen.

Die Grundrechtseingriffe entfallen nicht dadurch, dass der Abgleich mit „öffentlich zugänglichen personenbezogenen Daten" erfolgt, da der grundrechtliche Schutz personenbezogener Daten nicht auf Vorgänge der Privat- oder Intimsphäre beschränkt ist. Vielmehr werden auch öffentlich wahrnehmbare Vorgänge vom Grundrechtsschutz erfasst.[8] Das BVerfG vertritt die Auffassung, dass kein Grundrechtseingriff vorliegt, „wenn eine staatliche Stelle im Internet verfügbare Kommunikationsinhalte erhebt, die sich an jedermann oder zumindest an einen nicht weiter abgegrenzten Personenkreis richten".[9] Selbst wenn diese Rechtsprechung auf die „öffentlich zugänglichen personenbezogenen Daten aus dem Internet" gem. §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E anwendbar sein sollte, führt dies hier nicht zu einem Entfallen des Grundrechtseingriffs, da ein Eingriff jedenfalls dann

[3] Vgl. EuGH, NJW 2015, 463, 463 zur Videoüberwachung.

[4] Vgl. BVerfG, NVwZ 2007, 688, 690 zur Videoüberwachung.

[5] Vgl. EuGH, ZD 2020, 148, 150 zur Videoüberwachung. Von einer Anwendbarkeit der Unionsgrundrechte ist gem. Art. 51 Abs. 1 S. 1 GRCh auszugehen (Durchführung des Rechts der Union), da die vorgesehenen Maßnahmen unter anderem in den Anwendungsbereich der JI-Richtlinie fallen (s.u.).

[6] Vgl. EGMR, NJW 2011, 1333, 1334 zur Videoüberwachung.

[7] BVerfGE 150, 244, 265 f. zur automatisierten Kennzeichenerkennung.

[8] S. z.B. BVerfG, NVwZ 2007, 688, 690; bereits BVerfGE 65, 1, 45 hat festgestellt, dass es insoweit kein „belangloses" personenbezogenes Datum gibt.

[9] BVerfGE 120, 274, 344 f. („etwa, wenn die Behörde eine allgemein zugängliche Webseite im World Wide Web aufruft, eine jedem Interessierten offen stehende Mailingliste abonniert oder einen offenen Chat beobachtet").

vorliegt, wenn diese Daten „unter Hinzuziehung weiterer Daten ausgewertet werden“.[10] Eine solche Auswertung findet bei dem biometrischen Abgleich mit Daten zu Gesichtern und Stimmen statt.

Die vorgesehene Datenverarbeitung ruft somit Grundrechtseingriffe hervor[11] und bedarf daher einer gesetzlichen Grundlage, die dem Bestimmtheitsgebot und dem Grundsatz der Verhältnismäßigkeit genügt.[12] Die Anforderungen an die gesetzliche Grundlage – hier die §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E – hängen maßgeblich vom Gewicht des Grundrechtseingriffs ab.[13] Je schwerer dieser ist, desto höher sind die Anforderungen an die Bestimmtheit und die Verhältnismäßigkeit.[14]

Die genannten Regelungen erlauben Eingriffe von erheblichem Gewicht. Der vorgesehene biometrischen Abgleich mit „öffentlich zugänglichen personenbezogenen Daten aus dem Internet“ (bzw. „im Internet öffentlich zugänglichen Lichtbild- und Videodateien“) wird regelmäßig zahlreiche Personen erfassen, die für die Maßnahme keinen Anlass gegeben haben, was zu Einschüchterungseffekten führen und die Unbefangenheit bei der Ausübung von Grundrechten beeinträchtigen kann.[15] Insbesondere könnten Internetnutzer aus Furcht, in einen biometrischen Abgleich einbezogen zu werden, davon absehen, Bild-, Video- und Tonaufnahmen von sich in das Internet zu stellen, was ggf. auch andere Grundrechte, etwa die Meinungsfreiheit, beeinträchtigen kann.[16] Gewichtserhöhend ist zudem in Rechnung zu stellen, dass der Abgleich von den betroffenen Personen nicht bemerkt wird (er aus ihrer Sicht also heimlich erfolgt)[17] und mit dem Gesicht und der Stimme zwei menschliche Merkmale verwendet werden, denen einen hohe Persönlichkeitsrelevanz nicht abzusprechen ist.[18]

Das Eingriffsgewicht wird ferner dadurch erhöht, dass mögliche Fehlerkennungen für die betroffenen Personen mit Nachteilen einhergehen können (z.B. weitere polizeiliche Maßnahmen gegen eine fälschlicherweise als Straftäter identifizierte Person).[19] Die Erkennungsleistung von Gesichtserkennung ist maßgeblich von den Umständen ihres konkreten Einsatzes abhängig. Werden Bildaufnahmen von geringer Qualität herangezogen, was bei Suchen im Internet nicht ausgeschlossen werden kann, kann die Erkennungsleistung

[10] BVerfGE 120, 274, 345.

[11] Vgl. auch Hornung/Schindler, ZD 2017, 203 zu Eingriffen bei Gesichtserkennung in Verbindung mit Videoüberwachung.

[12] Z.B. BVerfGE 120, 378, 401 und BVerfGE 150, 244, 278 f. zur automatisierten Kennzeichenerkennung; s. bereits BVerfGE 65, 1, 44. Für die Unionsgrundrechte s. Art. 52 Abs. 1 GRCh.

[13] Allg. zum Eingriffsgewicht bei Gesichtserkennung s. Schindler, Biometrische Videoüberwachung, 2021, 471 ff.

[14] Z.B. BVerfGE 120, 378, 401 ff.

[15] S. BVerfGE 120, 378, 402 zur automatisierten Kennzeichenerkennung; BVerfG, NVwZ 2007, 688, 691 zur Videoüberwachung.

[16] S. bereits BVerfGE 65, 1, 43 zu Abschreckungseffekten, die sich auf die Ausübung von Grundrechten auswirken können; zu Abschreckungseffekten und Verhaltensanpassungen s.a. Büscher et al., DuD 2023, 503.

[17] S. BVerfGE 120, 378, 402 f.

[18] Allg. zur Persönlichkeitsrelevanz z.B. BVerfGE 120, 378, 402. Vgl. auch Art. 9 Abs. 1 DSGVO und Art. 10 Abs. 1 JI-RL, demnach es sich bei biometrischen Daten (z.B. Gesichtsbilder, Art. 4 Nr. 14 DSGVO, Art. 3 Nr. 13 JI-RL) um besondere Kategorien personenbezogener Daten handelt, die besonders geschützt sind.

[19] Zur Berücksichtigung von Nachteilen z.B. BVerfGE 120, 378, 403.

sehr gering sein.[20] Es ist dann davon auszugehen, dass viele Treffer Fehlererkennungen (false positive) sein werden. In diesem Zusammenhang ist zudem zu berücksichtigen, dass Gesichtserkennungssysteme unter Umständen bei verschiedenen Bevölkerungsgruppen (z.B. mit Blick auf Hautfarbe, Alter und Geschlecht) unterschiedlich gut funktionieren,[21] was dazu führen kann, dass Angehörige bestimmter Bevölkerungsgruppen einem erhöhten Risiko von Fehlerkennungen ausgesetzt sind. Dies kann eine diskriminierende Wirkung entfalten.

Für die Bestimmung des Eingriffsgewichts ist zudem von Bedeutung, was für Informationen durch den biometrischen Abgleich über die betroffenen Personen erhoben werden können und wozu diese genutzt werden können. Dient der Abgleich allein der Identifizierung von Personen, gegen die der Verdacht einer Straftat besteht oder von denen eine Gefahr ausgeht, um sie aufzufinden und weiteren polizeilichen Maßnahmen zu unterwerfen (z.B. Festnahme), ist dies mit Blick auf die stattfindende Informationsverarbeitung weit weniger eingriffsintensiv als die Nutzung der durch den Abgleich gewonnenen Informationen, um weitere Schlüsse auf das Verhalten, die Lebensumstände und die Vorlieben (etc.) der betroffenen Personen zu ziehen.[22] Werden etwas durch den Abgleich zahlreiche Treffer bzgl. einer Person erzielt, kann dies unter Umständen Rückschlüsse auf ihr Bewegungsverhalten (z.B. bei Bildaufnahmen, die sie an verschiedenen Orten zeigen) oder ihre persönlichen Vorlieben (z.B. Bilder, die die Person bei bestimmten Tätigkeiten zeigen) ermöglichen. Werden diese Erkenntnisse zusammengetragen, kann dies weitreichende Erkenntnisse über die betroffene Person vermitteln, was die Persönlichkeitsrelevanz der Maßnahme steigert.

Gewichtsmildernd kann grundsätzlich in Rechnung gestellt werden, dass der Abgleich nur mit „öffentlich zugänglichen personenbezogenen Daten“ (bzw. „im Internet öffentlich zugänglichen Lichtbild- und Videodateien“) erfolgen darf.[23] Allerdings ist dabei zu berücksichtigen, dass dies – je nach dem, was unter „öffentlich zugänglichen personenbezogenen Daten“ zu verstehen ist – auch Daten (insbesondere Bild- und Videoaufnahmen) erfassen kann, die gegen den Willen der betroffenen Person und ggf. unter Verletzung strafrechtlicher Vorschriften (z.B. § 201a StGB, § 33 KUG, § 106 UrhG) in das Internet gestellt wurden.[24] Gerade in solchen Fällen ist es problematisch, dass die Rechtsverletzung durch Heranziehung dieser Daten für den biometrischen Abgleich fortgesetzt wird und es zu einer Verletzung von Vertraulichkeitserwartungen kommen kann. Dies wirkt sich gewichtserhöhend aus.

Die Grenze zur Menschenwürdewidrigkeit (Art. 1 Abs. 1 GG, Art. 1 GRCh) wird bei den vorgesehenen Maßnahmen aber nicht überschritten. Die Menschenwürde schützt die Subjektqualität des Menschen. Diese wird durch die staatliche Informationserhebung und Beobachtung grundsätzlich nicht verletzt.[25] Auch ist eine menschenwürdewidrige „umfassende

---

[20] S. hierzu z.B. die Erfahrungen bei Gesichtserkennung in Verbindung mit Videoüberwachung bei den Pilotprojekten am Hauptbahnhof Mainz (2006-2007) und am Bahnhof Berlin Südkreuz (2017-2018), https://www.bka.de/DE/UnsereAufgaben/Forschung/ForschungsprojekteUndErgebnisse/Foto-Fahndung/foto-fahndung_node.html; https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung_down.pdf;jsessionid=B00C5E4B9341D9F8733EF8508A6D9C46.2_cid324?__blob=publicationFile&v=1.

[21] Dazu z.B. Grother/Ngan/Hanaoka, Face Recognition Vendor Test (FRVT). Part 3: Demographic Effects, 2019, https://doi.org/10.6028/NIST.IR.8280.

[22] S. BVerfGE 120, 378, 403 ff.

[23] Vgl. BVerfGE 120, 378, 404 für die Erfassung von Verhaltensweisen, die „für jedermann ohne weiteres erkennbar“ sind.

[24] S.a. BT-Drs. 20/12806, 25.

[25] Z.B. BVerfGE 109, 279, 313 zur akustischen Wohnraumüberwachung.

Registrierung und Katalogisierung der Persönlichkeit“[26] bei dem Abgleich biometrischer Daten zu Gesichtern und Stimmen mit öffentlich zugänglichen personenbezogenen Daten aus dem Internet nicht zu befürchten. Eine Erstellung von „Totalabbildern“[27] der Persönlichkeit der betroffenen Personen wird hierdurch nicht ermöglicht.[28]

Schließlich führt der Abgleich im Regelfall auch nicht zu einer Verletzung des unantastbaren Kernbereichs privater Lebensgestaltung. Der Kernbereich privater Lebensgestaltung schützt einen höchstpersönlichen Bereich (z.B. „innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art“ und „die nichtöffentliche Kommunikation mit Personen des höchstpersönlichen Vertrauens“) vor staatlicher Ausforschung.[29] Voraussetzung für den Schutz ist ein Geheimhaltungswillen des Betroffenen.[30] Der in §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E vorgesehene Abgleich ist auf öffentlich zugängliche Daten aus dem Internet beschränkt. Diese Daten werden häufig schon deshalb keinen Kernbereichsbezug aufweisen, weil sie von der betroffenen Person selbst öffentlich gemacht wurden, so dass es an dem Geheimhaltungswillen fehlt. Im Einzelfall ist eine Erhebung und Verarbeitung kernbereichsrelevanter Daten aber nicht ausgeschlossen (wenn etwa Bild- oder Tonaufnahmen aus dem Internet in den Abgleich einbezogen werden, die den höchstpersönlichen Lebensbereich betreffen und ohne den Willen des Betroffenen in das Internet eingestellt wurden). Angebracht ist daher ein gesetzlicher Kernbereichsschutz.[31]

Insgesamt ist von einem erheblichen Grundrechtseingriff durch die in §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E vorgesehenen Maßnahmen auszugehen. Andererseits ist die mit den Regelungen angestrebte effektive Bekämpfung von Straftaten von großer verfassungsrechtlicher Bedeutung.[32] Eine der zentralen Aufgaben des Staates ist die Gewährleistung der Sicherheit der Bevölkerung, aus der der Staat als Institution „die eigentliche und letzte Rechtfertigung herleitet“.[33] Dass es ein praktisches Bedürfnis für eine polizeiliche Suche nach Straftätern und Störern mittels biometrischer Gesichtserkennung im Internet geben kann, zeigt der Fall Daniela Klette, bei dem ein investigativer Journalist mit einem Gesichtserkennungssystem Fotos der Ex-RAF-Terroristin im Internet gefunden hat.[34]

Es obliegt dem Gesetzgeber, einen angemessenen Ausgleich der verschiedenen Interessen herzustellen. Dabei sind hohe Anforderungen an die Bestimmtheit und Verhältnismäßigkeit der vorgesehenen Regelungen zu stellen. Anlass, Zweck und Grenzen des Eingriffs sind hinreichend bereichsspezifisch, präzise und normenklar festzulegen. Wesentliche Entscheidungen über die Eingriffsbefugnisse der Behörden und deren Reichweite muss der Gesetzgeber treffen.[35] Er muss mit den Reglungen zudem einen legitimen Zweck (dies ist hier ohne Zweifel der Fall) mit geeigneten, erforderlichen und angemessenen Mitteln verfolgen. Das Gewicht des Grundrechtseingriffs darf nicht außer Verhältnis zum Gewicht der damit

---

[26] BVerfGE 65, 1, 53; BVerfGE 27, 1, 6.

[27] BVerfGE 65, 1, 53.

[28] S. hierzu Hornung/Schindler, ZD 2017, 203, 206 zur Verbindung von Videoüberwachung mit Gesichtserkennung.

[29] BVerfGE 141, 220, 276 f.

[30] BVerfGE 80, 367, 374.

[31] S. BVerfGE 141, 220, 277 ff.; so auch BT-Drs. 20/12806, 25 f.

[32] S. z.B. BVerfGE 100, 313, 388 f.

[33] BVerfGE 49, 24, 56 f.

[34] S. z.B. https://www.ndr.de/nachrichten/niedersachsen/Gesichtserkennung-LKA-Praesident-fordert-Debatte-um-Software,gesichtserkennung134.html.

[35] Z.B. BVerfGE 120, 378, 407 f. zum Bestimmtheitsgebot.

verfolgten Ziele stehen.[36] Dabei sind ggf. verfahrens- und organisationsrechtliche Vorkehrungen zu treffen, um der Gefahr der Verletzung von Grundrechten entgegenzuwirken.[37]

Die §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E genügen in ihrer derzeitigen Form diesen Anforderungen nicht.

2.1.2 Bewertung einzelner Aspekte der vorgesehenen Regelungen

Die §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E regeln den nachträglichen biometrischen Abgleich durch das BKA, die BPOL sowie die Strafverfolgungsbehörden. Die Vorschriften ähneln sich hinsichtlich Inhalt und Aufbau, wobei § 98d StPO-E Abweichungen bei bestimmten Formulierungen aufweist.

2.1.2.1 Datenabgleich

§§ 10b Abs. 1, 39a Abs. 1, 63b Abs. 1 BKAG-E und § 34b Abs. 1 BPolG-E erlauben es, „biometrische Daten zu Gesichtern und Stimmen […] mit öffentlich zugänglichen personenbezogenen Daten aus dem Internet mittels einer automatisierten Anwendung zur Datenverarbeitung biometrisch ab[zu]gleichen“. § 98d Abs. 1 StPO-E ist diesbezüglich abweichend formuliert. Dort heißt es: „durch Erkennung des Gesichts und der Stimme dürfen deren biometrische Daten […] mit biometrischen Daten aus im Internet öffentlich zugänglichen Lichtbild- und Videodateien nachträglich mittels einer automatisierten Anwendung zur Datenverarbeitung abgeglichen werden“. Fraglich ist, ob diese sprachlichen Abweichungen Absicht sind. Die unterschiedlichen Formulierungen könnten zu Rechtsunsicherheiten führen und sollten – so dasselbe gemeint ist – auch sprachlich angeglichen werden. Vorzugswürdig scheint dabei, da präziser, die Formulierung „aus im Internet öffentlich zugänglichen Lichtbild- und Videodateien“ anstelle von „öffentlich zugänglichen personenbezogenen Daten aus dem Internet“.

Bei § 98d Abs. 1 StPO-E ist auffällig, dass nur von „Lichtbild- und Videodateien“ gesprochen wird, während laut der Gesetzesbegründung auch ein Abgleich mit Audiodateien möglich sein soll.[38] Für letzteres spricht auch, dass eine Erkennung der Stimme erfolgen darf. Dies sollte angepasst werden.

2.1.2.1.1 Biometrischen Daten zu Gesichtern und Stimmen

Mit Blick auf das Bestimmtheitsgebot sollte gesetzlich definiert werden, was unter „biometrischen Daten“ zu verstehen ist. Naheliegend – aber nicht zwingend – ist eine Bezugnahme auf die Definition in Art. 3 Nr. 13 JI-RL (s.a. § 46 Nr. 12 BDSG). Die neue KI-VO enthält ebenfalls eine Definition biometrischer Daten in Art. 3 Nr. 34 KI-VO, die aber – trotz EG 14 KI-VO – von der Definition in der JI-RL (und der DSGVO) abweicht. Schon deshalb sollte klargestellt werden, was unter „biometrischen Daten“ zu verstehen ist.

Ebenfalls sollte (wenigstens durch Aussagen in der Gesetzesbegründung, die bei der Auslegung herangezogen werden können) geklärt werden:

- Darf auch mit Daten zu Gesichtern und Stimmen gesucht werden, wenn diese bearbeitet wurden? Denkbar wäre es z.B., eine Person, die auf einem alten Fahndungsfoto zu sehen ist, künstlich altern zu lassen, um dann mit diesem bearbeiteten Bild im Internet zu suchen.

[36] Z.B. BVerfGE 120, 378, 427 f. zum Grundsatz der Verhältnismäßigkeit.

[37] So bereits BVerfGE 65, 1, 44.

[38] BT-Drs. 20/12806, 24.

- Darf auch mit künstlich erstellten Fotos gesucht werden? Zu denken ist z.B. an ein Phantombild, das aufgrund einer Zeugenbeschreibung am Computer (evtl. unter Einsatz von KI) erstellt wurde.
- Umfassen „biometrische Daten zu Gesichtern" auch sog. softbiometrische Merkmale (Soft Biometrics[39])? Ist es z.B. erlaubt, mittels Beschreibung eines Gesichts im Internet zu suchen (z.B. Beschreibung von Hautfarbe, Geschlecht, Alter, Form von Mund und Nase, Augenfarbe)? Bei einem weiten Verständnis des Begriffs der biometrischen Daten eines Gesichts könnte dies ebenfalls erfasst sein.
- Ist es zulässig, mit unvollständigen Gesichtsbildern (z.B. Bilder, die nur einen Teil des Gesichts zeigen) im Internet zu suchen? Zur automatisierten Kennzeichenerkennung enthält z.B. § 14a Abs. 2 S. 4 HSOG die Vorgabe, dass ein Abgleich „nur mit vollständigen Kennzeichen" erfolgen darf.[40] Eine solche Vorgabe käme auch für die hier relevanten Vorschriften in Betracht.

Darf auch mit bearbeiteten, künstlich erstellten oder unvollständigen Bildern sowie aufgrund von Täterbeschreibungen im Internet gesucht werden, erhöht dies wahrscheinlich die Zahl der Trefferfälle, wobei aber viele Trefferfälle Fehlerkennungen sein werden, was wiederum das Risiko erhöht, dass unbeteiligte Personen Gegenstand weiterer Ermittlungen werden.

§§ 10b Abs. 1, 39a Abs. 1, 63b Abs. 1 BKAG-E sprechen davon, dass das es sich um biometrische Daten handeln muss, auf die das BKA „zur Erfüllung seiner Aufgaben zugreifen darf". Ähnliche Formulierungen finden sich in § 34b Abs. 1 BPolG-E („Berechtigung zum Abruf hat"). Es werden damit letztlich alle Daten erfasst, auf die die Behörden in irgendeiner Form zugreifen dürfen.[41] Ausgeschlossen sind – beim BKA – lediglich Daten, die durch einen verdeckten Einsatz technischer Mittel in oder aus Wohnungen oder verdeckten Eingriff in informationstechnische Systeme erlangt wurden, s. §§ 10b Abs. 3, 39a Abs. 6, 63b Abs. 6 BKAG-E i.V.m. § 12 Abs. 3 BKAG (§ 34b BPolG-E und § 98d StPO-E scheinen einen solchen Ausschluss nicht vorzusehen). Durch den Verweis auf § 12 Abs. 2 BKAG in §§ 10b Abs. 3, 39a Abs. 6, 63b Abs. 6 BKAG-E sollen überdies „die Vorgaben der hypothetischen Datenneuerhebung auf die gegenständliche Maßnahme übertragen" werden.[42] Die Bedeutung dieser Vorgabe ist unklar.

Es sollte präzisiert werden, aus welchen Quellen bzw. Beständen die Daten stammen dürfen (z.B. nur Daten aus bestimmten Fahndungsbeständen; vgl. z.B. die Vorschriften zum Fahndungsbestand bei der automatisierten Kennzeichenerkennung in § 14a Abs. 2 HSOG[43]). Derzeit fehlt es diesbezüglich an einer bereichsspezifischen und präzisen Regelung.

2.1.2.1.2 Öffentlich zugängliche personenbezogene Daten aus dem Internet

Der Abgleich darf bei §§ 10b Abs. 1, 39a Abs. 1, 63b Abs. 1 BKAG-E und § 34b Abs. 1 BPolG-E mit „öffentlich zugänglichen personenbezogenen Daten aus dem Internet" erfolgen. Die Formulierung ist sehr unbestimmt gefasst. Es sollte definiert werden, was unter „öffentlich

---

[39] S. https://en.wikipedia.org/wiki/Soft_biometrics.

[40] Im Folgenden wird des Öfteren auf die automatisierte Kennzeichenerkennung Bezug genommen, da diese in technischer Hinsicht mit der biometrischen Erkennung „verwandt" ist (es werden zwei oder mehr Datensätze auf Übereinstimmung hin abgeglichen).

[41] BT-Drs. 20/12806, 19 spricht bzgl. § 10b BKAG-E davon, „dass im Informationssystem oder -verbund Daten als Grundlage des Abgleichs vorhanden" sein müssen. Eine Beschränkung auf das Informationssystem (§ 13 BKAG) oder den Informationsverbund (§ 29 BKAG) ist im Wortlaut der Vorschrift (anders als in § 16a BKAG-E) aber nicht angelegt.

[42] BT-Drs. 20/12806, 19.

[43] S. dazu auch BVerfGE 120, 378, 409 ff.

zugänglichen […] Daten“ zu verstehen ist. Dies gilt auch für die „öffentlich zugänglichen Lichtbild- und Videodateien“ in § 98d StPO-E.

Eine allgemein anerkannte Definition öffentlich zugänglicher Daten gibt es nicht.[44] Die Gesetzesbegründung spricht insoweit von Daten, „die von jedermann verwendet werden können, beispielsweise aus sozialen Medien, soweit sich diese nicht an einen spezifisch abgegrenzten Personenkreis richten“.[45] Dies wirft die Frage auf, ob auch Daten erfasst werden, die erst nach Anmeldung bei einem sozialen Netzwerk oder einem vergleichbaren Online-Dienst einsehbar sind, wobei die Anmeldung grundsätzlich allen Personen offensteht. § 10 Abs. 5 S. 2 BDSG a.F. definierte Daten als „allgemein zugänglich“, wenn sie „jedermann, sei es ohne oder nach vorheriger Anmeldung, Zulassung oder Entrichtung eines Entgelts, nutzen kann.“ Dies würde dafürsprechen, auch Daten als öffentlich zugänglich zu verstehen, die erst nach einer Anmeldung abrufbar sind. Der Gesetzgeber sollte dies klären. Je weiter der Begriff der öffentlich zugänglichen Daten gefasst wird, desto stärker ist das Eingriffsgewicht, da die Menge der heranziehbaren Daten steigt.

Dem Wortlaut nach erlauben die §§ 10b Abs. 1, 39a Abs. 1, 63b Abs. 1 BKAG-E, § 34b Abs. 1 BPolG-E und § 98d Abs. 1 StPO-E den Abgleich mit allen „öffentlich zugänglichen personenbezogenen Daten aus dem Internet“ bzw. mit allen „mit biometrischen Daten aus im Internet öffentlich zugänglichen Lichtbild- und Videodateien“ (vorbehaltlich der immer zu beachtenden Verhältnismäßigkeit im Einzelfall). Weitere gesetzliche Einschränkungen sind nicht vorgesehen. Dies führt dazu, dass zahlreiche Personen betroffen sein können – potenziell alle Internetnutzer weltweit –, die weit überwiegend keinen Anlass für die Maßnahme gegeben haben, was das Eingriffsgewicht maßgeblich erhöht (s.o.).

Der Gesetzgeber sollte diesbezüglich Einschränkungen vorsehen. Zu denken ist etwa daran, dass der Abgleich je nach Situation nur Daten betreffen darf, die auf Servern in einem bestimmten Land oder einer bestimmten Region gehostet werden oder die über einen bestimmten Online-Dienst (z.B. Facebook, wenn bekannt ist, dass die gesuchte Person nur diesen Dienst nutzt) veröffentlicht wurden. Derartige gesetzliche Einschränkungen würden dazu führen, dass die Zahl der potentiell betroffenen Personen ggf. deutlich sinkt, was das Eingriffsgewicht verringert. Es sind sicher auch andere Arten der Einschränkung denkbar, aber es sollte auf jeden Fall nach Möglichkeit vermieden werden, dass bei jedem Abgleich potentiell alle Internetnutzer weltweit betroffen sind (vgl. diesbezüglich z.B. die – hier nicht ohne Weiteres übertragbaren – Einschränkungen in § 14a Abs. 1 S. 4 HSOG: „nicht flächendeckend“, „nur auf Bundesautobahnen und Europastraßen“ etc.).

Problematisch ist zudem, dass die „öffentlich zugänglichen personenbezogenen Daten aus dem Internet“ bzw. die „im Internet öffentlich zugänglichen Lichtbild- und Videodateien“ auch Daten umfassen können, die gegen den Willen der betroffenen Person und ggf. unter Verletzung strafrechtlicher Vorschriften in das Internet gelangt sind und nun Teil des Abgleichs werden (s.o.). Es ist zu überlegen, ob es technische Verfahren gibt, die die Heranziehung solcher Daten nach Möglichkeit ausschließen. Sollten solche technischen Verfahren existieren bzw. realisierbar sein, sollte ihre Verwendung gesetzlich vorgeschrieben werden. Die Heranziehung solcher Daten ist nach Möglichkeit auszuschließen.

2.1.2.1.3 Abgleich mittels einer automatisierten Anwendung zur Datenverarbeitung

§§ 10b Abs. 1, 39a Abs. 1, 63b Abs. 1 BKAG-E, § 34b Abs. 1 BPolG-E und § 98d Abs. 1 StPO-E erlauben es, die genannten Daten „mittels einer automatisierten Anwendung zur

[44] S.a. Hornung/Gilga, CR 2020, 367, 369.

[45] BT-Drs. 20/12806, 18.

Datenverarbeitung biometrisch ab[zu]gleichen“ (bzw. dass sie „mittels einer automatisierten Anwendung zur Datenverarbeitung abgeglichen werden“).

Das BVerfG verlangt, dass der Gesetzgeber „technische Eingriffsinstrumente genau bezeichnet“, was aber nicht so konkret sein muss, dass die Formulierungen „jede Einbeziehung kriminaltechnischer Neuerungen ausschließen“.[46] Die Regelung technischer Details (z.B. genau bezeichnete technische Spezifikationen) ist nicht erforderlich. Allerdings sind die in §§ 10b Abs. 1, 39a Abs. 1, 63b Abs. 1 BKAG-E, § 34b Abs. 1 BPolG-E und § 98d Abs. 1 StPO-E verwendeten Formulierungen („mittels einer automatisierten Anwendung zur Datenverarbeitung biometrisch abgleichen“) angesichts des erheblichen Eingriffsgewichts der vorgesehenen Maßnahmen zu unbestimmt.[47] Die gesetzlichen Vorgaben zur Durchführung des Abgleichs sollten spezifiziert und konkretisiert werden. Es sollte aus den gesetzlichen Formulierungen in Grundzügen hervorgehen, wie der Abgleich in technischer Hinsicht abzulaufen hat. Dabei sollte unter anderem erkennbar sein, ob die „öffentlich zugänglichen personenbezogenen Daten aus dem Internet“ für den Abgleich zunächst heruntergeladen und bei den Behörden gespeichert werden dürfen. Die Speicherung würde einen zusätzlichen Grundrechtseingriff darstellen. So dies erlaubt sein soll, stellt sich die Frage, wie damit umzugehen ist, dass dabei möglicherweise Daten gespeichert werden, die strafrechtlich anderweitig relevant sind (s.o.). Die gewählten Formulierungen sollten zudem deutlich machen, dass es nicht zu einer Erstellung von „Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet“ (Art. 5 Abs. 1 UAbs. 1 lit. e KI-VO) kommen darf, um mögliche Verstöße gegen die KI-VO auszuschließen (s.u.).

Aufgrund der Fehleranfälligkeit biometrischer Erkennung (s.o.) könnte ferner vorgeschrieben werden, dass nur Erkennungssysteme verwendet werden dürfen, die hinsichtlich der Erkennungsgenauigkeit vorab festgelegten Qualitätsstandards genügen bzw. ein Zertifizierungsverfahren durchlaufen haben. Dabei sollte insbesondere sichergestellt werden, dass die Systeme bei Menschen unterschiedlichen Alters und Geschlechts (etc.) gleichgut funktionieren, um mögliche Diskriminierungen auszuschließen.

Mit Blick auf die Entscheidung des BVerfG zur automatisierten Datenanalyse[48] wäre es problematisch, wenn bei dem Abgleich gem. §§ 10b Abs. 1, 39a Abs. 1, 63b Abs. 1 BKAG-E, § 34b Abs. 1 BPolG-E und § 98d Abs. 1 StPO-E selbstlernende Systeme zum Einsatz kommen würden. In der Entscheidung hat das Gericht bei „der automatisierten Datenanalyse oder -auswertung“, die „im Vorfeld einer konkretisierten Gefahr“ stattfinden soll, verlangt, dass der Einsatz selbstlernender Systeme im Gesetz ausdrücklich ausgeschlossen sein muss.[49] Es sollte geprüft werden, inwieweit diese Rechtsprechung hier relevant ist, da die §§ 10b, 39a, 63b BKAG-E und § 34b BPolG-E ein Tätigwerden auch im Gefahrenvorfeld erlauben.

Die §§ 10b Abs. 1, 39a Abs. 1, 63b Abs. 1 BKAG-E, § 34b Abs. 1 BPolG-E und § 98d Abs. 1 StPO-E sehen vor, dass ein Abgleich mit Daten „aus im Internet öffentlich zugänglichen Echtzeit-Lichtbild- und Echtzeit-Videodateien […] ausgeschlossen“ ist. Damit soll ein Abgleich mit „Live-Streams“ und „Live-Video einer Webcam eines öffentlich zugänglichen

---

[46] BVerfGE 112, 304, 316.

[47] In der Gesetzesbegründung heißt es dazu: „Unter einem biometrischen Abgleich im Sinne der Vorschrift ist die technisch gestützte Überprüfung der Übereinstimmung von biometrischen Signaturen mit dem Ergebnis einer Übereinstimmungsbewertung zu verstehen.“, BT-Drs. 20/12806, 18. Was in diesem Zusammenhang unter „biometrischen Signaturen“ zu verstehen ist, ist unklar. Der Begriff wird – soweit ersichtlich – vor allem im Kontext elektronischer Unterschriften verwendet, s. z.B. https://www.validatedid.com/de/biometrische-signatur. Es sollte ein anderer Begriff verwendet werden, um Rechtsunsicherheiten vorzubeugen.

[48] BVerfGE 165, 363.

[49] BVerfGE 165, 363, 418.

Ortes“ ausgeschlossen werden.[50] Dies ist zu begrüßen. Da die Vorschriften auch einen Abgleich mit biometrischen Daten zu Stimmen erlauben, sollte der Abgleich mit Echtzeit-Audioaufnahmen und -dateien ebenfalls explizit ausgeschlossen werden. Dass der Abgleich nur „nachträglich“ zulässig ist, ergibt sich auch aus den Überschriften von §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E. Im Gesetzestext findet dies aber nur in § 98d Abs. 1 StPO-E Erwähnung („nachträglich mittels einer automatisierten Anwendung“). Dies sollte für die anderen Regelungen übernommen werden, um mehr Klarheit zu schaffen.

Soweit die Gesetzesbegründung darauf abstellt, dass bei Live-Veranstaltungen ggf. „auch das Publikum erfasst wird“,[51] bleibt festzuhalten, dass dies ohne Weiteres auch bei aufgezeichneten Aufnahmen, mit denen ein Abgleich zulässig ist, der Fall sein kann. Generell ist der Übergang vom Echtzeit-Abgleich (im Sinne von live bzw. verzögerungsarm[52]) zum nachträglichen Abgleich fließend. Wird etwa ein Video aufgezeichnet und mit einer gewissen Verzögerung, z.B. am nächsten Tag, für den Abgleich herangezogen, mag es sich nicht mehr um einen „Abgleich mit […] Echtzeit-Lichtbild- und Echtzeit-Videodateien“ im Sinne der genannten Vorschriften handeln; die Auswirkungen auf die betroffenen Personen und die Erkenntnisse, die dadurch gewonnen werden können, sind aber im Zweifel dieselben. Entscheidend ist in solchen Fällen daher nicht so sehr, wann der Abgleich stattfindet, sondern in welchem Umfang (das ganze Video oder nur Teile davon, Zahl der betroffenen Personen etc.) dies erfolgt.

2.1.2.1.4 Eingriffsschwelle

Der Abgleich ist gem. § 10b Abs. 1 BKAG-E und § 98d Abs. 1 StPO-E zulässig, wenn eine Straftat im Sinne des § 100a Abs. 2 StPO bekämpft werden soll. § 100a Abs. 2 StPO enthält neben sehr schweren Straftaten (z.B. Mord und Totschlag gem. §§ 211, 212 StGB, s. § 100a Abs. 2 Nr. 1 lit. h StPO), deren Bekämpfung es grundsätzlich rechtfertigen kann, biometrische Daten zu Gesichtern und Stimmen mit öffentlich zugänglichen personenbezogenen Daten aus dem Internet abzugleichen, auch weit weniger schwerwiegende Straftaten (z.B. Bandendiebstahl, Sportwettbetrug und Verstöße gegen das Konsumcannabisgesetz, § 100a Abs. 2 Nr. 1 lit. j und p, Nr. 7a StPO), deren Bekämpfung nicht so gewichtig ist, dass sie die in § 10b Abs. 1 BKAG-E und § 98d Abs. 1 StPO-E vorgesehenen eingriffsintensiven Maßnahmen rechtfertigen kann. Die Bezugnahme auf § 100a Abs. 2 StPO geht somit zu weit. Die zu bekämpfenden Straftaten sind auf sehr schwere Straftaten zu beschränken, z.B. auf Straftaten im Sinne von § 138 StGB oder auf die in § 129a StGB aufgeführten Straftaten – ggf. auch noch strenger. Dies würde auch besser zum Titel des Gesetzesentwurfs passen, der auf die Terrorismusbekämpfung („Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung“) und nicht auf die Bekämpfung von Bandendiebstählen, Betrügereien bei Sportwetten oder Verstößen gegen das Konsumcannabisgesetz abstellt.

Die §§ 10b, 39a, 63b BKAG-E und § 34b BPolG-E erlauben zudem ein Tätigwerden im Vorfeld konkreter Gefahren (z.B. wenn „das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine Straftat nach § 5 Absatz 1 Satz 2 begehen wird“). Dies ist nach der Rechtsprechung des BVerfG grundsätzlich zulässig.[53] Im Gegenzug sollten die Befugnisse der Behörden dann aber auch sehr bestimmt gefasst werden, was hier nicht immer der Fall ist (s.o. und s.u.).

---

[50] BT-Drs. 20/12806, 18 und 25.

[51] BT-Drs. 20/12806, 18.

[52] Echtzeit meint wohl eigtl. etwas anderes, wird hier aber erkennbar im Sinne von „live“ verwendet, s. https://de.wikipedia.org/wiki/Echtzeit. Ggf. sollte deutlich gemacht werden, was unter Echtzeit zu verstehen ist.

[53] BVerfGE 141, 220, 272 f.

Die in den Regelungen vorgesehenen Subsidiaritätsklauseln („auf andere Weise aussichtslos oder wesentlich erschwert wäre“) sind grundsätzlich zu begrüßen. Sie sollten – zumindest bei § 98d StPO-E – aber dahingehend verschärft werden, dass der biometrische Abgleich nur zulässig ist, wenn die Zielerreichung „auf andere Weise aussichtslos wäre“. Dies würde dazu beitragen, dass es sich um eine Maßnahme handelt, die nur ergriffen werden darf, wenn andere Maßnahmen ausgeschöpft wurden.

2.1.2.2 Erhebung und Verarbeitung von Daten im Treffer- und Nichttrefferfall

Wird beim Abgleich „biometrische[r] Daten zu Gesichtern und Stimmen“ mit „öffentlich zugänglichen personenbezogenen Daten aus dem Internet“ (bzw. „biometrische[n] Daten aus einem Strafverfahren mit biometrischen Daten aus im Internet öffentlich zugänglichen Lichtbild- und Videodateien“) ein Treffer erzielt, können Informationen über die betroffene Person gewonnen werden (wird die Person z.B. in einem Video aufgefunden, das erkennbar zu einer bestimmten Zeit an einem bestimmten Ort gefertigt wurde, ergibt sich daraus, dass die Person zu dieser Zeit an diesem Ort war).

Die §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E regeln nicht, ob und in welchem Umfang Daten im Rahmen des Abgleichs erhoben und gespeichert werden dürfen (auch wenn sich eine gewisse Eingrenzung aus der Zielsetzung ergibt, eine Person zu identifizieren oder ihren Aufenthaltsort zu ermitteln). Ein Rückgriff auf die allgemeinen Generalklauseln zur Datenverarbeitung verbietet sich, da es um die Regelung spezifischer Eingriffsbefugnisse geht. Es sollte daher gesetzlich geregelt werden, welche Daten erhoben und gespeichert werden dürfen – und damit auch, welche nicht. So bestimmt z.B. § 14a Abs. 4 S. 1 HSOG bzgl. der automatisierten Kennzeichenerkennung, dass im Trefferfall „das Kennzeichen, die Bildaufzeichnung des Fahrzeugs sowie Angaben zu Ort, Fahrtrichtung, Datum und Uhrzeit gespeichert werden“ dürfen. Damit reagierte der Gesetzgeber auf die Kritik des BVerfG, dass in der ursprünglichen Vorschrift nicht geregelt war, „welche Daten überhaupt erhoben werden dürfen“.[54] Dabei gilt: Je mehr Informationen erhoben werden dürfen, desto schwerer wird der zu rechtfertigende Grundrechtseingriff und desto schwieriger ist die Wahrung der Verhältnismäßigkeit.

Werden Informationen aus verschiedenen Trefferfällen zusammengefügt, kann dies unter Umständen Rückschlüsse auf das Bewegungsverhalten der betroffenen Person (z.B. bei Bildaufnahmen, die sie an verschiedenen Orten zeigen) oder ihre persönlichen Vorlieben (z.B. Bilder, die die Person bei bestimmten Tätigkeiten zeigen) ermöglichen. Werden diese Erkenntnisse zusammengetragen, kann dies weitreichende Erkenntnisse über die betroffene Person vermitteln. So dies zulässig sein soll, steigert dies die Persönlichkeitsrelevanz – und damit das Eingriffsgewicht – der vorgesehenen Maßnahmen erheblich (s.o.). Im Interesse der Wahrung der Verhältnismäßigkeit ist daher zu überlegen, ein solches Vorgehen explizit auszuschließen. So schreibt z.B. § 14a Abs. 2 S. 5 HSOG für die automatisierte Kennzeichenerkennung vor, dass „Bewegungsbilder […] nicht erstellt werden [dürfen]“.

Dass die §§ 10b Abs. 7, 39a Abs. 7, 63b Abs. 7 BKAG-E, § 34b Abs. 6 BPolG-E und § 98d Abs. 5 StPO-E bestimmen, dass im Rahmen des Abgleichs erhobene Daten nach Durchführung des Abgleichs unverzüglich zu löschen sind, soweit sie keinen konkreten Ermittlungsansatz aufweisen, ist zu begrüßen. Es sollte dann aber auch – wie bereits angesprochen – geregelt werden, welche Daten im Rahmen des Abgleichs überhaupt erhoben werden dürfen. Die

[54] BVerfGE 120, 378, 425.

Regelungen über die Löschung sollten zudem sicherstellen, dass in Nichttrefferfällen keine irgendwie gearteten personenbezogenen Daten dauerhaft gespeichert werden dürfen.[55]

Der in §§ 10b Abs. 6, 39a Abs. 5, 63b Abs. 5 BKAG-E, § 34b Abs. 5 BPolG-E und § 98d Abs. 4 StPO-E vorgesehene Kernbereichsschutz ist zu begrüßen, insbesondere auch, weil ggf. Daten in den Abgleich einbezogen werden können, die gegen den Willen des Betroffenen in das Internet eingestellt wurden (s.o.).[56]

2.1.2.3 Menschliche Kontrolle

Biometrische Erkennung kann je nach Situation sehr fehleranfällig sein (s.o.). Werden Fehlerkennungen zur Grundlage polizeilicher Maßnahmen, kann dies für die betroffenen Personen negative Folgen haben und sie erheblich beeinträchtigen (s.o.). Im Zusammenhang mit der Durchführung des Abgleichs sollte daher gesetzlich vorgeschrieben werden, dass alle ermittelten Treffer unverzüglich durch eine qualifizierte Person, die insbesondere die technischen Grenzen der eingesetzten Verfahren kennt, überprüft werden müssen. Alle Nichttreffer sind durch diese Person unverzüglich zu löschen. Zudem ist vorzusehen, dass weitere Maßnahmen (z.B. Veranlassung der Festnahme einer Person) erst im Anschluss an die menschliche Überprüfung erfolgen dürfen (vgl. insoweit § 14a Abs. 4 S. 3 HSOG: „Weitere Maßnahmen dürfen erst nach Überprüfung des Trefferfalls anhand des aktuellen Fahndungsbestands erfolgen.“).

2.1.2.4 Adressaten

§ 10b Abs. 2 BKAG-E lautet: „Die Maßnahme nach Absatz 1 Satz 1 darf gegen die in § 18 Absatz 1 sowie § 19 Absatz 1 Satz 1 Nummer 1 und 2 bezeichneten Personen durchgeführt werden.“ Die Regelung erscheint hinsichtlich der einbezogenen Personenkreise fragwürdig. Zu den aufgeführten Personen gehören Verurteilte, Beschuldigte, Verdächtige und Anlasspersonen (§ 18 Abs. 1 BKAG) sowie Personen, die als künftige Zeugen oder Opfer in Betracht kommen (§ 19 Abs. 1 S. 1 Nr. 1 und 2 BKAG). Vergleichbare Formulierungen finden sich in §§ 39a Abs. 2, 63b Abs. 2 BKAG-E und § 34b Abs. 2 BPolG-E, die auf die auf §§ 17, 18 und 20 BPolG verweisen. Es sollte kritisch geprüft werden, ob der Personenkreis insgesamt zu weit gefasst ist. Dies gilt etwa für die Inanspruchnahme von Nichtstörern gem. § 20 BPolG i.V.m. §§ 39a Abs. 2, 63b Abs. 2 BKAG-E und § 34b Abs. 2 BPolG-E. Ggf. sind dann aber jedenfalls höhere Anforderungen an die Durchführung der Maßnahme zu stellen.

2.1.2.5 Antrag und Anordnung durch ein Gericht

Soweit §§ 10b Abs. 4, 39a Abs. 3, 63b Abs. 3 BKAG-E bestimmen, dass die Maßnahmen „nur auf Antrag der zuständigen Abteilungsleitung durch das Gericht angeordnet werden“ dürfen, ist der darin enthaltene Richtervorbehalt grundsätzlich zu begrüßen. Dies gilt auch für § 34b Abs. 3 BPolG-E und § 98d Abs. 2 StPO-E.

Fraglich ist allerdings, ob es bei einem nachträglichen Abgleich der Regelungen zur Anordnung durch die Abteilungsleitung bzw. die Staatsanwaltschaft bei Gefahr im Verzug bedarf. Jedenfalls sollte vorgeschrieben werden, dass alle ggf. bereits erhobenen Daten unverzüglich zu löschen sind, wenn das Gericht die Anordnung nicht bestätigt. Dies ist – so scheint es – nur in § 98d Abs. 5 S. 3 StPO-E ausdrücklich geregelt.

Bzgl. der Regelungen in §§ 10b Abs. 4, 39a Abs. 3, 63b Abs. 3 BKAG-E stellt sich die Frage, ob auch die Vertretung der Abteilungsleitung antragsbefugt sein soll, wie dies z.B. in § 55

[55] S.a. BT-Drs. 20/12806, 26 f. bzgl. der Einbeziehung von § 98d StPO-E in die Aufzählung der Maßnahmen in § 101 StPO.

[56] S.a. BT-Drs. 20/12806, 25 f.

Abs. 3 BKAG geregelt ist. Soll dies nicht der Fall sein, sollte dies – zumindest in der Gesetzesbegründung – erwähnt werden, um Rechtsunsicherheiten zu vermeiden. Fraglich ist zudem, ob § 90 Abs. 1 BKAG ergänzt werden sollte.

Die §§ 10b Abs. 4, 39a Abs. 3, 63b Abs. 3 BKAG-E, § 34b Abs. 3 BPolG und § 98d Abs. 2 StPO-E enthalten keine Vorgaben zur zulässigen Dauer der gerichtlichen Anordnung bzw. der Maßnahme. Zu überlegen ist, ob eine zeitliche Befristung der Anordnung vorgesehen werden sollte, vgl. z.B. § 55 Abs. 6 S. 2 BKAG.

Allgemein ergibt sich aus §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E nicht, wie oft und in welchem zeitlichen Rahmen der biometrische Abgleich durchgeführt werden darf. In der Gesetzesbegründung heißt es diesbezüglich: „Die Anordnung kann lediglich als Rechtsgrundlage für einen einzelnen, technisch fehlerfreien Abgleichvorgang dienen. Wiederholte, sich gar einer Echtzeitüberwachung annähernde Such- und Abgleichvorgänge sind nicht zulässig.“[57] Dieses Verständnis ist zu begrüßen, da es den Umfang der Maßnahme – und damit auch das Eingriffsgewicht – einschränkt, sollte sich aber im Gesetzeswortlaut wiederfinden.

2.1.2.6 Outsourcing an private Unternehmen

Es ist grundsätzlich denkbar, die Durchführung des in §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E geregelten biometrischen Abgleichs an ein privates Unternehmen auszulagern, das im Auftrag der Behörden tätig wird. Dies wäre allerdings sehr kritisch zu sehen, da Strafverfolgung und Gefahrenabwehr hoheitliche Aufgaben sind. Die Einbindung privater Unternehmen oder Stellen in den Abgleich und die Auswertung der Daten sollte daher explizit ausgeschlossen werden.

2.1.2.7 Zeitlich begrenzter Geltung, Berichts- und Evaluationspflichten

Aufgrund des Umstandes, dass es sich bei der biometrischen Erkennung um ein vergleichsweise neues und auch potentiell fehleranfälliges Verfahren handelt, sollte die Geltung der §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E zeitlich begrenzt werden.

Zudem sollten Berichtspflichten der ausführenden Behörden gegenüber dem Parlament und der Öffentlichkeit vorgesehen werden, um eine öffentliche Diskussion über Art und Ausmaß der auf diese Befugnisse gestützten Maßnahmen zu ermöglichen.[58] Gem. § 98d Abs. 6 S. 2 StPO-E, ist nach Beendigung der Maßnahme „die Stelle zu unterrichten, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz bei öffentlichen Stellen zuständig ist“.[59] Diese sinnvolle Regelungen scheint bei bei §§ 10b, 39a, 63b BKAG-E und § 34b BPolG-E nicht vorgesehen zu sein. Dies sollte geändert werden.

Überdies sollte vorgesehen werden, dass die Vorschriften bzw. die auf ihrer Grundlage durchgeführten Maßnahmen nach Ablauf einer bestimmten Zeit unter Hinzuziehung unabhängiger wissenschaftlicher Einrichtungen zu evaluieren sind. Dabei sollte ergebnisoffen geprüft werden, ob die Vorschriften die in sie gesetzten Erwartungen erfüllt haben oder aber ob sie nutzlos sind und/oder zu übermäßigen Grundrechtseingriffen geführt haben und daher abgeschafft werden sollten.

2.1.3 Überwachungsgesamtrechnung

In seiner Entscheidung zur Vorratsdatenspeicherung hat das BVerfG ausgesprochen, dass „die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf“, da dies der

[57] BT-Drs. 20/12806, 19 und 25

[58] S. dazu BVerfGE 141, 220, 285.

[59] S. dazu BT-Drs. 20/12806, 26.

„verfassungsrechtlichen Identität der Bundesrepublik Deutschland“ widerspricht. Die Speicherung von Telekommunikationsverkehrsdaten könne „nicht als Vorbild für die Schaffung weiterer vorsorglich anlassloser Datensammlungen dienen“. Vielmehr sei der Gesetzgeber gezwungen, „bei der Erwägung neuer Speicherungspflichten oder -berechtigungen in Blick auf die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen […] größere Zurückhaltung“ walten zu lassen.[60]

Diese Rechtsprechung wird in Teilen der Literatur dahingehend verstanden, dass das BVerfG eine „Gesamtbetrachtung des Stands staatlicher Überwachung“[61] fordere. Der Gesetzgeber habe eine „Überwachungsgesamtrechnung“[62] durchzuführen, was eine „doppelte Verhältnismäßigkeitsprüfung“ erfordere: Zum einen müsse jede Überwachungsmaßnahme für sich gesehen bzgl. ihrer Verhältnismäßigkeit überprüft werden. Zum anderen sei im Rahmen einer Gesamtbetrachtung aller verfügbaren Überwachungsmaßnahmen die Verhältnismäßigkeit der daraus resultierenden Gesamtbelastung geschützter Freiheiten zu prüfen.[63]

Der aktuelle Koalitionsvertrag enthält ein Bekenntnis zur Überwachungsgesamtrechnung.[64] Dem Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht wurde die Aufgabe erteilt, eine solche Gesamtrechnung zu erstellen.[65] Inwieweit Überlegungen zur Überwachungsgesamtrechnung in die Regelungen in §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E eingeflossen sind, ist nicht erkennbar, wäre mit Blick auf den Koalitionsvertrag aber wünschenswert.

2.2 JI-Richtlinie

2.2.1 Anwendungsbereich

Die vorgesehenen Regelungen in §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E fallen in den Anwendungsbereich der Richtlinie (EU) 2016/680 (JI-RL), die die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, regelt (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 JI-RL).[66] Die Richtlinie ist in innerstaatliches Recht umzusetzen (Art. 288 AEUV). Nationalstaatliche Regelungen, die in ihren Anwendungsbereich fallen, müssen ihren Vorgaben genügen.

2.2.2 Rechtmäßigkeit der Verarbeitung

Gem. Art. 8 JI-RL bedarf es einer Rechtsgrundlage, aus der sich die Ziele der Verarbeitung, die personenbezogenen Daten, die verarbeitet werden sollen, und die Zwecke der Verarbeitung ergeben. Dies spricht dafür, dass genau geregelt werden sollte, welche personenbezogenen Daten durch den Abgleich erhoben werden und wie sie weiterverarbeitet werden dürfen (s. dazu bereits oben). Soweit biometrische Daten im Sinne von Art. 3 Nr. 13 JI-RL verarbeitet werden, wovon bei den vorgesehenen Regelungen auszugehen ist, ist die Verarbeitung gem. Art. 10 JI-RL „nur dann erlaubt, wenn sie unbedingt erforderlich ist und vorbehaltlich geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person erfolgt“. Dies macht deutlich,

[60] BVerfGE 125, 260, 324.

[61] Roßnagel, NJW 2010, 1238, 1240.

[62] Roßnagel, NJW 2010, 1238, 1242.

[63] Roßnagel, NJW 2010, 1238, 1240.

[64] Koalitionsvertrag 2021-2025, 86 f.; s.a. Löffelmann, GSZ 2024, 18.

[65] S. https://netzpolitik.org/2024/ueberwachungsgesamtrechnung-jetzt-gehts-los.

[66] Zum Anwendungsbereich Hornung/Schindler/Schneider, ZIS 2018, 566.

dass die Verarbeitung auf das absolut Notwendige zu beschränken ist. Der Gesetzgeber sollte prüfen, ob dies bei den vorgesehenen Regelungen tatsächlich der Fall ist.

2.2.3 Weitere Vorgaben

Gem. Art. 11 JI-RL sind Entscheidungen, die ausschließlich auf einer automatischen Verarbeitung personenbezogener Daten beruhen, grundsätzlich verboten. Dass eine solche automatisierte Entscheidung beim biometrischen Abgleich gegeben sein kann, kann angesichts der Rechtsprechung des EuGH zur Erstellung von Score-Werten nicht von vornherein ausgeschlossen werden.[67] Dies spricht dafür, dass Vorgaben zur menschlichen Aufsicht und Kontrolle vorgesehen werden sollten, um zu verhindern, dass hervorgebrachte Ergebnisse ausschließlich auf der automatischen Verarbeitung personenbezogener Daten beruhen (s. dazu bereits oben).

Art. 13 i.V.m. Art. 12 JI-RL verpflichtet zur Einhaltung von Informationspflichten. Demnach ist in den nationalen Regelungen vorzusehen, dass betroffenen Personen bestimmte Informationen zur Verfügung gestellt werden. Es sollte überprüft werden, ob die Regelungen in §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E (ggf. im Zusammenspiel mit den weiteren Vorschriften im BKAG, BPolG, StPO und BDSG) diesen Vorgaben tatsächlich entsprechen. Zumindest im Zusammenhang mit § 98d StPO-E sind Informationspflichten durch Anpassung von § 101 StPO vorgesehen. Es sollte zudem geprüft werden, ob die Regelungen die weiteren Betroffenenrechte in Art. 12 ff. JI-RL beachten. Generell – dies ergibt sich auch aus grundrechtlichen Anforderungen – ist die Durchführung der Maßnahme möglichst transparent zu gestalten. Informationen über durchgeführte Maßnahmen können z.B. auch auf der Website der Behörden veröffentlicht werden (EG 39 JI-RL).

Art. 25 JI-RL verlangt, „dass in automatisierten Verarbeitungssystemen zumindest die folgenden Verarbeitungsvorgänge protokolliert werden: Erhebung, Veränderung, Abfrage, Offenlegung einschließlich Übermittlung, Kombination und Löschung. Die Protokolle über Abfragen und Offenlegungen müssen es ermöglichen, die Begründung, das Datum und die Uhrzeit dieser Vorgänge und so weit wie möglich die Identifizierung der Person, die die personenbezogenen Daten abgefragt oder offengelegt hat, und die Identität des Empfängers solcher personenbezogenen Daten festzustellen.“ Es sollte geprüft werden, ob die Protokollierungspflichten in §§ 10b Abs. 8, 39a Abs. 8, 63b Abs. 8 BKAG-E, § 34b Abs. 7 BPolG-E und § 98d Abs. 6 StPO-E (ggfs. im Zusammenspiel mit den weiteren Vorschriften im BKAG, BPolG, StPO und BDSG, s. etwa § 81 BKAG, § 76 BDSG) diesen Vorgaben genügen.

Es sollte insgesamt geprüft werden, ob möglicherweise weitere Vorgaben der JI-RL zu beachten sind.

2.3 Verordnung über künstliche Intelligenz

Die Verordnung über künstliche Intelligenz (KI-VO)[68] ist am 1.8.2024 in Kraft getreten. Sie gilt grundsätzlich ab dem 2.8.2026, wobei im Einzelnen Abweichungen vorgesehen sind (Art. 113 KI-VO). Als EU-Verordnung gilt die KI-VO unmittelbar (Art. 288 AEUV) und genießt Anwendungsvorrang vor entgegenstehendem nationalen Recht.

Die KI-VO folgt einem risikobasierten Ansatz (EG 26 KI-VO) und stellt an unterschiedliche KI-Systeme (und teilweise KI-Modelle) unterschiedliche Anforderungen. Dies betrifft insbesondere die verbotenen Praktiken im KI-Bereich (Art. 5 KI-VO), Hochrisiko-KI-Systeme

[67] S. EuGH, NZA 2024, 45.

[68] Verordnung (EU) 2024/1689.

(Art. 6 ff. KI-VO), KI-Modelle mit allgemeinem Verwendungszweck (Art. 51 ff. KI-VO) sowie Transparenzpflichten für Anbieter und Betreiber bestimmter KI-Systeme (Art. 50 KI-VO).

Fraglich ist, ob die Regelungen in §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E mit der KI-VO in Konflikt geraten. Diesbezüglich sei vorangestellt, dass es derzeit keine Rechtsprechung, keine Leitlinien der Kommission (Art. 96 KI-VO) und auch keine Äußerungen der (gem. Art. 70 KI-VO erst noch zu bestimmenden) nationalen Aufsichtsbehörden gibt. Bei den folgenden Ausführungen handelt es sich somit um vorsichtige vorläufige Einschätzungen.

2.3.1 Anwendungsbereich

Die KI-VO ist insbesondere auf Anbieter und Betreiber von KI-Systemen mit Unionsbezug anwendbar (Art. 2 Abs. 1 lit. a und b KI-VO). Zentral ist damit die Frage, ob bei Maßnahmen nach §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E KI-Systeme zum Einsatz kommen. Dies ist weder von den in den genannten Vorschriften verwendeten Formulierungen („mittels einer automatisierten Anwendung zur Datenverarbeitung“ etc.) noch von einem allgemeinen Verständnis des Begriffs der KI abhängig. Entscheidend ist vielmehr, ob die von den Behörden konkret eingesetzten Systeme KI-Systeme im Sinne von Art. 3 Nr. 1 KI-VO sind.

Ein KI-System im Sinne von Art. 3 Nr. 1 KI-VO[69] ist „ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können“. Was dies konkret bedeutet, ist momentan unklar. In der Literatur werden diesbezüglich sehr unterschiedliche Ansätze vertreten.[70] Eine gewisse Klarheit werden erst die Leitlinien der Kommission gem. Art. 96 Abs. 1 UAbs. 1 S. 1 lit. f KI-VO bringen. Im Folgenden wird unterstellt, dass es sich bei den im Rahmen von §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E eingesetzten biometrischen Erkennungs-Systemen um KI-Systeme handelt.[71] Die Behörden wären dann Betreiber (und ggf. auch Anbieter) dieser KI-Systeme (Art. 2 Abs. 1 lit. a und b i.V.m. Art. 3 Nr. 3 und 4 KI-VO).

Die KI-VO gilt gem. Art. 2 Abs. 3 KI-VO nicht in Bereichen, die nicht unter das Unionsrecht fallen, „und berührt keinesfalls die Zuständigkeiten der Mitgliedstaaten in Bezug auf die nationale Sicherheit“. Die nationale Sicherheit betrifft nach der Rechtsprechung des EuGH „den Schutz der grundlegenden Funktionen des Staates und der grundlegenden Interessen der Gesellschaft“,[72] z.B. vor „terroristische[n] Aktivitäten“.[73] Welche behördlichen Tätigkeiten und Maßnahmen dies im Einzelnen umfasst, ist umstritten.[74] Nationale Sicherheit ist jedenfalls tendenziell eng zu verstehen. Zu denken ist z.B. an bestimmte Tätigkeiten der Nachrichtendienste. Auch wenn der hier maßgebliche Gesetzentwurf die Terrorismusbekämpfung verbessern sollen („Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung“), ist doch nicht anzunehmen, dass die in ihm geregelten Befugnisse zur Bekämpfung bestimmter Straftaten mittels biometrischer Erkennung die nationale

[69] S. auch EG 12 KI-VO.

[70] Statt vieler Wendehorst/Nessler/Aufreiter/Aichinger, MMR 2024, 605, die dem Begriff des KI-Systems „Unbestimmtheit und geringe Überzeugungskraft“ attestieren.

[71] In BT-Drs. 20/12806, 25 wird die Möglichkeit erwähnt, „dass der Abgleich auch mittels eines KI-Systems erfolgen kann“.

[72] EuGH, BeckRS 2021, 15289 Rn. 67.

[73] EuGH, NJW 2021, 53, 538.

[74] S. BeckOK Datenschutzrecht/Bäcker, 49. Edition, DSGVO Art. 2 Rn. 9 ff. für Art. 2 Abs. 2 lit. a i.V.m. EG 16 DSGVO.

Sicherheit im Sinne von Art. 2 Abs. 3 KI-VO betreffen. Es handelt sich letztlich um „normales“ Polizei- und Strafverfahrensrecht, das nicht unter die Ausnahme in Art. 2 Abs. 3 KI-VO fällt. Somit ist von der Anwendbarkeit der KI-VO auszugehen.

2.3.2 Verbotene Praktiken im KI-Bereich

Fraglich ist, ob die in §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E geregelten Verfahren – so dabei KI-Systeme zum Einsatz kommen (s.o.) – zu den verbotenen Praktiken im Sinne von Art. 5 KI-VO gehören können. Dies hätte zur Folge, dass ihr Einsatz („Verwendung“) mit Geltung der KI-VO unzulässig wäre.

2.3.2.1 Biometrische Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen

Art. 5 Abs. 1 UAbs. 1 lit. h KI-VO verbietet die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme (Art. 3 Nr. 42 KI-VO) in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken (Art. 3 Nr. 46 und 45 KI-VO), wobei aber Ausnahmen gesetzlich vorgesehen werden können. Art. 3 Nr. 44 KI-VO versteht unter einem öffentlich zugänglichen Ort „einen einer unbestimmten Anzahl natürlicher Personen zugänglichen physischen Ort“. Die §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E regeln den biometrischen Abgleich im Internet, also im digitalen – d.h. nicht-physischen – Raum. Die dafür eingesetzten Erkennungssysteme befinden sich in den Räumlichkeiten der ausführenden Behörden (BKA, BPOL etc.) und sind nicht einer unbestimmten Anzahl natürlicher Personen zugänglich. Art. 5 Abs. 1 UAbs. 1 lit. h KI-VO ist daher bereits aus diesem Grund nicht einschlägig. Zudem sollen die vorgesehenen Regelungen einen Echtzeit-Abgleich gerade ausschließen, so dass es auch an einem Echtzeit-Fernidentifizierungssystem, „bei dem die Erfassung biometrischer Daten, der Abgleich und die Identifizierung ohne erhebliche Verzögerung erfolgen“ (Art. 3 Nr. 42 KI-VO), fehlt. Dies wäre ggf. anders zu bewerten, wenn ein Abgleich mit dem „Live-Video einer Webcam“[75] im öffentlichen Raum (z.B. an einem Bahnhof oder einem Flughafen) zulässig wäre. Ein solcher ist hier aber gerade nicht vorgesehen (s.o.).

2.3.2.2 Biometrische Kategorisierung

Art. 5 Abs. 1 UAbs. 1 lit. g KI-VO verbietet das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von Systemen zur biometrischen Kategorisierung, mit denen natürliche Personen individuell auf der Grundlage ihrer biometrischen Daten (Art. 3 Nr. 34 KI-VO) kategorisiert werden, um ihre Rasse, ihre politischen Einstellungen, ihre Gewerkschaftszugehörigkeit, ihre religiösen oder weltanschaulichen Überzeugungen, ihr Sexualleben oder ihre sexuelle Ausrichtung zu erschließen oder abzuleiten. Die Vorschrift erscheint missraten, da nicht erkennbar ist, wie aus biometrischen Daten z.B. auf die Gewerkschaftszugehörigkeit einer Person geschlossen werden kann. Für den Bereich der Strafverfolgung bestehen Ausnahmen. Soweit erkennbar, sollen die §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E eine solche Kategorisierung aber nicht erlauben, was in den Vorschriften ggf. aber noch deutlicher gemacht werden sollte.

2.3.2.3 Datenbanken zur Gesichtserkennung

Art. 5 Abs. 1 UAbs. 1 lit. e KI-VO verbietet das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von „KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen erstellen

[75] BT-Drs. 20/12806, 18.

oder erweitern“.[76] Ob dieses Verbot den Regelungen in §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E entgegensteht, ist von verschiedenen Faktoren abhängig. Die Verarbeitung von Stimmen wird von dem Verbot vornherein nicht erfasst.

Fraglich ist zunächst, was unter „Datenbanken zur Gesichtserkennung“ zu verstehen ist. Der Begriff wird in der KI-VO nicht definiert. Allgemein ist eine Datenbank ein System zur elektronischen Datenverwaltung, um große Datenmengen zu speichern und bedarfsgerecht zur Verfügung zu stellen.[77] Ob eine solche Datenbank beim biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet erstellt oder erweitert wird, hängt von der technischen Ausgestaltung und der konkreten Durchführung des Abgleichs statt (s.o.) und lässt sich derzeit nur schwer einschätzen. Sollten im Rahmen des Abgleichs zunächst große Datenmengen aus dem Internet heruntergeladen und für den Abgleich aufbereitet werden, könnte es sich um eine Datenbank zur Gesichtserkennung im Sinne von Art. 5 Abs. 1 UAbs. 1 lit. e KI-VO handeln. Bei kurzfristigen Speichervorgängen oder anderen technischen Verfahren im Zusammenhang mit dem biometrischen Abgleich sollte dies hingegen nicht der Fall sein – insbesondere, wenn alle Daten, die nicht zu Treffern geführt haben und die keinen konkreten Ermittlungsansatz aufweisen, unverzüglich wieder gelöscht werden.

Fraglich ist zudem, wann ein „ungezielte[s] Auslesen von Gesichtsbildern aus dem Internet“ vorliegt. Der Begriff des „ungezielte[n] Auslesen[s]“ wird in der KI-VO nicht definiert. Ein solches Auslesen könnte vorliegen, wenn Gesichtsbilder aus dem Internet zur Erstellung oder Erweiterung der „Datenbanken zur Gesichtserkennung“ heruntergeladen oder anderweitig ausgewertet werden, ohne dass vorab klar ist, ob die Gesichtsbilder mit der gesuchten Person in irgendeinem Zusammenhang stehen. Es ist aber sicher auch ein anderes Begriffsverständnis möglich, etwa dahingehend, dass es an einem ungezielten Auslesen fehlt, wenn der gesamte Vorgang von Beginn an darauf abzielt, eine bestimmte Person gezielt aufzufinden.

Art. 5 Abs. 1 UAbs. 1 lit. e KI-VO ist von vornherein – wie die gesamte KI-VO – nicht anwendbar, wenn bei der Erstellung oder Erweiterung der „Datenbanken zur Gesichtserkennung“ durch das „Auslesen von Gesichtsbildern aus dem Internet“ keine KI-Systeme im Sinne von Art. 3 Nr. 1 KI-VO zum Einsatz kommen. Dies könnte der Fall sein, wenn die „Datenbanken zur Gesichtserkennung“ durch einfache Downloader oder Crawler erstellt und erweitert werden, die nicht von Art. 3 Nr. 1 KI-VO erfasst werden.

Der biometrische Abgleich selbst, also die biometrische Auswertung von „Datenbanken zur Gesichtserkennung“, wird von Art. 5 Abs. 1 UAbs. 1 lit. e KI-VO – zumindest dem Wortlaut nach – nicht verboten.

2.3.3 Hochrisiko-KI-Systeme

Zu den Hochrisiko-KI-Systemen gehören gem. Art. 6 Abs. 2 i.V.m. Anhang III Nr. 1 lit. a KI-VO biometrische Fernidentifizierungssysteme. Ein biometrisches Fernidentifizierungssystem ist gem. Art. 3 Nr. 41 KI-VO „ein KI-System, das dem Zweck dient, natürliche Personen ohne ihre aktive Einbeziehung und in der Regel aus der Ferne durch Abgleich der biometrischen Daten einer Person mit den in einer Referenzdatenbank gespeicherten biometrischen Daten zu identifizieren“. Da die biometrische Erkennung im Rahmen von §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E ohne aktive Einbeziehung der betroffenen Personen und – da sie über das Internet stattfindet – aus der Ferne erfolgt, erscheint es vertretbar, von einem

[76] EG 43 KI-VO begründet das Verbot damit, dass durch die Erstellung von „Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet […] das Gefühl der Massenüberwachung verstärkt und [es] zu schweren Verstößen gegen die Grundrechte“ kommen kann. Hintergrund sind wahrscheinlich private Angebote wie Clearview und PimEyes, s. dazu Hornung/Schindler, DuD 2021, 515.

[77] S. https://de.wikipedia.org/wiki/Datenbank.

biometrischen Fernidentifizierungssystem auszugehen (auch wenn man die Frage aufwerfen mag, inwieweit dabei ein Abgleich „mit den in einer Referenzdatenbank gespeicherten biometrischen Daten“ erfolgt). Zudem ist im Einzelfall zu prüfen, ob Art. 6 Abs. 2 i.V.m. Anhang III Nr. 7 KI-VO einschlägig ist.

Wenn ein Hochrisiko-KI-System vorliegt, gelten für Anbieter die Pflichten gem. Art. 16 KI-VO und für Betreiber die Pflichten nach Art. 26 KI-VO. Betreiber von Hochrisiko-KI-Systemen zur nachträglichen biometrischen Fernfernidentifizierung (Art. 3 Nr. 43 KI-VO) haben insbesondere die Vorgaben des Art. 26 Abs. 10 KI-VO zu beachten (Genehmigung einer Justizbehörde oder einer Verwaltungsbehörde binnen 48 Stunden, kein Einsatz „in nicht zielgerichteter Weise“, Dokumentation „in der einschlägigen Polizeiakte“ etc.). Es sollte geprüft werden, ob die §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E so gestaltet sind, dass den dortigen Anforderungen genügt werden kann.

2.4 Fazit

Die §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E sollen es dem BKA, der BPOL und den Strafverfolgungsbehörden erlauben, biometrische Daten zu Gesichtern und Stimmen mit Daten aus dem Internet abzugleichen. Ein solcher Abgleich ist nicht von vornherein verfassungs- und europarechtswidrig. Die konkret vorgeschlagenen Regelungen genügen den verfassungs- und europarechtlichen Anforderungen aber nicht. Sie sind zu unbestimmt und erlauben unverhältnismäßige Grundrechtseingriffe. Je nach technischer Umsetzung stehen auch Verstöße gegen die KI-VO im Raum. Es ist aber grundsätzlich möglich, verfassungs- und europarechtskonforme Regelungen zu schaffen.

3 Regelungen zur automatisierten Datenanalyse

Die § 16a BKAG-E und § 34a BPolG-E sehen eine automatisierte Datenanalyse vor. Demnach dürfen das BKA und die BPOL personenbezogene Daten im Zusammenhang mit der Abwehr bestimmter Gefahren und der Verfolgung und Verhütung bestimmter Straftaten „mittels einer automatisierten Anwendung zur Datenverarbeitung zusammenführen und darüber hinaus zum Zwecke der Analyse weiterverarbeiten“.

Die Regelungen erlauben die Verarbeitung personenbezogener Daten und damit Eingriffe in das Grundrecht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, das Grundrecht auf Schutz personenbezogener Daten gem. Art. 7 und 8 GRCh sowie das Recht auf Achtung des Privat und Familienlebens gem. Art. 8 EMRK (vgl. dazu bereits oben). Konkret führt dabei die Nutzung vorab erhobener Daten über den ursprünglichen Anlass hinaus und die damit einhergehende Erlangung neuen Wissens zu Eingriffen.

Die automatisierte Datenanalyse ist laut der Rechtsprechung des BVerfG nicht von vornherein verfassungsrechtlich unzulässig.[78] Die Anforderungen an eine Ermächtigung zur Durchführung der automatisierten Datenanalyse sind vom Eingriffsgewicht abhängig. Das Eingriffsgewicht der automatisierten Datenanalyse kann je nach gesetzlicher Ausgestaltung der Regelungen sehr unterschiedlich sein. Es hängt insbesondere vom Gewicht vorausgegangener Datenerhebungseingriffe sowie der Art und Weise, wie die Datenanalyse durchgeführt wird, ab.[79] Bei „einer Begrenzung der Befugnis auf eine sehr schlichte Form des Abgleichs einer überschaubaren Zahl von Daten näher eingegrenzter Herkunft“ ist es eher gering. Ist hingegen etwa „die Erstellung von genaueren Bewegungs-, Verhaltens- oder Beziehungsprofilen“

[78] BVerfGE 165, 363, 388 f.

[79] S. hierzu BVerfGE 165, 363, 389 ff.

zulässig, steigt es an. Allgemein wird es „durch Art, Umfang und denkbare Verwendung der Daten sowie die Gefahr ihres Missbrauchs bestimmt“.[80]

Mit Blick darauf, ist das Eingriffsgewicht bei § 16a BKAG-E und § 34a BPolG-E als erheblich anzusehen. § 16a Abs. 1 BKAG-E erlaubt dem BKA das Zusammenführen und Weiterverarbeiten von personenbezogenen Daten, die „im Informationssystem oder im polizeilichen Informationsverbund“ gespeichert sind. Daten nach § 12 Abs. 3 BKAG (verdeckter Einsatz technischer Mittel in oder aus Wohnungen, verdeckter Eingriff in informationstechnische Systeme) dürfen gem. § 16a Abs. 4 BKAG-E nicht weiterverarbeitet werden. § 34a BPolG-E stellt auf personenbezogene Daten ab, die die BPOL „zur Erfüllung der ihr obliegenden Aufgaben weiterverarbeitet oder für die sie eine Berechtigung zum Abruf hat“. Weitere Einschränkungen sind bzgl. der Zahl und Herkunft Daten nicht erkennbar. Im Rahmen der Weiterverarbeitung können gem. § 16a Abs. 4 BKAG-E und § 34a BPolG-E „insbesondere datei- und informationssystemübergreifend Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen hergestellt, unbedeutende Informationen und Erkenntnisse ausgeschlossen, Suchkriterien gewichtet, die eingehenden Erkenntnisse zu bekannten Sachverhalten zugeordnet sowie gespeicherte Daten statistisch ausgewertet werden“. Diese Auflistung möglicher Formen der Weiterverarbeitung im Rahmen der Analyse ist nicht abschließend („insbesondere“),[81] so dass auch in dieser Hinsicht keine Eingrenzung (z.B. ein Verbot der Erstellung von Bewegungs-, Verhaltens- oder Beziehungsprofilen) erkennbar ist. Hinsichtlich der Methoden und Verfahren der Analyse sprechen die Regelungen von „einer automatisierten Anwendung zur Datenverarbeitung“ (wie auch in den Vorschriften für den biometrischen Abgleich, s.o.). Dies ist sehr weit formuliert und enthält ebenfalls so gut wie keine Eingrenzung. Die automatisierte Analyse soll nicht nur zur Abwehr konkreter Gefahren, sondern auch im Vorfeld konkreter Gefahren zulässig sein. Ein besonderes Gewicht kann überdies die Verwendung selbstlernender Systeme haben,[82] die in den vorgesehenen Vorschriften nicht ausgeschlossen wird.

Derart schwerwiegende Eingriffe sind nur unter engen Voraussetzungen zu rechtfertigen,[83] wobei „Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle“ zu stellen sind.[84] Allgemein sind bereichsspezifische und präzise Regelungen erforderlich,[85] die auch verfahrens- und organisationsrechtliche Vorkehrungen vorsehen, um der Gefahr der Verletzung von Grundrechten entgegenzuwirken.[86]

Die Verfassungskonformität der vorgesehenen Regelungen ist vor diesem Hintergrund zweifelhaft. Die Regelungen erlauben letztlich eine sehr weitreichende Analyse fast aller personenbezogener Daten, auf die das BKA und die BPOL Zugriff haben, ohne dass nennenswerte Einschränkungen erkennbar sind. Vorgesehen ist allerdings, dass beim Einsatz selbstlernender Systeme sicherzustellen ist, dass keine diskriminierenden Algorithmen herausgebildet oder verwendet werden und die eingesetzten Verfahren nach Möglichkeit nachvollziehbar sein müssen (§ 16a Abs. 5 BKAG-E und § 34a Abs. 3 BPolG-E i.V.m. § 22 Abs. 3 Satz 2 und 3 BKAG-E). Dies ist sicher zu begrüßen, ergibt sich bzgl. der Diskriminierung aber bereits aus Art. 3 GG. Es gibt in § 16a BKAG-E und § 34a BPolG-E keine Vorgaben zu Löschungspflichten, zum Umgang mit den Daten Unbeteiligter, zu Rollen-

[80] BVerfGE 165, 363, 398 ff.

[81] S.a. BT.Drs, 20/12806, 21.

[82] BVerfGE 165, 363, 408.

[83] BVerfGE 165, 363, 410.

[84] BVerfGE 165, 363, 412.

[85] BVerfGE 120, 378, 407 f. zum Bestimmtheitsgebot

[86] S. bereits BVerfGE 65, 1, 44.

und Rechtekonzepten oder zur Zugriffskontrolle (vgl. z.B. die Regelungen in § 25a HSOG, mit denen der hessische Gesetzgeber versucht hat, die Vorgaben des BVerfG umzusetzen). Die Erstellung umfassender Persönlichkeitsprofile durch Verknüpfung einzelner Daten wird nicht ausgeschlossen.[87] Es bestehen daher insgesamt Bedenken, ob die § 16a BKAG-E und § 34a BPolG-E den verfassungsrechtlichen Anforderungen genügen, die das BVerfG in seiner Entscheidung zur automatisierten Datenanalyse präzisiert hat.

Es sollte zudem geprüft werden, ob die vorgesehenen Vorschriften zur automatisierten Datenanalyse mit der Richtlinie (EU) 2016/680 (JI-RL) im Einklang stehen. Dies gilt auch hinsichtlich der Verordnung über künstliche Intelligenz (KI-VO).

4 Regelungen zur Weiterverarbeitung von Daten

Gem. § 22 BKAG-E darf das BKA bei ihm vorhandene personenbezogene Daten zur Entwicklung, Überprüfung, Änderung oder zum Trainieren von IT-Produkten weiterverarbeiten und an Dritte übermitteln, soweit dies erforderlich ist, insbesondere weil unveränderte Daten benötigt werden (Nr. 1) oder eine Anonymisierung oder Pseudonymisierung der Daten nicht oder nur mit unverhältnismäßigem Aufwand möglich ist (Nr. 2).

Die Übermittlungsbefugnis an Dritte sollte gestrichen werden. Es ist nicht die Aufgabe des BKA, Dritte (z.B. private Unternehmen) mit Trainingsdaten zu versorgen. Die beim BKA vorhandenen Daten können sensible Informationen enthalten, deren Verarbeitung nach europäischem Recht nur eingeschränkt zulässig ist (vgl. Art. 10 JI-RL, Art. 9 DSGVO). Die rechtmäßige Weiterverarbeitung durch Dritte ist praktisch nur schwer zu kontrollieren. Allgemein ist die Frage, unter welchen Voraussetzungen personenbezogene Trainingsdaten verarbeitet werden dürfen, derzeit noch nicht abschließend geklärt. Auf eine Übermittlung an Dritte durch das BKA sollte daher verzichtet werden.

In der Gesetzesbegründung wird darauf abgestellt, dass „es sich um IT-Produkte handeln [muss], die das Bundeskriminalamt für die eigene Aufgabenwahrnehmung entwickelt oder nutzt“.[88] Dies ergibt sich aus dem Gesetzeswortlaut in dieser Deutlichkeit nicht. Sollte mit der Übermittlungsbefugnis gemeint werden, dass eine Übermittlung nur an Dritte zulässig sein soll, deren IT-Produkte das BKA nutzt, um diese im Auftrag des BKA zu trainieren, sollte dies jedenfalls deutlich gemacht werden.

[87] Zur unzulässigen „umfassende[n] Registrierung und Katalogisierung der Persönlichkeit durch die Zusammenführung einzelner Lebens- und Personaldaten zur Erstellung von Persönlichkeitsprofilen“ bereits BVerfGE 65, 1, 53; s.a. BVerfGE 27, 1, 6.

[88] BT-Drs. 20/12806, 22.