Mittwoch, 6. Oktober 2021

P9_TA(2021)0405

Künstliche Intelligenz im Strafrecht und ihre Verwendung durch die Polizei und Justizbehörden in Strafsachen

Entschließung des Europäischen Parlaments vom 6. Oktober 2021 zu dem Thema: Künstliche Intelligenz im Strafrecht und ihre Verwendung durch die Polizei und Justizbehörden in Strafsachen (2020/2016(INI))

(2022/C 132/02)

Das Europäische Parlament,

— unter Hinweis auf den Vertrag über die Europäische Union, insbesondere auf die Artikel 2 und 6, und auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

— unter Hinweis auf die Charta der Grundrechte der Europäischen Union (im Folgenden „Charta"), insbesondere die Artikel 6, 7, 8, 11, 12, 13, 20, 21, 24 und 47,

— unter Hinweis auf die Konvention zum Schutze der Menschenrechte und Grundfreiheiten,

— unter Hinweis auf das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV 108) und das dazugehörige Änderungsprotokoll (Übereinkommen 108+),

— unter Hinweis auf die Europäische Ethik-Charta der Europäischen Kommission für die Wirksamkeit der Justiz (CEPEJ) des Europarats über den Einsatz künstlicher Intelligenz in Justizsystemen,

— unter Hinweis auf die Mitteilung der Kommission vom 8. April 2019 mit dem Titel „Schaffung von Vertrauen in eine auf den Menschen ausgerichtete künstliche Intelligenz" (COM(2019)0168),

— unter Hinweis auf die von der hochrangigen Expertengruppe der Kommission für künstliche Intelligenz am 8. April 2019 veröffentlichten Ethik-Leitlinien für vertrauenswürdige künstliche Intelligenz,

— unter Hinweis auf das Weißbuch der Kommission vom 19. Februar 2020 mit dem Titel „Künstliche Intelligenz — ein europäisches Konzept für Exzellenz und Vertrauen" (COM(2020)0065),

— unter Hinweis auf die Mitteilung der Kommission vom 19. Februar 2020 mit dem Titel „Eine europäische Datenstrategie" (COM(2020)0066),

— unter Hinweis auf die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) ([1]),

— unter Hinweis auf die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates ([2]),

— unter Hinweis auf die Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG ([3]),

— unter Hinweis auf die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) ([4]),

([1]) ABl. L 119 vom 4.5.2016, S. 1.
([2]) ABl. L 119 vom 4.5.2016, S. 89.
([3]) ABl. L 295 vom 21.11.2018, S. 39.
([4]) ABl. L 201 vom 31.7.2002, S. 37.

— unter Hinweis auf die Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates ([5]),

— unter Hinweis auf seine Entschließung vom 19. Juni 2020 zu den Protestkundgebungen gegen Rassismus nach dem Tod von George Floyd ([6]),

— unter Hinweis auf seine Entschließung vom 14. März 2017 zu den Folgen von Massendaten für die Grundrechte: Privatsphäre, Datenschutz, Nichtdiskriminierung, Sicherheit und Rechtsdurchsetzung ([7]),

— unter Hinweis auf die Anhörung im Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) vom 20. Februar 2020 zu dem Thema: Künstliche Intelligenz im Strafrecht und ihre Verwendung durch die Polizei- und Justizbehörden in Strafsachen,

— unter Hinweis auf den Bericht über die Reise einer Delegation des LIBE-Ausschusses in die Vereinigten Staaten im Februar 2020,

— gestützt auf Artikel 54 seiner Geschäftsordnung,

— unter Hinweis auf die Stellungnahmen des Ausschusses für Binnenmarkt und Verbraucherschutz sowie des Rechtsausschusses,

— unter Hinweis auf den Bericht des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres (A9-0232/2021),

A. in der Erwägung, dass die digitalen Technologien im Allgemeinen und die durch künstliche Intelligenz (KI) ermöglichte starke Zunahme von Datenverarbeitung und Analytik im Besonderen außerordentlich vielversprechend sind und außerordentlich große Gefahren bergen; in der Erwägung, dass die Entwicklung der KI in den letzten Jahren einen großen Sprung nach vorn gemacht hat, was sie zu einer der strategischen Technologien des 21. Jahrhunderts macht, die das Potenzial hat, erhebliche Vorteile in Bezug auf Effizienz, Genauigkeit und Komfort zu bringen und damit positive Veränderungen für die europäische Wirtschaft und Gesellschaft zu bewirken, aber auch große Risiken für die Grundrechte und die auf Rechtsstaatlichkeit beruhenden Demokratien mit sich bringt; in der Erwägung, dass die KI nicht als Selbstzweck betrachtet werden sollte, sondern als ein Werkzeug, das den Menschen dient, mit dem letztendlichen Ziel, das menschliche Wohlergehen, die Fähigkeiten der Menschen und ihre Sicherheit zu steigern;

B. in der Erwägung, dass es trotz stetiger Fortschritte bei der Rechengeschwindigkeit und der Speicherkapazität der Computer noch keine Programme gibt, die es mit der menschlichen Flexibilität in ausgedehnteren Bereichen oder bei Aufgaben, die Kontextverständnis oder kritische Analyse erfordern, aufnehmen können; in der Erwägung, dass einige KI-Anwendungen das Leistungsniveau menschlicher Experten und Fachleute bei der Ausführung bestimmter spezifischer Aufgaben (z. B. im Bereich der Rechtstechnologie) erreicht haben und Ergebnisse mit drastisch höherer Geschwindigkeit und in sehr viel größerem Umfang liefern können;

C. in der Erwägung, dass einige Länder, darunter mehrere Mitgliedstaaten, mehr Gebrauch von KI-Anwendungen oder eingebetteten KI-Systemen in der Strafverfolgung und der Justiz machen als andere, was zum Teil auf fehlende Regulierung und auf regulatorische Unterschiede zurückzuführen ist, die den Einsatz von KI für bestimmte Zwecke ermöglichen oder verbieten; in der Erwägung, dass der zunehmende Einsatz von KI im Bereich des Strafrechts insbesondere auf den Verheißungen beruht, dass sie zur Abnahme bestimmter Arten von Straftaten und zu objektiveren Entscheidungen führen würde; in der Erwägung, dass diese Verheißungen jedoch nicht immer erfüllt werden;

D. in der Erwägung, dass die in der Charta verankerten Grundrechte und -freiheiten während des gesamten Lebenszyklus von KI und verwandten Technologien, insbesondere während ihrer Konzeption, ihrer Entwicklung, ihres Einsatzes und ihrer Verwendung, gewährleistet sein sollten und dass sie unter allen Umständen in der Strafverfolgung angewendet werden sollten;

E. in der Erwägung, dass die KI-Technologie so entwickelt werden sollte, dass sie den Menschen in den Mittelpunkt stellt, dass sie das Vertrauen der Öffentlichkeit verdient und dass sie stets im Dienste des Menschen arbeitet; in der Erwägung, dass KI-Systeme die ultimative Garantie bieten sollten, dass sie so konzipiert sind, dass sie stets von einer menschlichen Bedienungsperson abgeschaltet werden können;

F. in der Erwägung, dass es notwendig ist, dass KI-Systeme zum Schutz und Nutzen aller Mitglieder der Gesellschaft konzipiert werden (wobei bei der Ausgestaltung auch gefährdete und marginalisierte Bevölkerungsgruppen berücksichtigt werden müssen), dass sie nicht diskriminierend und sicher sind, dass ihre Entscheidungen erklärbar und transparent sind und dass sie die menschliche Autonomie und die Grundrechte respektieren, damit sie vertrauenswürdig sind, wie in den Ethik-Leitlinien der hochrangigen Expertengruppe für künstliche Intelligenz beschrieben;

([5]) ABl. L 135 vom 24.5.2016, S. 53.
([6]) ABl. C 362 vom 8.9.2021, S. 63.
([7]) ABl. C 263 vom 25.7.2018, S. 82.

G. in der Erwägung, dass die Union zusammen mit den Mitgliedstaaten eine maßgebliche Verantwortung dafür trägt, dass Entscheidungen im Umfeld des Lebenszyklus und des Einsatzes von KI-Anwendungen im Bereich der Justiz und der Strafverfolgung auf transparente Weise getroffen werden, die Grundrechte in vollem Umfang schützen und insbesondere keine Diskriminierung, Voreingenommenheit oder Vorurteile festschreiben, wo sie bestehen; in der Erwägung, dass bei den einschlägigen politischen Entscheidungen die Grundsätze der Notwendigkeit und der Verhältnismäßigkeit beachtet werden sollten, um die Verfassungsmäßigkeit und ein faires und humanes Justizsystem zu gewährleisten;

H. in der Erwägung, dass KI-Anwendungen große Chancen im Bereich der Strafverfolgung bieten können, insbesondere bei der Verbesserung der Arbeitsmethoden der Strafverfolgungs- und Justizbehörden und bei der effizienteren Bekämpfung bestimmter Arten von Straftaten, insbesondere von Finanzkriminalität, Geldwäsche und Terrorismusfinanzierung, sexuellem Missbrauch und Ausbeutung von Kindern im Internet sowie bestimmten Arten von Cyberkriminalität, und damit zur Sicherheit der EU-Bürger beitragen können, wenn sie auch gleichzeitig erhebliche Risiken für die Grundrechte der Menschen mit sich bringen können; in der Erwägung, dass eine undifferenzierte Anwendung von KI zum Zwecke der Massenüberwachung unverhältnismäßig wäre;

I. in der Erwägung, dass die Entwicklung und der Einsatz von KI-Systemen für Polizei- und Justizbehörden die Mitwirkung verschiedenster Einzelpersonen, Organisationen, Maschinenkomponenten, Software-Algorithmen und menschlicher Nutzer in einem häufig komplexen und herausfordernden Umfeld umfassen; in der Erwägung, dass sich die KI-Anwendungen für Strafverfolgung und Justiz in verschiedenen Entwicklungsphasen befinden, die von der Konzeptualisierung über Versuche mit Prototypen oder Evaluierungen bis hin zur Anwendung nach der Zulassung reichen; in der Erwägung, dass sich in Zukunft neue Einsatzmöglichkeiten ergeben können, wenn die Technologien dank der laufenden wissenschaftlichen Forschung weltweit ausgereifter werden;

J. in der Erwägung, dass ein klares Modell für die Zuweisung der rechtlichen Verantwortung für die potenziell schädlichen Auswirkungen von KI-Systemen im Bereich des Strafrechts unerlässlich ist; in der Erwägung, dass die Verwaltungsvorschriften in diesem Bereich stets die menschliche Verantwortlichkeit wahren sollten und in erster Linie darauf abzielen müssen, schädliche Auswirkungen überhaupt zu vermeiden;

K. in der Erwägung, dass letztendlich die Mitgliedstaaten für die Gewährleistung der uneingeschränkten Achtung der Grundrechte verantwortlich sind, wenn KI-Systeme auf dem Gebiet der Strafverfolgung und der Justiz eingesetzt werden;

L. in der Erwägung, dass das Verhältnis zwischen dem Schutz der Grundrechte und einer effektiven Polizeiarbeit bei den Diskussionen darüber, ob und wie KI in der Strafverfolgung eingesetzt werden sollte, stets ein wichtiger Faktor sein muss, da die Entscheidungen in diesem Bereich langfristige Auswirkungen auf das Leben und die Freiheit Einzelner haben können; in der Erwägung, dass dies besonders wichtig ist, da KI das Potenzial hat, ein fester Bestandteil unseres strafrechtlichen Ökosystems zu werden, indem sie Ermittlungsanalysen und -unterstützung bietet;

M. in der Erwägung, dass KI von den Strafverfolgungsbehörden genutzt wird bei Anwendungen wie Gesichtserkennungstechnologien — etwa zur Durchsuchung von Fahndungsdatenbanken und zur Identifizierung von Opfern von Menschenhandel oder sexueller Ausbeutung oder sexuellem Missbrauch von Kindern –, automatische Nummernschilderkennung, Sprecheridentifizierung, Spracherkennung, Lippenlesetechnologien, akustische Überwachung (d. h. Schusserkennungsalgorithmen), autonome Forschung und Analyse identifizierter Datenbanken, Vorhersage (vorausschauende Polizeiarbeit und Kriminalitäts-Hotspot-Analyse), Verhaltenserkennungswerkzeuge, moderne virtuelle Autopsie-Instrumente, die bei der Bestimmung der Todesursache nützlich sind, autonome Werkzeuge zur Erkennung von Finanzbetrug und Terrorismusfinanzierung, Überwachung sozialer Medien (Scraping und das Sammeln von Daten zum Aufspüren von Zusammenhängen) und automatisierte Überwachungssysteme mit unterschiedlichen Erkennungsfähigkeiten (wie Herzschlagerkennung und Wärmebildkameras); in der Erwägung, dass die vorgenannten Anwendungen neben anderen potenziellen oder künftigen Anwendungen von KI-Technologie in der Strafverfolgung einen sehr unterschiedlichen Grad an Zuverlässigkeit und Genauigkeit sowie an Auswirkungen auf den Schutz der Grundrechte und auf die Dynamik der Strafjustizsysteme aufweisen können; in der Erwägung, dass viele dieser Werkzeuge in Nicht-EU-Ländern eingesetzt werden, aber nach dem Besitzstand der Union im Bereich des Datenschutzes und nach der Rechtsprechung rechtswidrig wären; in der Erwägung, dass der routinemäßige Einsatz von Algorithmen, selbst mit einer geringen Falsch-Positiv-Rate, zu Fehlalarmen führen kann, deren Zahl bei weitem höher liegt als die Zahl der richtigen Alarme;

N. in der Erwägung, dass KI-Instrumente und -Anwendungen auch von der Justiz in mehreren Ländern weltweit eingesetzt werden, u. a. zur Unterstützung von Entscheidungen über die Untersuchungshaft, bei der Strafzumessung, der Berechnung der Rückfallwahrscheinlichkeit und der Festsetzung von Bewährungsstrafen, der Online-Streitbeilegung, der Bearbeitung der Rechtsprechung und der Bereitstellung eines erleichterten Zugangs zum Recht; in der Erwägung, dass dies die Möglichkeiten von People of Color und anderen Minderheiten verfälscht und schmälert; in der Erwägung, dass ihr Einsatz in der EU derzeit mit Ausnahme einiger Mitgliedstaaten hauptsächlich auf Zivilsachen beschränkt ist;

O. in der Erwägung, dass der Einsatz von KI in der Strafverfolgung eine Reihe von potenziell hohen und in einigen Fällen nicht hinnehmbaren Risiken für den Schutz der Grundrechte des Einzelnen mit sich bringt, wie etwa undurchsichtige Entscheidungsfindung, verschiedene Arten von Diskriminierung und dem zugrunde liegenden Algorithmus innewohnende Fehler, die durch Rückkopplungsschleifen verstärkt werden können, sowie Risiken für den Schutz der

Privatsphäre und personenbezogener Daten, den Schutz der Meinungs- und Informationsfreiheit, die Unschuldsvermutung, das Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren sowie Risiken für die Freiheit und Sicherheit des Einzelnen;

P. in der Erwägung, dass KI-Systeme, die von den Strafverfolgungs- und Justizbehörden eingesetzt werden, auch anfällig sind für KI-unterstützte Angriffe auf Informationssysteme und die Verfälschung von Daten („Data poisoning"), bei der absichtlich ein falscher Datensatz eingegeben wird, um verzerrte Ergebnisse zu erzielen; in der Erwägung, dass in diesen Situationen der daraus resultierende Schaden potenziell sogar noch bedeutender ist und zu einem exponentiell höheren Schadensausmaß sowohl für Einzelpersonen als auch für Gruppen führen kann;

Q. in der Erwägung, dass der Einsatz von KI im Bereich der Strafverfolgung und der Justiz nicht als bloß technisch machbar betrachtet werden sollte, sondern als eine politische Entscheidung, die die Konzeption und die Ziele der Strafverfolgung und der Strafrechtssysteme betrifft; in der Erwägung, dass das moderne Strafrecht auf der Auffassung beruht, dass die Behörden auf eine Straftat reagieren, nachdem diese begangen wurde, und nicht davon ausgeht, dass alle Menschen gefährlich sind und permanent überwacht werden müssen, damit ein potenzielles Fehlverhalten verhindert werden kann; in der Erwägung, dass KI-basierte Überwachungstechniken diesen Ansatz ernsthaft in Frage stellen und es dringend erforderlich machen, dass Gesetzgeber weltweit die Folgen der Zulassung des Einsatzes von Technologien gründlich prüfen, die dazu führen, dass der Mensch bei der Strafverfolgung und der Urteilsfällung eine geringere Rolle spielt;

1. bekräftigt, dass, da die Verarbeitung großer Mengen personenbezogener Daten im Mittelpunkt der künstlichen Intelligenz steht, das Recht auf Schutz des Privatlebens und das Recht auf den Schutz personenbezogener Daten für alle Bereiche der künstlichen Intelligenz gelten und dass der Rechtsrahmen der Union für den Datenschutz und den Schutz der Privatsphäre uneingeschränkt eingehalten werden muss; ruft daher in Erinnerung, dass die EU bereits Datenschutzstandards für die Strafverfolgung festgelegt hat, die die Grundlage für jegliche künftige Regulierung der KI für den Einsatz in der Strafverfolgung und der Justiz bilden; erinnert daran, dass die Verarbeitung personenbezogener Daten rechtmäßig und nach Treu und Glauben erfolgen sollte, dass die Zwecke der Verarbeitung angegeben, eindeutig und rechtmäßig sein sollten, dass die Verarbeitung dem Zweck, zu dem sie erfolgt, entsprechen, dafür erheblich sein und nicht darüber hinausgehen sollte, dass sie sachlich richtig sein und auf dem neuesten Stand gehalten werden sollte und dass unrichtige Daten, sofern keine Einschränkungen gelten, berichtigt oder gelöscht werden sollten, dass die Daten nicht länger als nötig aufbewahrt werden sollten, dass klare und angemessene Fristen für die Löschung oder für die regelmäßige Überprüfung der Notwendigkeit der Speicherung solcher Daten festgelegt werden sollten und dass die Verarbeitung auf sichere Weise erfolgen sollte; betont ferner, dass eine mögliche Identifizierung von Personen durch eine KI-Anwendung unter Verwendung von Daten, die zuvor anonymisiert wurden, verhindert werden sollte;

2. bekräftigt, dass alle KI-Lösungen für die Strafverfolgung und die Justiz auch die Grundsätze der Menschenwürde, der Nichtdiskriminierung und der Freizügigkeit, die Unschuldsvermutung und das Recht auf Verteidigung, einschließlich des Rechts zur Aussageverweigerung, die Freiheit der Meinungsäußerung und die Informationsfreiheit, die Versammlungs- und Vereinigungsfreiheit, die Gleichheit vor dem Gesetz, den Grundsatz der Waffengleichheit und das Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren gemäß der Charta und der Europäischen Menschenrechtskonvention in vollem Umfang achten müssen; betont, dass der Einsatz von KI-Anwendungen untersagt werden muss, wenn er nicht mit den Grundrechten vereinbar ist;

3. erkennt an, dass die Geschwindigkeit, mit der KI-Anwendungen weltweit entwickelt werden, keine erschöpfende Auflistung von Anwendungen zulässt und daher ein klares und kohärentes Governance-Modell erforderlich ist, das sowohl die Grundrechte des Einzelnen als auch Rechtsklarheit für die Entwickler in Anbetracht der ständigen Weiterentwicklung der Technologie gewährleistet; ist jedoch der Ansicht, dass in Anbetracht der Rolle und Verantwortung von Polizei- und Justizbehörden und der Auswirkungen von Entscheidungen, die sie zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Vollstreckung von strafrechtlichen Sanktionen treffen, der Einsatz von KI-Anwendungen dann als hochrisikoreich eingestuft werden muss, wenn die Möglichkeit besteht, dass er beträchtliche Auswirkungen auf das Leben von Einzelpersonen hat;

4. vertritt in diesem Zusammenhang die Auffassung, dass alle KI-Instrumente, die von den Strafverfolgungsbehörden oder der Justiz entwickelt oder eingesetzt werden, mindestens sicher, robust und zweckmäßig sein und den Grundsätzen der Fairness, der Datenminimierung, der Rechenschaftspflicht, der Transparenz, der Nichtdiskriminierung und der Erklärbarkeit entsprechen sollten und dass ihre Entwicklung, ihr Einsatz und ihre Verwendung einer Risikobewertung und einer strengen Prüfung der Notwendigkeit und Verhältnismäßigkeit unterliegen sollten, wobei die Schutzmaßnahmen in einem angemessenen Verhältnis zu den ermittelten Risiken stehen müssen; hebt hervor, dass das Vertrauen der Bürger in die Verwendung von in der EU entwickelter und eingesetzter KI von der uneingeschränkten Erfüllung dieser Kriterien abhängt;

5. erkennt den positiven Beitrag bestimmter Arten von KI-Anwendungen zur Arbeit der Strafverfolgungs- und Justizbehörden in der gesamten Union an; hebt beispielsweise die bessere Bearbeitung der Rechtsprechung hervor, die durch Instrumente mit zusätzlichen Suchoptionen ermöglicht wird; ist der Auffassung, dass es eine Reihe weiterer potenzieller Verwendungen von KI für die Strafverfolgung und die Justiz gibt, die unter Berücksichtigung der fünf Grundsätze der von

der Europäischen Kommission für die Wirksamkeit der Justiz (CEPEJ) angenommenen Ethik-Charta für den Einsatz künstlicher Intelligenz in Justizsystemen und deren Umfeld erforscht werden könnten, wobei den von der CEPEJ genannten „mit größten Vorbehalten zu betrachtenden Verwendungen" besondere Aufmerksamkeit gewidmet werden sollte;

6. betont, dass jede Technologie zweckentfremdet werden kann, und fordert daher eine strenge demokratische Kontrolle und unabhängige Aufsicht über alle KI-fähigen Technologien, die von Strafverfolgungs- und Justizbehörden eingesetzt werden, insbesondere über solche, die für die Massenüberwachung oder das Erstellen von Massenprofilen zweckentfremdet werden können; nimmt daher mit großer Sorge das Potenzial bestimmter KI-Technologien zur Kenntnis, die in der Strafverfolgung für Massenüberwachungszwecke eingesetzt werden; unterstreicht das rechtliche Erfordernis, eine Massenüberwachung mittels KI-Technologien zu verhindern, die per definitionem nicht den Grundsätzen der Notwendigkeit und Verhältnismäßigkeit entspricht, und den Einsatz von Anwendungen zu verbieten, die dazu führen könnten;

7. betont, dass der in einigen Nicht-EU-Ländern verfolgte Ansatz hinsichtlich der Entwicklung, des Einsatzes und der Verwendung von Massenüberwachungstechnologien unverhältnismäßig in Grundrechtspositionen eingreift und daher von der EU nicht übernommen werden darf; betont daher, dass auch die Schutzmaßnahmen gegen den Missbrauch von KI-Technologien durch Strafverfolgungs- und Justizbehörden unionsweit einheitlich geregelt werden müssen;

8. betont das Potenzial für Verzerrung und Diskriminierung, das sich aus dem Einsatz von KI-Anwendungen wie etwa maschinellem Lernen ergibt, einschließlich der Algorithmen, auf denen solche Anwendungen beruhen; stellt fest, dass Verzerrungen den zugrunde liegenden Datensätzen innewohnen können, insbesondere wenn historische Daten verwendet, von den Entwicklern der Algorithmen eingeführt oder bei der Implementierung der Systeme in der realen Welt erzeugt werden; weist darauf hin, dass die von KI-Anwendungen gelieferten Ergebnisse zwangsläufig von der Qualität der verwendeten Daten beeinflusst werden und dass solche inhärenten Verzerrungen die Tendenz haben, allmählich zuzunehmen und dadurch bestehende Diskriminierungen fortzusetzen und zu verstärken, insbesondere für Personen, die bestimmten ethnischen Gruppen oder Gemeinschaften, die aufgrund von Rassismus benachteiligt sind, angehören;

9. unterstreicht die Tatsache, dass viele der derzeit verwendeten algorithmusgesteuerten Identifizierungstechnologien unverhältnismäßig viele Personen falsch identifizieren und falsch klassifizieren und daher Menschen, die aufgrund von Rassismus benachteiligt sind, Personen, die bestimmten ethnischen Gemeinschaften angehören, LGBTI-Personen, Kindern und älteren Menschen sowie Frauen Schaden zufügen; erinnert daran, dass Einzelpersonen nicht nur das Recht haben, korrekt identifiziert zu werden, sondern auch das Recht, überhaupt nicht identifiziert zu werden, es sei denn, dies ist aus zwingendem und rechtmäßigem öffentlichem Interesse gesetzlich vorgeschrieben; betont, dass KI-Vorhersagen, die auf Merkmalen einer bestimmten Personengruppe beruhen, dazu führen, dass bestehende Formen der Diskriminierung verstärkt und reproduziert werden; ist der Auffassung, dass große Anstrengungen unternommen werden sollten, um automatisierte Diskriminierung und Voreingenommenheit zu vermeiden; fordert robuste zusätzliche Schutzmaßnahmen, wenn KI-Systeme in der Strafverfolgung oder in der Justiz bei Minderjährigen oder in Bezug auf sie eingesetzt werden;

10. betont die Machtasymmetrie zwischen denjenigen, die KI-Technologien einsetzen, und denjenigen, die ihnen unterworfen sind; betont, dass es zwingend erforderlich ist, dass der Einsatz von KI-Instrumenten durch Strafverfolgungs- und Justizbehörden nicht zu einem Faktor der Ungleichheit, der sozialen Spaltung oder der Ausgrenzung wird; unterstreicht die Auswirkungen des Einsatzes von KI-Instrumenten auf die Verteidigungsrechte von Verdächtigen, die Schwierigkeit, aussagekräftige Informationen über ihre Funktionsweise zu erhalten, und die daraus resultierende Schwierigkeit der Anfechtung ihrer Ergebnisse vor Gericht, insbesondere durch Personen, gegen die ermittelt wird;

11. nimmt die Risiken zur Kenntnis, die insbesondere mit Datenlecks, Verstößen gegen die Datensicherheit und unbefugtem Zugriff auf personenbezogene Daten und andere Informationen im Zusammenhang beispielsweise mit strafrechtlichen Ermittlungen oder Gerichtsverfahren verbunden sind, die von KI-Systemen verarbeitet werden; betont, dass die Sicherheitsaspekte von KI-Systemen, die in der Strafverfolgung und in der Justiz eingesetzt werden, sorgfältig geprüft werden und hinreichend robust und widerstandsfähig sein müssen, um die potenziell katastrophalen Folgen böswilliger Angriffe auf KI-Systeme abzuwenden; unterstreicht die Bedeutung eingebauter Sicherheit (security by design) sowie einer spezifischen menschlichen Aufsicht vor dem Betrieb bestimmter kritischer Anwendungen und fordert daher, dass Strafverfolgungs- und Justizbehörden nur KI-Anwendungen einsetzen, die dem Grundsatz des „eingebauten Datenschutzes" (privacy and data protection by design) entsprechen, um eine schleichende Ausweitung auf andere Zwecke zu vermeiden;

12. betont, dass kein KI-System, das von Strafverfolgungsbehörden oder der Justiz eingesetzt wird, in die Lage versetzt werden sollte, die körperliche Unversehrtheit von Menschen zu schädigen oder Einzelpersonen Rechte zu übertragen bzw. rechtliche Verpflichtungen aufzuerlegen;

13. erkennt die Herausforderungen an, die sich angesichts der Komplexität der Entwicklung und des Betriebs von KI-Systemen in Bezug auf die korrekte Zuweisung rechtlicher Verantwortung und Haftung für potenzielle Schäden stellen; hält es für notwendig, eine klare und faire Regelung für die Zuweisung der rechtlichen Verantwortung und Haftung für die möglichen nachteiligen Folgen zu schaffen, die durch diese fortgeschrittenen digitalen Technologien verursacht werden;

betont jedoch, dass das Ziel in erster Linie darin bestehen muss, das Eintreten solcher Folgen von vornherein zu verhindern; fordert daher die Anwendung des Vorsorgeprinzips bei allen Anwendungen von KI im Rahmen der Strafverfolgung; betont, dass die rechtliche Verantwortung und Haftung immer bei einer natürlichen oder juristischen Person liegen muss, die bei Entscheidungen, die mit Hilfe von KI getroffen werden, immer identifiziert werden muss; betont daher die Notwendigkeit, die Transparenz der Unternehmensstrukturen, die KI-Systeme herstellen und verwalten, sicherzustellen;

14. erachtet es sowohl für die Wirksamkeit der Ausübung von Verteidigungsrechten als auch für die Transparenz der nationalen Strafrechtssysteme für wesentlich, dass ein spezifischer, klarer und präziser Rechtsrahmen die Bedingungen, Modalitäten und Folgen des Einsatzes von KI-Instrumenten im Bereich der Strafverfolgung und der Justiz sowie die Rechte der betroffenen Personen und wirksame und leicht zugängliche Beschwerde- und Rechtsbehelfsverfahren, einschließlich gerichtlicher Rechtsbehelfe, regelt; unterstreicht das Recht der Parteien eines Strafverfahrens auf Zugang zu dem Datenerhebungsprozess und den damit verbundenen Bewertungen, die durch den Einsatz von KI-Anwendungen vorgenommen oder erlangt wurden; unterstreicht die Notwendigkeit, dass die Vollstreckungsbehörden, die an der justiziellen Zusammenarbeit beteiligt sind, bei der Entscheidung über ein Ersuchen um Auslieferung (oder Übergabe) an einen anderen Mitgliedstaat oder einen Nicht-EU-Staat prüfen, ob der Einsatz von KI-Instrumenten in dem ersuchenden Land das Grundrecht auf ein faires Verfahren offenkundig beeinträchtigen könnte; fordert die Kommission auf, Leitlinien für die Durchführung einer solchen Prüfung im Rahmen der justiziellen Zusammenarbeit in Strafsachen herauszugeben; besteht darauf, dass die Mitgliedstaaten im Einklang mit den geltenden Rechtsvorschriften sicherstellen sollten, dass Einzelpersonen darüber informiert werden, wenn Strafverfolgungsbehörden oder die Justiz KI-Anwendungen bei ihnen einsetzen;

15. weist darauf hin, dass Menschen nicht in der Lage sein werden, eine unabhängige Bewertung vorzunehmen, wenn sie sich ausschließlich auf von Maschinen generierte Daten, Profile und Empfehlungen stützen; weist auf die potenziell schwerwiegenden nachteiligen Folgen in Fällen — insbesondere im Bereich der Strafverfolgung und der Justiz — hin, in denen Einzelpersonen zu sehr auf den scheinbar objektiven und wissenschaftlichen Charakter von KI-Instrumenten vertrauen und nicht die Möglichkeit in Betracht ziehen, dass ihre Ergebnisse falsch, unvollständig, irrelevant oder diskriminierend sein könnten; betont, dass ein übermäßiges Vertrauen in die von KI-Systemen gelieferten Ergebnisse vermieden werden sollte, und hebt hervor, dass die Behörden Vertrauen und Wissen aufbauen müssen, um eine algorithmische Empfehlung zu hinterfragen oder ihr nicht zu folgen; hält es für wichtig, realistische Erwartungen an solche technologischen Lösungen zu haben und keine perfekten Lösungen für die Strafverfolgung und die Aufdeckung aller begangenen Straftaten zu versprechen;

16. betont, dass im Kontext von Justiz und Strafverfolgung die Entscheidung, die rechtliche oder ähnliche Wirkungen entfaltet, immer von einem Menschen getroffen werden muss, der für die getroffenen Entscheidungen zur Rechenschaft gezogen werden kann; ist der Ansicht, dass diejenigen, die KI-gestützten Systemen unterworfen sind, die Möglichkeit haben müssen, Rechtsmittel einzulegen; erinnert daran, dass eine Person nach EU-Recht das Recht hat, nicht einer ausschließlich auf einer automatisierten Verarbeitung von Daten beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie erheblich beeinträchtigt; betont ferner, dass automatisierte Einzelentscheidungen nicht auf besonderen Kategorien personenbezogener Daten beruhen dürfen, es sei denn, es bestehen geeignete Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person; betont, dass das Unionsrecht eine Profilerstellung, die zu Diskriminierung natürlicher Personen auf der Grundlage bestimmter Kategorien personenbezogener Daten führt, verbietet; weist darauf hin, dass Entscheidungen im Bereich der Strafverfolgung fast immer Entscheidungen sind, die aufgrund der exekutiven Qualität von Strafverfolgungsbehörden und ihren Maßnahmen eine rechtliche Wirkung gegenüber der betroffenen Person nach sich ziehen; stellt fest, dass der Einsatz von KI menschliche Entscheidungen beeinflussen und sich auf alle Stadien von Strafverfahren auswirken kann; vertritt daher die Auffassung, dass Behörden, die KI-Systeme einsetzen, extrem hohe rechtliche Standards einhalten und menschliches Tätigwerden sicherstellen müssen, insbesondere bei der Analyse von Daten, die von solchen Systemen stammen; verlangt daher, dass das souveräne Ermessen von Richtern und die Entscheidungsfindung in jedem Einzelfall nicht angetastet werden; fordert ein Verbot des Einsatzes von KI und verwandten Technologien für die Erstellung von Vorschlägen von Gerichtsentscheidungen;

17. fordert algorithmische Erklärbarkeit, Transparenz, Rückverfolgbarkeit und Überprüfung als notwendigen Teil der Aufsicht, um sicherzustellen, dass die Entwicklung, der Einsatz und die Nutzung von KI-Systemen für Justiz und Strafverfolgung den Grundrechten entsprechen und das Vertrauen der Bürger genießen, sowie um sicherzustellen, dass die von KI-Algorithmen erzeugten Ergebnisse für die Nutzer und die diesen Systemen unterworfenen Personen verständlich gemacht werden können und dass Transparenz über die Quelldaten und die Art und Weise besteht, wie das System zu einer bestimmten Schlussfolgerung gelangt ist; weist darauf hin, dass es Strafverfolgungs- und Justizbehörden in der Union — zur Gewährleistung der technischen Transparenz, Robustheit und Genauigkeit — nur erlaubt sein sollte, solche Instrumente und Systeme zu erwerben, deren Algorithmen und Logik überprüfbar und zumindest der Polizei und der Justiz sowie den unabhängigen Prüfern zugänglich sind, um ihre Bewertung, Prüfung und Kontrolle zu ermöglichen, und dass sie von den Verkäufern nicht verschlossen oder als „geschützt“ gekennzeichnet werden dürfen; weist ferner darauf hin, dass eine Dokumentation in klarer, verständlicher Sprache über die Art des Dienstes, die entwickelten Instrumente, die Leistung und die Bedingungen, unter denen sie erwartungsgemäß funktionieren, sowie die Risiken, die sie verursachen könnten,

bereitgestellt werden sollte; fordert daher die Justiz- und Strafverfolgungsbehörden auf, für proaktive und vollständige Transparenz in Bezug auf private Unternehmen zu sorgen, die ihnen KI-Systeme für die Zwecke der Strafverfolgung und der Justiz zur Verfügung stellen; empfiehlt daher die Verwendung von Open-Source-Software, wo immer dies möglich ist;

18. empfiehlt den Strafverfolgungs- und Justizbehörden, die Bereiche zu ermitteln und zu bewerten, in denen einige maßgeschneiderte KI-Lösungen von Nutzen sein könnten, und sich über bewährte Verfahren für den Einsatz von KI auszutauschen; fordert, dass die Mitgliedstaaten und die EU-Agenturen geeignete Verfahren für die öffentliche Beschaffung von KI-Systemen einführen, wenn diese in einem Kontext der Strafverfolgung oder Justiz eingesetzt werden, um die Einhaltung der Grundrechte und der geltenden Rechtsvorschriften zu gewährleisten, wobei auch sichergestellt werden muss, dass die Software-Dokumentation und die Algorithmen den zuständigen Behörden und Aufsichtsbehörden zu Überprüfungszwecken zur Verfügung stehen und zugänglich sind; fordert insbesondere verbindliche Regeln, durch die eine öffentliche Offenlegung von öffentlich-privaten Partnerschaften, Verträgen und Akquisitionen und des Zwecks, für den sie beschafft werden, vorgeschrieben wird; betont, dass die Behörden mit den notwendigen Finanzmitteln und mit dem erforderlichen Fachwissen ausgestattet werden müssen, damit gewährleistet ist, dass die ethischen, rechtlichen und technischen Anforderungen, die mit dem Einsatz von KI verknüpft sind, uneingeschränkt erfüllt werden;

19. fordert die Rückverfolgbarkeit von KI-Systemen und des Entscheidungsprozesses, die ihre Funktionen umreißt, die Fähigkeiten und Grenzen der Systeme definiert und durch eine verpflichtende Dokumentation nachvollziehbar macht, woher die bestimmenden Kriterien für eine Entscheidung stammen; unterstreicht die Bedeutung einer vollständigen Dokumentation der Trainingsdaten, ihres Kontexts, ihres Zwecks, ihrer Genauigkeit und ihrer Nebenwirkungen sowie ihrer Verarbeitung durch die Urheber und Entwickler der Algorithmen und ihrer Einhaltung der Grundrechte; betont, dass es immer möglich sein muss, die Rechenvorgänge eines KI-Systems auf eine für Menschen verständliche Form zu reduzieren;

20. fordert, dass vor der Einführung oder dem Einsatz von KI-Systemen für die Strafverfolgung oder die Justiz eine obligatorische Folgenabschätzung für die Grundrechte durchgeführt wird, um mögliche Risiken für die Grundrechte abzuschätzen; erinnert daran, dass die vorherige Datenschutzfolgenabschätzung für jede Art der Verarbeitung obligatorisch ist, insbesondere bei der Verwendung neuer Technologien, die wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führen wird, und ist der Ansicht, dass dies bei den meisten KI-Technologien im Bereich der Strafverfolgung und der Justiz der Fall ist; unterstreicht die Sachkenntnis von Datenschutzbehörden und Grundrechtsagenturen, wenn es um die Bewertung dieser Systeme geht; betont, dass diese Folgenabschätzungen für die Grundrechte so offen wie möglich und unter aktiver Beteiligung der Zivilgesellschaft durchgeführt werden sollten; fordert, dass die Folgenabschätzungen auch klare Angaben zu den Schutzmaßnahmen enthalten, die erforderlich sind, um die ermittelten Risiken zu bewältigen, und dass sie vor dem Einsatz eines KI-Systems so weit wie möglich öffentlich zugänglich gemacht werden;

21. betont, dass nur eine robuste europäische KI-Governance mit unabhängiger Evaluierung die notwendige Umsetzung der Grundrechtsprinzipien ermöglichen kann; fordert eine regelmäßige obligatorische Prüfung aller von Strafverfolgungsbehörden und der Justiz eingesetzten KI-Systeme, die das Potenzial haben, das Leben von Einzelpersonen erheblich zu beeinträchtigen, durch eine unabhängige Behörde, um algorithmische Systeme, ihren Kontext, ihren Zweck, ihre Genauigkeit, ihre Leistung und ihr Ausmaß zu testen und zu bewerten und, sobald sie in Betrieb sind, um unerwünschte und nachteilige Auswirkungen zu erkennen, zu untersuchen, zu diagnostizieren und zu beheben und um sicherzustellen, dass die KI-Systeme wie beabsichtigt funktionieren; fordert daher einen klaren institutionellen Rahmen für diesen Zweck, einschließlich einer angemessenen Regulierungsaufsicht und Beaufsichtigung, um eine vollständige Umsetzung sicherzustellen und eine demokratische Debatte in voller Sachkenntnis über die Notwendigkeit und Verhältnismäßigkeit von KI im Bereich der Strafjustiz zu gewährleisten; betont, dass die Ergebnisse dieser Prüfungen in öffentlichen Registern zur Verfügung gestellt werden sollten, sodass die Bürgerinnen und Bürger die KI-Systeme, die eingesetzt werden, kennen und wissen, welche Maßnahmen getroffen werden, um einer Verletzung von Grundrechten abzuhelfen;

22. betont, dass die Datensätze und algorithmischen Systeme, die bei der Erstellung von Klassifizierungen, Bewertungen und Vorhersagen in den verschiedenen Phasen der Datenverarbeitung bei der Entwicklung von KI und verwandten Technologien verwendet werden, auch zu einer unterschiedlichen Behandlung und einer unmittelbaren und mittelbaren Diskriminierung von Personengruppen führen können, insbesondere da die Daten, die zum Trainieren von Algorithmen für die vorausschauende Polizeiarbeit verwendet werden, die aktuellen Überwachungsprioritäten widerspiegeln und folglich dazu führen können, dass bestehende Vorurteile reproduziert und verstärkt werden; betont daher, dass KI-Technologien, insbesondere wenn sie für die Strafverfolgung und die Justiz eingesetzt werden, interdisziplinäre Forschung und Beiträge erfordern, auch aus den Bereichen der Wissenschafts- und Technologiestudien, der Forschung zum Thema „Critical Race“ (Rasse als Analysekategorie des Rechts), der Behindertenforschung und anderen Disziplinen, die sich mit dem sozialen Kontext befassen, einschließlich der Art und Weise, wie Unterschiede konstruiert werden, sowie der Arbeit der Klassifizierung und ihrer Folgen; betont daher, dass systematisch in die Einbeziehung dieser Fachrichtungen in Studien und Forschung über künstliche Intelligenz auf allen Ebenen investiert werden muss; betont ferner, wie wichtig es ist, dass sich in den Teams, die diese KI-Systeme für die Strafverfolgung und die Justiz konzipieren, entwickeln, testen, warten, einsetzen und beschaffen, möglichst die Vielfalt der Gesellschaft im Allgemeinen als nichttechnisches Mittel zur Verringerung der Diskriminierungsrisiken widerspiegelt;

23. weist weiter darauf hin, dass für eine angemessene Rechenschaftspflicht, Verantwortung und Haftung eine spezielle Schulung in Bezug auf die ethischen Bestimmungen, die potenziellen Gefahren, die Beschränkungen und die richtige Verwendung der KI-Technologie, insbesondere für die Mitarbeiter von Polizei und Justiz, erforderlich ist; betont, dass durch angemessene fachliche Schulungen und Qualifikationen sichergestellt werden sollte, dass die Entscheidungsträger über das Risiko der Voreingenommenheit aufgeklärt werden, da die Datensätze auf diskriminierenden und vorurteilsbelasteten Daten beruhen können; unterstützt die Gründung von Sensibilisierungs- und Bildungsinitiativen, damit Einzelpersonen, die in der Strafverfolgung und der Justiz arbeiten, sich der Einschränkungen, Fähigkeiten und Risiken, die die Nutzung von KI-Systemen nach sich zieht, einschließlich des Risikos einer Automatisierungsverzerrung, bewusst sind und sie verstehen; erinnert daran, dass die Einbeziehung von Fällen von Rassismus seitens der Polizeikräfte bei der Erfüllung ihrer Pflichten in KI-Trainingsdatensätze unweigerlich zu rassistischen Verzerrungen in den von KI generierten Erkenntnissen, Bewertungen und Empfehlungen führen wird; wiederholt daher seinen Aufruf an die Mitgliedstaaten, Antidiskriminierungsmaßnahmen zu fördern und nationale Aktionspläne gegen Rassismus im Bereich der Polizei und der Justiz zu entwickeln;

24. stellt fest, dass vorausschauende Polizeiarbeit zwar zu den KI-Anwendungen gehört, die im Bereich der Strafverfolgung eingesetzt werden, warnt jedoch davor, dass vorausschauende Polizeiarbeit zwar die gegebenen Datensätze zur Identifizierung von Mustern und Korrelationen analysieren kann, aber nicht die Frage der Kausalität beantworten und keine verlässlichen Vorhersagen über individuelles Verhalten machen kann und daher nicht die alleinige Grundlage für ein Eingreifen darstellen darf; weist darauf hin, dass mehrere Städte in den Vereinigten Staaten ihre Nutzung von Systemen der vorausschauenden Polizeiarbeit nach Prüfungen eingestellt haben; erinnert daran, dass während der Erkundungsreise des LIBE-Ausschusses in die Vereinigten Staaten im Februar 2020 den Mitgliedern von den Polizeidienststellen der Stadt New York und von Cambridge (Massachusetts) mitgeteilt wurde, dass sie ihre Programme für vorausschauende Polizeiarbeit wegen mangelnder Wirksamkeit, diskriminierender Auswirkungen und praktischer Misserfolge hatten auslaufen lassen und sich stattdessen der bürgernahen Polizeiarbeit zugewandt hatten; nimmt zur Kenntnis, dass dies zu einem Rückgang der Kriminalitätsraten geführt hat; spricht sich daher gegen den Einsatz von KI durch Strafverfolgungsbehörden aus, um Vorhersagen über das Verhalten von Einzelpersonen oder Gruppen auf der Grundlage von historischen Daten und früherem Verhalten, Gruppenzugehörigkeit, Standort oder anderen derartigen Merkmalen zu treffen und damit zu versuchen, Personen zu identifizieren, die wahrscheinlich eine Straftat begehen werden;

25. nimmt die verschiedenen Arten der Nutzung von Gesichtserkennung zur Kenntnis, wie z. B. Verifizierung/Authentifizierung (d. h. Abgleich des Gesichts einer anwesenden Person mit einem Foto in einem Ausweisdokument, z. B. intelligente Grenzen), Identifizierung (d. h. Abgleich eines Fotos mit einer bestimmten Fotodatenbank) und Erkennung (d. h. Erkennung von Gesichtern in Echtzeit aus Quellen wie CCTV-Aufzeichnungen und Abgleich mit Datenbanken, z. B. Überwachung in Echtzeit), die jeweils unterschiedliche Auswirkungen auf den Schutz der Grundrechte haben; ist fest davon überzeugt, dass der Einsatz von Gesichtserkennungssystemen durch Strafverfolgungsbehörden auf eindeutig gerechtfertigte Zwecke beschränkt sein sollte, bei denen die Grundsätze der Verhältnismäßigkeit und Notwendigkeit sowie das geltende Recht uneingeschränkt eingehalten werden; bekräftigt, dass die Nutzung von Gesichtserkennungstechnologie mindestens den Anforderungen der Datenminimierung, Datengenauigkeit, Speicherbegrenzung, Datensicherheit und Rechenschaftspflicht genügen sowie rechtlich erlaubt, fair und transparent sein und einem spezifischen, expliziten und rechtmäßigen Zweck dienen muss, der im Recht des Mitgliedstaats oder dem Unionsrecht eindeutig definiert ist; ist der Auffassung, dass Verifizierungs- und Authentifizierungssysteme nur dann weiterhin erfolgreich eingesetzt und verwendet werden können, wenn ihre nachteiligen Auswirkungen abgeschwächt und die vorgenannten Kriterien erfüllt werden können;

26. fordert darüber hinaus das dauerhafte Verbot der Verwendung einer automatisierten Analyse und/oder Erkennung anderer menschlicher Merkmale, wie Gangart, Fingerabdrücke, DNA, Stimme und anderer biometrischer und verhaltensbezogener Signale, in öffentlich zugänglichen Räumen;

27. fordert ein Moratorium für den Einsatz von Gesichtserkennungssystemen für Strafverfolgungszwecke, die die Funktion der Identifizierung haben — es sei denn, sie werden ausschließlich für die Identifizierung von Verbrechensopfern verwendet –, bis die technischen Standards als vollständig grundrechtskonform angesehen werden können, die erzielten Ergebnisse unverzerrt und nicht diskriminierend sind, der Rechtsrahmen strenge Vorkehrungen gegen Missbrauch und strenge demokratische Kontrolle und Überwachung vorsieht und empirische Nachweise für die Notwendigkeit und Verhältnismäßigkeit des Einsatzes solcher Technologien vorliegen; stellt fest, dass die Systeme nicht verwendet oder eingesetzt werden sollten, wenn die oben genannten Kriterien nicht erfüllt sind;

28. äußert seine große Besorgnis über die Nutzung privater Gesichtserkennungsdatenbanken durch Akteure der Strafverfolgung und Nachrichtendienste wie Clearview AI, eine Datenbank mit mehr als drei Milliarden Bildern unter anderem von EU-Bürgern, die illegal in sozialen Netzwerken und anderen Teilen des Internets gesammelt wurden; fordert die Mitgliedstaaten auf, den Akteuren der Strafverfolgung zwingend vorzuschreiben, dass sie offenlegen, ob sie die Technologie Clearview AI oder gleichwertige Technologien anderer Anbieter nutzen; erinnert an die Stellungnahme des Europäischen Datenschutzausschusses (EDSA), wonach die Nutzung eines Dienstes wie Clearview AI durch Strafverfolgungsbehörden in der Europäischen Union wahrscheinlich nicht mit der Datenschutzregelung der Union im Einklang stünde; fordert ein Verbot der Nutzung privater Gesichtserkennungsdatenbanken in der Strafverfolgung;

29. nimmt die Machbarkeitsstudie der Kommission zu möglichen Änderungen am Beschluss zum Prümer Vertrag ([8]), auch hinsichtlich Gesichtsbildern, zur Kenntnis; nimmt frühere Untersuchungen zur Kenntnis, wonach keine potenziellen neuen Identifikationsmerkmale, etwa die Iris- oder Gesichtserkennung, in einem forensischen Kontext so zuverlässig wären wie die DNA oder Fingerabdrücke; erinnert die Kommission daran, dass jeder Gesetzgebungsvorschlag faktengestützt sein und dem Grundsatz der Verhältnismäßigkeit entsprechen muss; fordert die Kommission nachdrücklich auf, den Rahmen des Beschlusses zum Prümer Vertrag nur zu erweitern, wenn solide wissenschaftliche Nachweise für die Zuverlässigkeit der Gesichtserkennung in einem forensischen Kontext im Vergleich zu DNA oder Fingerabdrücken vorliegen, nachdem sie eine umfassende Folgenabschätzung durchgeführt hat, wobei auch die Empfehlungen des Europäischen Datenschutzbeauftragten (EDSB) und des Europäischen Datenschutzausschusses (EDSA) zu berücksichtigen sind;

30. betont, dass die Verwendung biometrischer Daten im weiteren Sinne mit dem Grundsatz des Rechts auf Menschenwürde zusammenhängt, der die Grundlage für alle durch die Charta garantierten Grundrechte bildet; ist der Auffassung, dass die Nutzung und Erhebung biometrischer Daten für Zwecke der Fernidentifizierung, beispielsweise durch Gesichtserkennung im öffentlichen Bereich, sowie an automatischen Sicherheitsschleusen, die für Grenzkontrollen an Flughäfen verwendet werden, spezifische Risiken für die Grundrechte aufwerfen kann, deren Auswirkungen je nach Zweck, Kontext und Umfang der Verwendung erhebliche Unterschiede aufweisen könnten; hebt ferner die umstrittene wissenschaftliche Gültigkeit der Technologie zur Affekterkennung, wie z. B. Kameras, die Augenbewegungen und Veränderungen der Pupillengröße erkennen, in einem Kontext der Strafverfolgung hervor; ist der Ansicht, dass die Verwendung biometrischer Identifizierung im Kontext der Strafverfolgung und der Justiz immer als hochrisikoreich betrachtet werden sollte und daher zusätzlichen Anforderungen unterworfen werden sollte, wie es die hochrangige Expertengruppe der Kommission für KI empfiehlt;

31. äußert sich sehr besorgt über im Rahmen von Horizont 2020 finanzierte Forschungsprojekte, bei denen künstliche Intelligenz an Außengrenzen zum Einsatz kommt, beispielsweise das Projekt iBorderCtrl, ein „intelligentes Lügendetektionssystem“, das auf der Grundlage eines vor der Reise mit der Webcam des Reisenden aufgenommenen, per Computer automatisierten Interviews und einer KI-gestützten Analyse von 38 Mikroimpressionen Profile von Reisenden erstellt und in Ungarn, Lettland und Griechenland erprobt wird; fordert die Kommission daher auf, mit legislativen und nichtlegislativen Mitteln und erforderlichenfalls durch Vertragsverletzungsverfahren ein Verbot jeglicher Verarbeitung biometrischer Daten, einschließlich Gesichtsbildern, zu Strafverfolgungszwecken zu erwirken, wenn diese Verarbeitung zu einer Massenüberwachung in öffentlich zugänglichen Räumen führt; fordert die Kommission ferner auf, die Finanzierung von Forschungsarbeiten, Einsätzen oder Programmen im Zusammenhang mit biometrischen Identifikatoren einzustellen, bei denen die Möglichkeit besteht, dass sie zu einer wahllosen Massenüberwachung in öffentlichen Räumen führen; betont in diesem Zusammenhang, dass dem Einsatz von Drohnen bei Polizeieinsätzen besondere Aufmerksamkeit gewidmet werden sollte und dass ein strikter Rahmen dafür gelten sollte;

32. unterstützt die Empfehlungen der hochrangigen Expertengruppe der Kommission für KI, die sich für ein Verbot von KI-gestützter massenhafter Bewertung („Scoring“) von Einzelpersonen ausspricht; ist der Auffassung, dass jede Art der normativen Bewertung von Bürgern in großem Maßstab durch Behörden, insbesondere im Bereich der Strafverfolgung und der Justiz, zum Verlust von Autonomie führt, den Grundsatz der Diskriminierungsfreiheit gefährdet und nicht als mit den im EU-Recht kodifizierten Grundrechten, insbesondere der Menschenwürde, im Einklang stehend betrachtet werden kann;

33. fordert eine größere generelle Transparenz, um sich ein umfassendes Bild von dem Einsatz von KI-Anwendungen in der Union machen zu können; verlangt, dass die Mitgliedstaaten umfassende Informationen über die von ihren Strafverfolgungs- und Justizbehörden eingesetzten Instrumente, die Arten der verwendeten Instrumente, die Zwecke, für die sie eingesetzt werden, die Arten von Straftaten, auf die sie angewandt werden, und die Namen der Unternehmen oder Organisationen, die diese Instrumente entwickelt haben, bereitstellen; fordert die Strafverfolgungs- und Justizbehörden auf, auch die Öffentlichkeit zu informieren und ausreichende Transparenz in Bezug auf ihren Einsatz von KI und verwandten Technologien bei der Ausübung ihrer Befugnisse an den Tag zu legen, einschließlich der Offenlegung der Falsch-Positiv- und Falsch-Negativ-Raten der betreffenden Technologie; verlangt, dass die Kommission die Informationen an einer zentralen Stelle bündelt und aktualisiert; fordert die Kommission auf, auch Informationen über den Einsatz von KI durch die mit Strafverfolgungs- und Justizaufgaben betrauten Agenturen der Union zu veröffentlichen und zu aktualisieren; fordert den EDSB auf, die Rechtmäßigkeit der KI-Technologien und -Anwendungen zu bewerten, die von den Strafverfolgungsbehörden und der Justiz eingesetzt werden;

34. erinnert daran, dass KI-Anwendungen, einschließlich solcher, die im Rahmen der Strafverfolgung und der Justiz eingesetzt werden, weltweit in rasantem Tempo entwickelt werden; fordert alle europäischen Interessenträger, einschließlich der Mitgliedstaaten und der Kommission, nachdrücklich auf, durch internationale Zusammenarbeit sicherzustellen, dass sich Partner außerhalb der EU engagieren, um die Standards auf internationaler Ebene anzuheben und einen gemeinsamen und ergänzenden Rechts- und Ethikrahmen für den Einsatz von KI, insbesondere für die Strafverfolgung und die Justiz, zu finden, durch den die Charta, der europäische Besitzstand im Bereich des Datenschutzes und die Menschenrechte im weiteren Sinne uneingeschränkt geachtet werden;

([8]) Beschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität (ABl. L 210 vom 6.8.2008, S. 1).

35. fordert die Agentur der Europäischen Union für Grundrechte auf, in Zusammenarbeit mit dem EDSA und dem EDSB umfassende Leitlinien, Empfehlungen und bewährte Verfahren auszuarbeiten, um die Kriterien und Bedingungen für die Entwicklung, die Verwendung und den Einsatz von KI-Anwendungen und -Lösungen zur Nutzung durch Strafverfolgungs- und Justizbehörden weiter zu spezifizieren; sagt zu, eine Studie über die Umsetzung der Richtlinie zum Datenschutz bei der Strafverfolgung ([9]) durchzuführen, um zu ermitteln, wie der Schutz personenbezogener Daten bei Verarbeitungstätigkeiten von Strafverfolgungs- und Justizbehörden, insbesondere bei der Entwicklung oder dem Einsatz neuer Technologien, gewährleistet wird; fordert die Kommission ferner auf zu prüfen, ob spezifische legislative Maßnahmen erforderlich sind, um die Kriterien und Bedingungen für die Entwicklung, die Verwendung und den Einsatz von KI-Anwendungen und -Lösungen durch Strafverfolgungs- und Justizbehörden weiter zu spezifizieren;

36. beauftragt seinen Präsidenten, diese Entschließung dem Rat und der Kommission zu übermitteln.

([9]) Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89).