Rat der
Europäischen Union

Brüssel, den 12. September 2022
(OR. en)

12302/22

Interinstitutionelles Dossier:
2021/0106(COD)

LIMITE

JUR 579
TELECOM 364
COSI 217
JAI 1155
ENFOPOL 451

GUTACHTEN DES JURISTISCHEN DIENSTES [1]

Absender:	Juristischer Dienst
Betr.:	Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz – Angemessenheit von Artikel 114 und 16 AEUV als Rechtsgrundlagen der für Strafverfolgungs- und Justizbehörden geltenden Bestimmungen

I. EINLEITUNG

1. Mit der vorgeschlagenen Verordnung werden harmonisierte Vorschriften für das Inverkehrbringen und die Inbetriebnahme von Systemen der künstlichen Intelligenz (im Folgenden „KI-Systeme“) in der Union festgelegt (im Folgenden „vorgeschlagene Verordnung“).[2]

[1] Die in diesem Dokument enthaltene Rechtsberatung unterliegt dem Schutz nach Artikel 4 Absatz 2 der Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission und ist vom Rat der Europäischen Union nicht für die Öffentlichkeit freigegeben worden. Der Rat behält sich vor, im Falle einer unerlaubten Veröffentlichung seine Rechte geltend zu machen.

[2] Dok. 8115/21.

2. In der Sitzung der Gruppe „Telekommunikation und Informationsgesellschaft“ vom 7. April 2022 hat sich der Juristische Dienst des Rates dazu geäußert, ob die beiden Rechtsgrundlagen (Artikel 16 und 114 AEUV) für die vorgeschlagene Verordnung über Systeme der künstlichen Intelligenz („KI-Systeme“) angemessen sind. Die Erläuterungen bestätigten, dass die Artikel 16 und 114 AEUV die richtigen Rechtsgrundlagen für den Vorschlag sind und dass es nicht angemessen ist, anstelle von Artikel 114 AEUV auf Artikel 87 Absatz 2 AEUV zurückzugreifen. Auf Ersuchen der Gruppe werden die Erläuterungen, die der Vertreter des Juristischen Dienstes in der genannten Sitzung vorgetragen hat, im vorliegenden Gutachten schriftlich dargelegt und weiter ausgeführt.

3. KI-Systeme sind in Artikel 3 Nummer 1 der vorgeschlagenen Verordnung definiert. Im Allgemeinen entsprechen sie bestimmten Arten von Software. Die vorgeschlagene Verordnung gilt sowohl für Anbieter, die KI-Systeme in Verkehr bringen, als auch für Anbieter, die KI-Systeme in Betrieb nehmen. Darüber hinaus gilt die vorgeschlagene Verordnung auch für Nutzer. Ein Anbieter kann eine natürliche oder juristische Person oder eine Behörde/öffentliche Stelle sein, die ein KI-System entwickelt oder entwickeln lässt, um es unter ihrem eigenen Namen oder ihrer eigenen Marke in Verkehr zu bringen oder in Betrieb zu nehmen. Ein Nutzer kann jede natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle sein, die ein KI-System in eigener Verantwortung verwendet.

4. Gemäß den Begriffsbestimmungen in Artikel 3 könnten Strafverfolgungs- und Justizbehörden entweder als Anbieter und/oder Nutzer eines KI-Systems gelten. KI-Systeme, deren Zweckbestimmung gemäß der Definition des Anbieters die Strafverfolgung oder die Rechtspflege ist, gelten gemäß Anhang III als Hochrisiko-KI-Systeme. Daher unterliegen sie grundlegenden Anforderungen (Risikomanagement, Tests, Daten-Governance, technische Dokumentation, Transparenz, menschliche Aufsicht, Genauigkeit, Robustheit und Cybersicherheit) und Verpflichtungen (z. B. Qualitätsmanagementsysteme, technische Dokumentation, Konformitätsbewertung, Korrekturmaßnahmen, Informationspflichten, Pflichten von Einführern und Händlern) sowie Normen und Konformitätsbewertungen. Diese harmonisierten Vorschriften orientieren sich an den Produktsicherheitsvorschriften der Richtlinie 2006/42/EG (Maschinen)[3] und der Verordnung 2017/745 (Medizinprodukte)[4].

5. KI-Systeme, in deren Fall zu Strafverfolgungszwecken biometrische Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen eingesetzt werden, fallen unter die Kategorie der verbotenen KI-Systeme. Für dieses Verbot der Verwendung von KI-Systemen gelten jedoch Ausnahmen: Die Nutzung solcher Systeme kann von den Mitgliedstaaten genehmigt werden. Im Falle einer Genehmigung unterliegen die Systeme detaillierten Beschränkungen und Sicherheitsmaßnahmen, damit ihre Verwendung auf das absolut Notwendige beschränkt bleibt und das Grundrecht auf Schutz personenbezogener Daten gewahrt ist. Diese Beschränkungen und Sicherheitsmaßnahmen werden in der vorgeschlagenen Verordnung auf der Grundlage von Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) vorgesehen und sind durch nationales Recht zu ergänzen. Artikel 5 Absatz 1 Buchstabe d sowie Absätze 2, 3 und 4 der vorgeschlagenen Verordnung bilden eine *lex specialis* zur Richtlinie 2016/680 (Richtlinie zum Datenschutz bei der Strafverfolgung), die auf der Grundlage von Artikel 16 Absatz 2 AEUV erlassen wurde.

---

[3] Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG (ABl. L 157 vom 9.6.2006, S. 24).

[4] Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates (ABl. L 117 vom 5.5.2017, S. 1).

Gemäß Artikel 5 Absatz 1 Buchstabe d beschränken sich die Ziele dieser Systeme auf:

i) die gezielte Suche nach bestimmten potenziellen Opfern von Straftaten oder nach vermissten Kindern;

ii) das Abwenden einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder eines Terroranschlags;

iii) das Erkennen, Aufspüren, Identifizieren oder Verfolgen von Personen, die eine Straftat begangen haben oder der Begehung einer Straftat verdächtig sind, die in Artikel 2 Absatz 2 des Rahmenbeschlusses über den Europäischen Haftbefehl[5] genannt wird und in dem betreffenden Mitgliedstaat nach dessen Recht mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht ist.

Gemäß Artikel 5 Absatz 3 unterliegt der Einsatz solcher Technologien durch die Strafverfolgungsbehörden der vorherigen Genehmigung durch eine Justiz- oder Verwaltungsbehörde. In hinreichend begründeten dringenden Fällen kann jedoch zunächst ohne Genehmigung mit der Verwendung des Systems begonnen und die Genehmigung noch während der Nutzung oder im Anschluss daran beantragt werden.

Gemäß Artikel 5 Absatz 4 kann ein Mitgliedstaat beschließen, die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken zu genehmigen, und die erforderlichen detaillierten Vorschriften für die Beantragung, Erteilung und Ausübung der vorherigen Genehmigung sowie die betreffenden Straftaten festlegen.

6. Die Rechtsgrundlagen der vorgeschlagenen Verordnung sind Artikel 16 AEUV (Schutz personenbezogener Daten) und Artikel 114 AEUV (Funktionieren des Binnenmarkts). Somit stellt sich die Frage, ob diese Rechtsgrundlagen in Bezug auf die harmonisierten Vorschriften für von Strafverfolgungs- und Justizbehörden bereitgestellte oder verwendete KI-Systeme angemessen sind.

---

[5] Rahmenbeschluss 2002/584/JI des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten (ABl. L 190 vom 18.7.2002, S. 1).

7. Dieses Gutachten befasst sich in erster Linie mit der Angemessenheit der Rechtsgrundlage Artikel 114 AEUV im besonderen Kontext der Strafverfolgungsbehörden, die in mehreren Bestimmungen der vorgeschlagenen Verordnung erwähnt werden, d. h. in Bezug auf biometrische Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen und Hochrisiko-KI-Systeme gemäß Anhang III Nummer 6. Entsprechend wird darauf eingegangen, ob Artikel 87 Absatz 2 AEUV (polizeiliche Zusammenarbeit) anstelle von Artikel 114 AEUV als Rechtsgrundlage besser geeignet wäre, um die Bereitstellung und Nutzung von KI-Systemen durch Strafverfolgungsbehörden abzudecken (Abschnitt II). Das Fazit dieses Vermerks kann dann analog auf die in Anhang III genannten Justizbehörden bezüglich Hochrisiko-KI-Systeme übertragen werden.

8. Darüber hinaus wird in diesem Vermerk auf die Angemessenheit der zusätzlichen Rechtsgrundlage Artikel 16 AEUV und die Anwendung der Protokolle Nr. 21 und 22 im Zusammenhang mit der Nutzung biometrischer Echtzeit-Fernidentifizierungssysteme durch Strafverfolgungsbehörden in öffentlich zugänglichen Räumen eingegangen (Abschnitt III).

II. ANGEMESSENHEIT DER RECHTSGRUNDLAGE ARTIKEL 114 AEUV

9. Nach ständiger Rechtsprechung hängt die Rechtsgrundlage eines Rechtsakts der Union nicht davon ab, welches nach der Überzeugung eines Organs das angestrebte Ziel ist, sondern muss anhand objektiver, gerichtlich nachprüfbarer Kriterien bestimmt werden, zu denen insbesondere das Ziel und der Inhalt des Rechtsakts gehören. Ergibt die Prüfung eines Rechtsakts, dass er zwei Zielsetzungen hat oder zwei Komponenten umfasst, und lässt sich eine von ihnen als die hauptsächliche oder überwiegende ausmachen, während die andere nur nebensächliche Bedeutung hat, so ist der Rechtsakt nur auf eine Rechtsgrundlage zu stützen, und zwar auf die, die die hauptsächliche oder überwiegende Zielsetzung oder Komponente erfordert. Nur ausnahmsweise – wenn feststeht, dass der Rechtsakt gleichzeitig mehrere Ziele verfolgt, die untrennbar miteinander verbunden sind, ohne dass das eine gegenüber dem anderen nur zweitrangig oder mittelbar ist – kann ein solcher Rechtsakt auf die verschiedenen einschlägigen Rechtsgrundlagen gestützt werden, sofern diese Rechtsgrundlagen nicht Verfahren vorschreiben, die nicht miteinander vereinbar sind. Außerdem heißt es im ersten Satz von Artikel 114 Absatz 1 AEUV ausdrücklich, dass die Bestimmungen dieses Artikels gelten, *„[s]oweit in den Verträgen nichts anderes bestimmt ist“*. Somit ist die Heranziehung von Artikel 114 AEUV nur gerechtfertigt, wenn der Vertrag keine spezifischere Bestimmung enthält, die als Rechtsgrundlage für den Erlass des fraglichen Rechtsakts dienen kann.[6] Wenn der Vertrag eine spezifischere Bestimmung enthält, die als Rechtsgrundlage für den fraglichen Rechtsakt dienen kann, ist dieser also auf diese Bestimmung zu stützen.[7]

---

6 Gutachten des Juristischen Dienstes des Rates vom 17. Mai 2016, 9007/16, Nummer 6.

7 Urteil vom 29. April 2004 in der Rechtssache C-338/01, *Kommission gegen Rat*, EU:C:2004:253, Rn. 60.

A. ZIEL DER VORGESCHLAGENEN VERORDNUNG

10. Mit der vorgeschlagenen Verordnung werden das Inverkehrbringen, die Inbetriebnahme und die Verwendung einer bestimmten Art von Software (KI-Systemen) harmonisiert. Die Tatsache, dass Behörden und private Akteure Anbieter oder Nutzer solcher KI-Systeme sein können, ist an sich nicht unvereinbar mit der Rechtsgrundlage Artikel 114 AEUV.[8]

11. Darüber hinaus genügt die Tatsache, dass die Strafverfolgungsbehörden oder die in ihrem Namen handelnden Behörden zu den Anbietern oder Nutzern solcher KI-Systeme gehören können, nicht als Rechtfertigung dafür, als Rechtsgrundlage auf Artikel 87 AEUV zurückzugreifen. Um festzustellen, ob dies erforderlich ist, müssen Ziel und Inhalt der vorgeschlagenen Verordnung analysiert werden.

12. Die vorgeschlagene Verordnung ist allgemein – auch in Bezug auf biometrische Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen und Hochrisiko-KI-Systeme – darauf ausgerichtet, unionsweit für ein einheitliches und hohes Schutzniveau zu sorgen sowie zu verhindern, dass es durch uneinheitliche Regelungen zu Behinderungen des freien Verkehrs von KI-Systemen und damit zusammenhängenden Produkten und Dienstleistungen im Binnenmarkt kommt. Mit dem Vorschlag werden einheitliche Verpflichtungen für Akteure vorgesehen, und er gewährleistet den einheitlichen Schutz von zwingenden Gründen des Allgemeininteresses und der Rechte von Personen im gesamten Binnenmarkt (Erwägungsgrund 2). Konkret werden in der vorgeschlagenen Verordnung Vorschriften für das Inverkehrbringen und die Inbetriebnahme bestimmter KI-Systeme festgelegt, um das reibungslose Funktionieren des Binnenmarkts zu gewährleisten, sodass diesen Systemen der Grundsatz des freien Waren- und Dienstleistungsverkehrs zugutekommen kann (Erwägungsgrund 5). Insgesamt zielt der Vorschlag darauf ab, eine vertrauenswürdig konzipierte KI zu schaffen, die in allen Bereichen einsetzbar ist, indem ein vollständiges Regelwerk für die Entwicklung, Vermarktung und Verwendung KI-gestützter Produkte, Dienstleistungen und Systeme festgelegt wird. Da KI bei vielen Dienstleistungen und Produkten bereits eine Rolle spielt und auch in Zukunft eine Rolle spielen wird, folgt der Vorschlag der Logik des Binnenmarkts und sieht einen auf vier Risikokategorien gestützten „Rahmen für Produktsicherheit“ vor. Über ein verbindliches CE-Kennzeichnungsverfahren werden mit dem Vorschlag Anforderungen für den Marktzugang und die Zertifizierung von Hochrisiko-KI-Systemen auferlegt.

---

[8] Siehe Rechtsgutachten des Juristischen Dienstes des Rates (ST 11395/14, Nummern 39 bis 41) sowie Präzedenzfälle wie die Richtlinie (EU) 2016/2102, die Richtlinien 2014/24/EU, 2014/25/EU und 2014/23/EU.

13. Keines der erklärten Ziele der vorgeschlagenen Verordnung bezieht sich auf die Gewährleistung der Ziele der öffentlichen Sicherheit. Selbst wenn im Zuge der Harmonisierung des Inverkehrbringens/der Inbetriebnahme/Verwendung von KI-Systemen durch die Strafverfolgungsbehörden indirekt Ziele der öffentlichen Sicherheit erreicht werden sollten, hat der Gerichtshof[9] bei der Auslegung von Artikel 87 Absatz 2 AEUV im Lichte von Artikel 67 AEUV festgestellt, dass ein Rechtsakt der Union unter Berücksichtigung seines Zwecks und seines Inhalts nur dann auf den erstgenannten Artikel gestützt werden kann, wenn er unmittelbar mit den Zielen des Artikels 67 AEUV (d. h. in diesem Fall der Kriminalprävention und der polizeilichen Zusammenarbeit) zusammenhängt. Dies ist im Zusammenhang mit der vorgeschlagenen Verordnung ausgeschlossen, da die einzigen harmonisierten Vorschriften für die Nutzung solcher Systeme durch die Strafverfolgungsbehörden entweder (1) Produktsicherheitsvorschriften sind, die in Bezug auf das Inverkehrbringen/die Inbetriebnahme oder die Verwendung der KI-Systeme in gleicher Weise für alle Anbieter und Nutzer gelten, oder (2) Vorschriften über den Schutz personenbezogener Daten, für die Artikel 16 AEUV als Rechtsgrundlage hinzugefügt wurde (siehe Abschnitt III).

14. In einem anderen Fall hat der Gerichtshof[10], obwohl die Änderung der Feuerwaffenrichtlinie auf die Gewährleistung einer höheren öffentlichen Sicherheit im Zusammenhang mit terroristischer Bedrohung und anderen Formen der Kriminalität ausgerichtet war, entschieden, dass die Harmonisierung der Aspekte der Warensicherheit einer der wesentlichen Bestandteile ist, um das reibungslose Funktionieren des Binnenmarkts zu gewährleisten, weil uneinheitliche Regelungen in diesem Bereich Handelshemmnisse schaffen können[11].

---

9 Urteil vom 6. Mai 2014, *Europäische Kommission/Europäisches Parlament und Rat der Europäischen Union*, C-43/12, EU:C:2014:298.

10 Urteil vom 3. Dezember 2019, *Tschechische Republik/Europäisches Parlament*, C-482/17, EU:C:2019:1035.

11 Ebd., Rn. 57: *„Da die Besonderheit von Feuerwaffen allerdings – entgegen dem Vorbringen der Republik Polen – in deren Gefährlichkeit nicht nur für die Nutzer, sondern auch für die breite Öffentlichkeit besteht, wie der Gerichtshof dies bereits in Rn. 54 des Urteils vom 23. Januar 2018, Buhagiar u. a. (C-267/16, EU:C:2018:26), ausgeführt hat, erscheinen Erwägungen der öffentlichen Sicherheit, wie der fünfte Erwägungsgrund der Richtlinie 91/477 in Erinnerung ruft, im Rahmen einer Regelung über den Erwerb und den Besitz dieser Waren unabdingbar.“* Siehe auch Urteil vom 23. Januar 2018, *Albert Buhagiar u. a. gegen Justizminister*, C-267/16, EU:C:2018:26, Rn. 54: *„Insoweit ist zu beachten, dass sich der freie Verkehr von Feuerwaffen in Anbetracht der Gefahr, die sie für die Sicherheit von Personen darstellen, nur dadurch erreichen ließ, dass enge Voraussetzungen für ihre Verbringung zwischen Mitgliedstaaten festgelegt wurden, zu denen auch der Grundsatz der vorherigen Genehmigung durch die vom Verbringen solcher Waren betroffenen Mitgliedstaaten gehört.“*

15. Die Ziele der vorgeschlagenen Verordnung, einschließlich Artikel 5 Absatz 1 Buchstabe d sowie Absätze 2, 3 und 4 über die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen für die Zwecke der Strafverfolgung und die Bestimmungen über Hochrisiko-KI-Systeme gemäß Anhang III Nummer 6, stehen mit keinem Ziel der öffentlichen Sicherheit in einem direktem Zusammenhang. Vielmehr wird mit dem Vorschlag auf die wichtigsten Bedenken reagiert, die im Zusammenhang mit den Auswirkungen von KI-Systemen auf Gesundheit, Sicherheit und Grundrechte bestehen. Die einschlägigen Bestimmungen stehen also in einem direkten Zusammenhang mit dem Ziel, beim Inverkehrbringen/der Inbetriebnahme oder der Verwendung von KI-Systemen im Binnenmarkt für gleiche Wettbewerbsbedingungen zu sorgen sowie die Gesundheit, die Sicherheit und die Grundrechte der Nutzer zu schützen.

16. Vor diesem Hintergrund besteht das Hauptziel der vorgeschlagenen Verordnung darin, das Funktionieren des Binnenmarkts im Sinne von Artikel 114 AEUV zu verbessern, während die in Artikel 67 AEUV genannten Ziele nur mittelbar und beiläufig mit diesem Hauptziel verbunden sind.

B. INHALT DER VORGESCHLAGENEN VERORDNUNG

17. Die vorgeschlagene Verordnung enthält im Wesentlichen Vorschriften über die Voraussetzungen, die beim Inverkehrbringen (oder der Inbetriebnahme) eines bestimmten Produkts (einer KI-Software) gegeben sein müssen, damit für dessen (deren) Sicherheit und die Wahrung der Grundrechte gesorgt ist. Sie enthält ein vollständiges Regelwerk für die Entwicklung, Vermarktung und Nutzung KI-gestützter Produkte, Dienstleistungen und Systeme. In der vorgeschlagenen Verordnung ist weder eine Verpflichtung der Strafverfolgungsbehörden zur Verwendung eines rechtmäßig in Verkehr gebrachten KI-Systems vorgesehen, noch ist darin direkt geregelt, wie die Strafverfolgungsbehörden ein solches KI-System verwenden sollten. Vielmehr werden darin die Situationen, in denen die vorgesehene Verwendung eines KI-Systems – allein aufgrund dessen Verwendung durch Strafverfolgungs- oder Justizbehörden – als hochriskant gilt, eindeutig abgegrenzt.

18. Im Übrigen enthält Artikel 29 der vorgeschlagenen Verordnung Vorschriften bezüglich der Bedingungen für die Verwendung von Hochrisiko-KI-Systemen, die jedoch nicht sektorspezifisch sind, deren Anwendungsbereich begrenzt ist (hauptsächlich auf die Gebrauchsanweisung für das Produkt) und die untrennbar mit den Verpflichtungen verbunden sind, die im Rahmen der vorgeschlagenen Verordnung für Entwickler von KI-Systemen gelten. Sie räumt den Mitgliedstaaten zudem einen gewissen Spielraum ein, um weitere Vorschriften für die Verwendung solcher Hochrisiko-KI-Systeme vorzusehen. Was biometrische Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen, die für Strafverfolgungszwecke eingesetzt werden (Artikel 5), betrifft, regelt die vorgeschlagene Verordnung die Nutzung solcher Systeme unter dem Gesichtspunkt des Datenschutzes teilweise auf der Grundlage von Artikel 16 AEUV (siehe Abschnitt III).

19. Außerdem können nur die Mitgliedstaaten darüber entscheiden, ob die Möglichkeit vorgesehen wird, die Verwendung solcher biometrischer Echtzeit-Fernidentifizierungssysteme ganz oder teilweise zu genehmigen. Die konkreten Bedingungen für eine solche Verwendung sind weiterhin im nationalen Recht festzulegen, wobei die in der Verordnung vorgesehenen allgemeinen Kriterien und Sicherheitsmaßnahmen zu wahren sind: vorherige Genehmigung durch eine Justiz- oder Verwaltungsbehörde, Beantragung, Erteilung und Ausübung der vorherigen Genehmigung sowie Angabe der Straftaten, in deren Fall diese Systeme gegebenenfalls eingesetzt werden.

20. KI-Systeme sind eine besondere Art von Software. Bei den harmonisierten Vorschriften für das Inverkehrbringen oder die Inbetriebnahme/Verwendung von KI-Systemen handelt es sich somit um harmonisierte Produktsicherheitsvorschriften. Sie gelten einheitlich, ohne Unterscheidung zwischen öffentlichen und privaten Nutzern. Gemäß den einschlägigen Erwägungsgründen der vorgeschlagenen Verordnung sollte demnach in der gesamten Union für ein einheitliches und hohes Schutzniveau gesorgt werden. Gleichzeitig sollten uneinheitliche Regelungen, die den freien Verkehr von KI-Systemen und damit zusammenhängenden Produkten und Dienstleistungen im Binnenmarkt behindern, vermieden werden. Das dürfte durch die Festlegung einheitlicher Verpflichtungen für Akteure sowie durch die Gewährleistung eines einheitlichen Schutzes von zwingenden Gründen des Allgemeininteresses und Rechten von Personen im gesamten Binnenmarkt auf der Grundlage von Artikel 114 AEUV erreicht werden.[12]

21. Die vorgeschlagene Verordnung enthält mehrere Bezugnahmen auf Strafverfolgung, Grenzkontrolle und Justizverwaltung in Anhang III zu Hochrisiko-KI-Systemen (Punkte 6, 7 und 8). Sie schließen neben anderen Hochrisikosystemen auch eine detaillierte und erschöpfende Aufzählung gemäß Artikel 6 Absatz 2 zu den in Artikel 6 Absatz 1 genannten Produktsicherheitrisiken ein. Gemäß Artikel 6 Absatz 1 müssen einige KI-Systeme aufgrund ihrer voraussichtlichen Tragweite und der hohen Risiken für Grundrechte, Gesundheit und Sicherheit definitionsgemäß als hochriskant gelten. Andere als hochriskant geltende Systeme, die in Anhang III aufgeführt sind, umfassen die Bereiche Bildung, Verwaltung kritischer Infrastrukturen, Beschäftigung, biometrische Identifizierung und Kategorisierung sowie Zugang zu grundlegenden öffentlichen und privaten Diensten.

[12] Daher ist ein Rechtsrahmen der Union mit harmonisierten Vorschriften für künstliche Intelligenz erforderlich, um die Entwicklung, Verwendung und Verbreitung künstlicher Intelligenz im Binnenmarkt zu fördern und gleichzeitig einen hohen Schutz öffentlicher Interessen wie Gesundheit und Sicherheit und den Schutz der durch das Unionsrecht anerkannten und geschützten Grundrechte zu gewährleisten. Zur Umsetzung dieses Ziels sollten Vorschriften für das Inverkehrbringen und die Inbetriebnahme bestimmter KI-Systeme festgelegt werden, um das reibungslose Funktionieren des Binnenmarkts zu gewährleisten, sodass diesen Systemen der Grundsatz des freien Waren- und Dienstleistungsverkehrs zugutekommen kann (siehe Erwägungsgründe 2 und 5 des Vorschlags).

22. In solchen Vorschriften für Hochrisiko-KI-Systeme ist jedoch nicht festgelegt, ob solche Systeme von Strafverfolgungs- und Justizbehörden (oder Behörden in den anderen genannten Bereichen) eingesetzt werden sollten. Die vorgeschlagene Verordnung wird auf die tatsächliche Entwicklung von KI-Systemen, die von Strafverfolgungsbehörden eingesetzt werden können, sowie auf derzeit und in Zukunft eingesetzte KI-Systeme nur indirekt Einfluss nehmen. Daher beziehen sich die Vorschriften auf KI-Systeme, die von diesen Behörden gemäß ihrer „*Zweckbestimmung*“ eingesetzt werden (siehe z. B. Artikel 3 Nummer 12, Artikel 8 Absatz 2 und Anhang III). Die Einstufung eines bestimmten KI-Systems als hochriskant hat zur Folge, dass spezifische Vorschriften über Risikomanagement, Daten-Governance und technische Spezifikationen zur Anwendung kommen. Die Nutzer solcher Hochrisiko-KI-Systeme müssen die Gebrauchsanweisung befolgen, Protokoll führen und Datenschutz-Folgenabschätzungen durchführen.

23. Darüber hinaus können im Unionsrecht oder im nationalen Recht sowie unbeschadet der Möglichkeit der Nutzer, nach ihrem Ermessen eigene Ressourcen und Tätigkeiten zur Wahrnehmung der vom Anbieter angegebenen Maßnahmen der menschlichen Aufsicht zu organisieren (Artikel 29 Absatz 2 der vorgeschlagenen Verordnung), sonstige Pflichten der Nutzer festgelegt werden. Mit diesen Vorschriften werden weitere Vorkehrungen für den Schutz der Grundrechte im Zusammenhang mit Hochrisiko-KI-Systemen vorgesehen.

24. In diesem Zusammenhang sollte betont werden, dass die vorgeschlagene Verordnung keine Vorschriften enthält, die darauf abzielen, die Verwendung eines in Verkehr gebrachten Hochrisiko-KI-Systems durch Strafverfolgungsbehörden zu ermöglichen oder zu verhindern. Mit den vorgeschlagenen Vorschriften wird eine eigene Kennzeichnung (als hochriskant) für KI-Systeme eingeführt, die von den Strafverfolgungsbehörden aufgrund ihrer Zweckbestimmung entwickelt oder verwendet werden. Diese Verwendung würde dem nationalen Recht unterliegen, und bis zu einem gewissen Grad würde darüber von den Strafverfolgungsbehörden selbst entschieden. So sind in der vorgeschlagenen Verordnung in Artikel 29 (auf Gebrauchsanweisungen beschränkte) Mindestbedingungen für die Nutzung der Hochrisiko-KI-Systeme – einschließlich der in Anhang III Nummern 6, 7 und 8 aufgeführten Systeme – festgelegt, die durch nationales Recht ergänzt werden. Daher sollte im Einklang mit der Rechtsprechung des Gerichtshofs zwischen dem – nicht auf die Regelung der Nutzung von KI-Systemen durch Strafverfolgungsbehörden ausgerichteten – Ziel der vorgeschlagenen Verordnung einerseits und den für die Prüfung der Angemessenheit der Rechtsgrundlage irrelevanten unmittelbaren Auswirkungen[13] der vorgeschlagenen Verordnung andererseits unterschieden werden.

25. Die Nummern 6, 7 und 8 (Strafverfolgung, Migration und Justizverwaltung) sind bei Hochrisiko-KI-Systemen nicht vorherrschend. Nach der vorgeschlagenen Verordnung handelt es sich bei Hochrisiko-KI-Systemen nicht zwangsläufig um die in Anhang III aufgeführten Systeme. Bei den meisten Hochrisikosystemen handelt es sich vielmehr um die allgemein in Artikel 6 Absatz 1 Buchstaben a und b der vorgeschlagenen Verordnung (in Verbindung mit der Produktsicherheit) aufgeführten Systeme. Weitere Hochrisiko-KI-Systeme für andere Bereiche als Justiz und Inneres („JI“) sind in Anhang III unter den Nummern 1 (biometrische Identifizierung), 2 (kritische Infrastrukturen), 3 (allgemeine und berufliche Bildung) und 4 (Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit) aufgeführt. Sämtliche Nutzer solcher Hochrisiko-KI-Systeme unterliegen einer einheitlichen Regelung, die nicht von ihrem jeweiligen Status (z. B. ob sie Wirtschaftsakteure oder Behörden sind) abhängt, sondern unter dem Gesichtspunkt des Schutzes der Gesundheit, der Sicherheit und der Grundrechte festgelegt wird.

---

[13] Siehe Urteil des Gerichtshofs vom 21. Juni 2018, *Republik Polen gegen Europäisches Parlament und Rat der Europäischen Union*, C-5/16, EU:C:2018:483, Rn. 63 bis 68 und Urteil des Gerichtshofs vom 22. Juni 2022, *Leistritz AG gegen LH*, C-534/20, EU:C:2022:495, Rn. 28.

26. Die vorgeschlagene Verordnung enthält also harmonisierte Vorschriften für das Inverkehrbringen, die Inbetriebnahme und die Verwendung von KI-Systemen, unabhängig davon, ob die Systeme von privaten Akteuren oder Behörden, einschließlich – akzessorisch[14] – von Strafverfolgungs- und Justizbehörden, verwendet werden.

27. Abgesehen von der Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken, in deren Fall für die Verarbeitung personenbezogener Daten besondere Vorschriften gelten (siehe Abschnitt III), enthält die vorgeschlagene Verordnung keine harmonisierten Vorschriften für die Verwendung von Hochrisiko-KI-Systemen. Wie vorstehend in Nummer 18 und 19 erläutert, bezieht sich die Bezugnahme auf die Verwendung von Hochrisiko-KI-Systemen im Wesentlichen auf die Gebrauchsanweisung für das Produkt (Artikel 29) und steht im Zusammenhang mit den Entwicklern auferlegten Verpflichtungen. Wie in Nummer 22 dargelegt, liegt die Entscheidung darüber, ob Strafverfolgungs- oder Justizbehörden ein im Rahmen der vorgeschlagenen Verordnung rechtmäßig in Verkehr gebrachtes Hochrisiko-KI-System verwenden dürfen, beim nationalen Recht und den nationalen Behörden.

28. Daher ist Artikel 87 Absatz 2 AEUV, insbesondere Buchstabe a, keine geeignete Rechtsgrundlage für die vorgeschlagene Verordnung. Durch die Vorschriften des Vorschlags werden die Erhebung, Speicherung, Verarbeitung, Analyse und der Austausch relevanter Informationen weder gefördert noch behindert. Werden diese Tätigkeiten von Strafverfolgungsbehörden durchgeführt, so müssen lediglich einige unspezifische, harmonisierte Bedingungen eingehalten werden, damit die Rechte der Nutzer gewahrt sind. Ebenso gehört auch die Entwicklung gemeinsamer Ermittlungstechniken nicht zu den erklärten Zielen der vorgeschlagenen Verordnung. Die vorgeschlagenen Anforderungen an den Einsatz von Hochrisiko-KI-Systemen sind nicht spezifisch für den JI-Bereich und betreffen nicht die polizeiliche Zusammenarbeit im engeren Sinne des AEUV.

---

14 Siehe Gutachten des Gerichtshofs zum *Übereinkommen von Istanbul*, A-1/19, EU:C:2021:198, insbesondere Rn. 298 und 301.

29. In Bezug auf die Bestimmungen von Artikel 5 Absatz 4 der vorgeschlagenen Verordnung kann ein Mitgliedstaat dennoch beschließen, die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken zu genehmigen. Wenn er dies beschließt, ist der Mitgliedstaat verpflichtet, die erforderlichen detaillierten Vorschriften für die Beantragung, Erteilung und Ausübung der vorherigen Genehmigung sowie die betreffenden Straftaten, zu deren Ermittlung oder Verfolgung der Einsatz genehmigt wird, festzulegen.[15] Ausgehend von den Ergebnissen der Beratungen im Rat würden diese vorgeschlagenen Vorschriften nicht dazu führen, dass den jeweiligen nationalen Behörden neue Befugnisse übertragen würden. Vielmehr wird der Rückgriff auf bestehende oder etwaige künftige Mechanismen beschränkt, um den Schutz des Rechts auf Privatsphäre und personenbezogener Daten zu gewährleisten.

30. Vor diesem Hintergrund ist Artikel 114 AEUV die einzig geeignete Rechtsgrundlage für harmonisierte Vorschriften über Hochrisiko-KI-Systeme, einschließlich jener, die von Strafverfolgungs- und Justizbehörden verwendet werden, und eine Rechtsgrundlage im Bereich Justiz und Inneres gemäß dem Dritten Teil Titel V AEUV, wie Artikel 87 AEUV, ist in Bezug auf diese harmonisierten Vorschriften weder gerechtfertigt noch angemessen.

[15] Es sei darauf hingewiesen, dass Artikel 5 Absatz 4 des Vorschlags bestimmte Merkmale aufweist, die mit Artikel 15 Absatz 1 der Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) vergleichbar sind. Insbesondere sieht der Vorschlag für die Mitgliedstaaten die Möglichkeit vor, von bestimmten im Unionsrecht festgelegten Verboten abzuweichen. Nach ständiger Rechtsprechung fallen die nationalen Bestimmungen, die auf Ausnahmen von diesen Verboten ausgerichtet sind, zwangsläufig in den Anwendungsbereich des Unionsrechts, das wiederum zu einer diesbezüglichen Anwendung der Charta führt.

III. ANGEMESSENHEIT VON ARTIKEL 16 AEUV ALS ZUSÄTZLICHE RECHTSGRUNDLAGE

31. In der vorgeschlagenen Verordnung ist als Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Bereich der Strafverfolgung auch Artikel 16 AEUV vorgesehen, und die Erwägungsgründe 25 und 26 enthalten eine Bezugnahme auf Artikel 6a des Protokolls Nr. 21 und Artikel 2a des Protokolls 22 über die Verarbeitung personenbezogener Daten im Bereich der Kriminalprävention. Artikel 16 AEUV dient aus Sicht der Kommission ausschließlich als Rechtsgrundlage für jene Bestimmungen, mit denen die Verarbeitung biometrischer personenbezogener Daten gegenüber der Richtlinie 2016/680 zum Datenschutz bei der Strafverfolgung in ergänzender Weise Beschränkungen unterworfen wird. Artikel 5 Absatz 1 Buchstabe d ist als grundsätzliches Verbot formuliert, für das drei Ausnahmen gelten. Konkret ist die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken verboten, es sei denn, dies ist unbedingt erforderlich, um a) gezielt nach potenziellen Opfern von Straftaten zu suchen, b) einen drohenden Terroranschlag oder Angriff auf die körperliche Unversehrtheit/das Leben einer Person zu verhindern, c) eine Person, die eine Straftat begangen hat oder der Begehung einer Straftat verdächtig ist, ausfindig zu machen, zu identifizieren oder strafrechtlich zu verfolgen (unter Bezugnahme auf den Europäischen Haftbefehl). Für diese spezifische Nutzung von KI-Systemen durch Strafverfolgungsbehörden gelten gemäß Artikel 5 Absätze 2, 3 und 4 weitere Anforderungen, insbesondere eine Bewertung der Notwendigkeit und der Verhältnismäßigkeit, eine vorherige Genehmigung (außer in dringenden Fällen) und ein Beschluss der Mitgliedstaaten darüber, ob die spezifische Verwendung von KI-Instrumenten in solchen Fällen auf nationaler Ebene genehmigt werden soll.

32. Bei Artikel 5 handelt es sich um eine detaillierte Bestimmung zur Regelung einer spezifischen Nutzung von KI-Instrumenten, die nicht nur der Ergänzung des geltenden Rechtsrahmens der Union (der Richtlinie zum Datenschutz bei der Strafverfolgung, die ihrerseits auf Artikel 16 AEUV beruht) dient, sondern auch einen nationalen Umsetzungsrahmen erfordert.

33. Im Kern kann die spezifische Vorschrift in Artikel 5, obwohl sie als Verbot formuliert ist, als strenger und außerordentlicher Rahmen für die allgemeine Echtzeit-Überwachung von Personen in offenen Räumen durch KI-Instrumente zum Zweck ihrer Identifizierung bezeichnet werden. Das Verbot geht zudem über den einfachen Einsatz von Kameras zu Aufzeichnungszwecken hinaus, denn es bezieht sich auch auf den Einsatz von KI-Instrumenten zur automatisierten Erkennung menschlicher Merkmale (wie des Gesichts, aber auch der Gangart, von Fingerabdrücken, DNA, Stimme, Tastenanschlägen und anderen biometrischen oder verhaltensbezogenen Merkmalen) in öffentlich zugänglichen Räumen. Das beinhaltet auch die gleichzeitige Erfassung und Identifizierung von Personen durch den analytischen Vergleich/die Überprüfung von Daten. Ferner ist die Vorschrift auch unter dem Gesichtspunkt zu bewerten, dass die Echtzeit-Identifizierung durch private Nutzer im öffentlichen Raum (z. B. bei Veranstaltungen wie Fußballspielen) durchaus zulässig sein kann.

34. Weitere Präzisierungen der Kommission deuten darauf hin, dass derzeit kein Mitgliedstaat oder eventuell nur sehr wenige Mitgliedstaaten diesen konkreten Sachverhalt geregelt hat bzw. haben, um Strafverfolgungsbehörden den Einsatz von KI-Instrumenten zur Echtzeit-Erkennung von Personen im öffentlichen Raum zu gestatten. Zwar wurden praktisch keine belastbaren Beweise dafür erbracht, dass die geltenden Verfahrensweisen und Instrumente einer Änderung bedürfen, doch es scheint offensichtlich, dass dieser auf einem Verbot/Ausnahmen beruhende Ansatz bei künftigen Ermittlungstechniken, forensischen Methoden und Vorschriften zur Beweiserhebung berücksichtigt werden muss.

35. Was die Rechtsgrundlage betrifft, wird mit den Bestimmungen, die die Verarbeitung biometrischer personenbezogener Daten in ergänzender Weise (gegenüber der Richtlinie zum Datenschutz bei der Strafverfolgung) beschränken, offenbar das Ziel verfolgt, personenbezogene Daten durch die Festlegung geeigneter Schutzvorkehrungen zu schützen. Dieses Ziel ist untrennbar mit der Zielsetzung der Bestimmungen verbunden, die in den Anwendungsbereich von Artikel 114 AEUV fallen, ohne dass das eine gegenüber dem anderen nur zweitrangig und mittelbar ist. Mit der vorgeschlagenen Verordnung soll auf der Grundlage eines risikobasierten Ansatzes ein allgemeiner Rahmen für KI-Systeme festgelegt werden. In diesem Zusammenhang kann die horizontale Regelung von KI-Systemen strenge Schutzmaßnahmen umfassen, die für das spezifische KI-System der Echtzeiterkennung gelten. Ein solches spezifisches KI-System, das angemessene Schutzvorkehrungen zum Schutz personenbezogener Daten umfasst, ist daher untrennbar mit dem übergeordneten Ziel verbunden, das Funktionieren des Binnenmarkts zu verbessern, und ist demgegenüber weder zweitrangig noch mittelbar. Die vorgeschlagene Verordnung sollte daher im Einklang mit der einschlägigen Rechtsprechung (siehe Nummer 9) auf einer doppelten Rechtsgrundlage beruhen.

36. Die Frage, auf welche Rechtsgrundlage zur Regelung der Verarbeitung personenbezogener Daten in Bezug auf den Einsatz der Systeme gemäß Artikel 5 Absatz 1 Buchstabe d sowie Absätze 2 bis 4 der vorgeschlagenen Verordnung zurückgegriffen werden sollte, stellt sich jedoch weiterhin. Artikel 87 Absatz 2 Buchstabe a AEUV ist durchaus eine Rechtsgrundlage für Maßnahmen der Strafverfolgungsbehörden zur Verhütung, Aufdeckung und Untersuchung von Straftaten, wenn es um die Erhebung, Speicherung, Verarbeitung, Analyse und den Austausch relevanter Informationen geht.

37. Wie der Generalanwalt in seinen Schlussanträgen zum PNR-Abkommen mit Kanada (A1/15) ausgeführt hat, kann zwischen Artikel 16 AEUV zum einen und Artikel 87 Absatz 2 Buchstabe a AEUV sowie Artikel 82 Absatz 1 Buchstabe d AEUV zum anderen keine hierarchische Beziehung im Sinne von *lex generalis* zu *lex specialis* bestehen[16]. Wenn Maßnahmen zur Verhütung von Straftaten durchgeführt werden, ist Artikel 16 Absatz 2 AEUV die einzige Bestimmung, die für Vorschriften über den Schutz von Personen bei der Verarbeitung personenbezogener Daten durch die Strafverfolgungsbehörden der Mitgliedstaaten gilt. Die bloße Tatsache, dass in Artikel 5 auf die Auflistung schwerer Straftaten im Rahmenbeschluss über den Europäischen Haftbefehl verwiesen wird, ändert nichts an dieser Einschätzung: Diese Bezugnahme bedeutet nicht, dass dieser Rahmenbeschluss als solcher zur Anwendung kommt.[17] Es handelt sich dabei lediglich um eine Rechtsetzungstechnik zur Auflistung schwerer Straftaten – damit kein gesonderter Anhang erstellt werden muss.

38. Tatsache ist, dass die Vorschrift in Artikel 5 nicht eingeführt wird, um die Bedingungen für die Anwendung dieser JI-bezogenen Maßnahmen weiter abzugrenzen, sondern um sicherzustellen, dass Bedenken bezüglich der Grundrechte und vor allem der Notwendigkeit, bei der Erhebung und Verarbeitung biometrischer Daten das Recht auf Schutz der Privatsphäre und personenbezogener Daten zu wahren, in Zukunft bei jeder Verwendung biometrischer Echtzeit-Identifizierung durch KI-Systeme angemessen Rechnung getragen wird.

    Die Verordnung zielt diesbezüglich nicht darauf ab, ein neues verbindliches JI-spezifisches Verfahren festzulegen, sondern stützt sich vielmehr auf bewährte Verfahren, um die Wahrung der Grundrechte zu gewährleisten.

---

16 Siehe Schlussanträge des Generalanwalts P. Mengozzi vom 8. September 2016, *Entwurf eines Abkommens zwischen Kanada und der Europäischen Union*, Gutachten 1/15, EU:C:2016:656, Rn. 112 bis 120.

17 Zur Umsetzung dieser Auflistung schwerer Straftaten durch die Mitgliedstaaten siehe Urteil des Gerichtshofs vom 21. Juni 2022, *Ligue des droits humains gegen Ministerrat*, C-817/19, EU:C:2022:65, Rn. 150 bis 152.

39. Sollte Artikel 16 AEUV als zusätzliche Rechtsgrundlage angemessen sein, so stellt sich nun die Frage nach der Anwendung von Artikel 6a Protokoll Nr. 21und Artikel 2a Protokoll Nr. 22. Wie in den Erwägungsgründen 25 und 26 des Vorschlags erläutert wird, sind Irland oder Dänemark nämlich nicht an Artikel 5 Absatz 1 Buchstabe d und Absätze 2 und 3 der vorgeschlagenen Verordnung gebunden, wenn Strafverfolgungsbehörden in Irland oder Dänemark biometrische Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zur Verhütung von Straftaten einsetzen, wenn die beiden Mitgliedstaaten nicht an die entsprechenden Vorschriften über die polizeiliche Zusammenarbeit oder die justizielle Zusammenarbeit in Strafsachen gebunden sind. Das bedeutet nicht, dass in Artikel 5 Absatz 1 Buchstabe d sowie Absätze 2 und 3 Vorschriften über die polizeiliche Zusammenarbeit, z. B. Vorschriften über den Informationsaustausch zwischen Strafverfolgungsbehörden, enthalten sind. Es bedeutet lediglich, dass durch Artikel 5 Absatz 1 Buchstabe d und Absätze 2 und 3 der vorgeschlagenen Verordnung ähnlich wie durch die Richtlinie 2016/680 zum Datenschutz bei der Strafverfolgung, die auf der Grundlage von Artikel 16 AEUV als *lex generalis* erlassen wurde, nichts anderes, sondern allein die Verarbeitung biometrischer personenbezogener Daten im besonderen Kontext biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zur Verbrechensverhütung geregelt wird. Der Vorschlag der Kommission folgt in dieser Hinsicht dem Ansatz, den der Unionsgesetzgeber für die Richtlinie zum Datenschutz bei der Strafverfolgung gewählt hat, und er bestätigt, dass es in diesem Zusammenhang nicht gerechtfertigt ist, auf Artikel 87 Absatz 2 AEUV zurückzugreifen.

40. Neben Artikel 114 AEUV auch Artikel 16 AEUV aufzunehmen, ist in diesem Fall dadurch gerechtfertigt, dass die Nutzung eines genehmigten KI-Systems, das in das Recht auf den Schutz personenbezogener Daten eingreift, allein durch Artikel 5 Absatz 1 Buchstabe d sowie Absätze 2 und 3 geregelt wird, was das *lex specialis* zum allgemeinen Datenschutzrahmen darstellt. Solche *lex specialis*-Datenschutzvorschriften, die sich auf die Verwendung dieser sensiblen KI-Systeme auswirken, dürfen in Bezug auf die Rechtsgrundlage für den Binnenmarkt nicht als sekundäre oder mittelbare Rechtsvorschriften gelten. Daher ist die Aufnahme von Artikel 16 AEUV als Rechtsgrundlage in die vorgeschlagene Verordnung hinreichend begründet, und es ist nicht angemessen, hier auf Artikel 87 Absatz 2 Buchstabe a AEUV zurückzugreifen.

IV. FAZIT

41. In Anbetracht der vorstehenden Ausführungen ist der Juristische Dienst des Rates der Auffassung, dass

a) es gerechtfertigt und angemessen ist, als Rechtsgrundlagen für die vorgeschlagene Verordnung auf Artikel 16 und Artikel 114 AEUV zurückzugreifen,

b) es bezüglich der harmonisierten Vorschriften für KI-Systeme, die von Strafverfolgungs- oder Justizbehörden bereitgestellt oder verwendet werden können, weder gerechtfertigt noch angemessen ist, auf Artikel 87 Absatz 2 AEUV oder eine andere Rechtsgrundlage im Bereich Justiz und Inneres zurückzugreifen.