FRANKFURTER INSTITUT FÜR DAS RECHT DER EUROPÄISCHEN UNION fireu

# 49. Frankfurter Newsletter zum Recht der Europäischen Union

**(26.06.2023)**


## *Prof. Dr. Enrico Peuker**


# Kompetenzgrenzen der europäischen KI-Regulierung im Bereich der Gefahrenabwehr und Strafverfolgung

## I. Der Entwurf eines „Gesetzes über Künstliche Intelligenz“

Im April 2021 hat die Europäische Kommission den Entwurf einer Verordnung zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (nachfolgend: KI-VO-E) vorgelegt, den sie „Gesetz für Künstliche Intelligenz“ („Artificial Intelligence Act“) bezeichnet.[1] Nachdem das Europäische Parlament hierzu vor wenigen Tagen seine Verhandlungsposition festgelegt hat[2], kann der Entwurf nunmehr in die Trilog-Verhandlungen gehen. Die Verordnung zielt u.a. darauf, die Sicherheit von KI-Systemen im Unionsmarkt zu gewährleisten, die bestehenden Grundrechte und Werte der Union zu wahren, die wirksame Durchsetzung des geltenden Rechts zur Wahrung der Grundrechte sowie der Sicherheitsanforderungen an KI-Systeme zu stärken sowie die Entwicklung eines Binnenmarkts für rechtskonforme, sichere und vertrauenswürdige KI-Anwendungen zu erleichtern und eine Marktfragmentierung zu verhindern.[3]

---


* Inhaber der Professur für Öffentliches Recht, insb. Verwaltungsrecht an der Europa-Universität Viadrina Frankfurt (Oder). Der Beitrag geht auf ein Gutachten für das Bundesministerium des Innern und für Heimat zurück.


1 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, KOM(2021) 206 endg.

2 Änderungen des Europäischen Parlaments vom 14.6.2023, P9_TA(2023)0236.

3 KOM(2021) 206 endg., S. 3. Einen Überblick über den Verordnungsentwurf geben etwa *Spindler*, CR 2021, 361; *Ebert/Spiecker gen. Döhmann*, NVwZ 2021, 1188; *Rostalski/Weiss*, ZfDR 2021, 329; *Hofmeister*, DVBl. 2022, 625; *Linardatos*, GPR 2022, 58.

Zu diesem Zwecke wählt die Kommission einen horizontalen, d.h. nicht an einzelnen Wirtschaftssektoren oder Anwendungsbereichen, sondern an näher definierten Risiken der KI für Grundrechte ausgerichteten und grundsätzlich technikneutralen Regulierungsansatz.[4] In diesem Sinne verbietet der Entwurf zunächst bestimmte Praktiken im Bereich der Künstlichen Intelligenz, die mit einem unvertretbaren Risiko verbunden sind (Titel II, Art. 5 KI-VO-E). Für Hochrisiko-KI-Systeme stellt der Entwurf zwingende Anforderungen sowie Verpflichtungen der Betreiber solcher Systeme auf (Titel III, Art. 6 ff. KI-VO-E). Für KI-Systeme mit geringem Risiko sollen dagegen auch geringere Anforderungen gelten bzw. strengere Anforderungen nur freiwillig nach Maßgabe von Verhaltenskodizes (Art. 69 KI-VO-E) zu befolgen sein.

## II. Verbot der Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme

Zu den wegen eines unvertretbaren Risikos grundsätzlich verbotenen Praktiken zählt Art. 5 Abs. 1 lit. d KI-VO-E die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich-zugänglichen Räumen zu Strafverfolgungszwecken. Das sind KI-Systeme, die natürliche Personen aus der Ferne durch einen Abgleich der biometrischen Daten einer Person mit gespeicherten biometrischen Daten identifizieren sollen, ohne dass der Nutzer des KI-Systems vorher weiß, ob die Person anwesend sein wird und identifiziert werden kann, wobei die Erfassung biometrischer Daten, der Abgleich und die Identifizierung ohne erhebliche Verzögerung erfolgen.[5] Gerade die biometrische Fernidentifizierung stand denn auch im Mittelpunkt der Kritik auch des Europäischen Parlaments, die die Bedenken der Kommission aufgreift: Die biometrische Echtzeit-Fernidentifizierung natürlicher Personen in öffentlich zugänglichen Räumen sei ein besonderer Eingriff in die Rechte und Freiheiten der Person, da sie die Privatsphäre eines großen Teils der Bevölkerung beeinträchtige, ein Gefühl der ständigen Überwachung wecke und indirekt von der Ausübung der Versammlungsfreiheit und anderer Grundrechte abhalten könnten. Zudem bedeuteten die Unmittelbarkeit der Auswirkungen und die begrenzte Möglichkeit weiterer Kontrollen oder Korrekturen im Zusammenhang mit der Verwendung solcher Echtzeit-Systeme erhöhte Risiken für Rechte und Freiheiten der von Strafverfolgungsmaßnahmen betroffenen Personen.[6]

Nach dem 19. Erwägungsgrund des KI-VO-E soll eine Ausnahme von diesem grundsätzlichen Verbot soll nur dann zugelassen werden, wenn die Verwendung unbedingt erforderlich ist, um einem erheblichen öffentlichen Interesse zu dienen, dessen Bedeutung die Risiken überwiegt. Ein solches erhebliches öffentliches Interesse erkennt Art. 5 Abs. 1 lit. d KI-VO-E nur in drei eng begrenzten Fällen an. Die abschließende Aufzählung umfasst (i) die gezielte Suche nach bestimmten potenziellen Opfern von Straftaten oder nach vermissten Kindern, (ii) das Abwen-

---

4 KOM(2021) 206 endg., S. 12 f.

5 Definitionen in Art. 3 Nr. 36 f. KI-VO-E.

6 Entsprechende Bedenken hat das Europäische Parlament bereits in seiner Entschließung „Künstliche Intelligenz im Strafrecht und ihre Verwendung durch die Polizei und Justizbehörden in Strafsachen (2020/2016(INI)“ vom 6.10.2021 angemeldet, P9_TA(2021)0405, Ziffer 30.

den einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder eines Terroranschlags, und (iii) das Erkennen, Aufspüren, Identifizieren oder Verfolgen eines Täters oder Verdächtigen einer Straftat im Sinne des Art. 2 Abs. 2 des Rahmenbeschlusses 2002/584/JI des Rates über den Europäischen Haftbefehl, der in dem betreffenden Mitgliedstaat nach dessen Recht mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht ist. Damit ist allerdings noch keine Vorentscheidung für den Einsatz von biometrischen Echtzeit-Fernidentifizierungssystemen getroffen. Vielmehr ist es gemäß Art. 5 Abs. 4 KI-VO-E Sache der Mitgliedstaaten, in ihrem nationalen Recht vorzusehen, dass die Verwendung solcher Systeme innerhalb des durch Art. 5 Abs. 1 lit. d, Abs. 2 und 3 KI-VO-E gezogenen Rahmens vollständig oder teilweise genehmigt werden kann. Das Europäische Parlament schlägt nunmehr vor, die Beschränkung auf Strafverfolgungszwecke und die damit verbundenen Ausnahmetatbestände zu streichen, also die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen schlechthin zu verbieten.[7]

Unabhängig von einer möglichen Beschränkung auf Strafverfolgungszwecke beansprucht das im Verordnungsentwurf vorgesehene Verbot der Verwendung von biometrischen Echtzeit-Fernidentifizierungssystemen in öffentlichen Räumen nach Inkrafttreten der Verordnung gemäß Art. 288 Abs. 2 S. 2 AEUV unmittelbare Geltung, bindet also alle innerstaatlichen Stellen. Da sich der Verordnungsentwurf nicht auf den Einsatz solcher Systeme in grenzüberschreitenden Fällen beschränkt, gilt das Verwendungsverbot auch für rein innerstaatliche Sachverhalte der Gefahrenabwehr oder Strafverfolgung. Vom Anwendungsbereich des KI-VO-E ausgenommen sind gemäß Art. 2 Abs. 3 KI-VO-E lediglich KI-Systeme, die ausschließlich für militärische Zwecke entwickelt oder verwendet werden. Für eine solche Regelung im Bereich der Gefahrenabwehr und Strafverfolgung – zumal mit Blick auf rein innerstaatliche Sachverhalte – besteht indes keine einschlägige Kompetenzgrundlage.

### III. Datenschutzkompetenz als eine Rechtsgrundlage des Verordnungsentwurfs

Die Kommission stützt den Verordnungsentwurf zunächst auf die Binnenmarktkompetenz des Art. 114 AEUV und begründet dies mit dem Hauptziel des Vorschlags, durch die Festlegung harmonisierter Vorschriften, insbesondere in Bezug auf die Entwicklung, das Inverkehrbringen und den Einsatz von KI-gestützten Produkten und Diensten oder eigenständigen KI-Systemen, für ein reibungsloses Funktionieren des Binnenmarkts zu sorgen und die Gefahr einer Fragmentierung des Binnenmarkts sowie der Rechtsunsicherheit zu bannen, die aus eigenständigen Regulierungsinitiativen der Mitgliedstaaten erwachsen könnte.

Das grundsätzliche Verbot der Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlichen Räumen zu Strafverfolgungszwecken und seine Ausnahmen in Art. 5 Abs. 1 lit. b, Abs. 2-4 KI-VO-E zielen indes nicht auf ein reibungsloses Funktionieren des Bin-

[7] P9_TA(2023)0236, Änderungsvorschlag 220.

nenmarkts, sondern ausdrücklich auf den Schutz von Privatpersonen im Hinblick auf die Verarbeitung personenbezogener Daten. Für diese konkreten Verordnungsvorschriften zieht die Kommission daher Art. 16 AEUV als Rechtsgrundlage heran.[8]

Seit dem Vertrag von Lissabon stehen dem Unionsgesetzgeber mit Art. 16 Abs. 2 UAbs. 1 S. 1 AEUV drei spezifische Rechtsgrundlagen zum Erlass datenschutzrechtlicher Bestimmungen im ordentlichen Gesetzgebungsverfahren zur Verfügung. *Erstens* eine ausschließliche Gesetzgebungskompetenz für Vorschriften über die Datenverarbeitung durch Organe, Einrichtungen und sonstige Stellen der Union (Var. 1), die hier ersichtlich nicht einschlägig ist. *Zweitens* eine (wegen Art. 4 Abs. 1 AEUV) zwischen Union und Mitgliedstaaten geteilte Zuständigkeit zum Erlass von Vorschriften über den freien Datenverkehr (Var. 3). Diese spezielle Binnenmarktkompetenz verdrängt die allgemeine Binnenmarktkompetenz des Art. 114 AEUV[9], die bisher als Rechtsgrundlage für an die Mitgliedstaaten adressierte datenschutzrechtliche Sekundärrechtsakte herangezogen und vom EuGH extensiv ausgelegt wurde. Davon zu unterscheiden ist *drittens* eine zwischen Union und Mitgliedstaaten geteilte Zuständigkeit zum Erlass von Vorschriften über Datenverarbeitungen durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen (Var. 2). In Abgrenzung zur Kompetenzalternative des freien Datenverkehrs (Var. 3) ist hier die Datenverarbeitung ausschließlich durch öffentliche Stellen angesprochen, für die nunmehr eine eigene Kompetenzgrundlage besteht.[10] Insoweit hat der Vertrag von Lissabon die bisherige Akzessorietät zwischen Binnenmarkt und Datenschutz[11] aufgelöst, zugleich aber neue Auslegungs- und Abgrenzungsfragen zur Reichweite dieser Kompetenzvariante aufgeworfen.

### IV. Datenschutz als Annexkompetenz

Die Unionskompetenz für das Datenschutzrecht bei Datenverarbeitungen durch mitgliedstaatliche Stellen ist gemäß Art. 16 Abs. 2 UAbs. 1 S. 1 Var. 2 AEUV dadurch begrenzt, dass diese Datenverarbeitungen „im Rahmen der Ausübung von Tätigkeiten [stattfinden müssen], die in den Anwendungsbereich des Unionsrechts fallen“. Diese Kompetenzschranke, die sich mit ähnlicher Formulierung auch in Art. 51 Abs. 1 GRCh findet, ist unterschiedlichen Auslegungen zugänglich.[12]

---

8 KOM(2021) 206 endg., S. 7; vgl. auch die Erwägungsgründe 2 und 23.

9 Ebenso *Kingreen*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, Art. 16 AEUV Rn. 8; *M. Schröder*, in: Streinz (Hrsg.), EUV/AEUV, Art. 16 AEUV Rn. 10; *Schneider*, Die Verwaltung 44 (2011), 499 (505). Gegen ein Spezialitätsverhältnis aber *Brühann*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Europäisches Unionsrecht, Art. 16 AEUV Rn. 35 f.

10 *Klement*, JZ 2017, 161 (164); *Müller/Schwabenbauer*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, Kap. G Rn. 415.

11 *Kingreen*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, Art. 16 AEUV Rn. 6; *Klement*, JZ 2017, 161 (164) spricht von „Rabulistik alter Schule“, die dem auf die Wahrung seiner Kompetenzen bedachten europäischen Gesetzgeber durch die die Binnenmarktfinalität durchbrechende Kompetenznorm des Art. 16 Abs. 2 UAbs. 1 AEUV erspart bleibe.

12 Überblick bei *Albers*, in: Wolff/Brink (Hrsg.), Datenschutzrecht, Syst. L Rn. 32 ff.; vgl. auch *Müller/Schwabenbauer*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, Kap. G Rn. 417 ff.

Eine weite Auslegung sieht den Anwendungsbereich des Unionsrechts bereits dann als eröffnet an, wenn eine datenschutzrechtliche Regelung irgendeinen abstrakten Bezug zu einem allgemeinen Zuständigkeitsbereich der Union (jenseits der Binnenmarktkompetenz) aufweist, ohne dass es auf eine konkrete Regelungskompetenz ankomme. Die Union könne mittlerweile für alle Politikfelder ein eigenständiges Datenschutzrecht etablieren, was nach der Aufgabe der Säulenstruktur durch den Vertrag von Lissabon auch die polizeiliche und justizielle Zusammenarbeit in Strafsachen im Raum der Freiheit, der Sicherheit und des Rechts umfasse.[13] Die Regelungskompetenz solle sich hierbei auch auf rein innerstaatliche Datenverarbeitungen erstrecken, selbst wenn Art. 82 ff. oder Art. 87 ff. AEUV insoweit keine Sachkompetenz vermitteln, da unterschiedliche Standards für grenzüberschreitende und innerstaatliche Datenverarbeitungen nicht hinnehmbar seien, bei getrennten Regelungen anderenfalls ein Chaos von Rechtsregimen und zuständigen Stellen drohe.[14]

Dem ist entgegenzuhalten, dass mit einer solch weiten Auslegung nur solche Sachgebiete von der Datenschutzkompetenz der Union ausgenommen wären, die von den Zuständigkeitskatalogen der „Art. 3 bis 6 AEUV und den weiteren Zuständigkeitszuweisungen an die Union auch als Teilgebiete einer abstrakter gefassten Materie in keiner Weise erfasst sind“[15]. Da andererseits kaum ein Sachgebiet vorstellbar ist, bei dem nicht personenbezogene Daten verarbeitet würden, und jedes behördliche Handeln zugleich Informations- und damit meist Datenverarbeitung bedeutet, entstünde eine allumfassende Regelungskompetenz der Union für den Datenschutz, die den für das Rechtsverhältnis zwischen der Union und den Mitgliedstaaten zentralen Grundsatz der begrenzten Einzelermächtigung aus Art. 5 Abs. 1 S. 1, Abs. 2 EUV konterkariert.[16] Ebenso wenig überzeugt der Hinweis, dass unterschiedliche Standards für grenzüberschreitende und innerstaatliche Datenverarbeitungen nicht hinnehmbar seien, da bei getrennten Regelungen anderenfalls ein Chaos von Rechtsregimen und zuständigen Stellen drohe. Vielmehr zeigt das Beispiel der – einen grenzüberschreitenden Bezug voraussetzenden – europäischen Grundfreiheiten in ihrer Auslegung durch den EuGH, dass das Unionsrecht durchaus unterschiedliche Standards und Rechtsregime für grenzüberschreitende und rein in-

---

13 So ausdrücklich *Kingreen*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, Art. 16 AEUV Rn. 6, der aber zugleich von einer „sachgebietsunabhängige[n] Gesetzgebungskompetenz für den Datenschutz“ spricht; vgl. auch *Schneider*, Die Verwaltung 44 (2011), 499 (506 f.); *Spiecker gen. Döhmann/Eisenbarth*, JZ 2011, 169 (172); *von Lewinski*, DuD 2012, 564 (565); *Nguyen*, ZEuS 2012, 277 (286 f.).

14 So v.a. die Argumentation bei *Bäcker*, Stellungnahme zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages am 22.10.2012 zum Entwurf einer EU-Richtlinie über die Datenverarbeitung bei Polizei und Strafjustiz, A-Drs. 17(4)585 B, S. 4 ff.; ähnlich *Kieck/Pohl*, DuD 2017, 567 (568 f.); *Brühann*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Europäisches Unionsrecht, Art. 16 AEUV Rn. 67; *Stevens/Limberger*, JZ 2022, 656 (658).

15 *Klement*, JZ 2017, 161 (165).

16 *Bäcker*, Stellungnahme JI-RL, A-Drs. 17(4)585 B, S. 6 f.; zust. *Müller/Schwabenbauer*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, Kap. G Rn. 419.

nerstaatliche Sachverhalte hinnimmt und einer sog. Inländerdiskriminierung (d.h. der Schlechterstellung von innerstaatlichen Sachverhalten, auf die die Grundfreiheiten nicht anwendbar sind) nicht entgegensteht.[17]

Überzeugend ist vielmehr eine enge Auslegung, die das Datenschutzrecht als Querschnittsmaterie mit Annexcharakter, Art. 16 Abs. 2 UAbs. 1 S. 1 Var. 2 AEUV mithin als eine Annexkompetenz versteht. Hiernach fällt eine datenverarbeitende Tätigkeit nur dann in den Anwendungsbereich des Unionsrechts, wenn (1.) das Primärrecht der Union eine entsprechende Sachkompetenz zugewiesen und (2.) die Union von dieser Kompetenz auch Gebrauch gemacht hat. Die Tätigkeit muss daher im konkreten Fall durch Unionsrecht vorgeschrieben, veranlasst oder zumindest beschränkt sein; fehlen entsprechende unionsrechtliche Vorgaben, fällt die Tätigkeit einer mitgliedstaatlichen Behörde nicht in den Anwendungsbereich des Unionsrechts.[18]

## V. Regelungskompetenzen des Art. 87 Abs. 2 lit. a und Abs. 3 AEUV

Erforderlich ist somit eine (von Art. 16 Abs. 2 UAbs. 1 AEUV zu unterscheidende) Sachkompetenz der Union, in deren Rahmen der Unionsgesetzgeber dann auf Art. 16 Abs. 2 UAbs. 1 S. 1 Var. 2 AEUV gestützte Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten erlassen kann. Hierfür kommt grundsätzlich auch die Kompetenznorm des Art. 87 Abs. 2 AEUV für die polizeiliche Zusammenarbeit in Betracht, da sich Art. 16 AEUV auf alle Politikbereiche der Union erstreckt, zu denen seit dem Vertrag von Lissabon auch die polizeiliche und justizielle Zusammenarbeit in Strafsachen im Raum der Freiheit, der Sicherheit und des Rechts zählt. Das ergibt sich zum einen im Umkehrschluss aus Art. 16 Abs. 2 UAbs. 2 AEUV, demzufolge die auf der Grundlage des Art. 16 AEUV erlassenen Vorschriften die spezifischen Bestimmungen des Art. 39 EUV unberührt lassen, so dass nur die im Kontext der Gemeinsamen Außen- und Sicherheitspolitik erlassenen Vorschriften über den Schutz personenbezogener Daten auf Art. 39 EUV gestützt werden müssen. Zum anderen enthält Art. 87 Abs. 2 lit. a AEUV, der zum Erlass von Regelungen über das Einholen, Speichern, Verarbeiten, Analysieren und Austauschen sachdienlicher Informationen ermächtigt, wozu auch ermittlungsrelevante personenbezogene Daten zählen[19], keinen Hinweis auf den etwaigen Erlass von Bestimmungen über den Schutz personenbezogener Daten.

Der Wortlaut des Art. 87 Abs. 2 AEUV verweist für das Regelungsziel solcher Maßnahmen ausdrücklich auf die Zwecke des Abs. 1. Die Regelungen zum Einholen, Speichern, Verarbeiten,

---

17 Vgl. nur *Forsthoff/Eisendle*, in: Grabitz/Hilf/Nettesheim (Hrsg.), Das Recht der EU, Art. 45 AEUV Rn. 52 f. mit zahlreichen Nachweisen zur Rspr.

18 Formulierung bei *Klement*, JZ 2017, 161 (165); ebenso *Wolff*, in: Kugelmann/Rackow (Hrsg.), Prävention und Repression, S. 61 (66); *Grzeszick*, NVwZ 2018, 1505 (1507); *Müller/Schwabenbauer*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, Kap. G Rn. 422; ausführlich jüngst *Sandhu*, Grundrechtsunitarisierung durch Sekundärrecht, S. 127 ff.; a. A. *Marsch*, Das europäische Datenschutzgrundrecht, S. 337 f.; referierend *Pfeffer*, NVwZ 2022, 294 (297 f.).

19 EuGH, Gutachten 1/15 (PNR Kanada), ECLI:EU:C:2017:592, Rn. 99.

Analysieren und Austauschen von sachdienlichen Informationen müssen daher darauf abzielen, eine polizeiliche Zusammenarbeit zwischen den mitgliedstaatlichen Polizei- und Strafverfolgungsbehörden zu entwickeln. In der Praxis erfolgt die informationelle Zusammenarbeit der mitgliedstaatlichen Polizeibehörden häufig unter Verwendung automatisierter Informationssysteme.[20]

Zwingend erforderlich ist mithin ein grenzüberschreitender Bezug bei der polizeilichen informationellen Zusammenarbeit. Regelungen zum rein innerstaatlichen Umgang mit sachdienlichen Informationen können dagegen nicht auf Art. 87 Abs. 2 lit. a, Abs. 1 AEUV gestützt werden. Das stellt auch Art. 72 AEUV klar, demzufolge die Vorschriften zum Raum der Freiheit, der Sicherheit und des Rechts nicht die Wahrnehmung der Zuständigkeiten der Mitgliedstaaten für die Aufrechterhaltung der öffentlichen Ordnung und den Schutz der inneren Sicherheit berühren.

Insoweit das Verbot der Verwendung von biometrischen Echtzeit-Fernidentifizierungssystemen in öffentlichen Räumen zu Strafverfolgungszwecken auch für rein innerstaatliche Sachverhalte Geltung beansprucht, kommt Art. 87 Abs. 2 AEUV nicht als Rechtsgrundlage in Betracht. Da auch sonst keine einschlägige Kompetenzgrundlage für ein Verbot rein innerstaatlicher Datenverarbeitung durch Sicherheitsbehörden ersichtlich ist, fehlt es an der von der Annexkompetenz des Art. 16 Abs. 2 UAbs. 1 S. 1 Var. 2 AEUV vorausgesetzten Eröffnung des Anwendungsbereichs des Unionsrechts.[21]

Auch Art. 87 Abs. 3 AEUV kommt nicht als Rechtsgrundlage in Betracht, da der Einsatz von KI zur biometrischen Echtzeit-Fernidentifizierung in erster Linie der Informationsbeschaffung dient, an die sich erst später ggf. operative Maßnahmen der Gefahrenabwehr anschließen. Unter diesen operativen Maßnahmen werden bislang vor allem die grenzüberschreitende Observation, die grenzüberschreitende Nacheile, der Austausch von Verbindungsbeamten, die Bildung gemeinsamer Ermittlungsgruppen und kontrollierte Lieferungen verstanden.[22] Die informationelle polizeiliche Zusammenarbeit fällt dagegen unter Art. 87 Abs. 2 lit. a AEUV. Zudem verdeutlicht der Wortlaut des Art. 87 Abs. 3 AEUV („operative Zusammenarbeit zwischen den in diesem Artikel genannten Behörden“), dass es sich auch hier um die grenzüberschreitende Zusammenarbeit der Polizeibehörden handeln muss, rein innerstaatliche operative Tätigkeiten mithin nicht Gegenstand einer auf Art. 87 Abs. 3 AEUV gestützten Regelung sein können.

---

20 Vgl. nur *Dannecker*, in: Streinz (Hrsg.), EUV/AEUV, Art. 87 AEUV Rn. 5 ff. m.w.N.

21 Im Ergebnis auch *Schindler/Schomberg*, in: Friedewald u.a. (Hrsg.), Künstliche Intelligenz, Demokratie und Privatheit, S. 103 (124 f.); zumindest zweifelnd *Hornung*, AöR 147 (2022), 1 (63 m. Fn. 257).

22 Vgl. nur *Dannecker*, in: Streinz (Hrsg.), EUV/AEUV, Art. 87 AEUV Rn. 25 ff. m.w.N.

## VI. Ergebnis

Soweit der Unionsgesetzgeber mit der KI-VO also die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme durch nationale Sicherheitsbehörden in rein innerstaatlichen Fällen Sachverhalten verbieten möchte, fehlt ihm hierzu eine einschlägige Rechtsetzungskompetenz. Zudem sind keine Gründe ersichtlich, warum die Ziele des in Betracht gezogenen Verbots von den Mitgliedstaaten weder auf zentraler noch auf regionaler oder lokaler Ebene ausreichend verwirklicht werden können, sondern wegen seines Umfangs oder seiner Wirkungen auf Unionsebene besser zu verwirklichen sein sollen. Da sehr viele polizeiliche Datenverarbeitungen nach wie vor auf rein innerstaatliche Sachverhalte beschränkt sind, besteht insoweit kein Harmonisierungsbedarf.[23] Dem Unionsgesetzgeber sind daher auch durch das Subsidiaritätsprinzip des Art. 5 Abs. 3 UAbs. 1 EUV entsprechende Grenzen gesetzt.

**Frankfurter Institut für das**
**Recht der Europäischen Union**
fireu@euroap-uni.de
http://www.fireu.de

[23] *Müller/Schwabenbauer*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, Kap. G Rn. 421; ähnlich *Wolff*, in: Kugelmann/Rackow (Hrsg.), Prävention und Repression, S. 61 (67).