Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)493 J

Universität Bremen

IGMR
Institut für Informations-,
Gesundheits- und Medizinrecht

Universität Bremen | Postfach 33 04 40, 28334 Bremen
IGMR | FB06

Deutscher Bundestag
Ausschuss für Inneres und Heimat
- Sekretariat -
Platz der Republik 1
11011 Berlin

Fachbereich 06
Rechtswissenschaft

Prof. Dr. jur. Dennis-Kenji Kipker

Universitätsallee GW 1
28359 Bremen

Tel. 0421 5905 5465
Fax 0421 218 66052
kipker@uni-bremen.de

www.igmr.uni-bremen.de
igmr@uni-bremen.de

Bremen 22. September 2024

Schriftliche Stellungnahme

Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung

(BT-Drucksache 20/12806)

I. Zusammenfassung und kritische Gesamtbewertung

Die im Entwurf vorgelegten Vorschriften für ein Gesetz zur Verbesserung der Terrorismusbekämpfung (BT-Drs. 20/12806) übertreffen alles, was wir bislang an Vorschriften im Bereich digitaler Überwachung gesehen haben, indem hier Vorfelderhebung, Massendatenauswertung, Datenbankzusammenführung und künstliche Intelligenz miteinander kombiniert werden – im Ergebnis der sicherheitsbehördliche Daten-Supergau. Mit dieser Vorschrift wird die Vorfelderfassung von Daten vom Ausnahmefall

zum unbegründeten Regelfall gemacht. Und bei dieser Vorfelderfassung sprechen wir nicht nur von normalen personenbezogenen Daten wie Namen oder Anschriften, sondern von sensiblen Daten, die im Zweifelsfall gerade einen Abgleich mit biometrischen Daten ermöglichen sollen. Gegen diesen Vorstoß wirkt die Vorratsdatenspeicherung, über die wir seit mittlerweile fast 20 Jahren streiten, wie ein Spaziergang, weil hier im Vergleich zur biometrischen Datenerhebung nur Verkehrsdaten aus der Telekommunikation erhoben werden sollen und wir nicht von einer KI-gestützten Datenverarbeitung sprechen. Und dieses hier in diesen aktuellen Entwürfen vorgeschlagene Instrument gewinnt immer mehr an Gefährlichkeit, je mehr Daten im Internet gespeichert sind, die Tiefe des Eingriffs in die informationellen Grundrechte wird im Laufe der technischen Entwicklung somit dynamisch vertieft. Aufgrund der Tatsache, dass sehr viele Bürger:innen, die im Berufs- und Wirtschaftsleben stehen, mittlerweile teils ohne ihr Zutun im Internet auffindbar sind, kommen wir mit dem Vorschlag der viel befürchteten Dystopie des gläsernen Bürgers viel näher als jemals zuvor.

Überdies stellt sich die Frage, inwieweit die Vorschrift auch faktisch die verfassungsrechtlich verankerte Trennung zwischen Nachrichtendiensten und Polizeien aufhebt, indem über den völlig unbestimmten Datenzugriff aus dem Internet Daten als Vorfeldbefugnis miteinander verknüpft werden, die zunächst in keinerlei Bezug zueinander stehen können und inhaltlich weit entfernt von einer konkreten Gefahrenabwehr oder gar strafrechtlichen Verfolgung sein können. Der Vorschlag widerspricht somit grundlegenden rechtlichen Anforderungen, die das Bundesverfassungsgericht 1983 im Volkszählungsurteil bestimmt hat und die auch durch die Europäische Grundrechtecharta festgesetzt werden, indem hier gerade bestimmt

wird, dass jede Datenerhebung einer Rechtsgrundlage bedarf – dies schließt eine massenhafte Datenerhebung im Vorfeld ohne konkrete Bezüge und Verdachtsgrundlagen und im Zweifelsfall sogar ihre zusätzliche Speicherung als weiterer Eingriff aus. Nicht umsonst wurden Unternehmen wie Clearview AI gerade aufgrund dieses Handelns in verschiedenen Europäischen Staaten massiv datenschutzrechtlich bebußt, weil ein solches Vorgehen nicht mit der DSGVO in Einklang zu bringen ist.

Nicht zuletzt sind die im Befugnisentwurf vorgeschlagenen Rechtsbegriffe völlig unbestimmt. Es wird nicht definiert, was „vorhandene Sachverhalte“ oder „Echtzeit-Lichtbilder“ und „Echtzeit-Videodaten“ sind. Es sind überdies keinerlei konkrete flankierende Schutzregelungen vorgesehen, die der Sensitivität der erhobenen Daten, ihrer Massivität oder der Vorfeldwirkung der Datenverarbeitung Rechnung tragen. Allein schon aufgrund dieser Tatsachen sind die Regelungen nicht nur verfassungsrechtlich bedenklich, sondern vermutlich sogar verfassungswidrig, sodass es auf entsprechende Verstöße gegen Vorgaben aus dem AI Act als Hilfsargumentation nicht einmal mehr ankommen dürfte, die in Teilen durch die weit gefassten Begrifflichkeiten algorithmenbasierter Datenverarbeitung teils sogar umgangen werden könnten.

Überdies sind die Kernbereichsregelungen zu eng gefasst, indem „allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung“ ausgeschlossen werden sollen. Vorgaben zur Cybersicherheit lässt der Entwurf völlig außen vor, ebenso wie die Benennung konkreter Speicher- und Löschfristen, die eine enge zahlenmäßige Grenze für die Datenverarbeitung vorgeben. Auch ist in dem Entwurf die Rede davon, dass „diskriminierende Algorithmen weder herausgebildet noch verwendet werden dür-

fen“. Anstelle jedoch verlässliche Grundsätze und Rahmenbedingungen dafür aufzuzeigen oder untergesetzliche Konkretisierungen anzustoßen, wird die luftleere Formulierung mitten im Raum stehen gelassen. Genauso wenig ergiebig ist die Vorschrift, dass die „Nachvollziehbarkeit des verwendeten Verfahrens soweit wie technisch möglich sicherzustellen ist“. Anstelle butterweicher Formulierungen, die wie ein Feigenblatt für KI-Transparenz wirken, sollten zunächst valide technische Grundlagen erarbeitet werden, bevor überhaupt ein sicherheitsbehördlicher KI-Einsatz an dieser Stelle in Erwägung gezogen wird – bei dem in der gegenwärtigen Lage nicht einmal sichergestellt ist, ob er überhaupt geeignet ist, erstrebte Ermittlungserfolge herbeizuführen. Und auch die Kurzfristigkeit des Erfolgs, den sich die Bundesregierung hier verspricht, ist zweifelhaft, denn wir sprechen bei den hier vorgeschlagenen Maßnahmen über einen mehrjährigen Realisierungszeitraum. Vor diesem Hintergrund wirkt es geradezu fahrlässig, in einem schnellen Vorstoß „over the top“ ohne Technologie- und Risikofolgenabschätzung KI-gestützte Überwachung und Datenauswertung als Allheilmittel darzustellen.

Leider wirkt der Vorstoß in seiner Gesamtheit unüberlegt und unausgereift – auch daran erkennbar, dass die Bundesdatenschutzbeauftragte bei der Formulierung des Vorschlags nicht einbezogen wurde. Im Rahmen einer verfassungsrechtlichen Prüfung wären hier somit die Erforderlichkeit und rechtsstaatliche Verhältnismäßigkeit des Regierungsentwurfs nicht gegeben, auch die Geeignetheit ist wie zuvor dargestellt zweifelhaft. Das ist nicht nur juristisch höchst bedauerlich, sondern bürdet die nachgelagerte Rechtmäßigkeitskontrolle dieser Vorschriften wieder einmal der Zivilgesellschaft und letztlich dem Bundesverfassungsgericht auf, nachdem zunächst Fakten geschaffen wurden. Damit ist der gesetzgeberische Vor-

stoß nicht nur materiellrechtlich zu kritisieren, sondern auch das bisherige Vorgehen im Gesetzgebungsprozess evident in Frage zu stellen, denn hier wurden solche verfassungsrechtlichen Prüfgrundsätze missachtet, die jeder Jurastudent bereits im ersten Semester lernt.

Mit Blick auf diese gravierenden Defizite sollten deshalb unbedingt Möglichkeiten zur Befristung und sachgerechten Evaluierung der Maßnahmen vorgesehen werden, sollte sich eine Verabschiedung der rechtsfehlerhaften Vorschriften politisch nicht mehr vermeiden lassen. Die Vorgaben zur Befristung und Evaluierung sollten sich gesetzesübergreifend auf sämtliche Vorschriften beziehen, die einen biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet erlauben. Hierzu wäre denkbar, ein paritätisch besetztes und unabhängiges Kontrollgremium zur Technologiefolgenabschätzung im öffentlichen Sicherheitsbereich zu bilden, das über die notwendige fachliche Expertise zur Bewertung der Wirksamkeit, Notwendigkeit, technischen Rahmenbedingungen und grundrechtlichen Auswirkungen der eingesetzten Maßnahmen verfügt und regelmäßig öffentlich Bericht erstattet. Die Arbeit eines solche Gremiums kann inhaltlich auch über die Vorgaben des vorliegenden Gesetzentwurfs hinausgehen.

II. Zu den gesetzlichen Regelungen im Einzelnen:

Im Folgenden werden die zentralen Anforderungen, Herausforderungen und bisherigen Umsetzungsdefizite für die vorgeschlagenen gesetzlichen Änderungen im Einzelnen kommentiert. Da die mit den vorgeschlagenen gesetzlichen Regelungen verbundenen verfassungsrechtlichen Probleme für den Einsatz von automatisierten biometrischen Erkennungsverfahren vorschriftsübergreifend sind, werden daher nur die Kernregelungen kom-

mentiert. Die dabei getätigten rechtlichen, technischen und organisatorischen Erwägungen sind grundsätzlich auf alle weiteren Tatbestände übertragbar, die einen biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet im Rahmen einer datenbankgestützten Vorfeldanalyse ermöglichen.

Zu § 10b BKAG-E: Nachträglicher biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet

Die Vorschrift regelt, dass das BKA zur Ergänzung vorhandener Sachverhalte biometrische Daten zu Gesichtern und Stimmen, auf die es zur Erfüllung seiner Aufgaben zugreifen darf, mit öffentlich zugänglichen personenbezogenen Daten aus dem Internet mittels einer automatisierten Anwendung zur Datenverarbeitung biometrisch abgleichen darf. Diese Vorschrift leidet in ihrer tatbestandlichen Weite und Unbestimmtheit an verschiedenen Mängeln:

- Bereits unklar ist, was mit der „Ergänzung vorhandener Sachverhalte“ gemeint ist. Hier fehlt ein klarer Bezugspunkt, auf welche der vielfältigen Befugnisse und Aufgaben der Behörde referenziert wird und ob es um Sachverhalte der Zentralstellenfunktion, der internationalen Zusammenarbeit, Strafverfolgung, Terrorismusabwehr oder weiterer Befugnisse geht.

- Es fehlt an einer klaren und einschränkenden Definition des „biometrischen Datums“, das in dieser konkreten Form nicht im BKAG definiert wird. Der Anknüpfungspunkt „biometrische Daten zu Gesichtern und Stimmen“ bedarf näherer Konkretisierung, da hieran

auch die Wahl technischer Auswertungsmittel anknüpft, woraus sich eine Grundrechtsrelevanz ableitet.

- Zu konkretisieren ist überdies, was unter Daten zu verstehen ist, auf die das BKA „zur Erfüllung seiner Aufgaben zugreifen darf". Wie bereits dargestellt ist der gegenwärtige rechtliche Befugniskatalog des BKAG weit gefasst, sodass hier eine Konkretisierung mit einem deutlichen Bezugspunkt erfolgen sollte, um die tatbestandliche Weite der Vorschrift einzuschränken.

- Unbestimmt ist der Begriff der „öffentlich zugänglichen personenbezogenen Daten aus dem Internet". In der Vergangenheit wurde vielfach juristisch darüber diskutiert, welche Befugnisse V-Leute im Internet und Social Media haben sollten und wann ein im Internet abrufbares Datum als „öffentlich zugänglich" anzusehen ist, sodass dieses im Rahmen der Befugnisklausel auswertbar wäre.

- Die Technologie der zu verwendenden Datenverarbeitung zur Durchführung des biometrischen Datenabgleichs wird weder bezeichnet noch näher konkretisiert. Das ist jedoch zwingend erforderlich, um die grundrechtliche Eingriffstiefe zu bestimmen. Wenn schon nicht bestimmbar ist, welche Art von Technologie geeignet sein soll, einen Datenabgleich durchzuführen, stellen sich überdies Fragen der verfassungsrechtlichen Geeignetheit einer Maßnahme, da nicht bestimmbar ist, inwieweit die heranzuziehende Technologie überhaupt in der Lage sein soll, den beabsichtigten Ermittlungserfolg herbeizuführen. Überdies bezieht sich die Ermächtigungsgrundlage ausschließlich auf den „Datenabgleich" selbst als

nachgelagerte Stufe der Datenverarbeitung, nicht jedoch auf die „Datenerhebung“ als zwingend notwendige zeitlich vorgelagerte Stufe. Dies ist rechtssystematisch irreführend, da die Befugnisklausel in Unterabschnitt 1 zur „Datenerhebung“ verortet werden soll, dabei aber nicht beschrieben wird, auf welche Art und Weise diese Datenerhebung stattfindet, die jedoch denklogisch zwingend ist. Bei Annahme einer unbestimmten Vorfeldanalyse vorhandener biometrischer Daten aus dem Internet stellen sich gravierende verfassungsrechtliche Probleme, da es keinen datenschutzrechtlichen Legitimationstatbestand für eine umfassende Datenanalyse nicht betroffener Bürger „auf Vorrat“ oder beliebig im Vorfeld geben kann. Die damit verbundenen Fragestellungen tangieren einerseits das Datenschutzgrundrecht aus der Europäischen Grundrechtecharta, andererseits die grundlegenden verfassungsrechtlichen Festlegungen, die das Bundesverfassungsgericht im Jahr 1983 im Volkszählungsentscheid getroffen hat. Diese Vorgaben bestimmen, dass es keine zweckungebundene und generelle Datenverarbeitung im Vorfeld einer konkreten Maßnahme auf Vorrat geben darf – das gilt für private und öffentliche Einrichtungen gleichermaßen. Das hier skizzierte Vorgehen legt demgegenüber jedoch nahe, dass genau ein solcher unbestimmter und genereller Vorfeldabgleich im Sinne einer Massendatenauswertung intendiert ist. Sollte dies technisch so sein, so würde diese Vorgabe den grundlegenden verfassungsrechtlichen Prinzipien zuwiderlaufen. Überdies stellt sich die Frage, inwieweit ein genereller automatisierter Vorfeldabgleich mit dem ebenfalls verfassungsrechtlich verankerten Trennungsprinzip von Polizeien und Nachrichtendiensten zu vereinbaren ist, da eine Vielzahl der im Internet vorhandenen und ab-

gleichsrelevanten Daten in das weit vorgelagerte Vorfeld einer konkret absehbaren Gefahr oder geplanten Straftat fallen dürfte und auf diese Weise direkte nachrichtendienstliche Vorfeldbefugnisse unmittelbar mit Befugnissen zur Verhütung und Verfolgung von Straftaten in einer Sicherheitsbehörde kombiniert werden. Im Ergebnis stellen sich damit dieselben Probleme, die sich für eine von Clearview AI betriebene „Gesichtsdatenbank" stellen, auch für den deutschen Staat, da beide gleichermaßen die europäischen Datenschutzgrundsätze zu beachten haben.

- Der derzeitige Entwurf bezieht außerdem nicht die aus dem neuen europäischen KI-Gesetz (AI Act) folgenden Vorgaben und Anforderungen angemessen ein. Im Gegenteil – aufgrund der Offenheit der Formulierung der gesetzlichen Vorgaben im Sinne einer interpretativen „Technologiereserve" wäre es sogar möglich, Schutzregelungen aus dem KI-Gesetz auszuhebeln. Art. 5 Abs. 1 lit. e) KI-VO bestimmt klar, dass das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsmaßnahmen erstellen oder erweitern, zu den verbotenen Praktiken im KI-Bereich gehört. Daran müssen sich auch Befugnisgrundlagen des BKA messen lassen.

- Unter diesem Gesichtspunkt sind die in § 10b Abs. 1 Nr. 1-3 BKAG-E skizzierten tatbestandlichen Einschränkungen kein ausreichendes Korrektiv zur Herstellung der Verfassungsmäßigkeit der Vorschrift. So oder so ergeben sich hier erhebliche Unterschiede

auch zu einer ansonsten üblichen Quellen-TKÜ oder gar Online-Durchsuchung, da für die hier beabsichtigte Maßnahme gezielt massenhaft biometrische und damit sensible Daten im Sinne des Datenschutzes ausgewertet werden sollen, deren Verarbeitung im Vergleich zu herkömmlichen personenbezogenen Daten besonders hohen Rechtfertigungs- und Verarbeitungsvoraussetzungen unterliegt. Insoweit stellt sich unter diesem vergleichenden Aspekt ohnehin die Frage, ob der Katalog von Straftaten nach § 100a Abs. 2 StPO geeigneter Anknüpfungspunkt ist, denn er bezieht sich nur und im Speziellen auf die Telekommunikationsüberwachung, sodass auch Straftaten wie Wohnungseinbruchdiebstahl, Hehlerei, Sportwettbetrug, Urkundenfälschung und Bestechung umfasst sind. Ob solche vor allem wirtschaftsbezogenen Straftaten eine massenhafte biometrische Datenauswertung rechtfertigen, scheint höchst zweifelhaft – zumal die Intention des Sicherheitspakets diese Straftaten politisch eigentlich gar nicht adressiert.

- Für das einschränkende Kriterium nach § 10b Abs. 1 S. 2 BKAG-E sollte eine rechtsklare Definition der Begriffe „Echtzeit-Lichtbild“ und „Echtzeit-Videodateien“ vorgenommen werden. Überdies ist fraglich, wie das Ziel der „Aufenthaltsbestimmung“ einer Person erreicht werden soll, wenn der Echtzeit-Abgleich mit Daten aus dem Internet nicht möglich sein soll. Denkbar wäre, statische Daten aus dem Internet mit Echtzeit-Daten zu kombinieren, die nicht aus dem Internet stammen, so beispielsweise aus polizeilich zulässiger Videoüberwachung an öffentlichen Orten. Hier sind die tatbestandlichen Möglichkeiten nach den Landespolizeigesetzen und dem Bundespolizeigesetz aber eingeschränkt. Damit stellt

sich auch die Frage der Werthaltigkeit einer solchen Befugnisgrundlage. Im Ergebnis dürfte aber allein durch diesen Ausschluss keine signifikante Verbesserung mit Blick auf die bereits gegebene hohe Eingriffsintensität gegeben sein, da bereits durch die Breite der behördlichen Datenauswertung ein massiver Grundrechtseingriff stattfindet und die Einschränkung demgegenüber kaum weiter ins Gewicht fallen dürfte.

- Die bereits festgestellte tatbestandliche Weite des biometrischen Datenabgleichs erfährt eine weitere verfassungskritische Ausweitung durch die persönlichen Bezugspunkte in § 10b Abs. 2 BKAG-E. Demnach darf die Maßnahme gegen Verurteilte, Beschuldigte, Verdächtige einer Straftat, Anlasspersonen, Zeugen und Opfer einer künftigen Straftat durchgeführt werden. Zweifelhaft ist, weshalb eine biometrische Datenauswertung zusätzlich bei Personen möglich sein soll, soweit sie bei einer künftigen Strafverfolgung lediglich als Zeugen in Betracht kommen. Selbst wenn man annähme, dass ein erhebliches staatliches Interesse an der Strafverfolgung besteht und das Auffinden von Zeugen hierfür unerlässlich ist, so relativiert sich ebenjenes Interesse in Abwägung der betroffenen Schutzgüter doch erheblich, soweit es um lediglich wirtschaftsbezogene Straftaten wie Wohnungseinbruchdiebstahl, Hehlerei, Sportwettbetrug, Urkundenfälschung und Bestechung geht, deren wahrgenommener und auch rechtlich sanktionierter Unrechtsgehalt gegenüber Straftaten gegen Leib und Leben oder gemeingefährlichen Straftaten abfällt. Generell sollte für Personengruppen, bei denen keine unmittelbare Betroffenheit für Straftaten besteht, angedacht werden, begrenzende Tatbestände zu verwenden, soweit

diese in eine automatisierte Datenanalyse einbezogen werden. Insbesondere sollte klargestellt werden, warum die Auswertung von Daten dieser Personen einen Mehrwert für ein konkretes Ermittlungsverfahren darstellt. Dies ist im Einzelfall zu begründen, soweit technisch möglich.

- Die ohnehin schon verfassungsrechtlich kritische Reichweite der automatisierten Datenauswertungsbefugnisse wird nochmals dadurch verschärft, dass mit einem Verweis auf § 12 Abs. 2 BKAG unmittelbarer Bezug zu den Ausnahmen vom datenschutzrechtlichen Zweckbindungsgrundsatz hergestellt wird. Hierdurch wird quasi eine tatbestandsunabhängige Generalbefugnis geschaffen, soweit vergleichbar schwerwiegende Straftaten verhütet, aufgedeckt oder verfolgt oder vergleichbar bedeutsame Rechtsgüter geschützt werden sollen.

- Vor dem Hintergrund der technischen Unbestimmtheit der Ermittlungsmaßnahmen wird die verfassungsrechtliche Wirkkraft flankierender Schutzmaßnahmen wie der Richtervorbehalt absolut relativiert, denn fraglich ist, auf welche Phase der Datenverarbeitung sich die durch § 10b Abs. 4 BKAG-E festgeschriebene Anordnungsfestlegung bezieht und wo hier für einen eventuell ohnehin schon bestehenden Grundrechtseingriff noch klare Grenzen gezogen werden können.

- Da bereits unklar ist, welches technische Eingriffsmittel für Maßnahmen nach § 10b Abs. 1 BKAG-E eingesetzt wird, geht auch die Kernbereichsschutzregelung in Abs. 6 ins Leere. Soweit kein tech-

nischer Bezugspunkt und damit auch zeitlicher Bezugspunkt bekannt ist, inwieweit die Maßnahme in den Bereich der Vorfeldermittlung fällt, kann auch nicht rechtssicher festgestellt werden, wann die Kernbereichsrelevanz tangiert ist, die die Unzulässigkeit einer Verwertung der erlangten Daten zur Folge hat.

- Die Löschklausel in § 10b Abs. 7 BKAG-E ist ebenfalls unzureichend, da zu unbestimmt. Unklar ist der Zeitpunkt, zu dem der Datenabgleich stattgefunden hat. Außerdem wird nicht angegeben, welche Daten im Einzelnen nach Abs. 1 „erhobene Daten“ sind, da Abs. 1 lediglich einen „Abgleich“ von Daten regelt. Insoweit geht die Löschvorgabe hier ins Leere.

- Zu empfehlen wäre überdies zusätzlich die Festlegung von konkret bestimmten Maximalspeicherfristen, damit technisch ausgeschlossen ist, dass über unbestimmte Ermächtigungsgrundlagen eine generelle biometrische „Bürgerdatenbank“ in den Beständen des BKA angelegt wird. Das Anlegen einer solchen Datenbank wäre ohnehin aufgrund der zuvor skizzierten Prinzipien des deutschen und europäischen Datenschutzrechts verfassungswidrig.

- Nicht zuletzt fehlt es dem bisherigen Entwurf an flankierenden Regelungen, die bei derart eingriffsintensiven Befugnissen das Prinzip „Grundrechtsschutz durch Verfahren“ angemessen wiedergeben. Lediglich § 10b Abs. 8 BKAG-E enthält eine ausdrückliche Regelung zu Protokollierung, das allein kann aber nicht ausreichend sein – so ist durch diese Vorgabe nicht einmal die Revisionssicherheit gewährleistet. Es fehlen neben konkreten Vorgaben zur (automatisierten) Datenlöschung auch Vorgaben zum Zu-

griffsmanagement, zur Cybersicherheit, zur Sicherstellung der Zweckbindung, zur Manipulationsfestigkeit der Daten, zur Vertrauenswürdigkeit und Überprüfbarkeit der eingesetzten Datenauswertungstechnologie sowie zu algorithmenbasierten Diskriminierungspotenzialen. Derlei Vorgaben könnten ergänzend untergesetzlich beispielsweise durch Verordnungsermächtigung des fachlich zuständigen Ressorts bestimmt werden, würden aber im Ergebnis nicht ausreichend sein, um die evidenten verfassungsrechtlichen Bedenken erfolgreich auszuräumen, soweit nicht rechtsklare weitere Veränderungen an den Befugnisgrundlagen vorgenommen werden.

Zu § 16a BKAG-E: Automatisierte Datenanalyse

Die Vorschrift bestimmt, dass das BKA im Informationssystem oder im polizeilichen Informationsverbund gespeicherte personenbezogene Daten mittels einer automatisierten Anwendung zur Datenverarbeitung zusammenführen und darüber hinaus zum Zwecke der Analyse weiterverarbeiten kann, sofern dies zur Abwehr einer im Einzelfall bestehenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, im Zusammenhang mit Straftaten nach § 5 Abs. 1 S. 2 BKAG erforderlich ist. Wie auch für die vorangehende Vorschrift bereits festgestellt wurde, leidet auch der neu vorgeschlagene § 16a BKAG-E an seiner tatbestandlichen Weite und Unbestimmtheit:

- Zuvorderst ist völlig unbestimmt, ob die Datenzusammenführung auf bestimmte Datentypen beschränkt wird. Die gegenwärtige Entwurfsfassung legt entgegen einer Beschränkung im Gegenteil nahe, dass das BKA in Zukunft sämtliche im Informationssystem oder im polizeilichen Informationsverbund gespeicherte personenbezogene Daten zusammenführen und zu Analysezwecken weiterverarbeiten darf. Das würde die Zusammenführung der Daten aus dem Informationsverbund sämtlicher deutscher Polizeibehörden bedeuten. Umfasst sind damit bei Weitem nicht nur Beschuldigte, sondern ebenso auch hier wieder Zeugen oder Opfer bis hin zu gänzlich unbeteiligten Personen. Dieser Aufbruch der datenschutzrechtlichen Zweckbindung stellt in der Breite allein schon einen massiven Grundrechtseingriff dar, da Daten von Personen erfasst werden, die in keinster Weise mit dem im Sicherheitspaket skizzierten Zielen und Anforderungen in einem Zusammenhang stehen. Überdies werden die Daten im polizeilichen Informationsverbund für einen mehrjährigen Zeitraum gespeichert und können ebenso je nach Art der zu ermittelnden Straftat hochsensible personenbezogene Daten betreffen. Mit einer derartigen Generalklausel würden wie hier vorgeschlagen dennoch sämtliche Arten personenbezogener Daten ungeachtet ihrer Sensibilität juristisch die gleiche Behandlung und damit gleiche Wertigkeit erfahren. In der gegenwärtigen Entwurfsfassung wird nicht sichergestellt, dass ausschließlich solche Daten verarbeitet werden, die zur Erfüllung der gesetzlichen Aufgaben zwingend erforderlich sind.

- Obgleich der Wortlaut der Vorschrift in Abs. 1 S. 1 zunächst eine eng umrissene Einzelfallmaßnahme suggeriert, wird dies bei einem

Blick in die Entwurfsbegründung widerlegt. Dort heißt es vielmehr, dass die Datenzusammenführung „aus technischen Gründen“ vom Einzelfall und weiteren Eingriffsschwellen unabhängig sein muss. Ob mit dieser Interpretation eine Auslegung contra legem erfolgen soll, ist absolut unklar – zumindest aber setzt sich die Entwurfsbegründung in unmittelbaren Widerspruch zum Wortlaut der Entwurfsfassung. Damit wird aber eines deutlich: In technischer Hinsicht scheint vorgesehen zu sein, eine Vorfeldzusammenführung vorgenannter Datenbestände in einer umfassenden neuen BKA-Datenbank herbeizuführen, ohne dass die Zweckbindung der ursprünglich erhobenen Daten, ihre teilweise Sensibilität, die unterschiedlichen Eingriffsschwellen oder Löschfristen beachtet werden. Ebenso nennt der Entwurf des BKAG hier keine valide Rechtsgrundlage für eine solche Datenzusammenführung, da sich die einzelfallbezogenen tatbestandlichen Voraussetzungen allein auf die nachgelagerte Phase der „Datenanalyse“ beziehen, wie es auch der Titel der neu vorgeschlagenen Bestimmung suggeriert. Damit drängt sich der Eindruck des Aufbaus einer umfassenden Analysedatenbank beim BKA „durch die Hintertür“ auf, die verfassungsrechtlich auch unter den schon zuvor genannten Gesichtspunkten nicht legitimierbar wäre – entsprechend auch dem Wortlaut der Datenweiterverarbeitung „darüber hinaus zum Zwecke der Analyse“. Perpetuiert wird der massive Grundrechtseingriff weiter dadurch, dass zunächst in § 16a Abs. 1 S. 1 BKAG-E zwar hinreichend eng gefasste Eingriffsschwellen bestimmt werden, über eine eingeschobene Befugnisausdehnung in S. 2 der Anwendungsbereich der Vorschriften wieder aber in verfassungsrechtlich unzulässiger Weise erweitert wird.

- Weiterhin problematisch ist auch hier wie schon für § 10b BKAG-E skizziert die Technologieoffenheit der gewählten Formulierung und die damit einhergehende Dynamisierung der Eingriffsintensität. Indem lediglich von einer „automatisierten Anwendung zur Datenverarbeitung“ die Rede ist, können nicht nur Technologien von Data Mining und Data Warehousing Einsatz finden, sondern auch KI-gestützte Auswertungsmethoden. An keiner Stelle werden im Entwurf die damit einhergehenden Risiken weiter konkretisiert oder flankierende Schutzregelungen geschaffen, die zur Herstellung der Verfassungsmäßigkeit jedoch dringend geboten sind.

- Warum in Abs. 3 basierend auf der Zentralstellentätigkeit des BKA ebenfalls eine Befugnis zur Datenbankzusammenführung legitimierbar sein soll, erschließt sich nicht. Es ist ein allgemeiner verwaltungsrechtlicher Grundsatz, dass zwischen bloßen Aufgabenzuweisungsvorschriften und Befugnisgrundlagen zu unterscheiden ist. In dieser Weite ist nicht ersichtlich, weshalb es dieses zusätzlichen Tatbestands bedarf und das Tätigwerden des BKA nicht schon über die Regelung in Abs. 1 ermöglicht werden kann, die wie dargestellt ebenso tatbestandlich weit gefasst ist. Einer unnötigen Auffangregelung bedarf es insoweit nicht.

- Abs. 5 regelt zusätzlich den Einsatz von selbstlernenden Systemen im Rahmen eines pauschalen Verweises auf § 22 Abs. 3 S. 2 und 3 BKAG-E. Hier sollte eine Klarstellung erfolgen, dass dabei eine Weitergabe der Daten aus § 16a BKAG-E an Dritte nicht vorgesehen ist, um eine unzulässige Erweiterung des Anwendungsbe-

reichs der Vorschrift durch Vermengung der Befugnisgrundlagen sachlich auszuschließen.

Zu § 22 BKAG-E: Weiterverarbeitung von Daten zu weiteren Zwecken

Der neue Abs. 3 soll u.a. die Übermittlung von Daten an Dritte regeln, soweit dies zur Entwicklung, Überprüfung, Änderung oder zum Trainieren von IT-Produkten erforderlich ist. Soweit KI eingesetzt wird, bestehen besondere Risiken mit Blick auf den Datenschutz und die Technologiefolgenabschätzung, die hier nicht gebührend Berücksichtigung finden:

- Generell hat sich in den vergangenen Jahren mit Blick auf die Cybersicherheit gezeigt, dass eine Datenübermittlung an Dritte und die Verwendung von externen Tools und Rechenleistung hochrisikobehaftet sein kann, denn zu oft wurde die digitale Lieferkette bereits durch unzureichende Datensicherheitsmaßnahmen Dritter kompromittiert. Allein deshalb ist die genannte Vorschrift bereits hochkritisch zu sehen.

- Darüber hinaus fehlen hier unbedingt notwendige verfahrensrechtliche Konkretisierungen, die beispielsweise auch untergesetzlich durch Rechtsverordnung festgelegt werden können. Diese können zum Beispiel die Auswahlkriterien für Drittverarbeiter betreffen, aber insbesondere auch, welche Maßnahmen zur IT-Sicherheit diese zu realisieren haben, welchen Standards der Informationssicherheit dies entspricht und wie dies nachzuweisen und von den zuständigen Behörden nachvollziehbar zu überprüfen ist.

- Außerdem ist der gegenwärtige Wortlaut der Entwurfsfassung zur Weitergabe von Daten viel zu weit gefasst. Mit der Regelung über „bei ihm vorhandene Daten“ können auch sensible personenbezogene Daten an Dritte übermittelt werden. Die tatbestandliche Erweiterung durch die Formulierung „insbesondere“ stellt die rechtliche Möglichkeit zur Weiterübermittlung von Daten in die Beliebigkeit des BKA. Geradezu völlig unverständlich wirkt die Regelung, wonach die „Anonymisierung oder Pseudonymisierung der Daten nicht oder nur mit unverhältnismäßigem Aufwand möglich“ sein soll. Diese Regelung ist zu streichen, denn das BKA ist als verantwortliche Stelle verpflichtet, den technischen Datenschutz einzuhalten und kann diesen nicht ohne Weiteres aufgrund „unverhältnismäßiger Aufwände“ faktisch beliebig derogieren – gerade dann, wenn die Daten in die Weiterverarbeitung in Hochrisiko-Technologien einfließen sollen.

- Grundsätzlich zu begrüßen sind die Schutzregelungen in § 22 Abs. 3 S. 2 und 3 BKAG-E. Diese gehen aber nicht weit genug. So wird nicht bestimmt, wie sichergestellt werden soll, dass Algorithmen keine diskriminierende Wirkung entfalten sollen und was geschehen soll, falls eine solche Wirkung dennoch festgestellt wird. Auch wird nicht ausgeführt, wie die „Nachvollziehbarkeit des verwendeten Verfahrens“ zu gewährleisten ist. Auch hier würde es sich empfehlen, umfängliche untergesetzliche Konkretisierungen innerhalb des jeweiligen Ressorts vorzunehmen. Die pauschale Formulierung, dass das BKA durch „organisatorische und technische Maßnahmen zu gewährleisten hat, dass die Daten gegen unbefugte Kenntnisnahme zu schützen sind“, schafft in ihrer Abstraktheit in-

soweit keinen Mehrwert für die Sicherheit und Vertraulichkeit der Daten.

Bremen, den 22. September 2024

Prof. Dr. jur. Dennis-Kenji Kipker