21. Wahlperiode

Deutscher Bundestag
Innenausschuss

Wortprotokoll
der 41. Sitzung

Innenausschuss
Berlin, den 21. September 2026, 14:00 Uhr
Berlin, Konrad-Adenauer-Str. 1, 10557
Paul-Löbe-Haus, Raum 2 600

Vorsitz: Josef Oster, MdB

Tagesordnung - Öffentliche Anhörung

Tagesordnungspunkt 1 **Seite 5**

a) Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus

BT-Drucksache 21/6131

Federführend:
Innenausschuss

Mitberatend:
Ausschuss für Recht und Verbraucherschutz
Ausschuss für Digitales und Staatsmodernisierung

Gutachtlich:
Parlamentarischer Beirat für nachhaltige Entwicklung und Zukunftsfragen

Berichterstatter/in:
Abg. Johannes Wiegelmann [CDU/CSU]
Abg. Markus Matzerath [AfD]
Abg. Johannes Schätzl [SPD]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]
Abg. Ferat Koçak [Die Linke]

b) Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit

BT-Drucksache 21/6132

Federführend:
Innenausschuss

Mitberatend:
Ausschuss für Recht und Verbraucherschutz
Ausschuss für Digitales und Staatsmodernisierung
Haushaltsausschuss (mb und § 96 GO)

Gutachtlich:
Parlamentarischer Beirat für nachhaltige Entwicklung und Zukunftsfragen

Berichterstatter/in:
Abg. Johannes Wiegelmann [CDU/CSU]
Abg. Steffen Janich [AfD]
Abg. Johannes Schätzl [SPD]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]
Abg. Clara Bünger [Die Linke]

c) Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen

BT-Drucksache 21/6806

Federführend:
Ausschuss für Recht und Verbraucherschutz

Mitberatend:
Innenausschuss
Ausschuss für Digitales und Staatsmodernisierung

Gutachtlich:
Parlamentarischer Beirat für nachhaltige Entwicklung und Zukunftsfragen

Berichterstatter/in:
Abg. Johannes Wiegelmann [CDU/CSU]
Abg. Steffen Janich [AfD]
Abg. Johannes Schätzl [SPD]
Abg. Dr. Lena Gumnior [BÜNDNIS 90/DIE GRÜNEN]
Abg. Clara Bünger [Die Linke]

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

Federführend:
Innenausschuss

Mitberatend:
Ausschuss für Recht und Verbraucherschutz
Ausschuss für Digitales und Staatsmodernisierung

Berichterstatter/in:
Abg. Johannes Wiegelmann [CDU/CSU]
Abg. Christopher Drößler [AfD]
Abg. Ingo Vogel [SPD]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]
Abg. Clara Bünger [Die Linke]

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

Federführend:
Innenausschuss

Mitberatend:
Ausschuss für Recht und Verbraucherschutz

Berichterstatter/in:
Abg. Johannes Wiegelmann [CDU/CSU]
Abg. Steffen Janich [AfD]
Abg. Johannes Schätzl [SPD]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]
Abg. Clara Bünger [Die Linke]

Anwesende Mitglieder des Innenausschusses

Fraktion	Ordentliche Mitglieder	Stellvertretende Mitglieder
CDU/CSU	Oster, Josef Seif, Detlef Strauss-Köster, Dr. Katja Walch, Siegfried Wiegelmann, Johannes	
AfD	Janich, Steffen	
SPD	Schätzl, Johannes	Wegge, Carmen
BÜNDNIS 90/DIE GRÜNEN	Notz, Dr. Konstantin von	Gumnior, Dr. Lena Mihalic, Dr. Irene
Die Linke	Bünger, Clara	Vogtschmidt, Donata

Anwesende Mitglieder des Ausschusses für Recht und Verbraucherschutz

Fraktion	Ordentliche Mitglieder	Stellvertretende Mitglieder
CDU/CSU	Hierl, Susanne Moser, Christian	
AfD	Jacobi, Fabian	

21. Wahlperiode

Deutscher Bundestag
Innenausschuss

Liste der Sachverständigen

Öffentliche Anhörung am Montag, 21. September 2026, 14.00 Uhr
„Digitale Ermittlungsbefugnisse“

Hadmut Danisch[2)]

RA **Kai Kempgens**[4)]
Deutscher Anwaltverein (DAV), Berlin

Martina Link[1)]
Vizepräsidentin des Bundeskriminalamts

Prof. Dr. Markus Löffelmann[3)]
Hochschule des Bundes für öffentliche Verwaltung, Berlin

Prof. Dr. Markus Möstl[1)]
Lehrstuhl Öffentliches Recht II - Universität Bayreuth

Alexander Poitz[3)]
Stellvertretender Bundesvorsitzender - Gewerkschaft der Polizei, Berlin

Dr. Andreas Schmidtke[1)]
Richter am Oberlandesgericht Düsseldorf

Pia Sombetzki[5)]
AW AlgorithmWatch gGmbH, Berlin

---

1) Vorschlag: Fraktion der CDU/CSU
2) Vorschlag: Fraktion der AfD
3) Vorschlag: Fraktion der SPD
4) Vorschlag: Fraktion BÜNDNIS 90/DIE GRÜNEN
5) Vorschlag: Fraktion Die Linke

Beginn der Sitzung: 14.03 Uhr

Tagesordnungspunkt 1

a) Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus

BT-Drucksache 21/6131

b) Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit

BT-Drucksache 21/6132

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

Amt. Vors. **Josef Oster** (CDU/CSU): Verehrte Kolleginnen und Kollegen, meine sehr geehrten Damen und Herren, ich darf Sie am heutigen Nachmittag sehr herzlich begrüßen zu unserer öffentlichen Anhörung hier im Innenausschuss, die ich als amtierender Vorsitzender leiten darf. Ich freue mich, dass wir uns an diesem bewegten Tag drei ganz konkreten Gesetzentwürfen widmen können und uns darüber gemeinsam austauschen werden. Gegenstand der heutigen Anhörung sind drei Gesetzentwürfe der Bundesregierung zur Stärkung digitaler Ermittlungsbefugnisse. Das betrifft die Drucksachen 21/6131, 21/6132 und 21/6806. In diese Anhörung über diese drei Gesetzentwürfe sind ein Antrag der Fraktion von BÜNDNIS 90/DIE GRÜNEN auf der Drucksache 21/6913 und ein weiterer Antrag der Fraktion Die Linke auf der Drucksache 21/6917 einbezogen. In dem Gesetzentwurf auf der Drucksache 21/6806 geht es um die Änderung der Strafprozessordnung für den Bereich digitaler Ermittlungsmaßnahmen. Hierfür ist der Rechtsausschuss zuständig. Da aber die drei Gesetzentwürfe inhaltlich sehr eng zusammenhängen, haben sich Innen- und Rechtsausschuss entschieden, alle drei Gesetzentwürfe in einer Anhörung gemeinsam zu behandeln. Deshalb sitzen wir hier heute Nachmittag zusammen und der Innenausschuss wird federführend diese Gesamtanhörung leiten. Deshalb sitze ich hier. Diesem Vorgehen hat der Rechtsausschuss zugestimmt; dafür auch an dieser Stelle ein herzliches Dankeschön. Ich denke, damit haben wir ein gutes Verfahren gefunden, um diese komplexe Materie ausschussübergreifend sachgerecht behandeln zu können.

Ich darf an dieser Stelle die anwesenden Mitglieder des Rechtsausschusses und die der weiteren mitberatenden Ausschüsse sehr herzlich begrüßen. Ich danke den Damen und Herren Sachverständigen, dass Sie unserer Einladung heute hier nachgekommen sind und uns gleich mit Ihrer Expertise zur Verfügung stehen werden und anschließend die Fragen der Kolleginnen und Kollegen beantworten werden. Ich begrüße herzlich in alphabethischer Reihenfolge als Sachverständige, Herrn Hadmut Danisch, herzlich willkommen. Ich darf begrüßen, Herrn Kai Kempgens, Frau Martina Link und Herrn Professor Markus Löffelmann. Auf der anderen Seite von mir aus gesehen darf ich Herrn Professor Markus Möstl herzlich begrüßen. Ein herzliches Willkommen an Herrn Alexander Poitz. Dr. Andreas Schmidtke und Frau Pia Sombetski, auch Ihnen ein herzliches Willkommen in dieser Runde.

Für die Bundesregierung darf ich den Parlamentarischen Staatssekretär aus dem Bundesinnenministerium herzlich begrüßen – lieber Herr de Vries, ein herzliches Willkommen in dieser Runde. Angekündigt ist noch die Parlamentarische Staatssekretärin aus dem Bundesministerium der Justiz, Frau Anette Kramme, die sicherlich gleich noch zu uns stoßen wird. Die Sitzung wird live im Bundestagsfernsehen übertragen und ab morgen in der Mediathek des Deutschen Bundestages für die Öffentlichkeit zum Abruf bereitstehen.

Wir hatten, wie immer, um schriftliche Stellungnahmen gebeten, die haben Sie uns dankenswerterweise zur Verfügung gestellt. Wir haben diese den Ausschussmitgliedern weitergeleitet. Ich darf darauf hinweisen, dass von dieser Sitzung ein Wortprotokoll erstellt und später auch veröffentlicht wird.

Wir haben uns wie üblich ein Zeitfenster von 14.00 bis 16.00 Uhr vorgenommen und werden diese Zeit wie folgt nutzen: Es wird zunächst jede Sachverständige, jeder Sachverständige die Möglichkeit bekommen, ein Eingangsstatement, möglicherweise ergänzend zur schriftlichen Stellungnahme, abzugeben, welches bitte eine Dauer von drei Minuten nicht überschreiten sollte. Nach diesen Eingangsstatements werden wir dann in die Fraktionsfragerunden eintreten. Die Abgeordneten aus dem Innenausschuss kennen das natürlich, wir machen das immer so – für die anderen erkläre ich es einmal: In den Fragerunden haben wir das Verfahren so, dass entweder zwei Fragen an einen Sachverständigen gerichtet werden können oder je eine Frage an zwei Sachverständige. Das Zeitfenster beträgt zwei Minuten. Auf diese Frage/Fragen wird dann unmittelbar geantwortet und auch die Antwort sollte zwei Minuten nicht überschreiten. Das machen wir in den Fraktionsrunden und dann gucken wir einmal, wie viele Fraktionsrunden wir am Ende schaffen werden. Wenn es dazu bis hierhin keine Wortmeldungen gibt, dann würde ich jetzt in die Eingangsstatements einsteigen und dem Alphabet nach darf Herr Hadmut Danisch beginnen. Herr Danisch, Sie haben drei Minuten Zeit, Ihre Stellungnahme zu erläutern.

SV **Hadmut Danisch**: Vielen Dank für die Einladung. Ich betrachte diese drei Gesetzentwürfe aus drei verschiedenen Blickwinkeln, nämlich als Informatiker und langjähriger Datenschutztätiger mit Datenschutzerfahrung, dann mit der Erfahrung aus einem Jahr Tätigkeit in der Vorratsdatenspeicherung mit etwa 2 000 behandelten Strafverfahren im Jahr 2009, und der dritte Blickwinkel ist der als Betroffener eines Strafermittlungsverfahrens, weil mir als Blogger vorgeworfen wurde, eine Politikerin des Deutschen Bundestags angeblich beleidigt zu haben – das Verfahren wurde eingestellt, weil keine Straftat vorlag; man hatte dieses vorgeschobene Strafverfahren oder Strafermittlungsverfahren verwendet, um Kontodaten auszuspähen – das sind also die drei Blickwinkel, aus denen ich diese Sache betrachte. Ich bin nicht grundsätzlich gegen biometrische Fahndungsmethoden. Ich habe nur 150 Meter weg von dieser Wohnung gewohnt, in der man Daniela Klette festgenommen hat. Das ist schon in der Nachbarschaft passiert und es gab da auch entsprechend Gespräche. Es gibt also grundsätzlich schon eine Bereitschaft dazu. Ich halte aber diese Gesetzentwürfe hier für qualitativ nicht gut. Ich habe also trotz der kurzen Zeit, die mir zur Verfügung stand, relativ viele Fehler, Inkonsistenzen, falsche Begriffe, Unlogik, Verständnisfehler darin gefunden und bin der Meinung, dass diese Gesetzentwürfe zumindest einer erheblichen Überarbeitung und Verbesserung bedürfen. Ich halte sie in ihrer derzeitigen Form nicht für tageslichttauglich und habe an verschiedenen Stellen festgestellt, dass da Verständnisfehler oder Missverständnisse vorliegen. Ich bin also nicht grundsätzlich gegen biometrische Fahndungsmethoden, sehe aber einen Bedarf an wesentlich höherer Sorgfalt und einer verbesserten Vorgehensweise. Ich halte die Vorgehensweise hier nicht für ausreichend und nicht für geeignet.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke, Herr Danisch. Dann gehen wir in der Runde weiter. Das Wort erhält Herr Kempgens.

SV **Kai Kempgens** (DAV): Ja, vielen Dank für die Einladung. Unsere schriftlichen Stellungnahmen liegen Ihnen vor, hier nur ein paar wesentliche Punkte: Aus Sicht des Deutschen Anwaltsvereins war es angesichts der wachsenden technischen Möglichkeiten höchste Zeit, klare und eindeutige Regelungen und rechtliche Rahmenbedingungen für automatisierte digitale Ermittlungsmaßnahmen zu schaffen. Umgekehrt formuliert, zu bestimmen, was erlaubt ist und was eben nicht erlaubt ist. Man sollte sich aus Sicht des Deutschen Anwaltsvereins auch grundsätzlich nicht vor modernen Ermittlungsmöglichkeiten verschließen. Das soziale Zusammenleben ist ganz stark in der digitalen Welt abgebildet – natürlich müssen dort auch Informationen gesammelt und ermittelt werden können. Jetzt muss man sich klarmachen, menschlichen Ermittlungspersonen sind solche Recherchen schon immer erlaubt. Selbstverständlich darf jede Polizeibeamte, jeder Polizeibeamter nach den gewachsenen Verfahrensordnung im Internet recherchieren, Bilder anschauen, und auch Einblick in Daten fremder Verfahren nehmen und die auswerten. Aber das Novum und letztendlich der Gamechanger liegt bei den Gesetzesentwürfen in der Automatisierung. Es war bisher so: Gerade der Faktor

Mensch war bei diesen ganzen Überlegungen der grundrechtlich limitierende Faktor. Ein einziger Ermittler konnte nicht alle Bilder im Internet anschauen, eine einzige Ermittlerin konnte nicht alle Asservate, alle digitalen Daten gleichzeitig nach Ermittlungsansätzen durchsuchen. Automatisierte Analysen heben diese Grenzen jetzt aber gänzlich auf. In naher Zukunft werden wir breiter, schneller, intelligenter automatisiert suchen können. Und das wird im Einzelfall leistungsfähiger sein als alle Ermittlerinnen und Ermittler in der Bundesrepublik gleichzeitig in diesem Fall. Auch wenn man die Nutzung solcher Tools erwägen sollte, muss man sich dabei bewusst sein, dass man es hier mit einer völlig anderen Dimension hinsichtlich der Analysebreite und der Analysetiefe zu tun hat. Die hier in Rede stehenden Ermittlungsnormen würden die Erstellung umfangreicher Persönlichkeitsprofile und umfangreicher Auswertung in der Tiefe einzelner persönlicher Daten ermöglichen. Das Bundesverfassungsgericht hat in der jüngeren Rechtsprechung enge Voraussetzungen geschaffen und wir meinen, der hier vorgesehene automatisierte Bildabgleich, der bereits bei Straftaten „mittlerer Klasse“ greift – im Gesetzentwurf steht „im Einzelfall mit erheblicher Bedeutung“ – könnte dann bereits entsprechende Ermittlungen bei einer fahrlässigen Körperverletzung zulassen. Der Straftatenkatalog des § 100a Absatz 2 StPO geht auch sehr weit. Das ist für die verfassungsrechtlichen Vorgaben des Bundesverfassungsgerichts bei Weitem nicht ausreichend. Hinzu kommt kein vorgesehener Richtervorbehalt, dadurch keine effektive Kontrolle, keine Zweckbindung der gewonnenen Daten, keine Verwendungs- und Verwertungsvorbehalte. Erforderlich wäre gewesen, zumindest eine Begrenzung des Analyseumfangs auf entsprechende Datenquellen, dass es vordefiniert ist, und zwar limitiert durch einen konkreten Auffindeverdacht. Man darf nur da suchen, wo man auch vermutet, etwas zu finden und nicht völlig uferlos, wie es vorgesehen ist, in allen Datenquellen. Es fehlt zudem an einer Dokumentation und Protokollierung. Insofern spricht sich der Deutsche Anwaltsverein gegen diese Gesetzesentwürfe aus und fordert eine Neukonzeption. Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank, Herr Kempgens. Wir fahren fort mit Martina Link, die durchaus häufiger im Ausschuss zu Gast ist.

SVe **Martina Link** (BKA): Vielen Dank, Herr Vorsitzender. Ich würde mich gerne auf zwei wesentliche Änderungen beschränken, die durch die Gesetzesentwürfe ermöglicht werden, nämlich einmal die automatisierte Datenanalyse und zum zweiten den biometrischen Internetabgleich: Die automatisierte Datenanalyse ist für das BKA als Ermittlungsbehörde, aber auch als Zentralstelle für die Unterstützung des Bundes und der Länder bei der Kriminalitätsbekämpfung von erheblicher Bedeutung. Wir erlangen tagtäglich im Zuge unserer Ermittlungsverfahren große Datenmengen, digitale Datenmengen, beispielsweise durch die Sicherstellung von Smartphones, von digitalen Datenträgern, und wir erlangen gleichzeitig als Zentralstelle für den Informationsaustausch eine Vielzahl schriftlicher Informationen. Die Verarbeitung und Auswertung dieser Datenmengen sind für uns wesentlicher Bestandteil unserer Arbeit. Die vorgesetzten Regelungen versetzen uns in die Lage, diese Daten, die in unterschiedlichsten Formaten und Datenbeständen aktuell gespeichert sind, strukturiert auszuwerten, darüber Zusammenhänge zu erkennen und neue Ermittlungsansätze zu gewinnen. Es geht dabei ausdrücklich nicht darum, neue Datenbanken aufzubauen, sondern es geht ausschließlich darum, das Verknüpfen und Erschließen von bereits rechtmäßig erhobenen und bei uns gespeicherten Daten zu ermöglichen. Entsprechend ist eine Anbindung dieser geplanten Anwendungen an andere, an externe Register beispielsweise oder gar an Internetdienste nicht zulässig. Zulässig ist ausschließlich die Einbeziehung einzelner zusätzlicher Datenquellen, die ebenfalls zuvor rechtmäßig erhoben werden mussten.

Auch der automatisierte biometrische Internetabgleich ist ein unersetzliches Ermittlungsinstrument, insbesondere für die Identifizierung und Lokalisierung von Straftätern und Gesuchten. Sie ermöglicht es mithilfe öffentlich zugänglicher Daten aus dem Internet, Hinweise zur Identität eines Tatverdächtigen, zum Aufenthaltsort von Personen oder zu möglichen Tat- und Täterzusammenhängen zu gewinnen. Und für die Anwendung dieser Befugnis gelten sehr hohe rechtliche Anforderungen. Die Straftat muss im Einzelfall von erheblicher Bedeutung sein. Die Strafverfolgung oder Gefahrenabwehr muss auf andere Weise aussichtslos oder wesentlich erschwert sein. Bei der Nutzung eines privaten Anbieters aus einem Drittland wird diese Eingriffsschwelle nochmals erhöht. Zulässig ist eine solche Abfrage nur zum Zwecke des Schutzes der nationalen Sicherheit und sie unterliegt einem

Richtervorbehalt. Aus polizeifachlicher Sicht sind diese Anforderungen und insbesondere der Richtervorbehalt sehr hoch, denn nach unserer Bewertung ist der biometrische Internetabgleich, faktisch eine Dateiabfrage, deutlich weniger eingriffsintensiv als eine Öffentlichkeitsfahndung, bei der nicht nur Fotos des Betroffenen, sondern detaillierte Personenbeschreibungen und der der Ausschreibung zugrunde liegende Sachverhalt veröffentlicht und für jedermann sichtbar werden.

Eine wichtige Anmerkung zum Schluss: Der im Gesetzentwurf zur Änderung der Strafprozessordnung für biometrische Abfragen in Drittstaaten vorgesehene Weg der justiziellen Rechtshilfe ist aus unserer Sicht ebenso wenig praktikabel wie der als Alternative in der Begründung vorgesehene Weg, nachdem die Länder entsprechende Erhebungen über das BKA als Zentralstelle durchführen sollen. Hier bedarf es auch für die Länder einer unmittelbaren Abfragemöglichkeit, so wie es für das BKA im Gesetzentwurf zur Stärkung digitaler Ermittlungsbefugnisse vorgesehen ist. Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke schön, Frau Link. Und es fährt fort, Herr Professor Löffelmann, bitte.

SV **Prof. Dr. Markus Löffelmann** (HS Bund): Vielen Dank, Herr Vorsitzender, meine Damen und Herren Abgeordneten. Betrachtet man die Genese des deutschen Sicherheitsrechts über die vergangenen 20 oder 25 Jahre, dann kann man eine gewisse Vorliebe der Gesetzgeber in Bund und Ländern feststellen, verfassungsgerichtliche Vorgaben sehr kleinteilig umzusetzen. Diese pragmatische Taktik funktioniert für die Entscheidung des Bundesverfassungsgerichts von 2023 zur automatisierten Datenanalyse nicht. Denn in dieser Entscheidung äußert sich das Gericht nur sehr selektiv zu dieser wichtigen Thematik. Es zeigt Kriterien auf, die der Gesetzgeber bei der Schaffung gesetzlicher Regelungen zu berücksichtigen habe, fordert eine präzise gesetzliche Einhegung, lässt aber zugleich einen breiten gesetzgeberischen Gestaltungsspielraum – und das macht es erforderlich, diese Entscheidung weiterzudenken. Meines Erachtens verfehlen die gegenständlichen Gesetzentwürfe diesen Anspruch, weil sie sich im Wesentlichen an einer Aussage des Gerichts in einer Randnummer dieser Entscheidung orientieren, dabei aber andere Aussagen, den Kontext der Entscheidung und anderer Entscheidungen zum Sicherheitsrecht, weitgehend ausblenden.

Dadurch kommt Mehreres zu kurz. Erstens, es fehlt in diesen Regelungen zur automatisierten Datenanalyse eine präzise gesetzliche Einhegung zu Art und Umfang der zur automatisierten Analyse zur Verfügung stehenden Daten und der zulässigen Analysemethoden. Zweitens, die Regelungen genügen meines Erachtens auch nicht den vom Verfassungsgericht artikulierten Anforderungen an individuellen Rechtsschutz und aufsichtliche Kontrolle. Und drittens, und das möchte ich ausdrücklich betonen, schneidet diese Herangehensweise das Instrument der automatisierten Datenanalyse bewusst für einen breiten Anwendungsbereich polizeilicher Tätigkeit ab.

Was bislang sowohl auf Bundes- als auch Länderebene fehlt, ist ein kohärentes Regelungskonzept, das Kategorien der Schutzwürdigkeit von personenbezogenen Daten und Kategorien der Leistungsfähigkeit und Risikoanfälligkeit von Analysemethoden zu den mit der Analyse verfolgten repressiven und präventiven Zwecken ins Verhältnis setzt. Die Herstellung dieser Verhältnismäßigkeit ist eine ureigene gesetzgeberische Aufgabe. Ein solches Stufenmodell ist meines Erachtens auch eine zwingende Voraussetzung für die Verwirklichung des beabsichtigten Datenhauses der Polizei. Denn wenn man Regelungen zur bevorratenden Speicherung solcher Daten schafft, muss man zugleich festlegen, für welche Analysezwecke die Daten zur Verfügung stehen. Verfassungsrechtliche Risiken anderer Aspekte des Gesetzespakets lassen sich meines Erachtens durch kleinere Nachjustierungen minimieren. Für die automatisierte Datenanalyse trifft das nicht zu. Hier ist noch Grundlagenarbeit erforderlich. Und deshalb möchte ich an Sie appellieren, das nicht aus dem Blick zu verlieren. Dieses Instrument dürfte das mächtigste sein, über das der Gesetzgeber in den letzten 20, 25 Jahren zu entscheiden hatte. Ich bedanke mich.

Amt. Vors. **Josef Oster** (CDU/CSU): Herzlichen Dank. Als nächstes erhält das Wort für sein Eingangsstatement Herr Professor Möstl.

SV **Prof. Dr. Markus Möstl** (Universität Bayreuth): Vielen Dank. Die Gewährleistung von Sicherheit ist eine Staatsaufgabe, von der die Institution Staat, wie das Bundesverfassungsgericht sagte, ihre eigentliche und letzte Rechtfertigung herleitet. Es ist für das Vertrauen der Bürger in ihren Staat daher

von entscheidender Bedeutung, dass die Befugnisse der Sicherheitsbehörden mit den Herausforderungen der Zeit und den technischen Möglichkeiten Schritt halten. Alle Befugnisgruppen dieses Gesetzespakets knüpfen je auf ihre Weise an diese Ausgangsüberlegung an.

Erstens: Die Befugnisse zur Sicherung von Verkehrsdaten betreffen ein Grundproblem polizeilicher Ermittlungsarbeit unter den Bedingungen moderner Kommunikation. Wie wird sichergestellt, dass der immer wichtigere Raum elektronischer Kommunikation nicht zu einem Raum wird, in dem keine Spuren mehr hinterlassen werden, sodass eine spurenbasierte polizeiliche Ermittlungsarbeit strukturell unmöglich wird und so ein Raum entsteht, der, obwohl für die Planung und Begehung von Straftaten von höchster Relevanz zum rechtsfreien Raum zu werden droht? Dass die hier hinterlassenen digitalen Spuren von den Kommunikationsbetreibern nicht oder nur kurz gespeichert werden, ist ein seit langem bekanntes Problem. Zur Einlösung seiner Sicherheitsaufgabe muss der Staat eine Art moderner elektronischer Spurensicherung anordnen können. Hierzu gehört die anlassbezogene vorsorgliche Datensicherung, wie sie nunmehr eingeführt werden soll.

Zweitens: Auch die automatisierte Datenanalyse betrifft eine Grundfrage moderner Ermittlungsarbeit. Inwieweit darf die Polizei das bei ihr rechtmäßig vorhandene Wissen in einer technisch effektiven Weise, das heißt, möglichst automatisiert und nicht mühsam per Hand durchsuchen, analysieren und zusammenführen, um so eine effektive Gefahrenabwehr zu ermöglichen? Artikel 87 Absatz 1 Satz 2 Grundgesetz bringt mit seinem altmodischen Wort „polizeiliches Auskunfts- und Nachrichtenwesen“ in einer bleibend gültigen und verallgemeinerungsfähigen Weise zum Ausdruck, wie wichtig das Anliegen der effektiven Zusammenführung des bei der Polizei verstreut vorhandenen Wissens ist. Zu einem *zeitgemäßen* polizeilichen Auskunfts- und Nachrichtenwesen gehört die automatisierte Datenanalyse, wie sie nun ermöglicht werden soll.

Drittens: Der Fall Klette, bei dem es Journalisten mittels einer ihnen zugänglichen Technik des automatisierten biometrischen Abgleichs mit öffentlichen Internetdaten gelang, eine Spur aufzutun, die den staatlichen Ermittlern verborgen geblieben war, weil sie über keine Befugnis zum Einsatz einer solchen Technik verfügten, ist ein Lehrstück dafür, wie wichtig für das Vertrauen der Bevölkerung in ihre Polizei zeitgemäße und dem Stand der Technik entsprechende Ermittlungsbefugnisse sind. Dass der Entwurf diese Lücke schließen will, ist zu begrüßen. Der Abgleich rechtmäßig vorhandener Daten mit öffentlichen Internetdaten scheint mir ein zwar erhebliches, aber kein besonders herausgehobenes Gewicht zu haben. Dementsprechend ist die Eingriffsschwelle, die auf Schutzgüter von zum Teil nur erheblicher Bedeutung abstellt, in Ordnung. Ich bedanke mich.

Amt. Vors. **Josef Oster** (CDU/CSU): Herzlichen Dank, Herr Professor Möstl. Ich darf dann die Parlamentarische Staatssekretärin Annette Kramme herzlich begrüßen. Herzlich willkommen. Vielen Dank, dass Sie dieser Anhörung beiwohnen. Wir fahren in unserer Reihenfolge fort. Das Wort erhält Alexander Poitz.

SV **Alexander Poitz** (GdP): Vielen Dank, sehr geehrter Herr Vorsitzender, sehr geehrte Abgeordnete, sehr geehrte Damen und Herren. Vielen Dank für die Einladung und die Möglichkeit, unsere Position als Gewerkschaft der Polizei zu den vorliegenden Gesetzentwürfen darzustellen. Mein Name ist Alexander Poitz, ich bin stellvertretender Bundesvorsitzender der GdP.

Kriminalität verlagert sich zunehmend in den virtuellen Raum. Wir haben einen monetären Schaden durch Cybercrime von über 200 Milliarden Euro jährlich. Eine Underground-Economy mit einer Art Jobvermittlung zur Straftatenvorbereitung und -begehung – ein enormes kriminelles Personengeflecht. Unsere Polizeien des Bundes und der Länder machen dennoch tagtäglich einen guten Job, vielen Dank dafür. Jedoch jonglieren wir Personal an der Belastungsgrenze, haben eine mangelhafte Vernetzung, keine einheitliche IT-Infrastruktur, stehen enormen Datenmengen gegenüber, einer steigenden Anzahl an Extremisten, Terroristen, veralteter Technik und in die Jahre gekommener Ermittlungsbefugnisse. Es scheint schon etwas wie der Kampf David gegen Goliath. Deshalb befürworten wir die Gesetzentwürfe zum einen zur Weiterentwicklung der StPO, als auch des BKA-Gesetzes und des Bundespolizeigesetzes.

Die polizeiliche Königsdisziplin ist die Prävention. Schaut man sich die Fahndung, Täteridentifizierung, Kommunikations- und Bewegungsprofile an, sind wir als Sicherheitsbehörden noch nicht im

21. Jahrhundert angekommen. Der Schwerpunkt liegt leider oft auf einem tatbezogenen Ansatz. Händische Auswertungen über Excel-Listen, analoge Spurensuche bedeutet enormer personeller und zeitlicher Aufwand. Mit den vorgeschlagenen Befugnissen zur Biometrie, Datenanalyse und bei IT-Produkten wird ein deutlicher täterbezogener Schwerpunkt verfolgt. Wir wissen von kriminellen Vorbereitungen/Handlungen, es fehlen uns aber die Erkenntnisse, Vorfeldermittlungen, die Ermittlungsansätze aufgrund einer gewissen digitalen Blindheit. Aus händischen Auswertungen, Funkzellenauswertungen, Datenabfragen in unzähligen Systemen wird eine klare Nutzung und ein Abgleich mit ohnehin öffentlichen Daten mit einem Anlass, Zweckbindung, Protokollierung und Löschverpflichtungen. Mithilfe einer automatisierten Datenanalyse werden aus Excel-Listen strukturierte Datenpakete mit direktem Tat- und bestenfalls Personenbezug. Konkrete Identifizierung oder Zeitbeziehungen, Kommunikations-stränge – es sollen keine neuen Datensammlungen entstehen, sondern rechtmäßig erhobene polizeiliche Daten zweckgebunden, strukturiert sowie verknüpft werden.

Die Eingrenzung des § 5 BKA-Gesetz hinsichtlich des Terrorismus auf interne Datensysteme sowie die Anordnungsbefugnis halten wir für sachgerecht. Auch die Sicherungsanordnung von Verkehrsdaten gewährleistet einen Beweismittelverlust. Mit der fortschreitenden Technisierung muss der Entwicklung, Anpassung zur Überprüfung von IT-Produkten Rechnung getragen werden.

Eine starke Strafverfolgung als Rechtsstaat. Grundlage eines erfolgreichen Ermittlungsverfahrens sind Beweise. Die Ermittlungen sowie Identifizierung relevanter Personen, Beschuldigter, Zeugen ist hierbei wesentlich für die Beweisverdichtung. In Anbetracht enormer sichergestellter Datenmengen, beispielsweise bei Smartphones oder Ähnlichen, ist eine automatisierte technische Auswertung im 21. Jahrhundert alternativlos. Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke schön. Als nächstes erhält das Wort Dr. Schmidtke.

SV **Dr. Andreas Schmidtke** (OLG Düsseldorf): Sehr geehrter Herr Vorsitzender, meine sehr geehrten Damen und Herren. Ich bedanke mich herzlich für die Einladung. Aus richterlicher Sicht ist die Einführung des biometrischen Internetabgleichs und der automatisierten Datenanalyse ausdrücklich zu begrüßen. Für eine effektive Gefahrenabwehr und Strafverfolgung sind beide Instrumente unverzichtbar. Der Staat muss, will er handlungsfähig und wehrhaft bleiben, mit der technischen Entwicklung Schritt halten. Es ist kaum vermittelbar, dass im IT-Zeitalter die ohnehin knappen Ressourcen in fehleranfällige manuelle Ermittlungen gebunden werden, wenn technische Verfahren schneller, zuverlässiger und oft überhaupt erst zum Erfolg führen. Der Weg, diese Ermittlungsmaßnahmen verfassungs- und europarechtskonform einzuführen, ist schmal. Insbesondere in seinen jüngeren Entscheidungen zur Datenanalyse und zum BKA-Gesetz hat das Bundesverfassungsgericht dezidiert vorgezeichnet, welchen verfassungsrechtlichen Anforderungen diese Regelungen im Einzelnen genügen müssen. Hinzu treten europarechtliche Vorgaben, insbesondere aus der KI-Verordnung, die den gesetzgeberischen Gestaltungsspielraum zusätzlich einengen. Bei Anwendung dieser Maßstäbe begegnen der biometrische Internetabgleich in der StPO und im BKAG als solcher keinen Bedenken. Bei der Identifizierung und Aufenthaltsermittlung stimmen, anders als teilweise dargelegt, Eingriffsschwelle und Gewicht überein. Für Zeugen sollte § 98d StPO allerdings zusätzlich eine personenbezogene Tatsachenschwelle vorsehen. Für die weitergehende Sachverhaltserforschung reicht die vorgesehene Eingriffsschwelle hingegen nicht aus. Sie sollte auf gesetzlich näher bestimmte schwere Straftaten beschränkt werden. Das BKAG ist insoweit enger gefasst und begegnet daher im Ergebnis keinen Bedenken. Bei der automatisierten Datenanalyse sind weitergehende Nachbesserungen erforderlich. Zweckändernd einbezogene Daten müssen einen hinreichend spezifischen Bezug zum Verfahren aufweisen. Eine Datenanalyse ins Blaue darf es nicht geben. Bei § 98e StPO ist insoweit nachzubessern. Vor allem berechtigt eine rechtmäßige Datenerhebung aber nicht dazu, bereits erhobene Daten schrankenlos zu einem umfassenden Analysebestand zusammenzuführen.

Der vorgehaltene Datenbestand braucht deshalb ein eigenständiges gesetzliches Speicherregime mit Speicherzweck, -schwelle und -dauer, was bislang fehlt.

Schließlich bleibt ein Einheitsmodell, das nur an eine ihrerseits nicht durchgehend tragfähige Schwelle anknüpft, für Fälle geringen Tat- und Gefahrengewichts verfassungsrechtlich angreifbar und es schöpft zugleich in besonders schweren

Fällen die potenziellen Ermittlungsmöglichkeiten nicht aus. Vorzugswürdig erscheint daher ein abgestuftes Regelungsmodell. Ein solches würde dem verfassungsrechtlichen Zusammenspiel von Eingriffsgewicht und Rechtfertigungsanforderungen deutlich besser gerecht und verhinderte zugleich, dass besonders gewichtige Fälle an Beschränkungen gebunden bleiben, die nur für niedrige Eingriffsschwellen erforderlich sind. Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Herzlichen Dank. Den Abschluss in dieser Eingangsrunde macht Frau Sombetzki.

SVe **Pia Sombetzki** (AlgorithmWatch): Sehr geehrter Herr Vorsitzender, sehr geehrte Abgeordnete, ich danke für die Möglichkeit zur Stellungnahme. Mein Name ist Pia Sombetzki. Ich bin Senior Policy Managerin bei der Menschenrechtsorganisation AlgorithmWatch und in meinen Eingangsworten möchte ich mich auf die Befugnisse für den automatisierten biometrischen Abgleich mit Daten aus dem Internet fokussieren. Diese sind meiner Ansicht nach zurückzuziehen, unter anderem eben auch, weil ich sie als nicht vereinbar mit höherrangigem Recht einordne.

Es folgen drei Hauptaspekte, an denen ich das festmache. Erstens: Die angesprochenen Eingriffsschwellen sind meiner Ansicht nach viel zu unspezifisch geregelt. Hier reichen Prognosen und Annahmen aus, warum man den biometrischen Abgleich zu rechtfertigen hat. Ganz pauschal soll man auch Sachverhalte erforschen können, also noch viel breiter, so sehe ich das, geht es eigentlich nicht. Und zweitens und bei dem Punkt möchte ich vertiefen, wird es vor allem an der Praxis vorbeigeregelt. Ein automatisierter biometrischer Abgleich fußt darauf, dass man eine Datenbank aufbaut und biometrische Templates vorhält. Nur so kann ein Abgleich durchgeführt werden, wenn er gebraucht ist, zum Beispiel, wenn das BKA das machen möchte. Das heißt, diese eingeführten Löschpflichten, die in den Gesetzen stehen, laufen ins Leere. Und die Folge ist, dass Menschen davon ausgehen müssen, mit ihren Gesichtern und Stimmen, übrigens auch über Videos und Fotos Dritter, in solchen Datenbanken erfasst und selbst in den privatesten Kontexten auffindbar und identifizierbar zu sein. Dies wissend kann der für Demokratien sehr unerwünschte „Chilling-Effekt“ entstehen, also ein Abschreckungseffekt, der dazu führen kann, dass man sich aus dem öffentlichen Leben zurückzieht, seine Meinungsfreiheit, Versammlungsfreiheit vielleicht nicht mehr so aktiv wahrnimmt und dies, weil man eben Angst haben könnte, man könnte unnötigerweise ins Visier der Polizei geraten. Dieses Problem haben auch die Gesetzgeber in Brüssel als solches anerkannt, weswegen die KI-Verordnung den Aufbau solcher Datenbanken verbietet. Und zusätzlich möchte ich auch anmerken, ist der Konflikt mit dem Datenschutzrecht offensichtlich. Europäische Datenschutzbehörden haben schon vor Jahren Bußgelder gegen kommerzielle Anbieter solcher Suchmaschinen, wie zum Beispiel von Clever AI, verhängt.

Und damit komme ich zu meinem dritten Punkt, der anschließt, denn um auf solche kommerziellen Anbieter dennoch zurückgreifen zu können, enthalten die Entwürfe noch obendrauf eine Art Auslagerungsbefugnis ins Ausland. So soll der Abgleich zum Beispiel in den USA oder Dubai durchgeführt werden können, wo die Anbieter sitzen. Und das sind, das möchte ich betonen, Orte, an denen biometrische Massenüberwachung schon längst Alltag ist. Die sollten wir uns nicht herbeiregeln. Sie wird dort für Zwecke der Unterdrückung von Protesten eingesetzt, zur Verfolgung von vermeintlich illegal Eingewanderten. Und das lässt mich zusammenfassend wirklich nur sagen, solche Überwachungstechnologie gehört nicht leichtfertig unter der Überschrift „Modernisierung der Polizei“ eingeführt. Wir sollten sie stattdessen als das betrachten, was sie ist – eine Technologie, die im Privaten für Stalking eingesetzt wird, aber eben auch für Repressionen, also ein beliebtes Instrument autoritärer Machthaber ist, mit denen wir uns in keinem Fall gleichmachen sollten. Vielen Dank für die Aufmerksamkeit.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank an Sie, Frau Sombetzki, für Ihr Eingangsstatement. Danke an alle, dass Sie sich so konsequent an das Zeitfenster gehalten haben. Das gibt jetzt genug Raum, um in die Fraktionsrunde einzusteigen. Ich habe es zu Beginn erklärt: Zwei Fragen an einen Sachverständigen oder jeweils eine an zwei Sachverständige, das ist unsere Regel. Maximal zwei Minuten gibt es als Fragezeitfenster, darauf kommt direkt die Antwort, auch in zwei Minuten. Und für die Unionsfraktion, mit der wir beginnen, erteile ich Herrn Wiegelmann das Wort. Herr Wiegelmann, bitte.

Abg. **Johannes Wiegelmann** (CDU/CSU): Vielen Dank, Herr Vorsitzender. Vielen Dank, an die Damen und Herren Sachverständigen. Ich habe jeweils eine Frage an Frau Vizepräsidentin Link und Herrn Professor Möstl, und zwar zum Komplex automatisierte Datenanalyse. Einmal eine tatsächliche und einmal eine rechtliche Betrachtung: Frau Link, könnten Sie uns den Mehrwert der automatisierten Datenanalyse für die polizeiliche Arbeit noch einmal vertiefter darstellen, die Zusammenhänge unter technischen Sichtpunkten und wie das ablaufen würde?

An Sie, Herr Professor Möstl, die Frage – das war schon in den Eingangsstatements der Debatte angezweifelt worden – ob die Regelungen zur automatisierten Datenanalyse verfassungsgemäß seien. Sie können in Ihrer Beurteilung nichts erkennen, was dafürspräche, dass die Vorgaben des Bundesverfassungsgerichts in der schon zitierten Leitentscheidung zur automatisierten Datenanalyse nicht beachtet worden wären. An welchen Stellen setzt dieser Entwurf diese Vorgaben um – vielleicht mit beantwortendem Blick auf die Erfahrungen aus den Ländern?

Amt. Vors. **Josef Oster** (CDU/CSU): Herzlichen Dank, Herr Wiegelmann. Dann beantworten wir das in der gestellten Reihenfolge. Frau Link, bitte, Sie beginnen.

SVe **Martina Link** (BKA): Vielen Dank. Vielleicht zunächst einmal ein kurzer Blick auf die Datenstruktur der Polizei, wie sie heute aussieht: Wir haben eine Vielzahl von Datenbeständen, in denen strukturiert Daten abgelegt sind. Und es gibt weitere Datenbestände, in denen die Daten unstrukturiert abgelegt sind. Das heißt, ich kann zum Beispiel nicht nach Personalien, Geburtsdaten oder Ähnlichem suchen, sondern es sind freitextliche Begriffe, in denen sich solche Daten befinden. Es sind Daten aus Telekommunikationsüberwachung oder aus Forensik. Diese Daten sind in unterschiedlichen Beständen abgelegt und sie sind darüber hinaus in unterschiedlichen Formaten abgelegt. Immer dann, wenn ich bestimmte Abgleiche machen möchte, muss ich mit einem Suchdatum jede einzelne dieser Dateien abfragen und die Ergebnisse, die ich bekomme, muss ich dann nebeneinanderlegen und versuchen, aus diesen Ergebnissen Zusammenhänge zu erlangen und zu erkennen. In dem Moment, wo es eine automatisierte Datenanalyse gäbe, gäbe es die Möglichkeit, übergreifend über diese Datenbestände hinweg zu suchen. Das heißt, Zusammenhänge, die wir aktuell gar nicht erkennen können oder nur in einer Vielzahl von Datenbeständen vielleicht zufällig erkennen, auf die könnte ich treffen. Ein kleines Beispiel dazu: Hinweis eines ausländischen Dienstes auf eine Person, genannt Al-Almani, die auf einem Volksfest im Rhein-Main-Gebiet einen Anschlag begehen möchte. Wir wissen, er soll eine Tätowierung tragen und eine Ehefrau aus dem Irak haben. Wir wissen nicht, ob sie irakische Staatsangehörige ist oder ob sie möglicherweise dort geboren ist. Bisherige Vorgehensweise: Jeder einzelne Datentopf muss manuell abgeglichen werden – Fallsysteme, INPOL, AZR, Einwohnermeldedaten. Dieser Abgleich ist kaum möglich. Künftig könnte man in eine Datenmaske genau das eingeben. Ich habe einen Al-Almani, der offensichtlich entweder deutscher Staatsangehöriger ist oder zumindest in Deutschland gelebt hat, der eine Tätowierung trägt und eine Ehefrau hat, die ebenfalls entweder im Irak geboren ist oder gelebt hat. Mit einer solchen Suchanfrage könnte ich über alle Datenbestände hinweg die vorhandenen polizeilichen Bestände durchsuchen und dadurch zu Erkenntnissen kommen.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke schön. Herr Professor Möstl.

SV **Prof. Dr. Markus Möstl** (Universität Bayreuth): Ich wurde nach den verfassungsrechtlichen Rahmenbedingungen gefragt. Es ist an dieser Stelle so, wie wir es jetzt leider im Sicherheitsbereich häufiger erleben. Wir haben eine Leitentscheidung des Bundesverfassungsgerichts und es ist eine Wissenschaft für sich geworden zu verstehen, was genau das Bundesverfassungsgericht gemeint hat. Zwei Wissenschaftler haben mindestens drei Meinungen zu diesem Thema. Das hängt mit der sehr großen Komplexität zusammen und der Tiefe der Überprüfung, mit der das Bundesverfassungsgericht die Dinge angeht. Mein Eindruck ist, dass der Gesetzentwurf, so wie die Länder auch, die Komplexität dadurch versucht zu vereinfachen, dass man sich in erster Linie einmal an dem Fall orientiert: Was ist es, wenn es ein „besonders schwerwiegender Eingriff“ ist? Wie sind dafür die Voraussetzungen, die das Bundesverfassungsgericht verlangt? Und das normieren wir jetzt einmal. Das schöpft nicht die Möglichkeiten aus, unterhalb dieser „schwerwiegenden Eingriffe“ niederschwellige, vielleicht

auch automatisierte Datenanalysen zu machen. Das haben Sie auch angewendet, aber das ist ein Einstieg, wo man sich noch einigermaßen festhalten kann. Dafür hat das Bundesverfassungsgericht im präventivpolizeilichen Bereich eine mindestens konkretisierte Gefahr für besonders gewichtige Rechtsgüter verlangt. An diese Schwelle hat sich der Entwurf nach meinem Eindruck gehalten. Deswegen halte ich ihn für verfassungskonform.

Amt. Vors. **Josef Oster** (CDU/CSU): Herzlichen Dank. Als Nächstes ist die AfD-Fraktion dran, Herr Janich, bitte.

Abg. **Steffen Janich** (AfD): Vielen Dank, Herr Oster. Die AfD befürwortet grundsätzlich technischen Fortschritt bei der Ermittlungsarbeit der Polizei, befürchtet aber, dass die Daten, die hier gesammelt werden, letztlich zu einer großen Datenkrake zusammenkommen und sieht die Problematik, dass nicht zweckgebundene Daten zu lange in den Systemen erhalten bleiben können. Datensouveränität ist ebenfalls ein Kritikpunkt, auf den wir natürlich hier in der Regelung Wert legen. Ich möchte meine zwei Fragen an Herrn Danisch stellen. Die erste Frage wäre, Herr Danisch, Sie haben früher Mängel bei behördlichen Auskunftsersuchen beschrieben. Welche diese Risiken bestehen aus Ihrer heutigen Erkenntnis fort und wie müssten Authentifizierung, Berechtigungsprüfung und Protokollierung ausgestaltet sein, um missbräuchliche Anfragen zu erkennen? Und meine zweite Frage: Wie muss ein System geschaltet sein, damit Verkehrsdaten zur Zweckerfüllung genutzt oder nach Fristablauf tatsächlich gelöscht werden? Wie müssen Sicherheitskopien, exportierte Datensätze und bereits erzeugte Analyseergebnisse dabei behandelt werden? Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke, das sind zwei Fragen an einen Sachverständigen, Herr Danisch, dann haben Sie bis zu vier Minuten Zeit, darauf zu antworten.

SV **Hadmut Danisch**: Danke schön. Zur ersten Frage: Authentifikation, Berechtigungsprüfung, Autorisation. Ich antworte aus meiner Tätigkeit 2009 als Leiter einer Abteilung in der Vorratsdatenspeicherung eines großen Internetproviders. Ich habe damals etwa 2 000 Fälle bearbeitet, die Eingangsprüfung gemacht und die Rechtsprüfung, dabei auch manchen Streit zum Beispiel mit dem Bundeskriminalamt gehabt, und habe damals feststellen müssen, dass es damals gar keine Authentifikation gab. Es kamen einfach irgendwelche Faxe herein von irgendwelchen Polizeistationen, die sich teilweise noch nicht einmal Polizei nannten, sondern „PI“ für Polizeiinspektion, was kein geschützter Begriff ist. Und ich hatte damals keine Möglichkeit, nachzuprüfen: Sind die berechtigt? Gibt es diese Polizeistation? Ist das authentifiziert? Ich habe tatsächlich zweimal Polizisten erwischt, die für private Zwecke nachgefragt haben. Damals gab es keinerlei Möglichkeit. Das könnte heute insofern etwas besser ausgehen, weil man das heute nicht mehr per Fax, sondern mit elektronischen Schnittstellen machen würde – hoffe ich zumindest. Aber grundsätzlich sehe ich hier in den Gesetzentwürfen keine Antwort auf diese Frage. Ich halte das für ein sehr großes, offenes Problem, das behandelt werden müsste. Auch im Rahmen des Rechtsschutzes, der Rechtsweggarantie des Betroffenen, denn der muss im Nachhinein auch nachvollziehen können, was passiert ist, weil er sich normalerweise während des Verfahrens nicht wehren kann, weil er das nicht gleich erfährt. Das ist eine der wesentlichen Baustellen hier. Und auch da sehe ich einen wunden Punkt und Bedarf an Nachbesserung.

Zur zweiten Frage: Die Löschung von Daten. Hier möchte ich aus meinen aktuellen Erlebnissen als Beschuldigter eines Strafermittlungsverfahrens, in dem man illegal Kontodaten von mir abgegriffen hat, berichten. Es gibt keine Löschmöglichkeit. In der Strafprozessordnung ist zunächst einmal nicht vorgesehen, dass aus der Strafermittlungsakte etwas entfernt wird. Eine Akte, die zumindest heute noch auf Papier geführt wird, wird fortlaufend nummeriert, paginiert. Und da ist es rechtlich, ich habe das extra geprüft, nicht vorgesehen, dass etwas, was einmal in dieser Akte drin ist, wieder entfernt wird. Datenschutzrechtlich haben Sie einen Anspruch auf Löschung. Wenn Daten erfasst werden, die dem Datenschutzrecht unterliegen, das wäre hier der Fall, haben Sie theoretisch einen Anspruch auf Löschung. Aber ich kann diesen Anspruch, obwohl ich es mit allen Mitteln versucht habe, nicht durchsetzen. Gerichte reagieren also gar nicht darauf. Es gibt formal keinen Rechtsweg. Sie können das nicht bei der Staatsanwaltschaft beantragen, genau genommen sind Gerichte auch nicht Vorgesetzte der Staatsanwaltschaft. Gerichte können, wenn sie entscheiden, eigentlich nur über die Verwendung innerhalb eines Gerichtsverfahrens entscheiden und sagen, diese Daten dürfen

nicht verwendet werden, aber die Staatsanwaltschaft nicht zur Löschung zwingen. Die Staatsanwaltschaft weiß gar nicht, dass sie das löschen muss, sie kennt die Verfahren nicht, und effektiv interessiert es niemanden. Der Einzige, der hierfür noch eintreten würde, wäre in dem Fall die Berliner Datenschutzbeauftragte, die Landesbeauftragte für Datenschutz und Informationsfreiheit, die grundsätzlich meiner Meinung ist, die sich aber seit drei Jahren nicht durchsetzen kann und die da auch keine Antwort bekommt. Die Datenerhebung war 2023 und ich habe es bis heute nicht geschafft, diese Daten löschen zu lassen.

Auch das ist ein erhebliches Problem, wenn diese Daten einmal in den Akten, einmal in der Polizei sind. Die wurden sogar weitergegeben an Zoll und Dritte und private Seiten – diese Daten werden überall verteilt und eine Löschung gibt es faktisch nicht, obwohl sie gesetzlich vorgesehen ist. Sie kriegen diese Daten nicht mehr heraus, sie können diese nicht mehr löschen.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke schön. Dann geht es weiter bei der SPD-Fraktion. Herr Schätzl, bitte.

Abg. **Johannes Schätzl** (SPD): Herzlichen Dank, Herr Vorsitzender. Zwei kurze Fragen an Herrn Professor Löffelmann: Jetzt haben Sie in Ihrer schriftlichen Stellungnahme, aber auch in Ihrem Vortrag des Öfteren vom „verfassungsrechtlichen Risiko“ gesprochen. Deswegen wäre die Frage, ob Sie uns konkrete Änderungen vorschlagen könnten, um dieses verfassungsrechtliche Risiko zu minimieren. Die zweite Frage geht in den Bereich biometrischer Abgleich, heraus aus dem verfassungsrechtlichen Risiko hinein in die KI-VO (KI-Verordnung) auf europäischer Ebene: Halten Sie diesen biometrischen Abgleich für KI-VO-konform? Und wenn ja, in welcher Form?

Amt. Vors. **Josef Oster** (CDU/CSU): Kompakte Fragen. Sie haben die Möglichkeit, darauf bis zu vier Minuten zu antworten, bitte.

SV **Prof. Dr. Markus Löffelmann** (HS Bund): Vielen Dank. Ich fange mit den „verfassungsrechtlichen Risiken“ an: Der Ausgangspunkt meiner Überlegungen ist zunächst einmal die Bestimmung der Eingriffsintensität. Was den biometrischen Abgleich anbelangt, kommt hier zum Tragen, dass es um breite Zwecke geht, nämlich nicht nur Identitäts- und Aufenthaltsermittlung, sondern eben auf Zeugen anwendbar und auch allgemein die Erforschung des Sachverhalts – es geht um sehr sensible Daten. Biometrische Daten sind nach europäischem Recht besonders sensible Daten. Es geht darum, dass diese beiden Maßnahmen eine sehr große Streuwirkung haben. Die Verarbeitung solch öffentlich zugänglicher biometrischer Daten stellt gerade nicht eine Verarbeitung dar, die keine Eingriffsintensität hätte, weil die Behörden sie wie jeder Dritte verarbeiten würden. Das ist technisch sehr anspruchsvoll. Das heißt also jeder, dessen Daten dort mitverarbeitet werden, die öffentlich zugänglich sind, der ist eben auch grundsätzlich Betroffener. Dann gibt es noch einen weiteren Punkt: Sie erinnern sich vielleicht, in der letzten Legislaturperiode wurde intensiv über die Überwachungsgesamtrechnung diskutiert. Der Ausgangspunkt war 2008, die Entscheidung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung. Da hat das Gericht gesagt, wenn der Gesetzgeber in Zukunft Instrumente der Massendatenverarbeitung einsetzt, dann ist er in seinen Verhältnismäßigkeitsabwägungen nicht mehr ganz so frei. Das alles führt mich zu der Überlegung, dass diese Maßnahmen zur Verarbeitung von biometrischen Daten in der Taxonomie des Bundesverfassungsgerichts als „schwere Eingriffe“ zu identifizieren wären. Mindestens als schwere Eingriffe. Das hätte dann zur Folge, wenn man in der Logik der Rechtsprechung bleibt, dass daran verfahrensrechtliche Sicherungen zu knüpfen wären, also möglicherweise ein Richtervorbehalt, ich kann mir vorstellen, dass man den auf die Variante „Zeugen und Ermittlung des Sachverhalts“ beschränkt. Die aufsichtliche Kontrolle ist ein ganz wichtiger Punkt. Das soll die Bundesbeauftragte für den Datenschutz besorgen. Wie wir aber seit April wissen – in einer Entscheidung betreffend sie und den BND hat das Bundesverwaltungsgericht festgestellt: Sie hat keine wehrhafte Rechtsposition. Da sehe ich doch einige weitere Probleme, wo man nachsteuern müsste.

Was die Vereinbarkeit, jetzt kommt die zweite Frage, aber ganz kurz, mit der KI-Verordnung anbelangt, habe ich weniger Bedenken, denn die KI-Verordnung ist in Deutschland unmittelbar anwendbares Recht. Die muss nicht in nationales Recht transformiert werden. Die gesetzlichen Regelungen, über die wir sprechen, sehen vor, dass nach dem Abgleich Daten zu löschen sind. Das würde nach meiner Einschätzung nicht dem Verbot widersprechen, dass keine Datenbanken zum Zweck des

biometrischen Abgleichs errichtet werden können. Die Gesetze sehen auch einige Regelungen vor, dass an die Datenverarbeitung keine nachteiligen Folgen geknüpft werden dürfen. Sie sehen, jedenfalls die StPO-Regelung, die Anordnung durch die Staatsanwaltschaft vor. Das sind alles Kriterien, die durch die KI-Verordnung vorgegeben werden. Da sehe ich weniger Probleme.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank, Herr Professor Löffelmann. Dann geht es weiter bei der Fraktion BÜNDNIS 90/DIE GRÜNEN. Herr Kollege Dr. von Notz.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Herr Vorsitzender, herzlichen Dank, meine Damen und Herren Sachverständigen, erstmal herzlichen Dank für Ihre Expertise und dass Sie uns hier helfen, zu versuchen, ein gutes Gesetz zu machen. Ich kann die Vizepräsidentin des BKA gut verstehen, wenn sie beschreibt, wie schwierig das ist mit all den Infos, auf denen die Polizei in all den verschiedenen Datenbanken sitzt und zur Verfügung hat, die sie aber nicht abfragen kann, jedenfalls nicht auf einem praktikablen Weg. Und Herr Professor Möstl hat es angesprochen, natürlich kann man aus der Rechtsprechung des Bundesverfassungsgerichts nicht eins zu eins erahnen, wie genau die Vorgaben für die Befugnisse, über die wir hier reden, wären, was das Gericht im Detail dazu jetzt sagen würde. Aber eines ist doch, glaube ich, völlig unstreitig: Wenn man jetzt solche Zugänge zu solchen Dateien schafft, dann entsteht daraus ein mächtiges Ermittlungsinstrument, das eine große Eingriffstiefe hat, wenn man das anwirft. Und dass der Staat, wenn er gegen Bürgerinnen und Bürger vorgeht, da besondere Dinge berücksichtigen muss, nämlich vor allen Dingen den Bestimmtheitsgrundsatz, wann sozusagen welche Daten von wem zu welchem Zweck abgefragt werden. Da würde ich Herrn Kempgens und Herrn Löffelmann fragen wollen, wenn Sie sich das angucken, was auf dem Tisch liegt, reicht es aus, oder können wir sie nicht gewinnen für unseren Ansatz, der hier auch mit auf dem Tisch liegt, doch etwas mehr mit Augenmaß vorzugehen, um am Ende ein Gesetz zu haben, das in Karlsruhe trägt und hält? Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke schön. Angesprochen ist unter anderem der Herr Kempgens. Mit Ihnen beginnen wir dann. Bitte schön.

SV **Kai Kempgens** (DAV): Ja, Sie müssen das vielleicht auf verschiedenen Ebenen sehen. Bestimmtheit bedeutet zum einen, dass wir wissen möchten: Was ist technisch erlaubt? Und wir haben, glaube ich, alle eins gemein: Wir können nicht in die Zukunft sehen, wir können uns nur den Status Quo an technischen Möglichkeiten anschauen und können uns ungefähr ausmalen, was damit eigentlich erlaubt würde. Erforschung des Sachverhalts ist alles, was den biometrischen Bildabgleich anbelangt. Und in der Fassung ist es nicht etwa so, dass es nur um Fahndungen geht, nur um den Fall Daniela Klette, sondern, „Erforschung des Sachverhalts“ ist *alles*. Das heißt, zu Ende gedacht, könnte man das gesamte Internet nach Bildern durchsuchen, die sehr beiläufig entstehen oder ohne, dass man es weiß, teilweise heimlich. Sie alle sind sicherlich in sehr vielen Bildern vertreten, und man könnte daraus sehr viele Informationen ziehen. Der automatische Zugriff darauf liefert unglaublich viele persönliche Informationen. Und möglicherweise sind die Verknüpfungsmöglichkeiten, mit denen wir uns im Moment befassen, lange nicht das, was die Technik in ein paar Jahren, vielleicht in einem Jahr, vielleicht in ein paar Monaten leisten wird. Das Gleiche gilt doch eigentlich auch für die Tiefenanalyse. Wenn ich mir da anschaue, beispielsweise die StPO-Regelung, da kann in Asservaten gesucht werden, also in beschlagnahmten Handys. Das geht sehr weit und da ist überhaupt nicht umfasst, überhaupt nicht bestimmt, wie weit denn überhaupt solch eine Datenanalyse gehen darf. Letztendlich muss man da auch sagen, das ist eigentlich alles. Und das ist nur die Bestimmtheit auf der obersten Ebene. Die weiteren Ebenen sind die Eingriffsnormen, die gerade bei dem biometrischen Bildabgleich mit dem Begriff „im Einzelfall erhebliche Bedeutung“ definiert sind. Darunter kann man sich nichts Konkretes vorstellen, auch die Rechtsprechung nicht. Die kann das Bundesverfassungsgericht fragen und darauf eine Entscheidung replizieren – aber das ist völlig unbestimmt. Und auf der dritten Ebene, wofür es verwandt werden darf, da gilt das genauso; und da ist es gerade bei der Tiefenanalyse so, wenn da die Rede davon ist, „soweit es erforderlich ist“, was soll man sich darunter vorstellen? Das ist jedenfalls keine ausreichende Bestimmtheit, einen Eingriff, ja oder nein, zu legitimieren und genau zu wissen, was erlaubt und was nicht erlaubt ist.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke schön. Herr Professor Löffelmann.

SV **Prof. Dr. Markus Löffelmann** (HS Bund): Vielen Dank für die Frage, Herr Abgeordneter. Herr Kempgens hat jetzt mehr den biometrischen Abgleich thematisiert. Deshalb würde ich gerne ein paar Worte zur automatisierten Datenanalyse sagen. Ich habe es bereits in meinem Eingangsstatement skizziert. Das zentrale Monitum hier ist meines Erachtens, dass der Gesetzgeber sich darüber Gedanken machen müsste, welche Daten konkret und welche Analysemethoden zum Schutz welcher Rechtsgüter zur Verfügung stehen sollen. Und da sind die Gesetzentwürfe alle sehr unbestimmt. Hier heißt es beispielsweise im § 98e StPO: Es dürfen Vorgangsdaten, Falldaten, Daten aus dem polizeilichen Informationssystem verarbeitet werden. Das sind Datenquellen, aber keine Datenarten. Dahinter verbergen sich eine große Bandbreite von Daten unterschiedlicher Schutzwürdigkeit. Da sind Grunddaten dabei, da sind Telekommunikationsdaten dabei, Gesundheitsdaten vielleicht und dergleichen, und das müsste man meines Erachtens dann schon aufdröseln. Wenn wir auf die Ebene der Länder gucken, da gibt es einige Regelungen, die ein bisschen weiter ausdifferenziert sind, beispielsweise in Baden-Württemberg, seit jüngerer Zeit in Rheinland-Pfalz. Da werden zumindest vom Gesetzgeber Kriterien vorgegeben, anhand derer die Abwägung im Einzelfall stattfinden soll. Auch das ist eine Möglichkeit. Man muss nicht alles ins Gesetz hineinschreiben. Das Bundesverfassungsgericht eröffnet in seiner Entscheidung ausdrücklich diese Möglichkeit, dass man bestimmte Spezifikationen auf die untergesetzliche Ebene verlagert, in Rechtsverordnungen, in Dienstvorschriften. Aber dafür, sagt das Gericht, muss der Gesetzgeber eben dann die Tür öffnen.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Den Abschluss der ersten Fraktionsrunde macht die Fraktion Die Linke, Frau Bünger.

Abg. **Clara Bünger** (Die Linke): Vielen Dank, Herr Vorsitzender. Ich habe zwei Fragen an Frau Sombetzki. Sie haben viel über den biometrischen Abgleich gesprochen. Darauf würde ich gern noch einmal zurückkommen. Sie haben im Eingangsstatement gesagt, dass die Löschpflichten ins Leere führen. Können Sie uns da noch ein bisschen mitnehmen in die Widersprüchlichkeit und vielleicht noch einmal sagen, warum Betreiber solcher Datenbanken von den Aufsichtsbehörden tatsächlich mit Bußgeldern belegt werden.

Und meine zweite Frage: Sie sagten ja in Ihrem Eingangsstatement, dass so etwas ein Repressionsinstrument aus dem Werkzeugkasten autoritärer Machthaber ist. Können Sie vielleicht noch einmal etwas dazu sagen, wo sonst auf der Welt es noch diese biometrischen Überwachungsmethoden der Öffentlichkeit gibt und unterscheidet sich das technologisch dann nicht doch von dem, was hier geplant ist? Vielleicht können Sie darauf noch ein bisschen näher eingehen. Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Frau Sombetzki, bitte.

SVe **Pia Sombetzki** (AlgorithmWatch): Danke für die Fragen. Zur Widersprüchlichkeit: Die theoretische Löschpflicht, die da im Gesetz steht, läuft dahingehend ins Leere, dass man für Abgleiche eine Referenzdatenbank braucht. Beim Lesen der Entwürfe hatte ich die Frage, wurde hier vielleicht einfach nicht verstanden, dass es nicht um die Suchergebnisse geht, die man wieder löschen sollte? Ich glaube, das ist ganz klar, wenn man sie nicht weiter braucht. Aber das führt eben nicht weit genug, weil ja der Überwachungsdruck darin besteht, dass überhaupt eine Datenbank entweder besteht und die Ermittlungsbehörden sie nutzen oder sie extra aufgebaut werden müssen. Die Streubreite wurde schon mehrmals angesprochen. Es sind einfach Unmengen von Unbeteiligten darin, die dort nichts zu suchen hätten. Konkret muss man an der Stelle auf Datenbanken Bezug nehmen. Da möchte ich auf die Praxis verweisen: Bei „Clearview AI“ kann man auf die Webseite gehen und die werben damit, dass sie 70 Milliarden Bilder in ihrer Datenbank haben. Die würden einen Teufel tun und Daten löschen, denn das würde das Produkt für sie nur verschlechtern. Auf diese Anbieter wollen wir zurückgreifen, so wie ich das in der Stellungnahme von Frau Link verstehe.

Und die Bußgelder sind leicht zu erklären: Nach dem Datenschutzrecht haben Anbieter wie „Clearview AI“ einfach ganz knallhart dagegen verstoßen, also Daten, sensibelste Daten, massenhaft gesammelt, niemanden danach gefragt, ob sie sie abspeichern können und auch nicht darauf reagiert, wenn man sie gelöscht haben möchte, keine zuständigen Personen, rechtlichen Personen in der EU benannt. Für all diese Rechtsverstöße gab es einfach Bußgelder, die ausgesprochen wurden, um

die 100 Millionen Euro. Das muss man sich einmal in Erinnerung rufen. Das ist schon ein paar Jahre her. Der baden-württembergische Landesdatenschutzbeauftragte hatte angefangen, gegen „PimEyes“ ein Verfahren zu starten. Da ist anscheinend unklar, wer zuständig ist, weil es eben noch die KI-Verordnung mit dem Verbot gibt. Das sollte aber geklärt werden.

Und zum zweiten Punkt: Natürlich hat man vielleicht die Überwachungskontexte, China, Russland, im Hinterkopf. Natürlich ist Deutschland nicht China. Aber technologisch gesehen ist es kein Riesenunterschied mehr, wenn man sich die genaue Überwachungstechnologie anschaut. In Hamburg haben wir das schon gesehen. Dort wird jetzt von einem chinesischen Unternehmen „Hikvision“ die Kamera am Hansaplatz installiert, um KI-gestützte Überwachung durchzusetzen. Da muss man sich einfach klar sein, dass man damit von den Möglichkeiten, die das an Überwachungsdruck erzeugt, nicht weit entfernt ist, wenn sich das weiter ausbreitet. Wir sind auf Bundesebene nicht allein mit dem Thema beschäftigt – alle Landesparlamente schaffen jetzt Befugnisse. Das Ganze kann zu einem Netz an Überwachungsinfrastruktur führen, von der wir uns vielleicht bisher noch nicht so richtig ausmalen konnten, was das dann in Gänze bedeutet. Die Anonymität im öffentlichen Raum so einzuschränken, das kann schon massive Effekte haben für das Ausleben von eigentlich demokratisch garantierten Freiheiten, die wir noch erhalten wollen. Wozu die ganze Sicherheit, wenn wir dafür mit unserer Freiheit bezahlen müssen? Es ist nicht einmal gesichert, dass es die Erfolge erzielt, die wir jetzt zum Beispiel dem biometrischen Abgleich zusprechen. Wir haben jetzt hier diesen einen Fall von Daniela Klette, der immer wieder angesprochen wird. Mir ist nicht bekannt, dass Journalisten jede Woche irgendwelche mutmaßlichen Täter aufspüren, wie das vielleicht an dieser einen Stelle einmal passiert ist. Dafür so massiv alle Freiheiten einzuschränken, sehe ich einfach überhaupt nicht als verhältnismäßig an.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke schön, Frau Sombetzki. Damit sind wir mit der ersten Runde durch. Wir liegen gut in der Zeit. Ich starte direkt die zweite Fraktionsrunde und für die Unionsfraktion erhält das Wort der Kollege Moser.

Abg. **Christian Moser** (CDU/CSU): Vielen Dank, Herr Vorsitzender. Vielen Dank an alle Sachverständigen für ihre Stellungnahmen und ihre heutigen Ausführungen. Meine Frage geht an Frau Link und Herrn Dr. Schmidtke und bezieht sich auf § 98d der Strafprozessordnung des Entwurfs, also den automatisierten biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet. In § 98d Absatz 1 Satz 2 des Entwurfs heißt es lapidar: „Ein Abgleich mit öffentlich zugänglichen Echtzeitdaten ist unzulässig.“ Was mich interessieren würde: Halten Sie das für sinnvoll? Wie sehen Sie das in Bezug auf die Ermittlungsarbeit oder schränkt das diese ein, sodass wir als Gesetzgeber hier noch einmal nachschärfen sollten? Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke schön. Frau Link.

SVe **Martina Link** (BKA): Vielen Dank. Die Einschränkung ist unter anderem vor dem Hintergrund aufgekommen, dass die KI-Verordnung entsprechende Einschränkungen vorsieht und insofern ist das eine Übertragung auf den nationalen Rahmen. Aus polizeilicher Sicht gibt es Situationen, insbesondere Fahndungssituationen, in denen es sicherlich hilfreich wäre, auch solche Fahndungen mit einzubeziehen. Da die KI-Verordnung hier entsprechende Einschränkungen vorgibt, glaube ich, ist es schwierig, auf nationaler Ebene darüber hinauszugehen.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke, Frau Link. Und Herr Dr. Schmidtke.

SV **Dr. Andreas Schmidtke** (OLG Düsseldorf): Vielen Dank für diese Frage. Es schränkt ein – das meine ich, versteht sich von selbst. Nun hatten wir hier verschiedentlich gehört, dass es insgesamt ein System ist, das nicht starr, sondern flexibel ist. Die hypothetische Zulassung von Echtzeitdaten würde eingriffserschwerend wirken und möglicherweise schwellenrelevant weitere verfassungsrechtliche Rechtfertigungsanforderungen nach sich ziehen. Das allein beantwortet Ihre Frage aber nicht, denn es ist möglich, hier flexibel zu reagieren. Dass man etwa diese sinnvollen Instrumente beispielsweise für die Aufenthaltsermittlung dann zieht und ziehen kann, wenn man sie benötigt. Und wenn sie gleichzeitig den verfassungsrechtlichen Anforderungen genügen. Die Antwort darauf, wenn man den Gedanken weiterspinnt, ist ein Differenzie-

rungsmodell. Ein Differenzierungsmodell dahingehend, dass etwa der Echtzeitdatenabgleich für Aufenthaltsermittlungen von Beschuldigten möglich ist, für besonders schwere Straftaten, möglicherweise auch lediglich Kapitalverbrechen. Das hätte auch Vorteile, weil man ja tätig werden will, auf niedriger Ebene zur Verfolgung von Kriminalität und auf mittlerer Ebene, wenn diese unverzichtbaren Instrumente nicht liegengelassen werden. Es hätte Vorteile, weil man diese eingangs angesprochene Eingriffserschwerung gerade nicht hätte, die man ins System einstellen muss.

Ein letzter Punkt mit Blick auf die Uhr. Was die KI-Verordnung angeht, habe ich eine andere rechtliche Wertung. Die KI-Verordnung lässt die Echtzeitdaten ausnahmsweise zu, aber eben nur für bestimmte Ausnahmen, etwa Freiheitsstrafe von mindestens vier Jahren. Das würde korrespondieren.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke schön. Es geht weiter bei der AfD-Fraktion. Herr Janich.

Abg. **Steffen Janich** (AfD): Vielen Dank. Meine erste Frage geht an Herrn Danisch und die zweite Frage würde ich an Frau Link vom BKA richten. Herr Danisch, Sie befürworten biometrische Fahndungen grundsätzlich, empfehlen aber die Ablehnung dieser Entwürfe. Welche drei Änderungen sind für eine tragfähige Neufassung unverzichtbar?

Meine zweite Frage an Frau Link wäre, welche Schulungen benötigen Beamte, um die Grenzen biometrischer Treffer und automatisierter Zusammenhänge beurteilen zu können? Welche Verantwortung muss bei besonders qualifizierten Fachkräften verbleiben? In diesem Zusammenhang würde mich noch interessieren: Wir werden in Zukunft sehr viele Analysedaten aus öffentlich zugänglichen Datenquellen mit in diese Ermittlungen einfließen lassen. Da wird es mitunter zur Fälschung von Datenmaterial kommen. Das Einfachste wäre zum Beispiel ein KI-Bild, aber auch manipulierte Bilder. Wie wird sich das dann beim BKA auf die Ermittlungsarbeit auswirken? Solche Fehlerbilder, die offensichtlich dann neben das Ermittlungsgeschehen reinpassen. Wenn Sie mit dieser Frage zu viel Antwortzeit brauchen, würde ich noch mal in der nächsten Runde auf Sie zurückkommen.

Amt. Vors. **Josef Oster** (CDU/CSU): Jawohl, dann Herr Danisch, bitte.

SV **Hadmut Danisch**: Vielen Dank. Drei Änderungen. Zunächst einmal, wie ich eingangs sagte, und da würde ich auf meine Ausarbeitung verweisen, halte ich eine qualitative Verbesserung allgemein für erforderlich. Ich halte diese drei Gesetze, die sich sehr ähnlich sind, die deutlich zusammengehören und ähnlich formuliert sind, für qualitativ unzureichend. Die müssen in verschiedener Hinsicht deutlich überarbeitet und verbessert werden, was auch die Konsistenz usw. betrifft.

Das Zweite ist, dass deutlich Grenzen gezogen werden müssen, wann diese Fahndungsmethoden eingesetzt werden können. Das hatten auch die anderen schon gesagt. Ich störe mich vor allem an dieser Formulierung, die man immer wieder trifft, dass man sagt: Entweder dieser Katalog aus § 100a Absatz 2 StPO und es heißt mal „und“ oder mal „oder“ oder mal „insbesondere“, jedes Mal ein bisschen anders formuliert. „Im Einzelfall von erheblicher Bedeutung“ ist auch jedes Mal ein bisschen unterschiedlich formuliert. In der Praxis bedeutet das gar nichts. Das ist ein Gummiparagraf. „Im Einzelfall erhebliche Bedeutung“ heißt auf Deutsch, dass der Staatsanwalt in die Akte einen Zettel legt und drauf schreibt „Verfügung“: „Ich bejahe die Bedeutung“ – mehr heißt das nicht. Er muss nur einen Zettel reinlegen, dann ist die Aktenbearbeitung erfüllt. Es gibt sogar Juristen, die der Meinung sind, dass diese Bedingung immer erfüllt ist, denn sonst würde erst gar nicht ermittelt. In dem Moment, wo man ermittelt, ist es auch von Bedeutung – das ist die Meinung mancher Juristen. Diese Formulierung heißt gar nichts. Da muss man Grenzen setzen.

Als dritten Punkt würde ich sehen, dass man die Praxis und Technik abgleicht, dass man das mit den technischen Gegebenheiten und mit dem praktischen Ablauf eines Strafermittlungsverfahrens in Einklang bringt. Einfach pragmatisch an die Sache herangehen und schauen, wie das läuft und dann eben auch solche Sachen wie, was ich eben angesprochen hatte, Löschpflichten, Löschansprüche usw., wie die umgesetzt werden, dass das „Ding“ einfach konkret durchgespielt wird und nicht nur theoretisch im Elfenbeinturm formuliert wird.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Frau Link.

SVe **Martina Link** (BKA): Die Problematik, die Sie angesprochen haben, Herr Janich, im Zusammenhang mit dem Risiko manipulierter Bilder, die besteht natürlich völlig unabhängig davon, ob es einen biometrischen automatisierten Internetabgleich gibt oder nicht. Das ist ein Thema, mit dem sich insbesondere die Forensikdienststellen in den Polizeien sehr intensiv beschäftigen müssen. Wenn wir einen Abgleich durchführen, und das gilt auch schon heute, wenn wir mit dem polizeilichen Gesichtserkennungssystem arbeiten, dann ist es heute so, dass die Fähigkeiten des Gesichtserkennungssystems, was inzwischen bundesweit eingeführt wurde, deutlich über dem liegt, was sowohl Lichtbildexperten als auch Lichtbildsachverständige beurteilen können. Das ist durch entsprechende Tests festgestellt worden. Nichtsdestotrotz ist es dabei geblieben und bleibt es auch zukünftig dabei, dass die Ergebnisse aus solchen Abgleichen von Menschen bewertet werden müssen, weil es nicht nur darum geht, ob das Bild nachvollziehbar ist und passt, sondern es geht immer auch um den Kontext – kann das zutreffen, passt das zu den sonstigen Indizien und Informationen, die man hat? Und bevor entsprechende Maßnahmen darauf aufgesetzt werden, muss der Polizeibeamte das erst noch einmal bewerten. Das heißt, es gibt niemals eine automatisierte Folge, ein System, KI gestützt, entdeckt irgendetwas und darauf wird unmittelbar eine Maßnahme aufgesetzt, sondern es braucht immer die Entscheidung und die Bewertung des Menschen, der dahinter ist, und zwar unabhängig davon, ob wir einen biometrischen Datenabgleich bekommen oder das wie heute im Zuge normaler Eins-zu-eins-Vergleiche von Bildern erfolgt. Vielleicht noch ein Wort. Bei uns gibt es sowohl Lichtbildsachverständige als auch Lichtbildexperten. Die Experten haben eine Ausbildung, die ist im Bereich vier Wochen plus Praxis. Die Sachverständigen haben eine dreijährige Sachverständigenausbildung.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Wir fahren bei der SPD-Fraktion fort. Frau Kollegin Wegge.

Abg. **Carmen Wegge** (SPD): Vielen Dank, Herr Vorsitzender. Ich habe eine Frage an Herrn Poitz und eine Frage an Herrn Löffelmann und würde mich gerne mit der automatisierten Datenanalyse beschäftigen. Zum einen würde mich von Herrn Poitz interessieren, ob Sie einmal darstellen beziehungsweise beschreiben können, anknüpfend an das, was Frau Link gerade gesagt hat, wie aktuell eine Datenanalyse in der Polizeiarbeit abläuft. Genauer, wie datei- und informationsübergreifende Systeme zusammengreifen, wie Zusammenhänge zwischen Verfahren, Vorgängen und Personengruppen identifiziert werden und vor allem auch, wie viel Zeit es in Anspruch nimmt. Wie sieht es da in der Praxis aus?

Und Herr Löffelmann, Ihre Stellungnahme war in Bezug auf die automatisierte Datenanalyse in § 98e StPO, § 9b und § 39b BKA-Gesetz sehr kritisch. Welche Schritte der Verfahrenssicherung leiten Sie aus der bisherigen Bundesverfassungsgerichtsrechtsprechung ab? Ein bisschen ist es schon angeklungen, aber mich würde vor allem interessieren, was Sie denn bezüglich der Protokollierung und der nachträglichen Kontrolle sehen, wo man da den Gesetzentwurf noch rechtssicherer ausgestalten kann.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke schön. Dann beginnt Herr Poitz mit der Beantwortung.

SV **Alexander Poitz** (GdP): Vielen Dank für die Frage. Ich fange einmal so an: Die Grundlage in Gefahrenabwehrverfahren oder Ermittlungsverfahren bei der Polizei sind Erkenntnisse, Informationen, Spuren, Indizien und auch Verhalten von Personen, die wir verfolgen. Da geht es um Kommunikation, Telefonnummern, Bilder, Nicknames und so weiter. Im Bereich der Gefahrenabwehr – viel wichtiger – da tickt die Uhr für uns. Ich hatte es vorhin im Eingangsstatement gesagt: polizeiliche Königsdisziplin ist die Prävention und in der derzeitigen Polizeipraxis, also in der Ermittlungsarbeit, das hat Frau Link schon erwähnt, prägt die Trennung verschiedener Datentöpfe unsere Arbeit. Wir haben verschiedene Datensammlungen, auf die wir zugreifen dürfen, zweckgebunden, und wir sind aufgrund des digitalen Zeitalters momentan mit einer Masse an Daten konfrontiert. Also Zusatzarbeit beispielsweise durch Sicherstellung von mobilen Endgeräten, digitalen Spuren aus dem virtuellen Raum. Und eine Datenanalyse, um auf die Frage zu kommen, basiert im Regelfall auf manueller Recherche und Abgleicharbeit unserer Ermittlerinnen und Ermittler. Im ersten Schritt heißt das, Anfragen an die verschiedenen Datenbanken zu stellen, also Landesdatenbanken, länderübergreifende Informationssysteme, INPOL ist schon gefallen, Verfahrensakten, Asservate, also einer Vielzahl an händischen Arbeiten. Und im zweiten Schritt erfolgt dann der Datenexport, also die Aufberei-

tung bzw. ein manuelles Zusammenführen in Excel-Listen oder CSV-Formaten, sodass man eine Fülle an Excel-Listen mit ganz vielen Informationen zum Verfahren, Gefahrenabwehrverfahren oder Ermittlungsverfahren, hat und das sodann in der Musteranalyse einer Prüfung zu unterziehen, ob es Zusammenhänge gibt, Übereinstimmung mit gewissen Informationen, Erkenntnissen, Telefonnummern, die an Orten aufgetaucht sind. Und zuletzt eine Verifizierung, d.h. sich mit der Originalakte und der Musteranalyse anzuschauen, ob es einen Abgleich mit Informationen aus der Originalakte gibt. Also viele händische manuelle Schritte, die man hier gehen muss. Und diese Datenmengen müssen auch datenschutzgerecht aufgearbeitet werden. Also immer mit einer Zweckbindung, mit einer Bestimmtheit. Allein das Auslesen mobiler Endgeräte, um an die Daten ranzukommen, beansprucht schon eine enorme Zeit. Durch eine technische Unterstützung erfolgt zwar eine Selektion, aber wir müssen trotzdem händisch über Matrizen und Listen diese Zusammenhänge und Daten herstellen. Und zum Zeitaspekt: Das ist schwer einzuschätzen, denn es ist abhängig von der Komplexität des Verfahrens, von den Datenmengen, die wir haben. Also pauschal nicht darstellbar, sondern aus einer Skala von Stunden bis hin zu Wochen, über die wir hier reden – und das betrifft nur die Datenanalyse. Und das ist nur Unterstützung, am Ende entscheidet ein Mensch über die hoheitlichen Maßnahmen.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Herr Professor Löffelmann fährt fort.

SV **Prof. Dr. Markus Löffelmann** (HS Bund): Vielen Dank für Ihre Frage, Frau Abgeordnete. Das Bundesverfassungsgericht fordert in seiner Entscheidung in jedem Fall für solche Formen der Datenanalyse, die unter hohen materiellen Schwellen nur zulässig sind, verfahrenssichernde Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle. Was heißt das? Man kann, wenn man diese Entscheidung analysiert, einige Gesichtspunkte herausdestillieren. Das Erste ist die Begründung im Einzelfall. Nur wenn solche Entscheidungen begründet sind, sind sie auch justiziabel und können im Wege des präventiven oder nachträglichen Rechtsschutzes überprüft werden. Die StPO-Regelung sieht eine solche Begründungspflicht vor. Wenn ich es richtig im Kopf habe, die BKA-Regelungen und die zum Bundespolizeigesetz nicht.

Zweitens: Protokollierung haben Sie angesprochen. Die einzelnen Verarbeitungsschritte müssen protokolliert werden. Sonst können sie nicht präventiv oder nachträglich überprüft werden.

Drittens: Wenn es sich um eingriffsintensive Formen der Datenanalyse handelt, liegt es in der Logik der gesamten Rechtsprechung des Bundesverfassungsgerichts zum Sicherheitsrecht, dass hier eine unabhängige Präventivkontrolle stattfinden müsste.

Viertens: Aufsichtliche Kontrolle. Ich habe es vorhin schon einmal im Zusammenhang mit dem biometrischen Abgleich angesprochen. Derzeit sind als aufsichtliches Kontrollmittel nur die Befugnisse der Bundesbeauftragten für den Datenschutz vorgesehen. Da haben wir eine Leerstelle, ein gewisses Problem. Wenn wir uns die Rechtsprechung des EGMR ansehen, der ist an dieser Stelle viel strenger. Der fordert eine wirksame ex-post-facto-Kontrolle. Das heißt, die muss auch in der Praxis effektiv sein. Da lässt sich hier ein Fragezeichen dran machen. Ich könnte noch andere Punkte anführen. Ein Rechte- und Rollenkonzept für den Zugriff, Schulungen, regelmäßige Fehleranalyse, Stand der Technik ist einzuhalten, Weiterentwicklung der technischen Systeme. Da gibt es einiges, woran man noch denken müsste.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Es geht weiter bei BÜNDNIS 90/DIE GRÜNEN, Frau Kollegin Dr. Gumnior.

Abg. **Dr. Lena Gumnior** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank. Ich habe zwei Fragen an Herrn Kempgens. Sie haben in Ihrem Eingangsstatement die Problematik der Anknüpfung an § 100a StPO angesprochen und schlagen in Ihrer Stellungnahme vor, sich am Straftatenkatalog des § 100b StPO zu orientieren und zusätzlich eine Beschränkung, um im Einzelfall auch schwere Straftaten vorzusehen. Warum ist aus Ihrer Sicht dieser Verweis im Gesetzentwurf problematisch? Welche praktischen Folgen können am Ende daraus erwachsen? Welche Straftaten und Rechtsgüter könnten solche Maßnahmen am Ende vielleicht rechtfertigen?

Als zweiter Punkt: Der Entwurf erlaubt in § 98d Absatz 1 StPO den automatisierten biometrischen Abgleich und zwar auch zur Erforschung eines Sachverhalts. Das haben Sie gerade in der ersten Fragerunde schon gestreift. Ich würde mich freuen, wenn Sie noch ein wenig mehr dazu sagen können,

warum Sie darin solch eine Gefahr sehen und warum das aus Ihrer Sicht einen Systemwechsel darstellt. Danke schön.

Amt. Vors. **Josef Oster** (CDU/CSU): Herr Kempgens bitte.

SV **Kai Kempgens** (DAV): Das Grundproblem, was man hat, ist, dass die Strafprozessordnung nur mittelbar verschiedene Straftatkataloge vorsieht, nach denen bestimmte Eingriffe, abgestuft nach Intensität, legitimiert sind. Eigentlich müsste man die ganze StPO ändern und einen Katalog von drei, vier oder fünf Kategorien machen: Mittelschwere, besonders schwere Straftaten, überragend schwere Straftaten, sowas in der Art. Das haben wir alles derzeit nicht und davon sind wir weit entfernt. Deshalb muss man auf diese vorhandenen Kataloge zurückgreifen. Jetzt wurde der 100a-Absatz-2-Katalog für Telekommunikationsüberwachungsmaßnahmen (TKÜ) geschaffen. Darin sind qualifizierte Delikte des Betruges, der Steuerhinterziehung, des Sportwettenbetruges und verschiedene andere Delikte enthalten. Das ist ein sehr weiter Katalog. Die Straftaten, die dort vorgesehen sind, spielen eher im Bereich der mittelschweren Kriminalität und sind nicht Straftaten, bei denen man sagt, da gehen wir mit der Ultima Ratio heran, da sind besonders eingriffsintensive Ermittlungsmaßnahmen legitimiert, das ist gerechtfertigt. Das sagt auch das Bundesverfassungsgericht in der jüngsten Entscheidung zur Quellen-TKÜ. Es wird auch vertreten, dass für die Quellen-TKÜ dieser Katalog beschränkt werden müsste. Deshalb muss man ausweichen. Dann müssen wir in den § 100b, der vielleicht auch bald überholt ist. Jedenfalls braucht man einen geringeren Katalog, als der im Moment im § 100b Absatz 2 vorgesehen ist. Der ist relativ weit gefasst.

Die andere Frage, was den biometrischen Bildabgleich anbelangt: Ich habe es eben schon gestreift. Der ursprüngliche Gesetzentwurf, der schon zwei Jahre oder drei Jahre zurückliegt, was den § 98d anbelangt, der sah noch die Fahndung nach Personen vor. Das war auch wesentlich prägnanter. Man hat den Fall Daniela Klette gesehen und hat sich gedacht, das muss doch auch behördlich möglich sein. Das ist keine automatische Argumentation. Was der Private darf, das darf die Behörde schon lange nicht – das ist kein Automatismus. Aber das war ein ganz anderer Zweck, nämlich Personen zu finden, nach denen man beispielsweise fahndet, wo man strafprozessuale Maßnahmen durchführen möchte. Jetzt haben wir zusätzlich die „Erforschung des Sachverhalts“. Das sind drei Wörter, die alles ändern. Das ermöglicht eigentlich alles. Was soll denn strafprozessual nicht Erforschung des Sachverhalts sein? Natürlich ist jede strafprozessuale Ermittlungsmaßnahme Erforschung des Sachverhalts. Das heißt, für jedweden Zweck sind solche Maßnahmen legitimiert – und das muss man sich einfach klar machen. Jetzt haben wir auf der anderen Seite die Maßnahme, nämlich den biometrischen Bildabgleich. Das muss man sich auch verinnerlichen. Es ist nicht nur so, dass Personen auf Bildern identifiziert werden, sondern, dass man suchen kann, mit wem haben bestimmte Personen, die so aussehen, die wir anhand des Bildes identifizieren, etwas gemeinsam und nicht etwa anhand des Namens, der Klarname, den viele Leute nicht angeben wollen, zu Recht. Wir haben einen Schutzreflex, dass wir unseren Namen nicht offenbaren wollen, wenn wir im Internet öffentlich auftreten. Bei Bildern ist es anders. Ich habe es eben schon gesagt. Häufig kann man gar nicht vermeiden, dass man fotografiert wird, bspw. auf einer Veranstaltung, auf einem Konzert, bei einer Demonstration oder bei irgendwelchen anderen Anlässen, beim Marathon beispielsweise. Eine automatische Auswertung nach biometrischen Kriterien ermöglicht es uns, genau zu schauen, mit wem diese Person Umgang hat. Wo geht sie hin? Wo hält sie sich wann, zu welchem Zeitpunkt auf? Was für Veranstaltungen besucht sie? Das ist ein Informationsumfang, der weitaus umfangreicher ist und der letztendlich ein komplettes Persönlichkeitsprofil in der Darstellung im öffentlichen Netz, in den sozialen Medien der Person ermöglicht und weitaus viel mehr Informationen zusammenträgt und wesentlich gläsernere Informationen über den Bürger und die Bürgerin offenbart, als es bisher der Fall war.

Amt. Vors. **Josef Oster** (CDU/CSU): Herzlichen Dank. Dann geht es weiter bei der Fraktion Die Linke. Frau Vogtschmidt, bitte.

Abg. **Donata Vogtschmidt** (Die Linke): Vielen Dank, Herr Vorsitzender. Ich hätte zwei Fragen an Frau Sombetzki. Ich würde gerne noch einmal bei der Frage der Anwendungspraxis der biometrischen Fahndung nachhaken. Im Gesetzentwurf ist ein abgestuftes System vorgesehen, also erst müssen Bundespolizei und BKA ihre eigenen Vergleichsdatenbanken aufbauen. Im besten Fall bei jedem Ein-

zelfall von Neuem. Aber wenn das nicht funktioniert, können Sie dann andere Behörden oder Unternehmen in der EU fragen, beziehungsweise damit beauftragen. Wenn das dann auch nicht funktioniert, dann könnten Sie Unternehmen in Drittstaaten beauftragen. Meine Frage ist, kommt das am Ende so? Bleiben Unternehmen in Drittstaaten die absolute Ausnahme? Oder würde es dann letztendlich doch regelmäßig bei „PimEyes“ oder „Clearview AI“ landen? Gerade mit Blick auf die größeren Unternehmen in der Branche würde mich auch interessieren, wie Sie da die Zuverlässigkeit der Ergebnisse einschätzen. Da steckt keine Intelligenz dahinter, sondern es geht eher um Wahrscheinlichkeiten. Das heißt, wie hoch sind die Fehlerquoten? Wie hoch sind die falsch positiven Treffer beim derzeitigen Stand der Technik, auch in Bezug auf die Analysedaten? Gibt es da weite Diskrepanzen bei unterschiedlichen Hautfarben oder äußeren Merkmalen? Wir wissen, dass KI in der Auswertung oft sehr rassistisch handelt. Ist dann die Gefahr sehr hoch, dass es größere Fehler gibt? Und gibt es irgendwelche Erkenntnisse auch zu falsch negativen Treffern? Also eine Person wird nicht entdeckt, obwohl sie dennoch da ist?

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank. Zwei Fragen an Frau Sombetzki. Bitte schön.

SVe **Pia Sombetzki** (AlgorithmWatch): Vielen Dank für die Frage. Zur Abstufung: Ich glaube, das kann man bei Frau Link in der Stellungnahme ganz gut nachvollziehen, denn sie schreibt ganz ausdrücklich, es ist nicht erforderlich in dem Sinne, dass bei Sicherheitsbehörden Daten gesammelt und gespeichert werden, weil man den Abgleich eben sozusagen an Dritte abgeben kann. Deswegen klingt das für mich überhaupt gar nicht nach Ausnahme, sondern eher nach der Regel. Sie verweisen auch auf den Aspekt in Bezug zur KI-Verordnung, dass das sowieso möglich ist zu tun, wenn es um Aspekte der nationalen Sicherheit geht. Nur frage ich mich dann, was man daraus schließen soll. Also kriegt jetzt einfach jeder biometrische Abgleich den „Nationale-Sicherheit-Stempel“ und dann kann man es auch in Drittländern machen? Ich frage mich schon ein bisschen, was die Konsequenz an der Stelle ist. Und deswegen wundere ich mich da auch, weil das ja überhaupt nicht zu den Debatten, die wir auch andernorts sehr lebhaft führen zu den digitalen Souveränitätsaspekten, sprich, die Daten sollten bei uns bleiben, wir wollen sie nicht an Drittstaaten oder kommerzielle Anbieter in Drittländern abgeben, an der Stelle passt. Da wundere ich mich schon sehr, dass das so explizit gesagt wird.

Was die Treffsicherheit angeht: Natürlich kann man sich vorstellen, da wird auch einmal jemand nicht entdeckt. Und wahrscheinlich ist das sogar so, dass Täter, die man sucht, nicht alle so nachlässig sind, wie eine Daniela Klette und nicht einfach ihre Bilder im Netz lassen, beziehungsweise doch die Option nutzen, wie das zum Beispiel bei „PimEyes“ leichter möglich ist als bei „Clearview AI“, doch einmal hinzugehen und seinen Datensatz dort zu löschen. Ich muss sagen, diese Daniela-Klette-Debatte holt mich persönlich nicht ganz ab, weil das leicht zu umgehen ist, wenn man es wirklich möchte. Andersherum ist aber bestehendes Problem, dass Leute fehlidentifiziert werden können, und das passiert gar nicht selten. Man muss sich nur die US-Berichterstattung, wo das alles schon längst gang und gäbe ist, mal anschauen: Fast jeden Monat gibt es einen Fall, wo eine Person, die zum Beispiel in den häufigsten Fällen schwarz ist, fehlidentifiziert wird, auch einmal in der Untersuchungshaft landet oder eben für ein paar Tage bis Wochen in Haft gerät. Einfach, weil sie vertauscht wurde, auch wenn es offensichtliche Widersprüche in den Verfahrensdaten gab: Teilweise Leute aus verschiedensten US-Staaten, die noch nie die Grenze übertreten hatten, auf einmal vermeintlich im Nachbarstaat gefunden wurden. Teilweise muss man schauen, dass es mit den dortigen polizeilichen Verfahrenspraxen zu tun hat und nicht nur mit dem System an sich. Und man muss auch anerkennen: Die Fehlerrate wird nie bei null sein, und dieses Risiko, Menschen zu verwechseln und die möglicherweise vielleicht eben nicht unbedingt sofort in Untersuchungshaft zu nehmen, aber zumindest einmal irgendwelche Folgemaßnahmen da anzusetzen, die zum Beispiel im Geheimen sind – von denen würden wir nicht einmal was hören. In den Medien wären das Fälle, die würden gar nicht bekannt werden. Und ob man jetzt dieses Risiko wirklich eingehen möchte, das möchte ich doch sehr in Frage stellen. Auch, weil das Risiko so ungleich verteilt ist, also manche Leute davon deutlich schwerer betroffen wären als andere. In einem Staat, in dem wir den Anspruch haben, Gleichbehandlungen in der Strafverfolgung zu leben und eben nicht einfach in Kauf nehmen, dass das bei den paar schwarzen Personen mit der

Identifizierung wieder einmal nicht funktioniert hat – das darf nicht unser Anspruch sein, das ist ganz klar. Gerade auch in Bezug auf den Aspekt, dass solche Systeme mit verschiedenen Wahrscheinlichkeiten arbeiten, ist das auch eben technologieinhärent. Es ist nicht zu vermeiden, dass das mal passiert, trotz aller Datenmengen, die man ansammelt und die man jetzt für die Verbesserung solcher Systeme auch anregen kann.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank für die Beantwortung dieser Fragen und für die zweite Runde, die wir jetzt hinter uns gebracht haben. Wir liegen gut in der Zeit. Ich schaue in die Reihen, ob wir eine dritte Runde haben möchten. Das scheint der Fall zu sein. Dann machen wir das. Wir beginnen wie üblich bei der Unionsfraktion und das Wort erhält Herr Kollege Wiegelmann.

Abg. **Johannes Wiegelmann** (CDU/CSU): Danke, Herr Vorsitzender. Ich will in der mutmaßlich letzten Fragerunde das Augenmerk nochmal auf den Komplex Sicherungsanordnung lenken und jeweils eine Frage an Sie, Herr Professor Möstl und Sie, Frau Link richten. Ich beginne bei Ihnen, Herr Professor Möstl, und zwar legen Sie in Ihrer Stellungnahme dar, dass eine abgesenkte Eingriffsschwelle bei der Sicherungsanordnung nach dem Entwurf des BKA-Gesetzes grundrechtskonform sei. Das Eingriffsgewicht sei durch die geringe Streubreite der anlassbezogenen Maßnahme und vor allem dadurch deutlich gemindert, dass der Staat noch keine Kenntnis von bestimmten Daten nähme. Könnten Sie diese Abwägung erläutern und das insbesondere unter dem Gesichtspunkt der Effektivität bei einem anderen Schwellenansatz? Und auch hier die Praktika und tatsächliche Betrachtung. Frau Link, an Sie die Frage: Können Sie uns noch einmal den Mehrwert der Sicherungsanordnung für die polizeiliche Arbeit in der Praxis darstellen? Danke schön.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank, Herr Wiegelmann. Wir beginnen bei Herrn Professor Möstl.

SV **Prof. Dr. Markus Möstl** (Universität Bayreuth): Es geht um eine Maßnahme der Spurensicherung, der rein vorsorglichen Spurensicherung. Es geht nicht um eine Maßnahme der staatlichen Kenntniserlangung. Deswegen wäre es grundlegend verkehrt, diese Maßnahme an den Eingriffsschwellen zu messen, die später für den Datenerhebungseingriff erforderlich sind. Wir sind weit im Vorfeld, es geht um einen Bereich, in dem zunächst nur Spuren erhalten bleiben sollen. Wenn man hier die Schwelle zu hoch ansetzt, dann verliert das Instrument seine Effektivität. Wir reden über ein Instrument, das in den Bereichen, wo die Vorratsdatenspeicherung nicht geht, eine gewisse Alternative bildet. Man muss bedenken, selbst eine Vorratsdatenspeicherung hätte das Bundesverfassungsgericht ja prinzipiell erlaubt. Das ist eine Maßnahme, die eine größere Streubreite hat, andererseits an keinerlei Verdachtsschwelle gebunden ist. Die ist wieder etwas anders zu beurteilen. Aber es muss sich eine sinnvolle Abstufung ergeben und bei dieser sinnvollen Abstufung ist die Eingriffsschwelle hier auf keinen Fall zu hoch anzusetzen, damit die Maßnahme hinreichend effektiv bleibt.

Amt. Vors. **Josef Oster** (CDU/CSU): Herzlichen Dank und Frau Link, bitte.

SVe **Martina Link** (BKA): In der polizeilichen Praxis wird die Sicherungsanordnung für das BKA am häufigsten in den Fällen eine Rolle spielen, in denen wir als Zentralstelle agieren. Das heißt, in denen wir noch keine Kenntnis haben, wer die zuständige Dienststelle ist, die dann beim Richter tatsächlich die Erhebung dieser Daten beantragen kann. Wir kriegen häufig Hinweise aus dem Ausland über bestimmte Sachverhalte, beispielsweise von Nachrichtendiensten, Hinweise beispielsweise auf Anschlagsplanungen in Deutschland. Dann ist es häufig so, dass es den Hinweis gab, dass vor einigen Tagen diese Täter schon in bestimmter Umgebung eine Ausspähung gemacht haben sollen. Jetzt muss man wissen, dass die Speicherung dieser Daten bei den Anbietern nach spätestens sieben bis acht Tagen überschrieben wird. Das heißt, wenn wir mit einigen Tagen Verzug eine solche Information kriegen und noch nicht wissen, wer die örtlich zuständige Dienststelle ist, die die konkrete Sicherung beim Richter beantragen könnte, haben wir als einzige Möglichkeit, eine solche Sicherungsanordnung zu beantragen, damit die Daten nicht verloren gehen. Das heißt nicht, dass wir tatsächlich Zugriff auf die Daten bekommen, sondern es geht ausschließlich darum, dass diese Daten nicht verloren gehen, um sie für spätere Ermittlungen verfügbar zu halten.

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank, Frau Link. Dann fahren wir fort bei der AfD-Fraktion, Herr Janich.

Abg. **Steffen Janich** (AfD): Vielen Dank. Meine erste Frage geht an Herrn Dr. Schmidtke und meine zweite an Herrn Kempgens vom Anwaltsverein. Die erste Frage, Herr Dr. Schmidtke: Welche Unterlagen braucht ein Gericht, um Rechtmäßigkeit und Aussagekraft einer automatisierten Analyse eigenständig zu beurteilen? Welche Folgen hat es, wenn ein Anbieter die Funktionsweise seines Systems nicht ausreichend offenlegt?

Und an Herrn Kempgens: Welche zusätzlichen Voraussetzungen sind aus Ihrer Sicht erforderlich, bevor Daten von Zeugen, Angehörigen und sonstigen unbeteiligten Personen analysiert werden dürfen? Wie lässt sich ein bloßer Kontakt von einem rechtlich erheblichen Zusammenhang unterscheiden? Vielen Dank.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke schön. Dann beginnt bitte Herr Dr. Schmidtke.

SV **Dr. Andreas Schmidtke** (OLG Düsseldorf): Vielen Dank für diese Frage. Ein Strafgericht schöpft für sein Urteil aus dem Inbegriff der Hauptverhandlung. In dieser Hauptverhandlung sind alle relevanten Beweismittel einzubringen. Im Rahmen einer Gesamtschau findet auf dieser Grundlage die richterliche Überzeugungsbildung statt. Naturgemäß gibt es, weil das Instrument neu ist, zur Datenanalyse keine Vergleichs- oder Erfahrungswerte, auf die ich hier zurückgreifen kann. Das Thema Gesamtschau meint aber, dass das Gericht aus allen Fakten zu schöpfen hat. Und selbstverständlich würde es nicht reichen, wenn das Ergebnis einer Datenanalyse als solche präsentiert wird. Vielmehr ist es Aufgabe des Gerichts, wie auch bei Sachverständigenanhörungen oder anderen Beweismitteln, sich die eigene Überzeugung von der Richtigkeit bzw. der Aussagekraft von Beweismitteln zu verschaffen. Man könnte sich das so vorstellen, dass das Ergebnis der Datenanalyse etwa als Urkunde präsentiert wird, die dann Eingang in das Verfahren bekommt. Das Verlesen einer solchen Urkunde, ihre strafprozessuale Zulässigkeit einmal unterstellt, führt hier nicht zu viel, sondern es ist die Gesamtschau, die dann entscheidend trägt. Insoweit hat die Frage, welche Unterlagen es braucht, um für das Gericht den Aussagegehalt dieser Datenanalyse zu validieren, eine nach erster Bewertung äußerst nachrangige Bedeutung. Denn maßgeblich ist der Mensch, der entscheidet und nicht die KI, die irgendein Ergebnis aufwirft.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke schön. Und Herr Kempgens.

SV **Kai Kempgens** (DAV): Ich verstehe Ihre Frage in Richtung der geplanten Änderung der Strafprozessordnung. Da muss man vielleicht noch einmal hervorheben: Wir reden über eine Datenanalyse zum Spurenansatz. Wir reden nicht über Ergebnisse, die als Beweise an sich eingeführt werden. Das macht den weiteren strafprozessualen Umgang damit sehr schwierig, denn nach der bisherigen Rechtsansicht in der Rechtsprechung des Bundesgerichtshofs, haben Fehler beim Spurenansatz erstmal keine Auswirkung auf das Strafverfahren an sich und auf die Beweiserhebung. Beispiel: Wenn auf illegale Weise eine Beweis-E-Mail gefunden wurde, wird natürlich die E-Mail in das Verfahren eingeführt und nicht etwa die Suchrecherche. Das ist erst einmal Theorie, das ist aber in der Praxis wesentlich diffiziler, als man sich das vorstellt und betrifft beispielsweise auch Ihre Frage zu der Unterscheidung zwischen losem Kontakt zwischen Zeugen oder zu einem Zeugen und der Erkennbarkeit der rechtlichen Relevanz. Die Antwort ist klar: Das kann man im Rahmen der Ermittlungen vorerst noch gar nicht beurteilen. Ein bloßes Kennverhältnis bedeutet nicht, dass jemand im kommunikativen Austausch mit demjenigen stand. Das verdeutlicht wieder umso mehr, dass solche Informationen erst einmal in einem Strafverfahren einer Bewertung unterliegen müssen, aber dass man gar nicht weiß, welche Rolle es spielen wird. Dass aber trotzdem die Analyse solcher Kennverhältnisse erst einmal relevant ist – und man möchte sich natürlich die Frage stellen, wie weit darf so etwas analysiert werden? Wie weit darf so etwas ausgewertet werden? Wie weit darf das zum Spurenansatz für weitere Ermittlungen verwandt werden oder eben nicht? Aber nach den derzeitigen Vorschriften spielt das im Strafverfahren an sich hinterher keine Rolle mehr.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke schön. Es geht weiter bei der SPD-Fraktion. Herr Kollege Schätzl.

Abg. **Johannes Schätzl** (SPD): Herzlichen Dank, Herr Vorsitzender. Herr Poitz, die erste Frage geht in Richtung Webcrawling, das wird jetzt bereits eingesetzt bei der Polizeiarbeit. Die Frage ist, wie wird es jetzt bereits eingesetzt und wie praxisnah ist das Ganze am Ende?

Und die andere Frage, Herr Professor Löffelmann, auch mir geht es um den Bereich der Übermittlung von personenbezogenen Daten im BKA-Gesetz. Die Übermittlung kann auch an Drittstaaten erfolgen zum Testen und Trainieren von IT-Systemen, auch von selbstlernenden Systemen. Wie bewerten Sie diese Vorschrift? Und zweite Teilfrage: Wer entscheidet am Ende, ob die Anonymisierung oder Pseudonymisierung von Daten unverhältnismäßig ist oder ob sie erfolgen muss?

Amt. Vors. **Josef Oster** (CDU/CSU): Vielen Dank für die Fragen. Die erste ging an Herrn Poitz. Bitte, Sie haben die Möglichkeit zu antworten.

SV **Alexander Poitz** (GdP): Vielen Dank für die Frage. Ich glaube, im digitalen Zeitalter kommen wir an solchen Tools in der momentanen Kriminalitätsbekämpfung nicht mehr vorbei. Aus unserer Bewertung ist das ein hilfreiches Tool. Wir haben den gesetzlichen Auftrag der Datensparsamkeit und das ist auch das Ziel. Deswegen ist eher das Fokus-Crawling der Schwerpunkt, was eine zielgerichtete Detektion und Selektion und Indexierung von gewissen Informationen in der polizeilichen Arbeit betrifft. Wir können durch ein gezieltes Scannen nach themenspezifischen Daten eine hohe Ressourceneffizienz beim Ermittlungsansatz einbringen. Und zu der Frage der polizeilichen Arbeit ist es momentan so, dass wir dieses Tool im Bereich der OSINT-Recherchen, also Open Source oder SOCMINT, also Social Media Recherchen einsetzen, sowohl beim BKA als auch bei den Landeskriminalämtern. Da geht es insbesondere um das Aufspüren von Betrugsshops, Fakeshops, wo dann Sperrungen hervorgerufen werden, Hasskriminalität, also Suche nach gewissen Schlüsselwörtern, dann die Bekämpfung von Kindesmissbrauch, CSRM, wo nach digitalen Signaturen oder Bildstrukturen gesucht werden kann und ein gewisses Darknet-Monitoring, um Schlüsselwörter zu detektieren, zu selektieren und zu indexieren. Allerdings muss man sagen, dass unsere Ermittlungsdienststellen mit technischen und rechtlichen Hürden konfrontiert sind, quasi im 21. Jahrhundert. Wir haben enorme Datenmengen, die wir zu scannen und zu selektieren haben. Es darf kein ungezieltes und anlassloses Crawlen des virtuellen Raums geben. Für uns als GdP ist es wichtig, dass am Ende der Kette die Entscheidungen, die hoheitlichen Maßnahmen von den Menschen getroffen werden. Deswegen ist eine kontinuierliche Weiterentwicklung des Fokus-Crawling für uns wichtig und für Ermittlungsbehörden unverzichtbar, um im digitalen Raum überhaupt noch handlungsfähig zu sein, an gewisse Informationen oder, wie ich es vorhin sagte, digitale Spuren heranzukommen. Der tatsächliche Erfolg hängt stark davon ab, wie gut die Algorithmen und die Bewegung krimineller Akteure angepasst werden, wie skalierbar wir auch als Ermittlungsbehörden sind. Danke schön.

Amt. Vors. **Josef Oster** (CDU/CSU): Danke. Die zweite Frage ging an Herrn Professor Löffelmann.

SV **Prof. Dr. Markus Löffelmann** (HS Bund): Vielen Dank für Ihre Fragen, Herr Abgeordneter. Die Problematik der Datenübermittlung an Drittstaaten wurde schon mehrfach thematisiert. Ich sehe das kritisch. Vorgesehen ist es einerseits, Sie haben es angesprochen, zum Trainieren von Systemen, andererseits kann aber auch der biometrische Abgleich in Drittstaaten erfolgen. Da ist es ein bisschen enger gefasst, unter den Vorbehalt der nationalen Sicherheit gestellt, wobei das gezielt diese Maßnahme aus dem Anwendungsbereich der KI-Verordnung ausnimmt. Da muss man sehen, dass der Vorbehalt der nationalen Sicherheit ein recht unscharfer Rechtsbegriff ist, der auch vom EuGH in dem Sinne ausgelegt wird, dass es um fundamentale Bestandsinteressen eines Staates geht. Aber das bringt eine gewisse Rechtsunsicherheit herein, wann so eine Übermittlung an Drittstaaten erfolgen darf. Ich möchte insoweit nur auf die Stellungnahme der Gewerkschaft der Polizei verweisen, wo es heißt, der Begriff dürfe dann nicht unverhältnismäßig eng ausgelegt werden, um solche Übermittlungen zu verunmöglichen. Die Risiken für den Datenschutz, die bei einer Übermittlung in Drittstaaten entstehen, die sind mit Händen zu greifen. Da muss man nur an den Cloud Act in den USA denken, der der Regierung den Zugriff auf sämtliche von privaten Unternehmen gespeicherten Daten ermöglicht. Und verfassungsrechtliche Vorgaben zu dieser Art von Auftragsdatenverarbeitung sind mir noch nicht bekannt. Aber was es gibt, sind Anforderungen, wenn Sicherheitsbehörden Daten an ausländische Stellen übermitteln, und zwar im nachrichtendienstlichen Bereich. Da verlangt dann das Bundesverfassungsgericht, dass man sich vergewissern muss, dass datenschutzrechtliche und menschenrechtliche Mindeststandards erfüllt werden. Das ist eine Stellschraube, die könnte man hier noch einbauen. Und zu Ihrer letzten Frage, wer entscheidet eigentlich, ob ein solcher Fall vor

liegt oder ob eine pseudonymisierte Anwendung ausreichend ist. Nach meiner Lesart entscheidet das allein das BKA.

Amt. Vors. **Josef Oster** (CDU/CSU): Jawohl, und es geht weiter bei BÜNDNIS 90/DIE GRÜNEN, Frau Dr. Gumnior.

Abg. **Dr. Lena Gumnior** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank. Ich starte mit meiner ersten Frage an Frau Sombetzki, noch einmal eine etwas allgemeinere Frage. Sie haben zum Ausdruck gebracht, dass Sie die Befugnisse grundsätzlich kritisieren, haben auch eine entsprechende Petition initiiert. Vielleicht können Sie aus Ihrer Sicht und Ihrer Tätigkeit noch einmal sagen, warum Sie eine so allgemeine Kritik daran äußern und warum es nicht nur um ein „bisschen mehr Überwachung“ geht, sondern dass die hier geplanten Maßnahmen eine neue Qualität und Eingriffstiefe haben.

Meine zweite Frage geht an Herrn Kempgens und jetzt ein bisschen detaillierter noch einmal zu der Frage: Welche Software wird eigentlich eingesetzt? Gibt es nach Ihrer Einschätzung eine KI-Software, die den Ermittlungsbehörden für die Maßnahmen nach § 98d StPO, die dort geplant sind, zur Verfügung steht und die unter verfassungsrechtlichen und unionsrechtlichen Vorgaben genutzt werden kann? Und daran anschließend, was für Risiken würde denn vor allem verfassungsrechtlich der Einsatz von „Palantir“ oder „PimEyes“ bergen? Danke schön.

Amt. Vors. **Josef Oster** (CDU/CSU): Jawohl. Und die erste Frage ging an Frau Sombetzki.

SVe **Pia Sombetzki** (Algorithm Watch): Danke für die Nachfrage. Ich glaube, Herr Kempgens hat es vorhin schon gut ausgeführt, dass es noch um den Charakter der automatisierten Auswertung geht, der das alles sehr verändert. Herr Poitz hat gerade erklärt, wie das so läuft mit den Crawlern und dass man das Fokus-Crawling schon benutzt. Das unterscheidet sich aber massiv in seiner Wirkung, die ein biometrischer Abgleich zum Beispiel auf alle Menschen hat, die bei Straftaten komplett unbeteiligt sind, beeinflusst die aber komplett mit. Alle werden einbezogen in eine Art von Datenbank, die so eingesetzt werden kann, dass sie auch sehr missbrauchsanfällig ist. Es ist einerseits das Vorhalten all dieser Daten, das ich als sehr schwierig einschätze und mit dem ich nicht d’accord gehe, dass das hier irgendwie verfassungsrechtlich zu tragen wäre – auch aus den angeführten datenschutzrechtlichen Aspekten. Und natürlich wünschen wir uns überhaupt nicht, dass man den Einsatz solcher Datenbanken jetzt auch noch staatlich legitimiert, dadurch, dass man sie nutzt. Ich höre das so raus. „Man darf hier auch den Kontext nicht zu eng fassen, in welchem man das dann noch machen darf“, zum Beispiel. Ich sehe das eher so, man darf ihn nicht zu weit fassen, nur, weil es irgendwelche Mittel gibt, die in der Welt sind, um vielleicht auch präventiv Straftaten vorweg verhindern zu wollen. Das ist erst einmal gar nicht gegeben, dass es überhaupt so funktioniert, wie erwünscht. Es ist eben auch nicht der Zweck, der die Mittel heiligt. Da würde ich schon noch einmal zur Vorsicht aufrufen, da nicht zu sehr von der eigentlichen Linie, die wir in anderen Debatten hören, also zum Beispiel, wenn es um „Palantir“ geht, zu sehr abzuweichen, dass wir die Souveränität hier komplett aufgeben wollen mit den sensibelsten Daten aller Bürgerinnen und Bürger!

Amt. Vors. **Josef Oster** (CDU/CSU): Danke schön. Die weitere Frage ging an Herrn Kempgens.

SV **Kai Kempgens** (DAV): Was die Frage der Software anbelangt, ist dies eine Frage der praktischen Umsetzung. Es ist völlig klar: So etwas lässt sich nicht in Echtzeit und ad hoc umsetzen. Das heißt, wir können ein Bild nicht in Echtzeit komplett im Internet mit anderen Bildern vergleichen lassen und für diesen Anlass alle im Internet vorhandenen Bilder herunterladen und vergleichen. Das geht von der Bandbreite her gar nicht und von der Rechenkapazität auch nicht. Das heißt, man muss eine Datenbank anlegen. Man muss eine Datenbank von Bildern anlegen, mit denen man dann das Beispielbild und das Referenzbild vergleicht und Übereinstimmungen feststellt. Genau da liegt das Problem. Die KI-Verordnung setzt einen Limiter davor, soweit es jedenfalls eine KI-gestützte Suche nach diesen Bildern anbelangt. Man kann die KI-Verordnung sogar noch weitergehend verstehen, dass es sowieso schwierig ist. Das heißt, allein da gibt es rechtliche Probleme. Aber in der Praxis würde das bedeuten, wenn es irgendwie geht, dass man eine behördliche Bildvergleichsdatenbank aufbauen muss. Der Vergleich mit „PimEyes“ oder „Clearview AI“ hinkt so ein bisschen, denn zum einen sind das Produkte, die nicht in Europa gehostet sind, das heißt, die Nutzung, abgesehen von der Spezialermächtigung, ist nicht möglich; aber auch die Vorgehensweise, die solche Anbieter wählen,

lässt sich hier behördlich nicht abbilden. Denn es werden nicht-reglementiert Bilder zusammengecrawlt, zusammengesucht und es wird unter Verstoß gegen alle möglichen Urheberrechtsvorschriften und alles Mögliche gearbeitet. Entsprechende Modi und Algorithmen können für ein behördliches Recherchesystem nicht verwandt werden, sodass man sich grundsätzlich fragt: Wie soll das überhaupt umgesetzt werden? Um das noch einmal zu sagen: KI-verordnungskonform und in der Praxis auch datenschutzkonform – da stehen so viele Fragezeichen dran, dass man sich fragt: Wie soll das denn eigentlich gehen?

Amt. Vors. **Josef Oster** (CDU/CSU): Danke. Den Abschluss in dieser Anhörungsrunde macht Frau Vogtschmidt für Die Linke.

Abg. **Donata Vogtschmidt** (Die Linke): Vielen Dank. Anschließend an meine Kollegin Frau Dr. Gumnior hatte ich noch einmal eine Frage, und zwar an Frau Sombetzki. Ebenfalls mit der Befugnis zum automatisierten biometrischen Gesichtsabgleich soll das Asylgesetz ausgestaltet werden und das BAMF würde also eine Befugnis wie das BKA oder auch die Bundespolizei erhalten. Mich würde interessieren: Wie blicken Sie auf diese Regelung, insbesondere mit Blick auf die tatbestandlichen Voraussetzungen und welche zusätzlichen Risiken würden Ihrer Meinung nach hier für schutzbedürftige Menschen zusätzlich entstehen?

Amt. Vors. **Josef Oster** (CDU/CSU): Das war eine Frage an Frau Sombetzki.

SVe **Pia Sombetzki** (AlgorithmWatch): Also ganz konkret wird hier die Rechtsverordnung, die festgelegt wurde, für die BAMF-Befugnis abgeschafft. Es gab eine Vorkehrung, die Risiken hätte abschwächen sollen. Die wird jetzt an der Stelle weggelöscht. Generell wird in dem Gesetz darauf verwiesen, dass Algorithmen, die herausgebildet werden, zum Beispiel auch für die Trainingsbefugnis gelten, dass man aufpassen möchte, dass die nicht diskriminierend sind. Das geht ein bisschen ins Leere, da überhaupt nicht beschrieben ist, wie diese Zielsetzung hergestellt werden soll und wer daran beteiligt ist. Zum Beispiel die BfDI als Akteurin, die die Aufsicht hat. Bei der BAMF-Befugnis generell finde ich es bemerkenswert, dass in der Begründung zum Gesetz steht, dass das als minderschwere Maßnahme im Vergleich mit der Auswertung von Datenträgern angesehen wird. Bei der vielfach besprochenen Streubreite, also die vielfache Betroffenheit aller möglicher Personen, finde ich es eine gewagte These. Natürlich bin ich jetzt auch nicht dafür, dass massenhaft Datenträger ausgewertet werden, aber dass der biometrische Abgleich durch diese Ansicht zur Standardmaßnahme wird, wenn keine Identitätsdokumente vorliegen, davon würde ich auf jeden Fall absehen wollen. Ich bin dafür, dass das nicht erlaubt sein sollte. Das hat mit den zusätzlichen Risiken zu tun, dass Asylsuchende einer Personengruppe angehören, die wahrscheinlich in den Datensätzen, mit denen solche Algorithmen trainiert werden, eher nicht gut vertreten ist. People of Color sind wahrscheinlich eine große Gruppe der Asylsuchenden und bei denen das Risiko einzugehen, sie sozusagen noch mehr verwechseln zu können, sehe ich als in die völlig falsche Richtung deutend. Das sollte auf jeden Fall zurückgezogen werden. Auch die Erlaubnis für das BAMF an der Stelle.

Amt. Vors. **Josef Oster** (CDU/CSU): Herzlichen Dank. Ich würde angesichts der Uhrzeit 15.51 Uhr zum Ende dieser Anhörung kommen wollen, wenn sich dagegen kein Widerspruch regt. Das sehe ich nicht. Dann darf ich mich für diese interessante Anhörung herzlich bedanken. Vor allen Dingen bei den Damen und Herren Sachverständigen, die uns hier mit ihrer Expertise zur Verfügung standen, im Vorfeld schon schriftliche Stellungnahmen hereingegeben haben und heute hier anwesend waren. Wir wissen alle sehr zu schätzen, dass sie das auf sich genommen haben. Es ist nicht selbstverständlich, hier in dieser Form dem Deutschen Bundestag zur Verfügung zu stehen. Ihnen allen dafür ein herzliches Dankeschön. Auch den Kolleginnen und Kollegen ein herzliches Dankeschön für die Teilnahme. Ich wünsche einen guten Tag und uns allen eine gute Sitzungswoche. Die Sitzung ist damit geschlossen.

Schluss der Sitzung: 15.51 Uhr

Josef Oster, MdB
Amtierender Vorsitzender