



Ausschussdrucksache 21(4)214 A
vom 17. September 2026

Schriftliche Stellungnahme

von Prof. Dr. Markus Möstl, Universität Bayreuth vom 4.9.2026
(übermittelt am 15.9.2026)

zu dem

- a) Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus
BT-Drucksachen 21/6131, 21/7265
- b) Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit
BT-Drucksachen 21/6132, 21/6511
- c) Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen
BT-Drucksache 21/6806
- d) Antrag der Abgeordneten Dr. Konstantin von Notz, Dr. Irene Mihalic, Dr. Lena Gumnior, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN
Rechtsstaat stärken, Grundrechte schützen – Moderne Polizeiarbeit gestalten
BT-Drucksache 21/6913
- e) Antrag der Abgeordneten Clara Bünger, Donata Vogtschmidt, Luke Hoß, weiterer Abgeordneter und der Fraktion Die Linke
Nein zu biometrischen Massenerkennungssystemen
BT-Drucksache 21/6917

Schriftliche Stellungnahme im Rahmen der öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages am 21.9.2026 zu den Gesetzentwürfen BT-Drs. 21/6131; 21/6132; 21/6806 und zu den Anträgen BT-Drs. 21/6913; 21/6017

Ich konzentriere meine Ausführungen – meiner polizeirechtlichen Ausrichtung entsprechend – vor allem auf die präventivpolizeilichen Aspekte der Gesetzesnovellen; strafprozessrechtliche und asylrechtliche Befugnisse streife ich allenfalls am Rande.

Die Gesetzentwürfe kreisen um bestimmte Befugnistypen, die dann in Bezug auf die unterschiedlichen Aufgabenbereiche von BKA (z.B. als Zentralstelle oder zur Gefahrenabwehr im Bereich des internationalen Terrorismus) und BPol im Einzelnen näher ausdifferenziert werden, hier aber dennoch gebündelt betrachtet werden können.

1) Sicherung von Verkehrsdaten (§ 10b, § 52 Abs. 3 BKAG-E)

Diese Befugnisse, die im Kontext der Regelungen des Gesetzentwurfs BT-Drs. 21/6581 (Gesetz zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren) gesehen werden müssen, betreffen ein Grundproblem der polizeilichen Ermittlungsarbeit unter den Bedingungen moderner elektronischer/digitaler Kommunikation: Wie wird sichergestellt, dass der – immer wichtiger werdende – (virtuelle) Raum elektronischer Kommunikation (sei es im Internet oder im Rahmen sonstiger Fernkommunikation) nicht zu einem Raum wird, in dem keine Spuren mehr hinterlassen werden, so dass eine spurenbasierte polizeiliche Ermittlungsarbeit (wie wir sie aus der traditionellen analogen Welt kennen) strukturell unmöglich wird und somit ein Raum entsteht, der, obwohl für die Planung und Begehung von Straftaten von höchster Relevanz, zum rechtsfreien Raum zu werden droht?

Polizeiliche Ermittlungen (seien sie präventiver oder repressiver Natur) sind davon abhängig, dass die Planung und Begehung von Straftaten Spuren hinterlässt, an die – dann an rechtsstaatlich hinreichend anspruchsvolle Eingriffsschwellen zu bindende – Ermittlungseingriffe anknüpfen können. In der traditionellen analogen Welt war dies sichergestellt. Je mehr Straftaten aber im virtuellen Raum elektronischer Kommunikation vorbereitet und begangen werden, umso stärker ist diese Prämisse des klassischen Ermittlungsrechts gefährdet. Denn die hier hinterlassenen Spuren werden von den Kommunikationsbetreibern nicht unbedingt oder nur sehr

kurzzeitig gespeichert und sie können auch anderweitig gelöscht werden. Es ist für die Erfüllbarkeit der staatlichen Garantie öffentlicher Sicherheit – unter den Bedingungen moderner elektronischer Kommunikation – daher von entscheidender Bedeutung, dass der Staat in dem zur Einlösung seiner Sicherheitsaufgabe nötigen Maße eine Art vorsorglicher elektronischer Spurensicherung anordnen darf.

Nicht ohne Grund hat das BVerfG daher schon früh (BVerfGE 125, 260) selbst eine allgemeine Vorratsdatenspeicherung von Verkehrsdaten nicht für per se verfassungswidrig, sondern prinzipiell (freilich nach Maßgabe näherer rechtsstaatlicher Maßgaben) durchaus für möglich gehalten. Dass der EuGH meinte, das in diesen Fragen ohnehin strenge BVerfG im Punkt der Vorratsdatenspeicherung noch einmal überholen zu müssen, ist im Blick auf die nötige Aufklärbarkeit von Gefahrenlagen und Straftaten durchaus nicht unproblematisch. Immerhin in Bezug auf IP-Adressen ist eine allgemeine Vorratsdatenspeicherung auch unionsrechtlich zulässig, und es ist nur folgerichtig und begrüßenswert, dass sie in einem anderen Gesetzgebungsverfahren (BT-Drs. 21/6581) nunmehr auch in Deutschland verwirklicht werden soll. Im Übrigen ist es wichtig, wenigstens anlassbezogene Maßnahmen der vorsorglichen Datensicherung einzuführen, damit die verfassungskonformen Ermittlungsbefugnisse von Polizei- und Strafverfolgungsbehörden nicht ins Leere laufen (dass es solche Sicherungsanordnungen gibt, setzt das Unionsrecht auch anderwärts voraus). Im Blick auf das Grundgesetz lässt sich sagen: Soweit Art. 10 GG die Erhebung von Verkehrsdaten gestattet, muss er es unter den Bedingungen der heute vorherrschenden flüchtigen elektronischen Kommunikation, soll die staatliche Sicherheitsaufgabe erfüllbar bleiben, auch gestatten, ausreichende Maßnahmen präventiver Datensicherung vorzusehen, damit von den verfassungskonformen Ermittlungsbefugnissen überhaupt Gebrauch gemacht werden kann.

Zu Recht soll mit den Gesetzentwürfen BT-Drs. 21/6581 sowie BT-Drs. 21/6131 nun für ausreichende Befugnisse der Polizeibehörden zur Sicherung von Verkehrsdaten gesorgt werden. Da es um eine zwar anlassbezogene, aber doch vorsorgliche Datensicherung zur Ermöglichung späterer – dann an hinreichende Eingriffsschwellen gebundene – Ermittlungseingriffe geht, ist es nur folgerichtig, dass die Befugnis zur Anordnung der Datensicherung noch nicht an diejenige (strenge) Eingriffsschwelle zu binden ist, die dann später für den Ermittlungseingriff gilt (die Voraussetzungen für die tatsächliche Datenerhebung müssen also – wie die Entwurfsbegründung zu Recht sagt – gerade noch nicht vorliegen). Auch grundrechtlich gesehen ist eine abgesenkte Eingriffsschwelle richtig: Denn zwar ist das Eingriffsgewicht einer anlassbezogenen Sicherungsanordnung gegenüber einer anlasslosen Vorratsdatenspeicherung ein Stück weit erhöht, weil sie doch einen gewissen anlassbezogenen Anfangsverdacht zum Ausdruck bringt, der bereits mit einer bestimmten Person in Verbindung gebracht wird (bei der allgemeinen Vorratsdatenspeicherung ist das nicht der Fall), andererseits ist das Eingriffsgewicht durch die weitaus geringere Streubreite (d.h. präzisere Wirkung) und vor allem dadurch, dass an dieser Stelle gerade noch keine staatliche Kenntnis von bestimmten Daten genommen wird, sondern nur sichergestellt werden soll, dass die Daten überhaupt vorhanden bleiben, auch deutlich gemindert.

Es scheint mir vor diesem Hintergrund folgerichtig und unproblematisch, dass die Befugnisse für die Anordnung der Sicherung bereits „tatsächliche Anhaltspunkte“ dafür ausreichen lassen, dass eine Sachlage vorliegen könnte, die dann zu einem Zugriff auf Verkehrsdaten berechtigt. Ebenso reicht es für das personale Verfangensein des Adressaten in die gefahrbezügliche Sachlage, dass er in einem „persönlichen oder räumlichen Bezug“ zu der (zu verhütenden) Straftat steht. Zöge man die Schwellen hier enger, würde das Instrument der vorsorglichen Datensicherung seine Effektivität weitgehend verlieren.

2) Automatisierte Datenanalyse (§ 9b, § 39b, § 63c BKAG-E, § 58b BPolG-E)

Auch die Befugnisse zur automatisierten Datenanalyse betreffen eine Grundfrage der Bedingungen moderner Ermittlungsarbeit: Inwieweit darf die Polizei das bei ihr rechtmäßig vorhandene, allerdings auf ganz unterschiedliche Dateien und Speicherorte verteilte Wissen in einer technisch effektiven Weise, d.h. möglichst automatisiert und nicht mühsam per Hand, durchsuchen, analysieren und zusammenführen, um es so möglichst schnell – und unter Ausschöpfung der heute bestehenden technischen Möglichkeiten (wie sie in vergleichbarer Weise auch anderwärts in Wirtschaft und Gesellschaft genutzt werden) – für die Gefahrenabwehr fruchtbar zu machen?

In diesem Zusammenhang scheint mir bislang in der allgemeinen Diskussion die Wertung des Art. 87 Abs. 1 S. 2 GG noch nicht hinreichend berücksichtigt worden zu sein. Mit seinem Abstellen auf das (altmodisch ausgedrückt) „polizeiliche Auskunfts- und Nachrichtenwesen“ bringt er nämlich in einer über den engeren föderalen Kontext (BKA als Zentralstelle) hinausgehenden, verallgemeinerbaren Weise die verfassungsrechtliche Wertung zum Ausdruck, wie wichtig ein funktionierendes Instrumentarium der effektiven Zusammenführung des auf viele Stellen und Orte verteilten Wissens der Polizei für die Einlösung der staatlichen Sicherheitsaufgabe ist. Ein funktionierendes „polizeiliches Auskunfts- und Nachrichtenwesen“ i.S.v. Art. 87 Abs. 1 S. 2 GG setzt unter den heutigen Bedingungen eben auch die prinzipielle Nutzbarkeit von Datenzusammenführungs- und Analyseplattformen voraus, wie sie die heutige Technik ermöglicht. Der Polizei solche Möglichkeiten vorzuenthalten und sie in Situationen, in denen moderne Datenanalyse aus rechtmäßig vorhandenem Wissen binnen kürzester Zeit zu verwertbaren Ergebnissen kommen kann, darauf zu verweisen, solche Daten über Wochen mühsam händisch auszuwerten, wäre eine eklatante Verletzung der staatlichen Schutzpflichten. Es verwundert daher nicht, dass auch mehrere Bundesländer vergleichbare Befugnisse kennen (z.B. Art. 61a BayPAG, § 47a ASOG Bln) und das BVerfG für den Einsatz derartiger Systeme zwar Maßgaben formuliert hat, ihn aber keineswegs (auch unter den derzeitigen Bedingungen eines möglichen Einsatzes) als prinzipiell ausgeschlossen ansieht (BVerfGE 165, 296).

Die Diskussion um die automatisierte Datenanalyse der Polizei wird erheblich dadurch belastet, dass hierfür momentan praktisch vor allem oder allein Systeme amerikanischer Anbieter vorhanden sind und zum Einsatz kommen können, die aus unterschiedlichen Gründen umstritten sind (Stichwort „Palantir“). Hieraus folgt aber nicht die Verfassungswidrigkeit der entsprechenden Befugnisnormen. Vielmehr sind Fragen der Verfassungsmäßigkeit des Gesetzes einerseits und seines Vollzuges andererseits prinzipiell auseinanderzuhalten; zu Recht weist die Entwurfsbegründung darauf hin, dass die gesetzlichen Befugnisnormen „technik- und produktneutral“ sind. Aber auch dass ein Einsatz von Produkten z.B. von „Palantir“ per se einen verfassungswidrigen Vollzug bedeuten müsste, kann ich nicht erkennen; soweit ich weiß (jedenfalls für Bayern scheint das der Fall zu sein; vgl. <https://www.stmi.bayern.de/news/detail/herrmann:-vera-ist-sinnvoll-und-notwendig/>) kommen in Deutschland nur Systeme zum Einsatz, deren Quellcode von deutschen Stellen zuvor geprüft worden ist und die in einer völlig abgeschotteten Weise (d.h. ohne dass physisch oder technisch die Möglichkeit bestünde, von außen auf die Plattform zuzugreifen) von der Polizei selbst betrieben werden; es erschließt sich mir nicht, inwiefern die digitale Souveränität Deutschlands durch so eine Gestaltung beeinträchtigt werden könnte. Zu bedenken ist schließlich, dass das BVerfG um die derzeitige Lage (welche Systeme können praktisch zum Einsatz kommen?) wusste, als es seine Grundsatzentscheidung zur Zulässigkeit der automatisierten Datenanalyse traf (BVerfGE 165, 296). Es hat hierin rechtsstaatliche Maßgaben für die Ausgestaltung

entsprechender Befugnisnormen formuliert. Entscheidend ist somit allein, ob diese Maßgaben eingehalten sind. Der Polizei verfassungsrechtlich zulässige Befugnisse so lange vorzuenthalten, bis ein eigenes deutsches/europäisches System erprobt und entwickelt ist, und in der Zwischenzeit in Kauf zu nehmen, dass Gefahren für höchstrangige Schutzgüter nicht schnell und effektiv genug bekämpft werden können, wäre meines Erachtens schwer verantwortbar.

Bei der mir hier möglichen überschlägigen ersten Beurteilung kann ich nichts erkennen, was dafür spräche, dass die Vorgaben des BVerfG in seiner Leitentscheidung zur automatisierten Datenanalyse nicht beachtet worden wären. Namentlich ist ein Eingriff selbst bei einer ein hohes Eingriffsgewicht bewirkenden Ausgestaltung jedenfalls bei Vorliegen einer konkretisierten Gefahr für besonders gewichtige Rechtsgüter verfassungsrechtlich zulässig. Die Befugnisnormen halten sich daran, sei es dass sie (wie in § 39b BKAG-E) an die Verhütung terroristischer Straftaten anknüpfen (vgl. BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 Ls. 4), sei es dass sie hinreichend gewichtige Rechtsgüter benennen. Bei § 9b Abs. 1 Nr. 2 BKAG-E kann allerdings eine einschränkende Auslegung des Schutzguts „Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist“ erforderlich sein (vgl. dazu im Kontext des § 39b BKAG-E auch die Entwurfsbegründung BT-Drs. 21/6131, S. 19 mit entsprechenden Hinweisen zur Rspr. des BVerfG: eingeschränkter Sachwertschutz). Die in § 58b Abs. 1 Nr. 2/3 BPolG-E vorgenommene „Übersetzung“ der Anforderungen an hinreichend gewichtige Schutzgüter in das spezifische Aufgabenprofil der Bundespolizei hinein scheint mir plausibel. Da es im Polizeirecht auf das Gewicht der zu schützenden Rechtsgüter und nicht auf die – terroristische oder nicht-terroristische – Motivation ihrer Gefährdung ankommt, halte ich es für bedenkenfrei, dass § 63c Abs. 1 Nr. 2 BKAG-E die Fallgruppe „individuelles Verhalten“ der konkretisierten Gefahr auch auf nicht terroristische Gefährdungen der hier genannten höchstrangigen Rechtsgüter erstreckt; auch das BVerfG hat dergleichen bereits getan (vgl. BVerfGE 155, 119 Rn. 149); seine Linie ist jedoch uneindeutig und wird im anhängigen Verfahren zum BayPAG (1 BvF 1/18 u.a.) wohl geklärt werden. Entsprechendes gilt für § 58a Abs. 1 Nr. 3 BPolG-E.

3) Automatisierter biometrischer Abgleich mit öffentlich zugänglichen Daten im Internet (§ 9a, § 39a, § 63b BKAG-E, § 58a BPolG-E)

Die bislang fehlenden und nunmehr geplanten Befugnisse zum automatisierten biometrischen Abgleich mit öffentlichen Internetdaten sind ein Lehrstück dafür, wie wichtig es ist, dass die Befugnisse der Polizei und der Ermittlungsbehörden technisch auf der Höhe der Zeit sind und nicht hinter dem zurückbleiben, was allgemein (auch durch nicht staatliche Akteure) einsetzbar ist. Es hat nach meinem Eindruck das Vertrauen der Bevölkerung in die Leistungsfähigkeit des Staates nicht unerheblich beeinträchtigt, als Journalisten mittels eines – ihnen offenbar ohne weiteres möglichen – biometrischen Abgleichs mit Internetdaten öffentlichkeitswirksam eine Spur zur seit langem gesuchten Terroristin Daniela Klette auf tun konnten, die den staatlichen Behörden verborgen geblieben war und dies auch musste, weil sie über keine Befugnisse zum Einsatz eines solchen Gesichtserkennungssystems verfügten (zur Problematik, wenngleich im Ergebnis durchaus kritisch, vgl. Hahn, Aber die Journalisten dürfen das doch auch, Verfassungsblog vom 31.3.2026). Dass derartige Erfahrungen staatlicher Ohnmacht das Vertrauen der Bevölkerung in den Staat zu erschüttern vermögen, darf nicht verwundern. Die Sicherheit des Staates und der Schutz seiner Bevölkerung sind Verfassungswerte, von denen die Institution Staat ihre eigentliche und letzte Rechtfertigung herleitet, wie es das BVerfG nicht ohne Grund sagt (BVerfGE 49, 24/56 f.). Hat die Bevölkerung den Eindruck, dass der Staat nicht hinreichend in der Lage ist, die Sicherheit von Staat und Bevölkerung zu gewährleisten, droht die Legitimität des Staates aufs

Schwerste gefährdet zu werden. In Zeiten des ohnehin um sich greifenden Vertrauensverlustes und des Erstarkens der politischen Ränder ist das ein gravierender Befund. Dafür zu sorgen, dass die Befugnisse der Sicherheitsbehörden auf dem Stand der Zeit sind und mit den technischen Entwicklungen Schritt halten, ist somit nicht nur ein Gebot der Verfassungsaufgabe Sicherheit, sondern auch ein wichtiger Dienst an der Stabilisierung des Vertrauens in unsere freiheitliche demokratische Ordnung. Dass über die Einführung neuer Polizeibefugnisse gestritten wird und potentielle Gefährdungen der Freiheitsrechte ernst genommen werden, ist sicher berechtigt. Ich wundere mich aber manchmal darüber, wie leichtfertig im Kampf für die Freiheitsrechte in Kauf genommen wird, dass unser Staat potentiell immer weiter delegitimiert und in seiner Handlungsschwäche bisweilen geradezu der Lächerlichkeit preisgegeben wird, obwohl doch auf der Hand liegen müsste, wie wichtig es gerade jetzt sein müsste, die Sicherheitsbehörden mit – freilich verfassungskonformen, aber doch hinreichend schlagkräftigen – Befugnissen auszustatten, die das Vertrauen in die Handlungsfähigkeit des Staates stärken und so unsere (keineswegs ungefährdete) freiheitliche Demokratie stabilisieren. Hierzu gehören auch ausreichende Befugnisse für einen biometrischen Abgleich mit öffentlich zugänglichen Internetdaten. Einzelne Länder haben inzwischen bereits entsprechende Rechtsgrundlagen geschaffen oder planen dies (z.B. § 28a ASOG Bln); es ist gut und richtig, dass der Bund nunmehr nachzieht.

Der mittels des biometrischen Abgleichs bewirkte Grundrechtseingriff scheint mir – entgegen mancher Behauptung – nicht als besonders gewichtig einzustufen zu sein. Es geht allein um den Abgleich bei der Polizei bereits rechtmäßig vorhandener Daten mit ohnehin bereits öffentlich zugänglichen (und daher in ihrer Schutzintensität geminderten) Internetdaten; ein Abgleich mit aus besonders eingriffsintensiven Maßnahmen gewonnenen Daten i.S.v. § 12 Abs. 3 BKAG ist überdies ausgeschlossen. Die Anforderungen an die Eingriffsschwelle sollte man vor diesem Hintergrund nicht zu hoch ansetzen; nicht zu fordern ist insbesondere, dass sich bei einem präventivpolizeilichen Einsatz die Eingriffsschwelle der konkretisierten Gefahr stets nur auf höchstrangige Schutzgüter beziehen müsste (Schutzgüter von erheblicher Bedeutung dürften ausreichen; allg. zu den hier anzulegenden flexiblen Kriterien: BVerfGE 170, 247 Rn. 80 ff.). Eine konkretisierte Gefahr der Begehung von Straftaten nach § 100a Abs. 2 StPO von auch im Einzelfall erheblicher Bedeutung zusätzlich zu weiteren Erforderlichkeits- und Subsidiaritätsvorbehalten (vgl. § 9a Abs. 1 BKAG-E) scheint mir vor diesem Hintergrund völlig ausreichend. Gleiches gilt für die konkretisierte Gefahr der Begehung terroristischer Straftaten nach § 39a Abs. 1 BKAG-E, der Straftatenbegehung nach § 58a Abs. 1 BPolG-E oder für bedeutende Rechtsgüter nach § 63 Abs. 1 BKAG-E. Die auf das „individuelle Verhalten“ abstellende Fallgruppe der konkretisierten Gefahr muss nach hier vertretener Ansicht je nach Eingriffsgewicht keineswegs stets auf die Abwehr terroristischer Gefahren beschränkt bleiben (siehe bereits oben 2. und BVerfGE 155, 119 Rn. 149). Die Löschungspflicht nach Durchführung verhindert den Aufbau biometrischer Datenbanken; der Abgleich muss ad hoc durchgeführt werden. Die auf eine konkrete Gefahr abstellende Eingriffsschwelle in § 39a Abs. 1 Nr. 1 a) BKAG-E scheint mir jedoch sprachlich unglücklich formuliert (sofern „eine im Einzelfall bestehende Gefahr ... besteht“).

Was die Befugnis angeht, den Abgleich im Ausland und durch Dritte durchführen zu lassen, ist bei Durchführung innerhalb der EU zu bedenken, dass hier das in der gesamten EU geltende Datenschutzniveau gewährleistet ist. Die Vergabe in den Bereich von Drittstaaten ist an weitere eingrenzende Voraussetzungen (nationale Sicherheit) und Subsidiaritätsanforderungen (technische Unmöglichkeit bzw. unverhältnismäßiger Aufwand einer Durchführung in der EU) geknüpft, u.a. auch an die allgemeinen datenschutzrechtlichen Anforderungen für Datenübermittlungen an Empfänger in Drittstaaten (§ 81 BDSG) sowie einen prinzipiellen Richtervorbehalt. Die Sorge und das Bemühen um digitale Souveränität sind sicher berechtigt. Auf einen Abgleich

mit öffentlich zugänglichen Internetdaten zu verzichten, bloß weil er im Inland oder in der EU derzeit technisch (noch) nicht möglich ist, schiene mir dennoch eine schwer verantwortbare Vernachlässigung der inneren bzw. hier sogar nationalen Sicherheit.

4) Entwicklung und Training von IT-Systemen (§ 22 Abs. 3, 4 BKAG-E; § 46 Abs. 3, 4 BPolG-E)

Das berechtigte Anliegen, der Polizei ein Agieren auf der Höhe der Zeit und des Stands der Technik zu ermöglichen, drückt sich auch in den für BKA und BPol zu schaffenden Befugnisnormen zur Zulässigkeit der Weiterverarbeitung vorhandener Daten für die Entwicklung und das Training von IT-Systemen (auch KI) aus. Dass hierfür eine explizite und spezifische Eingriffsermächtigung geschaffen wird, obwohl nicht einmal sicher ist, ob eine solche wirklich nötig ist oder allgemein datenschutzrechtliche Bestimmungen ausreichen könnten, ist rechtsstaatlich zu begrüßen. Das Eingriffsgewicht ist dadurch, dass es allein um das Entwickeln und die Testung von Systemen und nicht um ihren realen Einsatz für die Erfüllung von Polizeiaufgaben geht, deutlich gemindert. Eine mit verhältnismäßigem Aufwand mögliche Anonymisierung oder Pseudonymisierung ist vorrangig. Ein Training mit aus besonders eingriffsintensiven Maßnahmen gewonnenen Daten ist ausgeschlossen. Besondere Schutzvorkehrungen gegen die Herausbildung von diskriminierenden Algorithmen sind vorgesehen. Eine Bindung der Befugnis allein an die Erforderlichkeit der Maßnahme für die polizeiliche Aufgabenerfüllung scheint mir vor diesem Hintergrund verfassungsrechtlich vertretbar, ohne dass es weitergehender Eingriffsschwellen bedürfte. Dass im Rahmen der Entwicklung und Testung von Systemen, bei denen die Polizei mit Dritten, insb. auch Unternehmen, kooperiert, u.U. und nach näheren eingrenzenden Maßgaben eine Weitergabe von Daten an Dritte in Inland und EU notwendig sein kann, scheint mir unabweisbar.

Bayreuth, den 4.9.2026

Prof. Dr. Markus Möstl