Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)450 G

Hochschule der Akademie der Polizei Hamburg, Carl-Cohn-Straße 39, 22297 Hamburg

An den
Ausschuss für Inneres und Heimat
im Deutschen Bundestag
Platz der Republik 1
11011 Berlin

Prof. Eike Richter
Professur für Öffentliches Recht, insbesondere Recht der Digitalisierung und IT-Sicherheitsrecht
Hochschule der Akademie der Polizei Hamburg
Carl-Cohn-Straße 39, 22297 Hamburg
Tel.: +49(0)40-4286-24400
eike.richter@poladium.de

Stellungnahme zum Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes (Drucksache 20/10859)

Sehr geehrter Herr stellvertretender Vorsitzender,
sehr geehrte Damen und Herren Abgeordnete,

ich danke für die Gelegenheit zur Stellungnahme zum genannten Gesetzentwurf.

Ich konzentriere mich in meiner schriftlichen Stellungnahme auf zwei Themenbereiche des vorgelegten Gesetzentwurfs. Zunächst wird auf die Institutionalisierung der Datenschutzkonferenz eingegangen (dazu A). Im Anschluss nehme ich zur Erwägung Stellung, eine Regelung zur biometrischen Gesichtserkennung einzufügen (dazu B).

Um in der vorliegenden Stellungnahme Vorschriften des vorliegenden Gesetzentwurfs von geltenden Vorschriften unterscheiden zu können, sind erstere mit einem „-E“ in der Gesetzesbezeichnung ergänzt (z.B. § 16a BDSG-E). Seitenzahlen ohne Quellenangaben beziehen sich auf den Gesetzentwurf der Bundesregierung (Drucksache 20/10859).

Für einen schnellen Überblick verweise ich auf die nachstehende Übersicht sowie auf die grau hinterlegten Zusammenfassungen. Im Rahmen der Anhörung gehe ich gerne auf einzelne Punkte und weitere Themen des Gesetzentwurfs ein.

Die Ergebnisse zu den beiden genannten Themen lassen sich vorab wie folgt **zusammenfassen**:

> *1. Eine Ergänzung von § 16a BDSG-E um eine Befugnis der **Datenschutzkonferenz** zur verbindlichen Beschlussfassung über Auslegungsmaximen und andere Angelegenheiten des Datenschutzes sowie zur Öffentlichkeitsarbeit und zur Einrichtung einer gemeinsamen Geschäftsstelle wahrt bei entsprechender gesetzlicher Ausgestaltung die europa- und verfassungsrechtlichen Grenzen.*
>
> *2. Das Europa- und Verfassungsrecht steht einem bundesgesetzlichen **Verbot der biometrischen Gesichtserkennung** durch staatliche und private Akteure nicht grundsätzlich entgegen, gebietet ein solches Verbot aber auch nicht. Zur Wahrung der europa- und verfassungsrechtlichen Grenzen kommt insbesondere die Aufnahme einer allgemeinen Vorschrift in das BDSG in Betracht, nach der die biometrische Gesichtserkennung im öffentlichen Raum oder zur Überwachung und die Verarbeitung diesbezüglicher Daten verboten sind.*

Auf S. 27 und 53 finden sich zu beiden Themen Vorschläge für entsprechende Regelungen bzw. Ergänzungen im vorliegenden BDSG-E.

Akademie der POLIZEI Hamburg Fachhochschule

Überblick

A. Institutionalisierung der Datenschutzkonferenz

Im Koalitionsvertrag 2021-2025 (S. 17) haben sich die regierungstragenden Parteien zur Aufgabe gemacht:

> *„Zur besseren Durchsetzung und Kohärenz des Datenschutzes verstärken wir die europäische Zusammenarbeit, institutionalisieren die Datenschutzkonferenz im Bundesdatenschutzgesetz (BDSG) und wollen ihr rechtlich, wo möglich, verbindliche Beschlüsse ermöglichen.“*

Der vorgelegte Gesetzentwurf sieht in § 16a BDSG-E folgende Regelung vor:

> *„§ 16a Datenschutzkonferenz*
>
> *Die Aufsichtsbehörden des Bundes und der Länder im Sinne des § 18 Absatz 1 Satz 1 bilden die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz). Die Datenschutzkonferenz gibt sich eine Geschäftsordnung.“*

Der vorgelegte Regelungsentwurf beschränkt sich auf eine schlichte Benennung der Datenschutzkonferenz (DSK) und die Vorgabe, sich eine Geschäftsordnung zu geben. Er sieht von einer weitergehenden Institutionalisierung, insbesondere einer Befugnis der DSK zur verbindlichen Beschlussfassung über Auslegungsmaximen und anderen Angelegenheiten des Datenschutzes ab, um auch auf diese Weise die Durchsetzbarkeit und Kohärenz des Datenschutzrechts zu fördern. Entsprechendes gilt für die Verankerung einer Kompetenz zur gemeinsamen Öffentlichkeitsarbeit. Es stellt sich somit die Frage, welche rechtliche Möglichkeiten und Grenzen für den Bundesgesetzgeber für eine im Vergleich zu § 16a BDSG-E weitergehende Institutionalisierung der DSK – insbesondere im BDSG – bestehen.

Um diese Frage zu klären, sollen zunächst die Grenzen festgestellt werden, die der Bundesgesetzgeber zu beachten hat, wenn er eine weitergehende Kooperation, insbesondere eine Kompetenz zur Fassung verbindlicher Beschlüsse regeln will (dazu I). Soweit sich danach für den Bundesgesetzgeber ein rechtlich zulässiger, aber mit § 16a BDSG-E noch nicht ausgeschöpfter Gestaltungsspielraum ergibt, stellt sich in einem zweiten Schritt die Frage nach einer zweckmäßigen und im Vergleich zu § 16a BDSG-E erweiterten Ausgestaltung der Kooperation (dazu II). In einem letzten Schritt wird erörtert, wie die

in Betracht kommende Kooperationsausgestaltung rechtlich ausgestaltet werden kann, insbesondere durch eine entsprechende Regelung im BDSG (dazu III).

Die nachfolgenden Ausführungen beruhen im Wesentlichen auf einem entsprechenden Rechtsgutachten im Auftrag einer Arbeitsgemeinschaft der Datenschutzkonferenz, an dem der Unterzeichnete mitgewirkt hat und auf das im Übrigen verwiesen wird.[1]

I. Rechtliche Grenzen für den Bundesgesetzgeber zur Regelung einer Kooperation

Eine im Vergleich zum § 16a BDSG-E weitergehende Regelung zur Kooperation der DSK, die insbesondere gemeinsame und für die Mitglieder DSK verbindliche Entscheidungen über die Auslegung des Datenschutzrechts und über Stellungnahmen zu Datenschutzangelegenheiten, eine gemeinsame Öffentlichkeitsarbeit und eine gemeinsame Geschäftsstelle vorsieht, wahrt die europarechtlichen (dazu 1) und die grundgesetzlichen Grenzen (dazu 2).

1. Wahrung der europarechtlichen Grenzen

Das europäische Primär- und Sekundärrecht zieht einer Stärkung der Kooperation der Datenschutzaufsichtsbehörden oder einer darüberhinausgehenden Institutionalisierung der DSK **keine grundsätzlichen**, sondern allenfalls **spezifische Grenzen**.

a. Grenzen der Unabhängigkeit der Datenaufsichtsbehörden

Dies gilt insbesondere für die nach Art. 51 Abs. 1, 52 DSGVO zu garantierende **(völlige) Unabhängigkeit** der Aufsichtsbehörden.[2] Die Mitgliedstaaten sind grundsätzlich frei in ihrer Wahl, ihre Aufsichtsbehörden zu organisieren. Möglich ist auch – wie in Deutschland – eine föderale Organisation, sofern gewährleistet ist, dass eine bestimmte Stelle alle

1 Rechtliche Möglichkeiten zur Stärkung und Institutionalisierung der Kooperation der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK 2.0), Rechtsgutachten im Auftrag der AG DSK 2.0, vorgelegt von Eike Richter, Indra Spiecker gen. Döhmann unter Mitarbeit von Ref. iur. Mona Winau, Januar 2022, abrufbar unter www.bfdi.bund.de.

2 Zur Geltung nicht nur für den öffentlichen, sondern auch für den privaten Verarbeitungssektor vgl. EuGH, Urt. v. 9.3.2010, C-518/07, Kommission/Deutschland, ECLI:EU:C:2010:125, Rn. 30. Vgl. auch BVerfGE 65, 1 (46).

anderen Stellen im Europäischen Datenschutzausschuss (EDSA) vertritt und die Regeln des Kohärenzverfahrens aus Art. 63 DSGVO Beachtung finden (Art. 51 Abs. 3 DSGVO).[3] Dabei richtet sich die Unabhängigkeit der Aufsichtsbehörden nach dem Telos der Vorschriften auf die institutionelle Unabhängigkeit der Aufsichtsbehörden **von solchen Akteuren, die die Aufsichtsbehörden zu kontrollieren haben,** also etwa von der Regierung und der Verwaltung.[4] Eine solche Kontrollbeziehung besteht aber gerade nicht unter den Datenaufsichtsbehörden der Länder und des Bundes untereinander.

Soweit man daher die Unabhängigkeit überhaupt als Maßstab für das Verhältnis zwischen den Datenaufsichtsbehörden ansehen kann,[5] würde sie nicht eingeschränkt, wenn die hier in Rede stehende Erweiterung der Kooperationsregelung darauf beschränkt, die Kompetenz zu verbindlichen Beschlüssen nicht auf konkrete Kontrolleinzelfälle, sondern nur auf von solchen Einzelfällen **abstrahierte Angelegenheiten**, etwa die Auslegung von Rechtsvorschriften, zu beziehen. Die Unabhängigkeit jeder Aufsichtsbehörde, die Kontrollaufgabe in jedem ihr zugewiesenen Einzelfall durchzuführen, bliebe also von vornherein unberührt. Sie würde allenfalls auf einer abstrakten Ebene durch die Kooperation mitgeprägt, was sich jedoch nicht oder allenfalls, als eine geringe, dann aber zu rechtfertigende Einschränkung der Unabhängigkeit verstehen lässt.[6] Dies wird vor allem dann deutlich, wenn für die **Verbindlichkeit** der Beschlüsse Einstimmigkeit vorausgesetzt würde. Denn dann ist die Bindung an einen Beschluss der DSK Ausdruck einer Entscheidung, die jede Datenaufsichtsbehörde für sich und aus sich heraus treffen kann, und damit Ausdruck der eigenen Unabhängigkeit. Doch selbst wenn man ein geringeres Beschlussquorum, etwa die absolute Mehrheit ausreichen ließe, ginge damit allenfalls eine geringe Einschränkung der Unabhängigkeit einher, nämlich soweit eine Datenaufsichtsbehörde an einen Beschluss gebunden wird, obwohl sie sich nicht der Mehrheitsauffassung anschließen konnte. Denn auch dann ist der Beschluss in einem unabhängigen

3 Martini/Botta, DÖV 2022, 605, 607.

4 Vgl. EuGH, Urt. v.09.03.2010 - Rs. C-518/07 (Kommission/Deutschland), ECLI:EU:C:2010:125; EuGH, Urt. v. 16.10.2012 - C-614/10 (Kommission/Österreich), ECLI:EU:C:2012:631; EuGH, Urt. v. 8.4.2014 - C-288/12 (Kommission/Ungarn), ECLI:EU:C:2014:237.

5 Ablehnend etwa Diermann, Datenschutzaufsicht über die Tätigkeit der Finanzverwaltung, 2022, S. 90 und Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 999.

6 Generell zur Einschränkbarkeit der Unabhängigkeit etwa Grittmann, in: Taeger/Gabel, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 52 DSGVO Rn. 12; Kienle/Wenzel, ZD 2019, 107 (111); Martini/Botta, DÖV 2022, S. 605 (608).

Diskurs zustande gekommen, an dem jede Datenaufsichtsbehörde gleichberechtigt mitwirken konnte, und der – wie ausgeführt – ohnehin von vornherein gegenständlich keine konkreten Angelegenheiten einer einzelnen Datenaufsichtsbehörde betrifft. Demgegenüber steht der Mehrwert, im Interesse der Rechtssicherheit die Abgestimmtheit der Datenaufsichtsbehörden und die Vorhersehbarkeit ihrer Bewertungen und Vorgehensweisen zu stärken. Die Unabhängigkeit der einzelnen Datenaufsichtsbehörde, steht einer Pflicht, sich in der abstrakten Rechtsaufassung abstimmen zu müssen und dieser Auffassung zu folgen, nicht entgegen.[7] Freilich gilt dies nur – insoweit zieht die Unabhängigkeit eine spezifische Grenze –, wenn die so gewährleistete Unabhängigkeit der einzelnen Datenaufsichtsbehörde nicht sogleich wieder dadurch ausgehöhlt wird, dass die eingegangene und so intern strukturierte **Kooperation als solche** nicht in ihrer Unabhängigkeit geschützt ist.[8]

Dass so die europarechtlichen Grenzen und Vorstellungen zum Schutz aufsichtsbehördlicher Unabhängigkeit gewahrt werden, zeigt ein **Vergleich mit der Ausgestaltung des Europäischen Datenschutzausschusses** (EDSA) in Hinblick auf das Verhältnis der mitgliedstaatlichen Aufsichtsbehörden zueinander. In der letztlich auf Art. 65 DSGVO gründenden Verbindlichkeit der Entscheidungen des EDSA wird keine Verletzung der Unabhängigkeit der Aufsichtsbehörden gesehen, weil die EDSA selbst mit Unabhängigkeit ausgestattet sei und die Kohärenzentscheidung dazu führe, dass die Behörde zwar in ihrer Entscheidung eingeschränkt sei, gleichwohl aber immer noch in der Zuständigkeit unbeschränkt agiere.[9] Im Vergleich dazu dürfte die hier in Rede stehende Kooperation innerhalb der DSK sogar dahinter zurückbleiben. Denn sie würde sich auf die Vorgabe von Auslegungen und Interpretationen beschränken, aber die Ausgestaltung des Verfahrens, die eigentliche Einzelentscheidung und die Ausfüllung von Beurteilungs- und Ermessensspielräumen im Einzelfall unverändert den einzelnen Aufsichtsbehörden überlassen.

7 So auch Martini/Botta, DÖV 2022, S. 605 (608).

8 So auch Martini/Botta, DÖV 2022, S. 605 (608).

9 Spiecker gen. Döhmann, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht (Kommentar), 2019, Art. 64 DSGVO Rn. 2.

b. Grenzen der Grundsätze der Effektivität und Effizienz

Auch die Grundsätze der Effektivität und Effizienz dürften einer weitergehenden Kooperation nicht entgegenstehen. Nach ihnen darf das Verfahren und Vorgehen bei der Ausübung von Befugnissen durch die Aufsichtsbehörden nicht in einer Weise ausgestaltet sein, die eine wirksame **Wahrnehmung der Befugnisse beeinträchtigt**, ineffizient oder gar unmöglich macht.[10] Dafür bestehen keine Anhaltspunkte. Durch ihre Mitwirkung in der DSK dürfte die Effektivität und Effizienz der Arbeit der einzelnen Aufsichtsbehörden schon gegenwärtig nicht beschränkt sein. Eine weitergehende Kooperation könnte das Potenzial haben, die Effektivität und Effizienz der Datenschutzaufsicht zu steigern, etwa indem datenschutzrechtliche Normen für alle Behörden konkretisiert und so der Zweck des einheitlichen Vollzugs im Bundesgebiet gefördert wird.

c. Grenzen des Äquivalenzgrundsatzes

Entsprechendes gilt für den Grundsatz der Äquivalenz. Danach dürfen nationale Verfahren für den **Vollzug von Unionsrecht nicht ungünstiger ausgestaltet** sein als das Verfahren bei entsprechenden Sachverhalten, die nur innerstaatliches Recht betreffen (Äquivalenz).[11] Der Grundsatz wäre betroffen, wenn eine Stärkung der Kooperation der Datenschutzaufsichtsbehörden die Gefahr bürge, dass die Datenschutzaufsichtsbehörden im Rahmen der Ausübung ihrer Befugnisse dem Unionsrecht eine geringere Bedeutung zuweisen würden als dem nationalen Recht. Dafür bestehen keine Anhaltspunkte. Im Gegenteil: Die Beschlussfassung der DSK bezieht sich schon heute auf das **gesamte Datenschutzrecht**, etwa allgemein auf die Abstimmung von Positionen zu datenschutzrechtlichen Auslegungsfragen,[12] und zwar auf das mitgliedstaatliche und unionale Recht gleichermaßen.

10 Vgl. Selmayr, in: Ehmann/ders. (Hrsg.), DSGVO (Kommentar), 3. Aufl. 2024, Art. 58 Rn. 5. Näher zu den Grundsätzen Kibler, Datenschutzaufsicht im europäischen Verbund, § 2 (S. 128 ff). Vgl. auch EG 129 S. 4 in Anschluss an Art. 58 Abs. 4 DSGVO.

11 Ludwigs, NVwZ 2018, S. 1417 (1418).

12 S. dazu die Geschäftsordnung der DSK (GO DSK), Stand 27.2.2024, abrufbar unter www.datenschutzkonferenz-online.de, dort Ziffer III GO DSK.

d. Grenzen der verwaltungsorganisatorischen Gliederung der mitgliedstaatlichen Datenaufsicht

Auch die europarechtlichen Vorgaben zur Verwaltungsorganisation (insbes. Art. 51-59 DSGVO) ziehen einer weitergehenden Kooperation keine grundsätzlichen Grenzen. Vielmehr sehen sie die Möglichkeit der Einrichtung mehrerer Datenschutzaufsichtsbehörden ausdrücklich vor (s. Art. 51 Abs. 3 DSGVO), zeigen sich dabei aber **kooperativen aufsichtsbehördlichen Vorgehensweisen gegenüber aufgeschlossen** (vgl. Art. 60, 63 ff. DSGVO) oder können sogar im Interesse datenschutzrechtlicher Effektivität, Effizienz und Kohärenz als Ermutigung zur verstärkten Kooperation verstanden werden.[13]

e. Zusammenfassung

Das Europarecht schließt eine Regelung zur Stärkung der Zusammenarbeit der Datenaufsichtsbehörden von Bund und Ländern nicht aus. Um das Ziel einer verbesserten Kohärenz des Datenschutzrechts zu erreichen, aber auch um die europarechtlich geforderte Effizienz und Effektivität des Datenschutzrechts zu fördern, kann eine solche Regelung auch über den vorgelegten § 16a BDSG-E hinausgehen und etwa gemeinsame, verbindliche Beschlüsse vorsehen. Zur Wahrung der europarechtlich zu garantierenden Unabhängigkeit darf sich die Beschlusskompetenz nicht auf Einzelfälle beziehen, sondern muss sich auf abstrakte Angelegenheiten des Datenschutzes, etwa die Auslegung von Datenschutzvorschriften beschränken. Dabei muss gewährleistet werden, dass die DSK als solche bei ihrer Kooperationstätigkeit unabhängig ist.

2. Wahrung der grundgesetzlichen Grenzen

Eine weitergehende Kooperationsregelung wahrt auch die grundgesetzlichen Grenzen. Insbesondere was die grundgesetzliche Vollzugskompetenzordnung und die ihr entnommenen sog. Verbote der Mischverwaltung (dazu a) und der Mischfinanzierung (dazu b) betrifft, greift eine erweiterte Kooperation der DSK zwar in die Vollzugskompetenzordnung und die Kompetenzordnung zur Staatsfinanzierung ein, ist aber insoweit verfassungsrechtlich gerechtfertigt bzw. rechtfertigbar.

13 Zur Kritik am Vollzugsdefizit der früher geltenden Datenschutzrichtlinie vgl. Albrecht, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht (Kommentar), 2019, Einl. Rn. 186.

a. Keine Verletzung der Vollzugskompetenzordnung (sog. Verbot der Mischverwaltung)

aa. Begriff und Normativität

Vorliegend könnte vor allem das sog. Verbot der Mischverwaltung der beabsichtigen Stärkung der Kooperation eine Grenze ziehen. Dieses Verbot, das als solches dem Grundgesetz nicht explizit zu entnehmen ist, steht für den in den Art. 20 Abs. 1, 30, 70 ff., 83 ff., 92 ff. u. 109 ff. GG zum Ausdruck kommenden **Grundsatz eigenverantwortlicher Aufgabenwahrnehmung:** Bund und Länder haben die ihnen im Grundgesetz zugewiesenen Kompetenzen grundsätzlich selbständig und eigenverantwortlich wahrzunehmen. Insbesondere müssen die Gesetzesvollzugs- und Verwaltungszuständigkeiten von demjenigen Verband (Bund oder Land) wahrgenommen werden, dem diese Kompetenzen zugeordnet sind. Die Zuständigkeiten müssen also in diesem Sinne grundsätzlich getrennt sein. Sie konkretisieren die Staatsstrukturprinzipien des Bundesstaats-, Rechtsstaats- und Demokratieprinzips.[14] Für diese Wahrung der **Kompetenzordnung** hat sich die Bezeichnung des „Verbots der Mischverwaltung“ etabliert.[15]

Vorliegend kommt das Verbot der Mischverwaltung in den Blick, weil jeder Form der Kooperation zwischen den Datenaufsichtsbehörden inhärent ist (bzw. diese aus Gründen der Effizienz, der Gleichförmigkeit u.a. sogar darauf abzielt), dass die kooperierenden Aufsichtsbehörden jeweils an der Ausübung von Verwaltungskompetenzen mitwirken oder jedenfalls auf deren Ausübung einwirken, die nicht (nur) ihnen, sondern (auch) anderen Aufsichtsbehörden eines anderen Verbandes sachlich und örtlich zugewiesen sind. Dies führt dazu, dass der Vollzug des Datenschutzrechts insoweit nicht mehr nach Rechtsträgern getrennt, sondern „vermischt“ erfolgt.

Zugleich wird deutlich, dass es sich bei dem Verbot der Mischverwaltung zunächst nur um eine **deskriptive Sammelbezeichnung** für den grundsätzlich zwingenden Charakter der grundgesetzlichen Kompetenzzuweisungen für den Rechtsvollzug handelt, aus dem als solchem keine konturenscharfe Rechtsfolgerungen gezogen werden können,[16] schon

14 *Schulz*, DÖV 2017, S. 1028 (1029).
15 Vgl. *Gröpl*, in: Dürig/Herzog/Scholz (Hrsg.), GG (Kommentar), 103. EL 2024, Art. 91c Rn. 5 m.w.N.
16 Vgl. *Gröpl*, in: Dürig/Herzog/Scholz (Hrsg.), GG (Kommentar), 103. EL 2024, Art. 91c Rn. 5 m.w.N.

gar nicht ein absolutes Verbot.[17] Vielmehr begründet er in seiner Pauschalität und Plakativität die Gefahr, den rechtlichen Maßstab insoweit zu verkürzen, als es auch ein Zusammenwirken von Bund und Ländern geben kann, welches in diese allein maßgeblichen Kompetenzzuweisungen nicht eingreift. Ferner verkürzt er, dass selbst bei Vorliegen einer grundgesetzlichen Kompetenzzuweisung auch verfassungsrechtlich Ausnahmen möglich sind – unter den vom Bundesverfassungsgericht entwickelten strikten Beschränkungen. Die Bezeichnung „Verbot der Mischverwaltung“ steht somit nicht für mehr, als dass das Grundgesetz die Verwaltungstypen und -zuständigkeiten insbesondere in den **Art. 30, 83 ff. GG** grundsätzlich erschöpfend regelt und dass allein diese konkreten Regelungen den verfassungsrechtlichen Maßstab für die Verwaltungsorganisation und damit auch für den Grad der Kooperation bilden. Dies entspricht auch dem Ansatz des Bundesverfassungsgerichts in seinen für das sog. Verbot der Mischverwaltung maßgeblichen Entscheidungen.[18]

Nach Art. 30 GG erstreckt sich die Vollzugskompetenz der Länder auf die jeweils eigenen Landesgesetze. Darüber hinaus bestimmt Art. 83 Abs. 1 GG, dass die Länder grundsätzlich auch die Bundesgesetze als eigene Angelegenheit ausführen. Weil das Grundgesetz davon ausgeht, dass die Länder klar voneinander abgegrenzte und keine überlappenden Hoheitsgebiete haben und deswegen nicht in Kompetenzkonflikte kommen, liegt die Funktion der Art. 83 ff. GG vor allem darin, Bund und Länder voneinander organisatorisch zu scheiden und die Länder vor einem Eindringen des Bundes in ihren Verwaltungsbereich zu schützen.[19] In diesem Sinne geht es zur Auslotung der grundgesetzlichen Grenzen für die hier in Rede stehende Kooperation nicht um die Prüfung eines begrifflich unklaren und grundgesetzlich wenig angebundenen Verbots der Mischverwaltung, sondern

17 Vgl. BVerfGE 119, 331 (367).

18 Vgl. BVerfGE 63, 1 („Schornsteiger-Entscheidung“); 119, 331 („SGB II-Entscheidung“); 137, 108 (142 ff.); 139, 194 (226).

19 BVerfGE 137, 108, 147 Rn. 90 sowie 119, 331 (358, 364 und 366); 126, 77, 98. Vgl. auch *F. Kirchhof*, in: Dürig/Herzog/Scholz (Hrsg.), GG-Kommentar, 103. EL 2024, Art. 83, Rn. 111. Die weitgehende Zuweisung der Vollzugskompetenzen an die Länder ist auch vor dem Hintergrund der starken Kompetenzen des Bundes für die Gesetzgebung zu sehen.

darum, ob eine solche Kooperation konkrete Komptenzenzuweisungen des Grundgesetzes verletzen würde.[20] Was die Trennung der Verwaltungskompetenzen von Bund und Ländern betrifft, bringt das Bundesverfassungsgericht dies so zum Ausdruck, dass

> *„eine verwaltungsorganisatorische Erscheinungsform [...] nicht deshalb verfassungswidrig [ist], weil sie als Mischverwaltung einzuordnen ist, sondern nur, wenn ihr zwingende Kompetenz- oder Organisationsnormen oder sonstige Vorschriften des Verfassungsrechts entgegenstehen.“*[21]

Dies wäre bei einer hier in Rede stehenden, weitergehenden Kooperation der Datenaufsichtsbehörden nicht der Fall, wie die nachfolgende Erörterung zeigt.

bb. Eingriff in den Gewährleistungsbereich der Vollzugskompetenzordnung: liegt eine „Mischverwaltung“ vor?

Wem, unter welchen Voraussetzungen und in welchen Hinsichten die Aufgabe des Vollzugs der Gesetze zugeordnet ist, bestimmen vor allem die **Art. 83 ff. GG**. Sie bilden ein differenziertes und feingliedriges Geflecht von Kompetenznormen unterschiedlicher Reichweiten, die zudem erst mit Blick auf die konkret zu vollziehende Sachmaterie – hier das Datenschutzrecht – **greifbare Kompetenzzuordnungen** erkennen lassen, nämlich welchem Verband – Bund oder Ländern – welche Vorschriften des Datenschutzrechts zum Vollzug zugeordnet sind und welche Tätigkeiten mit welchen Anforderungen von einer solchen Vollzugsaufgabe umfasst sind. Erst vor dem Hintergrund einer solchen (in diesem Fall: datenschutzrechts-)spezifischen Bestimmung der Vollzugskompetenzverteilung zwischen Bund und Ländern – und nicht etwa an einem pauschalen Begriff der „Mischverwaltung“ – lässt sich feststellen, ob und welche Formen der Kooperation zwischen Bund und Ländern in die grundgesetzliche Vollzugskompetenzordnung eingreifen.

(1) Bei der Bestimmung der spezifischen Vollzugskompetenzverteilung ist zu beachten, dass sich das zu vollziehende Datenschutzrecht auf **drei Normebenen** – Union, Bund, Land – verteilt. Zudem beantwortet das Grundgesetz nicht ausdrücklich, wer – Bund oder Länder – für den **Vollzug von Unionsrecht** zuständig ist, was sich wegen der zentralen

20 Vgl. Trute, in: v. Mangoldt/Klein/Starck (Hrsg.), GG (Kommentar), 7. Aufl. 2018, Art. 83 Rn. 28; Hermes; in: Dreier (Hrsg.), GG (Kommentar), 3. Aufl. 2018, Art. 83 Rn. 47 ff; vgl. auch Broß/Mayer; in: von Münch/Kunig, Grundgesetz-Kommentar, 7. Aufl. 2021, Art. 83 Rn. 15 ff; BVerfGE 63, 1 (38); 108, 169 (182).

21 BVerfGE 63, 1 (38).

Bedeutung der DSGVO gerade für die Bestimmung der Kompetenzordnung im Datenschutzrecht besonders komplizierend auswirkt. Um die Lücke zu schließen, wird sich für die Zuordnung der Kompetenz zum Vollzug der DSGVO verbreitet an der grundgesetzlichen Verteilung der Gesetzgebungskompetenzen für das Datenschutzrecht orientiert. Eine Vorschrift der DSGVO wird demnach etwa dem Bund zum Vollzug zugeordnet, wenn sie – wäre sie eine deutsche Rechtsvorschrift – in die Gesetzgebungskompetenz des Bundes fallen *würde*. Allerdings führt dies im Bereich des Datenschutzrechts nur mit einer gewissen Einschränkung zu einer eindeutigen Zuordnung von Vollzugskompetenzen für das europäische Datenschutzrecht, denn das Grundgesetz sieht keine spezifische und ausdrückliche Gesetzgebungskompetenz für das Datenschutzrecht vor. Diese wird als Annex jener Gesetzgebungsmaterie im Sinne der Art. 73 f. GG entnommen, in deren Sachzusammenhang die Datenverarbeitung jeweils stattfindet.

(2) Auf dieser – komplexen – Grundlage lässt sich die Vollzugskompetenzverteilung im Bereich des Datenschutzrechts wie folgt skizzieren:

- Für die verwaltungsmäßige Ausführung der **Landesdatenschutzgesetze** und der landesspezialgesetzlichen Regelungen sind ausschließlich die Länder zuständig (Art. 30 GG).
- Das Gleiche gilt für den Vollzug **unionsrechtlicher Datenschutzregelungen**, die – wären sie mitgliedstaatliche Regelungen – in die Gesetzgebungskompetenz der Länder fielen.
- Der Vollzug **bundesrechtlicher sowie unionsrechtlicher Datenschutzregelungen**, die – wären sie mitgliedstaatliche Regelungen – in die Gesetzgebungskompetenz des Bundes fielen, fällt
    - **grundsätzlich** in die Vollzugskompetenz der **Länder**, d.h. von ihnen einzurichtende Behörden haben diese Regelungen auf Grundlage landesrechtlicher Verfahren auszuführen (Art. 83, 84 Abs. 1 S. 1 GG). Trifft der Bund aufgrund seiner Ausnahmekompetenzen aus Art. 84 Abs. 1 S. 2 oder S. 5 GG Regelungen zur Behördeneinrichtung und/oder zum Verwaltungsverfahren in den Ländern, haben die Länder die unionsrechtlichen Datenschutzregelungen nach diesen bundesrechtlichen Bestimmungen auszuführen, soweit sie

nicht aufgrund ihrer Abweichungskompetenz (Art. 84 Abs. 1 S. 2 Hs. 2 GG) anderes geregelt haben.

- **ausnahmsweise** in die Vollzugkompetenz des **Bundes**, wenn und soweit hierfür durch einfaches Bundesgesetz eine Bundesoberbehörde eingerichtet wurde (Art. 87 Abs. 3 S. 1 GG). Dies trifft etwa auf die Regelungen im BDSG zur Errichtung des BfDI und zu dessen Aufsicht über die öffentlichen Stellen des Bundes und über bestimmte Telekommunikationsdienstleistungsunternehmen zu.

In Hinblick auf die **Reichweite** der so zugeordneten Vollzugskompetenzen ist zu beachten: Auch wenn die Vollzugskompetenzvorschriften des GG nicht durchgängig von „Vollzug“ sprechen, sondern auch andere Begriffe zur Rechtsfolgenkonkretisierung verwenden (Einrichtung bzw. Errichtung der Behörden etc.), umfassen die so zugeordneten Vollzugskompetenzen regelmäßig die Festlegung aller Elemente und Aspekte, die zur **verwaltungsmäßigen Ausführung** der jeweiligen Gesetze notwendig sind, also insbesondere

- die **Verwaltungsorganisation**: die Ein- und Errichtung der Behörden, deren Ausgestaltung, innere Organisation und Ausstattung mit Personal und Sachmitteln, die Festlegung ihres Aufgabenkreises einschließlich der Übertragung von Aufgaben und Befugnissen sowie
- das **(innere und äußere) Verwaltungsverfahren**: die Art und Weise sowie die Form des Verwaltungshandelns, die behördliche Willensbildung und Entscheidung, deren Zustandekommen und Durchsetzung sowie verwaltungsinterne Mitwirkungs- und Kontrollvorgänge.

Soweit danach einem Verband (Bund oder Land) die Aufgabe des Vollzugs von gesetzlichen Datenschutzregelungen zugewiesen ist, hat er sie **mit eigenem Personal, eigenen Sachmitteln und eigener Organisation** wahrzunehmen.

(3) Auf Grundlage dieser datenschutzrechtsspezifischen Bestimmung der Vollzugskompetenzverteilung zwischen Bund und Ländern sprechen die überwiegenden Gründe dafür, dass eine im Vergleich zum vorgelegten § 16a BDSG-E weitergehende Kooperationsregelung in die verfassungsrechtliche Kompetenzordnung im Sinne der Art. 83 ff. GG

eingreift und daher in diesem Sinne als **Mischverwaltung** anzusehen ist. Denn die angedachten Erweiterungen führen dazu, dass die Datenschutzaufsichtsbehörden von Bund und Ländern in den ihnen jeweils nicht zugeordneten Vollzugsbereichen des Datenschutzrechts in einer Art und Weise mitwirken, die nach der Rechtsprechung des BVerfG als **verwaltungsmäßige Ausführung** anzusehen ist oder die die **eigenverantwortliche Wahrnehmung** durch die jeweils zuständige Datenschutzaufsichtsbehörde tangiert:[22]

- **Verbindliche Beschlüsse gemeinsamer Auslegungsmaximen** und Stellungnahmen zu Angelegenheiten des Datenschutzes durch die DSK betreffen die verwaltungsmäßige Ausführung im Sinne des Art. 83 GG. Zwar sind sie nicht Teil eines konkreten Verwaltungsverfahrens, sondern werden gleichsam „vor die Klammer“ gezogen und dienen deren abstrakter Vorbereitung. Aufgrund der Verbindlichkeit führen sie allerdings zu einer Einschränkung des Auslegungs- und ggf. Anwendungsspielraums in konkreten Verfahren und wirken so abstrakt in die verwaltungsmäßige Ausführung der jeweils zuständigen Aufsichtsbehörde ein.
- Auch eine **gemeinsame Öffentlichkeitsarbeit** von Bund und Ländern durch die DSK im Sinne einer Information der Öffentlichkeit über deren Tätigkeiten und der Veröffentlichung der von ihr beschlossenen Auslegungsmaximen und Stellungnahmen stellt eine gemeinsame Gesetzesausführung dar, die gemäß den grundgesetzlichen Kompetenzzuweisungen von Bund und Ländern jeweils eigenverantwortlich wahrzunehmen ist (vgl. auch Art. 57 Abs. 1 lit. b DSGVO). Öffentlichkeitsarbeit wirkt nach außen und ist damit Teil der verwaltungsmäßigen Ausführung der Gesetze, auch wenn sie keine rechtliche Regelungswirkung gegenüber dem Bürger entfaltet.
- Schließlich greifen auch die **Einrichtung und der Betrieb einer Geschäftsstelle** zur administrativen und inhaltlichen Begleitung der DSK in den Gewährleistungsgehalt der Kompetenzordnung aus Art. 83 ff. GG ein. Denn die Geschäftsstelle dient gerade und insbesondere der kooperativen Wahrnehmung von Aufgaben wie

22 Zur „verwaltungsmäßigen Ausführung“ s. BVerfGE 63, 1 Rn. 143 ff.; 119, 331 Rn. 154. Kriterien für eine Beurteilung, ab welchem Grad einer Kompetenzvermischung der Grundsatz der eigenverantwortlichen Aufgabenwahrnehmung nicht mehr gewahrt ist, lassen sich der Rechtsprechung hingegen nicht entnehmen.

der Bestimmung von Auslegungsmaximen und der Öffentlichkeitsarbeit, die ihrerseits – wie ausgeführt – die verwaltungsmäßige Ausführung betreffen.

cc. Rechtfertigung: handelt es sich um eine „verbotene“ Mischverwaltung?

Soweit man die genannten Weiterungen einer Kooperation als Eingriffe in die verfassungsrechtliche Kompetenzordnung für den Vollzug des Datenschutzrechts ansieht, folgt hieraus nicht automatisch die verfassungsrechtliche Unzulässigkeit. Wie bereits ausgeführt, ist das sog. Verbot der Mischverwaltung auch nach der Rechtsprechung des BVerfG nicht absolut zu verstehen, sondern zeigt sich **abwägungsoffen**. Es ist daher zu prüfen, inwieweit die jeweiligen Eingriffe in die Vollzugskompetenzordnung **ausnahmsweise gerechtfertigt** werden können.

Nach der Rechtsprechung des **BVerfG** ist eine Mischverwaltung nur dann mit den Vorgaben der Art. 83 ff. GG nicht vereinbar, wenn sie dem aus Rechtsstaats- und Demokratieprinzip folgenden Gebot der Rechts- und Verantwortungsklarheit nicht genügt oder die Grenzen der eigenverantwortlichen Aufgabenwahrnehmung durch eine nicht nur geringfügige Inanspruchnahme des nicht zuständigen Verwaltungsträgers überschreitet, die auch nicht aus einem besonderem Sachgrund gerechtfertigt werden kann und sich auf eine eng umgrenzte Verwaltungsmaterie beschränkt.[23] An diesem Maßstab lassen sich nicht nur die vorgelegte Regelung des § 16a BDSG-E, sondern auch die hier in Rede stehenden Erweiterungen der Kooperation rechtfertigen:

(1) So können die Kooperationserweiterungen, also das gemeinsame Fassen verbindlicher Beschlüsse, eine gemeinsame Öffentlichkeitsarbeit und die Einrichtung einer gemeinsamen Geschäftsstelle auf einen besonderen Sachgrund gestützt werden und betreffen auch nur eine eng umgrenzte Verwaltungsmaterie, so dass die **Grenzen eigenverantwortlicher Aufgabenwahrnehmung** gewahrt werden.

23 BVerfGE 119, 331 (367). Vgl. zur parallelen Anwendung der Kriterien der Verantwortungsklarheit und eigenverantwortlichen Aufgabenwahrnehmung auch Trute, v. Mangoldt/Klein/Starck (Hrsg.), GG (Kommentar), 6. Aufl. 2010, Art. 83 Rn. 19; Berger, Die Ordnung der Aufgaben im Staat, 2016, S. 61; eine Abschwächung der kompetenziellen Grenzen nimmt Burgi für Verwaltungstätigkeiten an, bei denen mangels klassischer Vollzugswirkung Rechtsstaats- und Demokratieprinzip nicht beeinträchtigt werden, in: Butzer/Kaltenborn/Meyer (Hrsg.), FS Schnapp, 2008, 18 (22 ff).

So besteht mit dem europarechtlich überformten Gebot eines effektiven und vereinheitlichten Vollzugs des Datenschutzrechts zur Behebung bestehender Vollzugsdefizite ein **besonderer Sachgrund**. Dies gilt insbesondere für die Datenverarbeitung privater Stellen, da für sie bundesweit grundsätzlich dieselben Vorschriften gelten, was im Interesse eines einheitlichen Vollzugs des Datenschutzrechts eine Abstimmung zwischen den Datenschutzbeauftragten erforderlich macht.[24] Dies wird durch die unionsrechtlich vorgesehene Teilnahme am europäischen Kohärenzverfahren und die damit einhergehende Notwendigkeit der Entwicklung gemeinsamer Positionen unterstrichen. Denn damit eine Abstimmung auch schon vor dem konkreten Einzelfall, der aus dem EDSA an die Aufsichtsbehörden herangetragen wird, grundsätzlich möglich wird, bedarf es weitergehender Kooperationsmechanismen. Dem würde insbesondere die Herstellung von Verbindlichkeit in der Auslegung von Rechtsfragen des Datenschutzes entsprechen. Dass für eine stärkere Kohärenz der Auslegung des Datenschutzrechts auch ein dringender praktischer Bedarf besteht, hat sich wiederholt gezeigt. Eine Harmonisierung oder Vereinheitlichung der datenschutzrechtlichen Auslegung erfolgt zwar auch auf unionsrechtlicher Ebene, insbesondere auch durch entsprechende Entscheidungen des EuGH. Eine gerichtliche Rechtsharmonisierung ist allerdings ein Effekt der nachträglichen Kontrollfunktion anhand von Einzelfällen. Er nimmt den Verwaltungen von Bund und Ländern nicht ihre orignäre Aufgabe der Ausführung der Gesetze und die damit verbundene Eigenständigkeit und Verantwortung. Die Ausführung der Gesetze umfasst aber vor allem und insbesondere deren Auslegung.

Die DSK wird zudem im Rahmen einer **eng umgrenzten Verwaltungsmaterie** tätig. Zwar hat das Datenschutzrecht einen Querschnittscharakter und betrifft dementsprechend viele Bereiche. Rechtsgegenständlich ist aber präzise umgrenzt, nämlich auf die Verarbeitung personenbezogener Daten bezogen. Zudem würden sich die Entscheidungen der DSK nicht auf Einzelfallentscheidungen erstrecken, sondern sich auf allgemeine Grundsätze und Auslegungen, die diesbezügliche Öffentlichkeitsarbeit und eine Geschäftsstelle beschränken. Entscheidungen und Maßnahmen im Einzelfall bleiben Sache der Aufsichtsbehörden, was die Verantwortlichkeiten zwischen der DSK und einzelner

24 Martini/Botta, DÖV 2022, S. 605 (610).

Aufsichtsbehörde klar abgrenzt. Insbesondere kämen der DSK keine Aufsichtsbefugnisse zu.[25]

(2) Eine Kooperationserweiterung wahrt auch das **Gebot der Rechts- und Verantwortungsklarheit**.[26] Die Datenschutzbeauftragten werden vom Parlament gewählt und erhalten so ein hohes Maß demokratischer Legitimation. Durch die Bindung an Beschlüsse über die Auslegung des Datenschutzrecht oder andere Entscheidungen, die sie nicht allein, sondern von der DSK getroffen werden, wird die demokratische Legitimationskette zum Wahlvolk ihres jeweiligen Bundeslandes geschwächt. Dies zumal dann, wenn sie an Mehrheitsentscheidungen gebunden werden, die sie selbst befürwortet.

Der insoweit gelockerte Zurechnungszusammenhang lässt sich aber durch die – rechtlich abzusichernde – **Unabhängigkeit** der DSK rechtfertigen.[27] Insbesondere wenn alle Datenschutzbeauftragten stimmberechtigt sind, garantiert ihre Unabhängigkeit einen von der Einflussnahme anderer Staatsorgane freien Entscheidungsprozess, als dessen Teil sie selbst Grundrechtsschutz gewährleisten (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), statt allein grundrechtsgebunden zu sein.[28] Insoweit kann die Mitwirkung an der kollektiven Willensbildung der DSK den Verlust an souveräner Entscheidungsmacht des einzelnen Datenschutzbeauftragten bis zu einem gewissen Grad kompensieren.[29] Um dem Grundsatz der Verantwortungsklarheit zu entsprechen, sollten die Entscheidungen der DSK gegenüber datenverarbeitenden Stellen und betroffenen Personen aber nicht unmittelbar gelten. Vielmehr sollten die Landesdatenschutzbeauftragten gemeinsame Entscheidungen jeweils als die ihrige umsetzen, auch mit Blick auf die örtliche Zuständigkeit (vgl. § 3 VwVfG).[30]

25 Martini/Botta, DÖV 2022, S. 605 (610).

26 Zu Folgenden auch Martini/Botta, DÖV 2022, S. 605 (610).

27 Vgl. hinsichtlich der Landesmedienanstalten BVerwG, Urt. v. 15.7.2020, 6 C 6.19, Rn. 38. Hierzu und zum Folgenden auch Martini/Botta, DÖV 2022, S. 605 (610 f.) m.w.N.

28 Anders stellte sich dies beim Glücksspielkollegium dar, das im grundrechtssensiblen Hoheitsbereich tätig war, vgl. Degenhart, Rechtsfragen des ländereinheitlichen Verfahrens nach dem Entwurf eines ersten Staatsvertrags zur Änderung des Staatsvertrags zum Glücksspielwesen, 2011, S. 26.

29 Vgl. BayVerfGH, Entsch. v. 25.9.2015, Vf. 9-VII/13, Vf. 4/VII/14, Vf. 10/VII/14, Rn. 157.

30 So auch Martini/Botta, DÖV 2022, S. 605 (610 f.).

dd. Zwischenergebnis

Am Maßstab der bundesverfassungsgerichtlichen Rechtsprechung sprechen die überwiegenden Gründe dafür, dass eine über § 16a BDSG-E hinausgehende Stärkung der Kooperation insbesondere in Form gemeinsamer und verbindlicher Entscheidungen über die Auslegung des Datenschutzrechts und über Stellungnahmen zu Datenschutzangelegenheiten, gemeinsamer Öffentlichkeitsarbeit und einer gemeinsamen Geschäftsstelle in die verfassungsrechtliche Kompetenzordnung für den Vollzug des Datenschutzrechts eingreift. Allerdings lässt sich dieser Eingriff verfassungsrechtlich rechtfertigen und damit als verfassungsrechtlich zulässige „Mischverwaltung" qualifizieren. So besteht mit dem europarechtlich überformten Gebot eines effektiven und vereinheitlichten Vollzugs des Datenschutzrechts zur Behebung bestehender Vollzugsdefizite ein besonderer Sachgrund. Die DSK wird zudem im Rahmen einer eng umgrenzten Verwaltungsmaterie tätig. Denn ihre Entscheidungen erstrecken sich nicht auf konkrete Einzelfälle, sondern beschränken sich auf allgemeine Grundsätze und Auslegungen in einem gegenständlich präzise umgrenzten Rechtsgebiet. Entscheidungen und Maßnahmen im Einzelfall bleiben Sache der Aufsichtsbehörden, was die Verantwortlichkeiten zwischen DSK und einzelner Aufsichtsbehörde klar abgrenzt. Dasselbe gilt für eine gemeinsame Öffentlichkeitsarbeit und eine die DSK unterstützende Geschäftsstelle, wenn und weil sie sich auf denselben Verwaltungsgegenstand beziehen.

b. Keine Verletzung der Kompetenzordnung zur Staatsfinanzierung (sog. Verbots der Mischfinanzierung)

Soweit die Aufsichtsbehörden in ihrer Zusammenarbeit über die DSK wie dargestellt gestärkt würden, erzeugt dies **Kosten**, die finanziert werden müssen. Insbesondere die Einrichtung und der Betrieb einer gemeinsamen Geschäftsstelle mit personalem Unterbau zur inhaltlichen und administrativen Begleitung der DSK ziehen Kosten nach sich. Damit stellt sich die Frage nach den verfassungsrechtlichen Grenzen und Vorgaben, wie die **Finanzierungslasten** verteilt sein dürfen, wenn Bund und Länder zusammenwirken. Diese Grenzen müssten gewahrt werden.

Die **bundesstaatliche Finanzverfassung** ist grundsätzlich zweigliedrig aufgebaut und unterscheidet die Ebene des Bundes und die der Länder (vgl. Art. 104a ff. GG). Aufgrund dieser grundgesetzlichen Vorstrukturierungen hängen die rechtlichen Grenzen für die Lasten- und Einnahmenverteilung innerhalb einer Kooperation in erster Linie von der Partnerkonstellation ab. Dabei normieren die Bestimmungen der Art. 104a ff. GG vor al-

lem Gebote und Zuweisungen, um die Staatsfinanzierung zu regeln. Sie bestimmen regelmäßig keine expliziten Verbote. Dementsprechend findet sich auch **kein ausdrückliches Verbot einer Mischfinanzierung**.[31] Im Sinne von nicht zu überschreitenden verfassungsrechtlichen Grenzen verboten sind dementsprechend solche Lastenverteilungen, die sich – im Umkehrschluss – nicht durch die Gebote und Zuweisungen der Art. 104a ff. GG rechtfertigen lassen.

Aus dem Gebot der getrennten Lasttragung folgt für Verwaltungsausgaben gem. Art. 104a Abs. 5 S. 1 Hs. 1 GG absolut (sog. **Trennungsgebot für Verwaltungsausgaben**) und für Zweckausgaben aus Art. 104a Abs. 1 GG grundsätzlich (sog. **allgemeines Trennungsgebot**), dass derjenige Verwaltungsträger, dem die Ausführung einer Aufgabe verfassungsrechtlich zugewiesen ist, auch die daraus resultierenden Kosten zu tragen hat. Dieser Lastenverteilungsgrundsatz verbietet, dass ein unzuständiger Verwaltungsträger solche Kosten trägt, die aus der Wahrnehmung einer Aufgabe resultieren, die eindeutig einem anderen Verwaltungsträger zugeordnet ist. Dieses Verbot setzt allerdings voraus, dass es sich überhaupt um nach unterscheidbaren Aufgaben trennbare Kosten handelt. Dementsprechend regelt Art. 104a GG solche Konstellation wie die vorliegende, in denen eine Aufgabe kooperativ wahrgenommen wird und die daraus resultierenden Kosten nicht zuordenbar sind, nicht unmittelbar. In diesen Fällen wird vertreten, die Rechtsfolge des Art. 104a dahingehend zu relativieren, dass eine **Aufteilung der Lastentragung entlang der grundsätzlich getrennten Vollzugskompetenzen zu treffen ist**.[32]

Bei der hier in Rede stehenden Erweiterung der DSK um eine Kompetenz zu gemeinsamen, verbindlichen Beschlüssen über die Rechtsauslegung, eine gemeinsame Öffentlichkeitsarbeit und eine gemeinsame Geschäftsstelle, sind die damit einhergehenden Verwaltungs- und Zweckausgaben für die Tätigkeiten in der DSK eine **Folge einer gemeinsamen Verwaltungstätigkeit** von Bund und Ländern. Sie lassen sich – wie oben ausgeführt – nicht mehr der Vollzugskompetenz des Bundes oder der Länder zuordnen.

31 Vgl. BVerfGE 81, 312 (314).

32 Sieckmann, in: Sachs (Hrsg.), GG (Kommentar), 9. Aufl. 2021, Art. 104a Rn. 18a; Dulde/Porsch, NVwZ 2011, 833 (834); Heun, in; Dreier (Hrsg.), GG (Kommentar), 3. Aufl. 2018, Art. 104a GG Rn. 21, 35; BVerwGE 81, 312 (314); a.A. Meyer, DVBl 2011, 449.

Die kooperative Erweiterung der DSK lässt sich somit nicht mehr ohne Weiteres auf das grundgesetzliche Gebot der getrennten Lastentrennung stützen und würde im Sinne einer „Mischfinanzierung“ die verfassungsrechtlichen Grenzen überschreiten, wenn für ihre Finanzierung keine angemessene Lastenverteilungsregelung zwischen Bund und Ländern entlang der getrennten Zuständigkeiten für die Ausführung des Datenschutzrechts getroffen wird. Dies ist insbesondere der Fall, wenn allein der Bund oder allein die Länder die DSK finanzieren sollten. Es ist daher eine **entsprechende gesetzliche Regelung zu treffen**, z.B. durch Übernahme des sog. **„Königsteiner Schlüssels“.** Die verfassungsrechtliche Kompetenzordnung zur Staatsfinanzierung ist dann gewahrt.

Die mit einer im Vergleich zu § 16a BDSG-E weitergehenden Kooperation einhergehenden Kosten wahren die finanzverfassungsrechtlichen Grenzen, wenn für deren Finanzierung eine angemessene, gesetzliche Lastenverteilungsregelung zwischen Bund und Ländern entlang der getrennten Zuständigkeiten für die Ausführung des Datenschutzrechts getroffen wird, z.B. durch Übernahme des sog. „Königsteiner Schlüssels“.

3. Zusammenfassung zu den rechtlichen Grenzen und Spielräumen für den Bundesgesetzgeber zur Regelung einer Kooperation

Soweit erwogen wird, die DSK über den vorgelegten § 16a BDSG-E hinaus in ihrer Kooperation zu stärken, indem sie insbesondere Kompetenzen bzw. Befugnisse erhält, über die Auslegung des Datenschutzrechts und über Stellungnahmen zu Datenschutzangelegenheiten verbindlich zu entscheiden, Öffentlichkeitsarbeit und eine Geschäftsstelle zu betreiben, wahrt dies grundsätzlich die europa- und verfassungsrechtlichen Grenzen.

Insbesondere was die grundgesetzliche Vollzugskompetenzordnung und Finanzverfassung und die ihr entnommenen sog. Verbote der Mischverwaltung und -finanzierung betrifft, greift die genannte weitergehende Kooperationsstärkung zwar in den verfassungsrechtlichen Gewährleistungsgehalte ein, ist aber insoweit verfassungsrechtlich gerechtfertigt bzw. rechtfertigbar, wenn folgende Grenzen und Spielräume eingehalten und durch eine entsprechende gesetzliche Regelung gewährleistet werden:

1. Die Beschlusskompetenz darf sich nicht auf Einzelfälle beziehen, sondern muss sich auf abstrakte Angelegenheiten des Datenschutzes, etwa die Auslegung von Datenschutzvorschriften beschränken.

2. Es muss gewährleistet werden, dass die DSK als solche bei ihrer Kooperationstätigkeit unabhängig ist.

3. Es muss eine Kostenregelung zur angemessenen Lastenverteilungsregelung zwischen Bund und Ländern entlang der getrennten Zuständigkeiten für die Ausführung des Datenschutzrechts getroffen wurden, z.B. in Form des sog. „Königsteiner Schlüssels“.

II. Erwägungen zur zweckmäßigen Ausgestaltung einer erweiterten Kooperation

Die vorstehenden Ausführungen haben die Grenzen bestimmt, die bei einer kooperativen Erweiterung der DSK zu beachten sind. Damit werden zugleich die Spielräume deutlich, die der Einschätzungsprärogative des Gesetzgebers zur konkreten Ausgestaltung der Kooperation verbleiben. Sie betreffen die Verbindlichkeit der Beschlüsse sowie Quoren, unten denen sie zustande kommen (dazu 1), zudem die verfahrensbezogene Ausgestaltung der gemeinsamen Öffentlichkeitsarbeit (dazu 2) sowie die Verortung der gemeinsamen Geschäftsstelle (dazu 3). Bei seinen Zweckmäßigkeitserwägungen sollte sich der Gesetzgeber von der Erkenntnis leiten lassen, dass die bisherige Zusammenarbeit in der DSK trotz der Bemühungen aller Beteiligten immer wieder zu stark divergierenden und sich für Private, Unternehmen und staatliche Akteure misslich auswirkenden Auslegungen der datenschutzrechtlichen Bestimmungen geführt hat, was sich insbesondere für einen effektiven und gleichmäßigen Grundrechtsschutz als Kernaufgabe der Aufsichtsbehörden häufig nicht als förderlich erwiesen hat.[33]

1. Verbindlichkeit, Gegenstände und Quoren der Beschlüsse

Mit der Stärkung der DSK verbindet sich das Ziel, die einheitliche inhaltliche Positionierung zwischen den deutschen Aufsichtsbehörden voranzutreiben, damit insgesamt eine höhere Effizienz zu erreichen und vorhandene Ressourcen besser zu nutzen. Dabei richtet die DSK schon heute ihren Fokus vor allem auf allgemeine Fragestellungen im Zusammenhang mit dem Datenschutzrecht (Auslegungshilfen, Leitlinien oder Empfehlungen zu einzelnen Datenschutzvorschriften) und stimmt hierüber mit einfacher bzw. bei

33 So auch Martini/Botta, DÖV 2022, 605, 606 m.w.N., insbesondere mit Hinweis auf die Privatwirtschaft, für die fehlende Einigkeit und Rechtssicherheit bei der Auslegung ein Dorn im Auge sei.

sog. Entschließungen mit Zweidrittel-Mehrheit ab.[34] Die Entscheidungen entfalten allerdings keine Bindungswirkung, weder gegenüber anderen privaten und staatlichen Akteuren noch zwischen den Datenschutzaufsichtsbehörden.

Inwieweit die hier in Rede stehende und grundsätzlich zulässige (s. vorstehend I) Erweiterung der Beschlusskompetenz dazu beisteuert, die beabsichtigte Kohärenz des Datenschutzrechts zu stärken, hängt maßgeblich von der Ausgestaltung der Verbindlichkeit der Beschlüsse und von den Quoren ab, die sie voraussetzen. So hätte eine Verbindlichkeit im Außenverhältnis eine weitreichende Wirkung, würde aber weitergehende Rechtsfragen, insbesondere der Rechtssubjektivität aufwerfen.[35] Dem Kohärenzziel wäre im Vergleich dazu auch bereits mit einer **Verbindlichkeit im Innenverhältnis** gedient, die dadurch sichergestellt würde, dass eine Verbindlichkeit im Außenverhältnis explizit durch Gesetz auszuschließen wäre. Selbst ein formal nur innenverbindlicher Beschluss dürfte das Kohärenzziel auch insoweit „nach außen“ fördern, als bei (außenstehenden) Akteuren **die Erwartungshaltung** erzeugt wird kann, dass sich die jeweilige Aufsichtsbehörde auch in ihren Entscheidungen nach außen an die innenverbindlichen Beschlüsse der DSK hält. Vor allem für überregional tätige Unternehmen hätte eine solche Verbindlichkeit den Vorteil höherer Rechtssicherheit. Zugleich würde sie misslichen Praktiken, wie die unternehmerische Einflussnahme auf die behördliche Zuständigkeit durch Wahl und Wechsel der Hauptniederlassung (sog. „Behörden-Hopping“, vgl. auch § 40 Abs. 2 Satz 1 BDSG i.V.m. Art. 4 Nr. 16 DSGVO) entgegenwirken.

Auch über die Festlegung notwendiger **Beschlussquoren** können die Auswirkungen von Verbindlichkeit gestaltet werden. So dürfte das Erfordernis der Einstimmigkeit und die damit einhergehende hohe Anforderung an die Kompromissfindung häufig dazu führen, dass die Beschlüsse inhaltlich eine hohe Abstraktion und Relativierung erfahren, was – auch wenn sie verbindlich sind – auf diese Weise ihre inhaltliche Steuerungskraft regelmäßig absenkt. Dies spricht für eine Beschlussfassung mit der **Mehrheit der Mitglieder**.

34 Siehe Ziffer IV.3 GO DSK.

35 Als institutionelle Beispiele auf nationaler Ebene sind die gemeinsamen Organe der Landesmedienanstalten (§§ 104 ff. Medienstaatsvertrag) bzw. das ehemalige Glücksspielkollegium der Länder (§ 9a Glücksspielstaatsvertrag a.F.) und auf Unionsebene der Europäische Datenschutzausschuss (EDSA) zu nennen, dazu auch Martini/Botta, DÖV 2022, 605, 607.

Schließlich ist es zwar nicht rechtlich geboten, aber zur Begrenzung der Beschlusskompetenz der DSK zu erwägen, diese auf **konkret benannte Gegenstände** zu beschränken. Es könnte ein abschließender Katalog von Gegenständen formuliert werden, auf die sich bindende Beschlüsse beziehen dürfen, z.B. auf Zuständigkeitskonflikte zwischen den Behörden oder auf grundlegende Rechtsfragen, die mehrere Landesdatenschutzbeauftragte in ihrer Amtsausübung betreffen.[36]

2. Gemeinsame Öffentlichkeitsarbeit

Mit der gemeinsamen Öffentlichkeitsarbeit soll insbesondere erreicht werden, dass die Auslegungsmaximen und Stellungnahmen der DSK auch nach außen gegenüber Verantwortlichen, Auftragsverarbeitern und Betroffenen effektiv kommuniziert werden können, um auch in der Praxis eine einheitliche Anwendung des Datenschutzrechts zu fördern. Damit wird ein allgemeiner, der Öffentlichkeit zugänglicher Wissensfundus über die Auslegung relevanter datenschutzrechtlicher Normen geschaffen. Gerade der viel kritisierten Rechtsunsicherheit, die bei den Adressaten des Datenschutzrechts durch unterschiedliche Auslegungshinweise, Empfehlungen und Praktiken der Aufsichtsbehörden entsteht, kann dadurch entgegengewirkt werden. Dabei kann das **Verfahren der Öffentlichkeitsarbeit** innerhalb der DSK unterschiedlich ausgestaltet werden. So ist zu empfehlen, auch Öffentlichkeitsverlautbarungen grundsätzlich dem Beschlussverfahren zu unterwerfen, um Missverständnisse zu vermeiden und klare Verantwortlichkeit für die Öffentlichkeitsarbeit zu begründen.[37]

3. Einrichtung einer gemeinsamen Geschäftsstelle

Die Einrichtung einer gemeinsamen Geschäftsstelle soll dazu beitragen, Effektivität und Effizienz der Kooperation zu stärken, etwa indem Verfahrensabläufe zu strukturiert und die jeweiligen wechselnden Vorsitze unter Wahrung von Kontinuität und Professionalität

36 Siehe Martini/Botta, DÖV 2022, S. 605 (608 f.).

37 So schon jetzt, allerdings nur auf der Ebene des Geschäftsordnungsrechts vorsehend Ziffer III GO DSK.

begleitet werden. Daher ist eine **passende Verortung und Organisation** der Geschäftsstelle zu empfehlen, die die Kooperation fördern und die Wissensdistribution aus den und in die Aufsichtsbehörden gleichmäßig absichern.

4. Zusammenfassung

Die unter Ziffer I.3 dargestellten europa- und verfassungsrechtlichen Grenzen eröffnen einen Gestaltungsspielraum für die konkrete Ausgestaltung der Kooperation, der unter Zweckmäßigkeitserwägungen ausgefüllt werden kann. Dabei ist Folgendes zu empfehlen:

1. Die Außenwirkung von Beschlüssen der DSK sollte im Gesetz explizit ausgeschlossen werden.

2. Es sollte im Gesetz festgelegt werden, dass Beschlüsse mit der Mehrheit der Mitglieder der DSK zustandekommen.

3. Die gesetzliche Grundlage für eine verbindliche Beschlussfassung kann einen abschließenden Katalog von Tatbeständen formulieren, in denen ein bindender Beschluss ergehen kann (z.B. Zuständigkeitskonflikte, übergreifende Bedeutung einer Rechtsfrage).

4. Es sollte gesetzlich vorgegeben werden, dass Öffentlichkeitsverlautbarungen grundsätzlich dem Beschlussverfahren unterliegen.

5. Im Gesetz sollte ein Rahmen für eine passende Verortung und Organisation der Geschäftsstelle festgelegt werden.

III. Rechtliche Umsetzung durch bundesgesetzliche Regelung im BDSG

Unter Wahrung der dargelegten europa- und verfassungsrechtlichen Grenzen (dazu vorstehend I) sowie unter Einbeziehung der Ausgestaltungsempfehlungen (dazu vorstehend II) könnte die Kooperation über den vorgelegten § 16a BDSG hinaus beispielsweise wie folgt normiert werden:

„(1) Die Aufsichtsbehörden des Bundes und der Länder im Sinne des § 18 Absatz 1 Satz 1 bilden die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz).

(2) Die Datenschutzkonferenz hat die Aufgabe

1. auf eine einheitliche Anwendung des Datenschutzrechts hinzuwirken,

2. zu Angelegenheiten des Datenschutzes Stellung zu nehmen und

3. die Öffentlichkeit hierüber zu informieren.

Aufgaben, Zuständigkeiten und Befugnisse der Aufsichtsbehörden nach Bundes- oder Landesrecht bleiben unberührt. Art. 52 Abs. 1 bis 3 der Richtlinie (EU) 2016/679 gelten für die Tätigkeit der Datenschutzkonferenz und für die Mitwirkung an ihr entsprechend.

(3) In Ihrem Aufgabenbereich entscheidet die Datenschutzkonferenz durch Beschluss der Mehrheit seiner Mitglieder. Beschlüsse binden die Mitglieder untereinander, entfalten im Übrigen keine Bindungswirkung, dienen nicht dem Schutz Dritter und begründen keine einklagbaren Rechte. Die Datenschutzkonferenz gibt sich eine Geschäftsordnung.

(4) Der Vorsitz der Datenschutzkonferenz informiert die Öffentlichkeit über die Tätigkeit und Beschlüsse der Datenschutzkonferenz nach Maßgabe ihrer Beschlüsse.

(5) Zur organisatorischen Unterstützung der Datenschutzkonferenz wird bei der oder dem Bundesbeauftragten eine Geschäftsstelle eingerichtet, die ebenso wie die Öffentlichkeitsarbeit hälftig vom Bund und von den Ländern nach dem Königsteiner Schlüssel zu finanzieren ist.“

Zu prüfen ist, ob diese Norm auch als **bundesgesetzliche Regelung im BDSG** erlassen werden darf.

1. Gesetz als notwendige und hinreichende Regelungsebene

Die dargelegte erweiterte Kooperation hätte ein verfassungsrechtliches Gewicht, das die **Wesentlichkeitsgrenze** überschreitet. Sie ist somit dem parlamentarischen **Gesetz** vorbehalten und kann damit nicht etwa als Verwaltungsvereinbarung normiert werden.[38] Dies gilt mit Blick auf die Relativierung des finanzverfassungsrechtlichen Trennungsgebots insbesondere auch für die Finanzierung der Kooperation, insbesondere einer einzurichtenden Geschäftsstelle. Allein durch untergesetzliche Abmachung der Beteiligten kann die verfassungsrechtliche Finanzordnung hingegen nicht modifiziert werden.[39]

Hingegen bedarf es **keiner** (zusätzlichen) Anpassung oder **Ergänzung der Verfassung**. Vielmehr beruht das Grundgesetz darauf, dass die verfassungsgemäß konstituierten und für bestimmte Bereiche vorgesehenen staatlichen Organe – wie die Verwaltung von Bund

38 Siehe dazu etwa Maurer/Waldhoff, Allgemeines Verwaltungsrecht, 21. Aufl. 2024, § 6 Rn. 3 ff.

39 Vgl. Siekmann, in: Sachs (Hrsg.), Grundgesetz (Kommentar), 9. Auflage 2021, vor § 104a, Rn. 27.

und Länder – in diesen Bereichen prinzipiell handeln dürfen, soweit sie die jeweils einschlägigen Grenzen des Verfassungsrechts beachten.[40] Das wäre vorliegend in dem Moment der Fall, in dem die Kooperation auf eine Rechtsgrundlage gestellt würde, die dem Wesentlichkeitsgrundsatz Rechnung trägt. Ein darüberhinausgehender, allgemeiner Vorbehalt der Verfassung für Staatstätigkeiten in dem Sinne, dass die staatlichen Organe ohne hinreichend explizite Ermächtigung im GG selbst nicht tätig werden dürfen, besteht nicht.[41] Eine verfassungsrechtliche Grundlage, die eine Kooperation zwischen den Aufsichtsbehörden in der beschriebenen Form einer DSK ausdrücklich zulässt, dürfte erst dann (und ggf. zusätzlich) notwendig werden, wenn man in der beabsichtigten Kooperation nicht nur einen Eingriff in die grundgesetzliche Kompetenzordnung sähe, sondern diesen Eingriff auch und entgegen der obigen Darlegungen nicht für verfassungsrechtlich gerechtfertigt und – auf Grundlage einer unveränderten Verfassung – auch nicht rechtfertigbar hielte.[42] Selbstverständlich würde eine entsprechende Verfassungsergänzung – etwa im Bereich der Art. 91a ff. GG – jedenfalls dazu beitragen, stets verbleibende Rechtsunsicherheiten zu minimieren.[43] Notwendig ist eine Verfassungsänderung nach der hier vorliegenden Bewertung jedoch nicht.

2. Gesetzgebungskompetenz des Bundes

Für die Umsetzung der Regelung als Vorschrift im BDSG müsste dem Bund die dafür notwendige Gesetzgebungskompetenz zustehen. Dabei ist insbesondere zwischen den Regelungen zu verbindlichen Beschlüssen über Auslegungsmaximen, zur Öffentlichkeitsarbeit und zur Einrichtung einer gemeinsamen Geschäftsstelle zu differenzieren.

40 Grzeszick, in: Dürig/Herzog/Scholz (Hrsg.), Grundgesetz-Kommentar, 95. EL 2021, Art. 20 Rn. 58 m.w.N.

41 Grzeszick, in: Dürig/Herzog/Scholz (Hrsg.), Grundgesetz-Kommentar, 95. EL 2021, Art. 20 Rn. 58.

42 Vgl. BVerfGE 98, 218 (246).

43 Dies gilt nicht nur in Hinblick auf die Vollzugskompetenzordnung nach Art. 30, 83 ff, sondern auch die Staatsfinanzierungsvorgaben der Art. 104a ff. GG. So wird auch Art. 91c Abs. 1 GG in Hinblick auf die Einrichtung des IT-Planungsrats nicht als zwingend notwendig erachtet, vgl. Siekmann, in: Sachs (Hrsg.), GG (Kommentar), 9. Aufl. 2021, Art. 91c GG Rn. 6 m.w.N. Anders wohl Kment, in: Jarass/Pieroth (Hrsg.), GG (Kommentar), 16. Aufl. 2020, Art. 91c GG Rn. 1. Dazu auch Gröpl, in: Dürig/Herzog/Scholz (Hrsg.), Grundgesetz-Kommentar, 95. EL 2021, Art. 91 Rn. 18 ff. u. Rn. 27. Zu den Grenzen solcher verfassungsrechtlichen Kooperationsnormen Sommermann, in: v. Mangoldt/Klein/Starck (Hrsg.), GG (Kommentar), 7. Aufl. 2018, Art. 20 Rn. 49.

a. Annexkompetenz zu Art. 23 Abs. 1 S. 2 GG

Gute Gründe sprechen dafür, speziell für die Zusammenarbeit der Aufsichtsbehörden in datenschutzrechtlichen Konkretisierungsfragen eine Gesetzgebungskompetenz wegen der unionsrechtlich vorgegebenen Notwendigkeit der Zusammenarbeit und Abstimmung zwischen den einzelnen Datenschutzaufsichtsbehörden für ein einheitliches Auftreten im unionsweiten Kohärenzverfahren als **Annexkompetenz** zu Art. 23 Abs. 1 S. 2 GG abzuleiten. Nach Art. 23 Abs. 1 S. 2 GG kann der Bund zur Verwirklichung eines vereinten Europas durch Gesetz mit Zustimmung des Bundesrats Hoheitsrechte übertragen.

Bereits die aktuelle Fassung des **§ 18 BDSG** wurde vom Bundesgesetzgeber auf eine solche Annexkompetenz und auf die Kompetenz für auswärtige Angelegenheiten gestützt.[44] Aus der Befugnis des Bundes, Hoheitsrechte auf die Union zu übertragen, folge dessen Befugnis, die Mitwirkung in einer unionsrechtlichen Institution (nämlich des EDSA) zu regeln, die auf der Übertragung von Hoheitsrechten beruhe. Der EDSA übe gerade keine mitgliedstaatliche, sondern eine unionale Verwaltungstätigkeit aus. Der mitgliedstaatliche Vertreter der Aufsichtsbehörden im EDSA habe eine doppelte Funktion als Repräsentant des Mitgliedstaats und als Teil einer unionsrechtlichen Institution. Betroffen sei mit der Vertretung daher die europäische Integration, die Sache des Bundes sei. Dies gelte auch dann, wenn innerstaatlich Länderkompetenzen betroffen seien. Den innerstaatlichen Kompetenzen der Länder sei durch das Zustimmungserfordernis des Bundesrats als institutionelles Element und das Mitwirkungsrecht der Länder an der Beschlussfassung über einen einheitlichen Standpunkt im europäischen Kohärenzverfahren als inhaltliches Element einer „kompetenzschonenden Kooperation“ Rechnung getragen.[45]

Auf die hier in Rede stehende Erweiterung der DSK lässt sich diese Begründung einer Annexkompetenz aus Art. 23 Abs. 1 S. 2 GG i.V.m. der Bundeskompetenz für auswärtige Angelegenheiten teilweise **übertragen**: Denn die DSK soll deshalb mit der Befugnis zur zur inhaltlichen Konkretisierung des Datenschutzrechts mit verbindlicher Wirkung für die Datenschutzaufsichtsbehörden ausgestattet werden, weil die Regulierung des Daten-

44 Zum Folgenden BT-Drs. 18/11325, S. 71.

45 BT-Drs. 18/11325 S. 71 f.

schutzrechts weitgehend auf die Union übertragen wurde, dessen **kohärente Anwendung zu gewährleisten** ist. In einem föderal strukturieren Staat betrifft dies unvermeidlich die *mitgliedstaatlichen* Verwaltungskompetenzen, also die Kompetenzverteilung zwischen Bund und Länder zur Ausführung des Datenschutzrechts in den Art. 30, 83 ff. GG.

Es ließe sich allerdings einwenden, dass es sich bei einer inhaltlichen Beschlussbefassung zur Vorbereitung der Ausführung des Unionsrechts, die letztverantwortlich von den mitgliedstaatlichen Aufsichtsbehörden selbst ausgeübt wird, weder um eine Mitwirkung in einer unionsrechtlichen Institution, die aufgrund vom Bund übertragener Hoheitsrechte geschaffen wurde, noch um eine Vertretung des Bundes in auswärtigen Angelegenheiten handelt. Vielmehr scheint die inhaltliche Konkretisierung unvermeidbare Voraussetzung für den Vollzug des Unionsrechts durch die Mitgliedstaaten zu sein, für dessen Organisation und Verfahren aber die nationale Rechtsordnung, also die grundgesetzliche Kompetenzordnung, gelten würde. Daraus ließe sich wiederum schließen, dass sich für die Erweiterung der DSK eine Annexkompetenz des Bundes nur insoweit aus Art. 23 Abs. 1 S. 2 GG ergibt, als durch die DSK die einheitliche Beschlussfassung für das Kohärenzverfahren und die Vertretung der Bundesrepublik im EDSA gewährleistet wird. Da dies aber gerade nicht vorgesehen ist, sondern die Regelung des § 18 BDSG beibehalten werden soll, bliebe für die hier in Rede stehenden Regelung einer erweiterten DSK keine Kompetenz mehr übrig, die sich aus Art. 23 Abs. 1 S. 2 GG ableiten ließe.

Eine solche Argumentation würde allerdings ausblenden, dass die Beschlüsse der DSK sich auf inhaltliche Fragen der Gesetzeskonkretisierung beziehen, die **sowohl bei der Abgabe eines gemeinsamen Standpunkts im unionsweiten Kohärenzverfahren als auch bei der Ausübung der nationalen Verwaltungskompetenzen relevant werden können**. Eine inhaltliche Differenzierung beider Zweckrichtungen ist zwar theoretisch denkbar, praktisch aber kaum möglich. Dies zeigt sich, wenn man annimmt, die DSK würde zukünftig auch die Positionierung im EDSA entgegen der jetzigen Regelung des § 18 BDSG leisten. Eine Differenzierung könnte dann lediglich nach der Bindungswirkung erfolgen. Gemeinsame Standpunkte im EU-Kohärenzverfahren wären in diesem Fall als bindend für die einzelnen Aufsichtsbehörden bei ihrem Auftreten gegenüber anderen mitgliedstaatlichen Behörden oder Unionseinrichtungen anzusehen, nicht jedoch für ihre Verwaltungstätigkeiten auf nationaler Ebene. Eine solche formale Trennung würde zu der

absurden Situation führen, dass eine solche DSK für ihren gemeinsamen Standpunkt im Kohärenzverfahren eine inhaltliche Konkretisierung der DSGVO-Normen beschließt, die einzelnen Aufsichtsbehörden aber außerhalb des Kohärenzverfahrens eine davon abweichende Auslegung derselben Normen vertreten und anwenden könnten, soweit keine verbindliche Beschlussfassung des EDSA in dieser Sache vorliegt. Dies liefe dem Ziel des VII. Kapitels der DSGVO eklatant zuwider, eine einheitliche Anwendung des Unionsrechts im gesamten Unionsgebiet herzustellen. Die **einheitliche Anwendung des Datenschutzrechts** innerhalb eines Mitgliedstaats muss dagegen als eine Voraussetzung für eine kohärente Anwendung innerhalb der Union angesehen werden. In diesem Sinne kann die kohärente Anwendung des Datenschutzrechts **verständigerweise nicht geregelt** werden, **ohne zugleich die föderale Kooperation der Datenaufsichtsbehörden** in dem dafür notwendigen Maß mit zu regeln.[46]

Der europäische Integrationsprozess im Bereich des Datenschutzrechts – konkretisiert durch die harmonisierten Bestimmungen der DSGVO[47] – setzt voraus, dass die Bestimmungen im Rahmen der nationalen Staatsstrukturen auch möglichst **einheitlich in den Mitgliedstaaten angewendet und vollzogen** werden.[48] Diese unionsweite Kohärenz setzt wiederum die interne Abstimmung und die einheitliche Rechtsanwendung innerhalb eines Mitgliedstaats voraus[49] und lässt sich auf nationaler Ebene am effektivsten durch verbindliche Entscheidungen wenigstens in allgemeinen Auslegungsfragen durch Kooperation mit einem Mindesteingriff in föderale Prinzipien verwirklichen.

Mit anderen Worten: Wenn dem Bund die Kompetenz zusteht, Hoheitsrechte im Bereich des Datenschutzrechts auf die Union zu übertragen und aus der Ausübung dieser unionalen Regelungskompetenz für die Mitgliedstaaten verbindliche (Ziel-)Vorgaben der Ko-

46 Vgl. zu den insoweit erhöhten, hier aber gut zu begründenden Voraussetzungen für eine Bundeskompetenz aus Art. 23 Abs. 1 S. 2 GG BVerfGE 106, 62 (115). Kritisch Martini/Botta, DÖV 2022, S. 605 (609, mit Fn. 52).

47 Vgl. EG 2 u. 3 DSGVO.

48 Vgl. zum Harmonisierungsbedarf als Anlass zur Reform des europäischen Datenschutzrechts, Albrecht, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht (Kommentar), 2019, Einl. Rn. 186.

49 Vgl. EG 135 S.1 i.V.m. EG 119 DSGVO.

operation und Kohärenz (Art. 51 Abs. 3, 60 ff. DSGVO) zur Gewährleistung eines gleichwertigen Grundrechtsniveaus in den Mitgliedstaaten und des freien Verkehrs personenbezogener Daten in der Union folgen (EG 123 S. 1 DSGVO), folgt daraus auch die **Kompetenz**, die dazu **notwendigen innerstaatlichen Verfahren** der Kooperation und Abstimmung **zu regeln**. Dies entspricht auch dem vorrangigen Ziel der DSGVO, das unter Geltung der DSRL deutlich hervorgetretene Vollzugsdefizit zu beheben,[50] indem vor allem die **verfahrens- und vollzugsrechtlichen Bestimmungen** angepasst und erweitert werden, während die inhaltlichen Vorgaben nur geringe Änderungen erfahren haben.[51] Das gesamte VII. Kapitel der DSGVO mit den Regelungen zur Zusammenarbeit der mitgliedstaatlichen Aufsichtsbehörden bis hin zum Kohärenzverfahren, das Verbindlichkeit herstellt, trägt diesem Anliegen Rechnung.

Eine gesetzliche Aufgaben- und Befugniszuweisung an die DSK, verbindliche Beschlüsse über Auslegungsmaximen und Stellungnahmen zu Angelegenheiten des Datenschutzes zu fassen, kann also umfänglich auf eine Bundeskompetenz als Annex zu Art. 23 Abs. 1 S. 2 GG gestützt werden, und zwar auch, soweit sie sich nicht nur auf die **Auslegung der DSGVO**, sondern **auch** des **Datenschutzrechts des Bundes und der Länder** erstreckt. Denn Art. 23 Abs. 1 S. 2 GG erfasst die Hoheitsrechte der Bundesrepublik ungeachtet ihrer jeweiligen föderalen Verankerung und damit insbesondere auch – wie dies Art. 23 Abs. 6 GG erkennbar voraussetzt – die öffentliche Gewalt im Kompetenzbereich der Länder.[52] Diese kompetenzielle Reichweite ist mit Blick auf die zentrale Aufgabe, die eine in ihrer Kooperation erweiterte DSK erfüllen soll, nämlich einheitliche Auslegungsmaximen und Stellungnahmen zu Angelegenheiten des Datenschutzes herauszugeben, auch sachlich geboten. Bereits die Abgrenzung von rein unionsrechtlichem Datenschutzrecht und solchem des Bundes und der Länder wäre zwar formal anhand der jeweiligen Rechtakte vorstellbar, mit Bezug auf die Sachregelung aber im Einzelnen schwierig und typischerweise nicht trennscharf möglich.

50 Albrecht, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht (Kommentar), 2019, Einl. Rn. 209.

51 Albrecht, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht (Kommentar), 2019, Einl. Rn. 212 ff.

52 Jarass, in: ders./Pieroth (Hrsg.), GG (Kommentar), 18. Aufl. 2024, Art. 23 Rn. 22.

Die DSGVO setzt einen harmonisierten Rechtsrahmen für das Datenschutzrecht, der zahlreiche Öffnungsklauseln vorsieht und jedenfalls in diesen Bereichen erst durch ergänzende Vorschriften des nationalen Rechts vervollständigt wird. Ergibt sich die Rechtslage in einem konkreten Anwendungsbereich erst aus dem **Zusammenspiel von unionsrechtlichen und nationalen Rechtsvorschriften**, stellt sich regelmäßig die Frage, ob es sich um Datenschutzrecht der Union oder des Bundes bzw. der Länder handelt. So normiert beispielsweise § 4 BDSG für die Videoüberwachung im öffentlichen Raum eine besondere Rechtsgrundlage. Ob diese Regelung im Anwendungsbereich des Unionsrechts nur die Videoüberwachung durch öffentliche Stellen erfasst, muss anhand einer unionsrechtskonformen Auslegung danach beantwortet werden, inwieweit sie auf eine Öffnungsklausel der DSGVO gestützt werden kann.[53] Eine Aussage über den Anwendungsbereich der bundesgesetzlichen Regelung setzt folglich eine Auslegung der entsprechenden Öffnungsklauseln des Unionsrechts voraus. Die Frage, welche datenschutzrechtlichen Anforderungen an eine nach § 4 BDSG zulässige Videoüberwachung zu stellen wären, müsste ebenfalls anhand der Vorgaben der DSGVO einerseits und den einschlägigen ergänzenden Vorschriften des BDSG und des jeweiligen Landesrechts andererseits beantwortet werden. Das Beispiel veranschaulicht, dass bei einer anwendungsbezogenen Konkretisierung des Datenschutzrechts, wie sie von den Aufsichtsbehörden bereitgestellt und durch die Abstimmung in der DSK vorbereitet werden soll, regelmäßig Normen des Unionsrechts verzahnt mit solchen des Bundes- oder Landesrechts anwendbar sein werden. Die Zuordnung von Auslegungsfragen als solche des Unionsrechts oder des Bundes- oder Landesrechts ist in diesen Fällen nicht eindeutig durchführbar.

Folgerte man daraus eine Beschränkung von DSK-Beschlüssen unter dem BDSG auf Stellungnahmen zu Angelegenheiten des Datenschutzrechts, die sich allein auf die unionsrechtlichen Rahmenvorgaben und damit nur einen Teil der einschlägigen Rechtsvorgaben bezögen, stellten solche Beschlüsse kaum taugliche Konkretisierungen für die Praxis bereit. Sie verfehlten damit einen zentralen Zweck der Aufgaben der DSK und der Ziele der DSGVO, die Rechtssicherheit für Verantwortliche, Auftragsverarbeiter und letztlich auch Betroffene zu verbessern. Es ist daher geboten, die innerstaatliche Abstimmung

53 Vgl. hierzu Frenzel, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG (Kommentar), 3. Aufl. 2021, § 4 Rn. 5.

auch auf das Bundes- und Landesdatenschutzrecht zu erstrecken, um eine einheitliche Anwendung des Datenschutzrechts im Bundesgebiet zu fördern und damit dem allgegenwärtigen Vollzugsdefizit entgegenzuwirken. Den Kompetenzen der Länder würde ebenso wie bei der gegenwärtigen Regelung durch die Zustimmungspflicht des Bundesrats für ein entsprechendes Bundesgesetz institutionell und inhaltlich durch die gleichwertige Mitwirkung der Länder und des Bundes an den Beschlüssen der DSK Rechnung getragen.

b. Hilfsweise: Verwaltungskompetenzen aus Art. 83 ff. GG oder Gesetzgebungszuständigkeiten aus Art. 70 ff. GG

Hilfsweise lassen sich Regelungskompetenzen des Bundes entweder aus den Ingerenzrechten des Art. 84 Abs. 1 GG (dazu a) oder aus dem Sachzusammenhang zu den konkurrierenden Gesetzgebungszuständigkeiten des Art. 74 Abs. 1 GG (dazu b) ableiten – allerdings im Vergleich zur Kompetenz aus Art. 23 Abs. 1 S. 2 GG jeweils **nur mit Einschränkungen**.

aa. Ingerenzrechte des Bundes aus Art. 84 Abs. 1 S. 2 Hs. 2 u. S. 5 GG

Zur Normierung der gemeinsamen verbindlichen Beschlussfassung über Auslegungsmaximen und Stellungnahmen ergibt sich das Gesetzgebungsrecht aus Art. 84 Abs. 1 S. 2 Hs. 1 GG. Die Bundeskompetenz erstreckt sich allerdings nur auf die Ausführung von Bundesrecht durch die Länder. **Als Gegenstand der Beschlussfassung** könnte daher nur Unionsrecht und Bundesrecht, **nicht Landesrecht** festgelegt werden. Zu beachten sind außerdem das Abweichungsrecht der Länder aus Art. 84 Abs. 1 S. 2 Hs. 2 GG und die Rück-Abweichungskompetenz des Bundes aus Art. 84 Abs. 1 S. 5 GG. Ein Verfahren der Öffentlichkeitsarbeit innerhalb der DSK ebenfalls auf Art. 84 Abs. 1 S. 2 Hs. 1 GG unter Beachtung der Abweichungskompetenzen aus Art. 84 Abs. 1 S. 2 Hs. 2 u. S. 5 GG gestützt werden. Aufgrund der Bundeskompetenz aus Art. 84 Abs. 1 S. 2 Hs. 1 GG kann eine gemeinsame **Geschäftsstelle nur als Einrichtung der Landesverwaltung** geschaffen werden. Für die Einrichtung einer Geschäftsstelle in Anbindung an den BfDI besteht keine Kompetenz des Bundes aus Art. 84 Abs. 1 GG.

bb. Gesetzgebungszuständigkeiten des Bundes kraft Sachzusammenhang zu Art. 74 Abs. 1 GG

Soweit man Art. 23 Abs. 1 S. 2 GG nicht für eine tragfähige Kompetenzgrundlage des Bundes ansieht und auch die Ingerenzrechte des Bundes aus Art. 84 Abs. 1 GG nicht für maßgeblich hält,[54] lässt sich eine Regelungskompetenz – allerdings ebenfalls nur mit Einschränkungen – aus den Gesetzgebungszuständigkeiten des Bundes nach Art. 70 ff. GG ableiten, wenn man die gesetzliche, verwaltungsbezogene Ausgestaltung der DSK gleichsam als (materielles) Datenschutzrecht begreift.

Zwar weist das Grundgesetz dem Bund die Gesetzgebungsbefugnis für das Datenschutzrecht nicht ausdrücklich zu. Allerdings lassen sich viele dem Bund etwa in den Art. 73 f. GG zugewiesene Sachmaterien häufig nicht sinnvoll regeln, ohne zugleich das Datenschutzrecht mitzuregeln. Für den Bereich der **privaten Datenverarbeitung** wird die Kompetenz des Bundes auf den **Sachzusammenhang zum bürgerlichen Recht, Recht der Wirtschaft und der Arbeit** gestützt, die ihm gem. Art. 74 Abs. 1 Nr. 1, Nr. 11 und Nr. 12 GG in konkurrierenden Gesetzgebungszuständigkeit zugewiesen sind. Hierauf ließe auch die weiterentwickelte DSK stützen, soweit sie mit ihren erweiterten Befugnissen im Bereich der privaten Datenverarbeitung tätig wird.[55]

Hingegen lässt sich eine Tätigkeit der DSK im den öffentlichen Datenverarbeitungsbereich nicht mehr auf die Gesetzgebungszuständigkeiten der Art. 70 ff. GG stützen.[56] Eine gesetzliche Normierung im BDSG müsste daher den **öffentlichen Datenverarbeitungsbereich von Zuständigkeit der DSK ausnehmen**. Am Maßstab der Art. 70 ff. GG stellt sich die Regelung der Datenverarbeitung durch staatliche Stellen als originäre Kompetenz der Länder dar. Der Bund kann grundsätzlich nur für seine eigenen öffentlichen Stellen Vorgaben erlassen, für öffentliche Stellen der Länder hingegen lediglich insoweit, als sie Bundesgesetze ausführen. Die entsprechende Lücke wäre durch einen Staatsvertrag zu schließen.

---

54 So wohl Martini/Botta, DÖV 2022, S. 605 (608 f.). Zum grundlegenden, verfassungsrechtlich ungeklärten Verhältnis zwischen den Verwaltungskompetenzen der Art. 83 ff. GG und den Gesetzgebungskompetenzen der Art. 70 ff. GG s. Trute, in: v. Mangoldt/Klein/Starck (Hrsg.), GG (Kommentar), 7. Aufl. 2018, Art. 83 Rn. 13.

55 Dazu Martini/Botta, DÖV 2022, S. 605 (608 f.) m.w.N. Siehe auch § 40 BDSG.

56 Zum Folgenden Martini/Botta, DÖV 2022, S. 605 (609) m.w.N.

3. Zusammenfassung

*Die Erweiterung der DSK mit den Aufgaben und Befugnissen einer (intern) verbindlichen gemeinsamen Beschlussfassung über Auslegungsmaximen und Stellungnahmen zu Angelegenheiten des Datenschutzes, einer gemeinsamen Öffentlichkeitsarbeit und zur Einrichtung einer Geschäftsstelle ist verfassungsrechtlich so gewichtig, dass sie auf der **Ebene des Gesetzes** normiert werden müsste.*

*Für eine Regelung im BDSG könnte sich der Bund auf eine **Annexkompetenz zu Art. 23 Abs. 1 S. 2 GG** mit Blick auf die Notwendigkeit eines innerstaatlichen Abstimmungsverfahrens der Datenschutzaufsichtsbehörden stützen, um die unionsrechtlich vorgegebenen Ziele der einheitlichen Anwendung des Datenschutzrechts und eines effektiven Vollzugs bestmöglich zu fördern.*

***Hilfsweise** ergibt sich eine Regelungskompetenz des Bundes aus den Ingerenzrechten des **Art. 84 Abs. 1 GG** oder aus den Gesetzgebungszuständigkeiten des Bundes kraft Sachzusammenhangs zu Art. 74 Abs. 1 GG. Die Bundeskompetenz erstreckt sich dann allerdings nur auf die Ausführung von Bundesrecht durch die Länder, so dass als Gegenstand der Beschlussfassung nur Unionsrecht und Bundesrecht, **nicht Landesrecht** bzw. der öffentliche Datenverarbeitungssektor festgelegt werden dürfte. Zudem bestünde für **die Einrichtung einer Geschäftsstelle keine Kompetenz** des Bundes.*

B. Einführung einer Regelung zur biometrischen Gesichtserkennung

Im Koalitionsvertrag 2021-2025 (S. 18 u. 109) haben sich die regierungstragenden Parteien zur Aufgabe gemacht:

> *„Biometrische Erkennung im öffentlichen Raum […] sind europarechtlich auszuschließen. […]. […] und den Einsatz von biometrischer Erfassung zu Überwachungszwecken lehnen wir ab. Das Recht auf Anonymität […] im öffentlichen Raum […] ist zu gewährleisten.“*

In der Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz – KI-VO) wurde die Verwendung biometrischer Identifizierungssysteme reguliert, ohne ihren Einsatz vollständig oder jedenfalls im öffentlichen Raum auszuschließen. Es stellt sich daher die Frage, ob und inwieweit ein Verbot biometrischer Gesichtserkennung durch staatliche und private Akteure im öffentlichen Raum bundesgesetzlich – etwa im BDSG

– unter Wahrung der verfassungsrechtlichen und europarechtlichen Grenzen normiert werden kann.

Dazu soll zunächst kursorisch auf den Stand der technischen Entwicklung biometrischer Gesichtserkennung sowie auf die Zwecke, Möglichkeiten und Risiken ihres Einsatzes durch private und staatliche Akteure eingegangen werden (dazu I). Im Anschluss sind anhand einer gedachten Verbotsnorm (dazu II) die europarechtlichen (dazu III) und die verfassungsrechtlichen Grenzen (dazu IV) für ein bundesgesetzliches Verbot der biometrischen Gesichtserkennung zu bestimmen, um abschließend aus verfassungsrechtlicher Perspektive auf Bedarf und Gebotenheit einer solchen Regelung (dazu V) einzugehen. Die Ergebnisse werden abschließend zusammengefasst und mit einem beispielhaften Regelungsvorschlag *für das BDSG* ergänzt (dazu VI).

I. Biometrische Gesichtserkennung – Stand der technischen Entwicklung und Zwecke, Möglichkeiten und Risiken ihres Einsatzes

Bei der biometrischen Gesichtserkennung handelt es sich um eine automatisierte Verarbeitung von digitalen Bildern, die Gesichter von natürlichen Personen enthalten, um bei diesen eine Identifizierung, Authentifizierung oder Kategorisierung durchzuführen.[57] Im hiesigen Kontext wird im Wesentlichen die biometrische Gesichtserkennung als die Form von Technologie betrachtet, die ein **menschliches Gesicht aus einem digitalen Bild erkennt** und extrahieren kann, um es dann vor allem mit Datenbanken oder –beständen zuvor identifizierter Gesichter **abzugleichen**.[58] Dies kann sowohl in Echtzeit als auch retrograd erfolgen. Der Echtzeit-Abgleich charakterisiert sich dadurch, dass die Erfassung biometrischer Daten ohne eine erhebliche Verzögerung erfolgt. Dies umfasst die sofortige Identifizierung sowie die Identifizierung mit zeitlich begrenzten kurzen Verzögerungen. Alle weiteren Einsatzformen biometrischer Gesichtserkennung werden der Ex-post-Fernidentifizierung zugewiesen. So werden also entweder unverzüglich oder im Nachhinein durch mathematische Berechnungen einer Erkennungssoftware Vergleiche von

57 Artikel-29-Datenschutzgruppe, Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten, 2012, S. 2, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_de.pdf [11.06.2024].

58 Hahn, Die Regulierung biometrischer Fernidentifizierung in der Strafverfolgung im KI-Verordnungsentwurf der EU-Kommission, ZfDR 2023, S. 142.

zuvor gespeicherten Gesichtsbildern mit videografierten Gesichtsbildern angestellt. Die die Gesichtsbilder verarbeitende Software unterscheidet dabei nach charakteristischen Eigenschaften der Gesichter, bildet diese in einem sog. Template ab und macht sie dadurch mathematisch vergleichbar. Hierbei werden die einen Menschen identifizierenden Merkmale des Gesichtsbereichs, wie seine Augenhöhlen, Wangenknochen, Ohren, Nase, Mund oder Kinn durch die Software lokalisiert und anschließend mittels algebraischer Verfahren in Merkmalsdaten codiert. Die dabei generierten Templates werden anschließend mittels mathematischer Algorithmen kombiniert. Abschließend wird durch die Software eine Berechnung zum Grad der Ähnlichkeit der untersuchten Gesichtsbilder angestellt. Abhängig von der konkreten Gestaltung der Erkennungssoftware, des verwendeten Verfahrens zur Mustererkennung und seiner Toleranzgrenzen wird ein Resultat ausgegeben, welches eine Einstufung vornimmt, inwiefern die überprüften Gesichtsbilder in ihren Identifikationsmerkmalen übereinstimmen oder nicht übereinstimmen.[59]

Bei der biometrischen Gesichtserkennung handelt es sich um eine **vergleichsweise junge Technologie**. Unter anderem wird der Einsatz von Gesichtserkennungssoftware in Deutschland seit 2002 durch das Bundesamt für Sicherheit in der Informationstechnik untersucht. So wurden beispielsweise Verfahren der Gesichtserkennung im praktischen Einsatz in Bezug auf den Einsatz von Personaldokumenten betrachtet.[60] Ferner werden weltweit Gesichtserkennungssysteme durch Akteure der Wirtschaft und staatlicher Institutionen erprobt und in Betrieb genommen. Auf staatlicher Seite ist etwa das Pilotprojekt „Sicherheitsbahnhof Berlin Südkreuz“ der Deutsche Bahn AG in Kooperation mit der Bundespolizei und dem Bundesministerium des Innern und für Heimat zu nennen, aber auch Projekte wie EasyPASS, das (teil-)automatisierte Grenzkontrollen an deutschen Flughäfen ermöglicht[61] oder das Gesichtserkennungssystem des Bundeskriminalamtes (GES),

59 Bundesamt für Sicherheit in der Informationstechnik, Biometrische Verfahren, Gesichtserkennung, abrufbar unter www.bsi.bund.de [11.06.2024].

60 Bundesamt für Sicherheit in der Informationstechnik, Projektreihe BioP, abrufbar unter www.bsi.bund.de [11.06.2024].

61 EasyPASS-Registered Traveller, www.easypass.de [11.06.2024].

welches seit 2008 im Einsatz ist.[62] Auch auf Seiten **privater Akteure** werden Einsatzmöglichkeiten biometrischer Gesichtserkennung erprobt oder betrieben. Amazon.com, Inc. bietet mit seinem Produkt „Amazon Rekognition“ eine Gesichtserkennungssoftware an, die für die Gesichtsanalyse oder die Suche nach Gesichtern zur Verifizierung und zur Identifizierung von Personen verwendet wird.[63] Ebenso forschte der Konzern Meta an dem open source Modell „DeepFace“, einer Erkennungssoftware, die Gesichter in Digitalen Bildern erkennen und feststellen soll, ob die verglichenen Gesichter identisch sind oder nicht. Dabei soll die Software eine Genauigkeit von 97,35 Prozent erreichen.[64] Nicht zuletzt nutzen bereits eine Vielzahl an Bürgerinnen und Bürger Deutschlands bewusst oder unbewusst biometrische Gesichtserkennungssoftware über ihre elektronischen Endgeräte wie den Privaten- oder Arbeitscomputer sowie das Smartphone. Hierbei werden die verschiedenen Erkennungssoftware-Produkte wie „FaceID“ der Apple Inc. oder „Windows Hello“ der Microsoft Corporation dafür verwendet, um mittels des Gesichts der nutzenden Person das Endgerät zu entsperren oder die Sicherheitstechnologie der Zwei-Faktorauthentifizierung bei digitalen Einkäufen oder dem Online-Banking zu nutzen.[65] Nicht zuletzt erreichte die biometrische Gesichtserkennung mediale Aufmerksamkeit, als private Personen mittels der frei verfügbaren Gesichtserkennungssoftware „PimEyes“ den Aufenthaltsort einer zur Fahndung ausgeschriebene RAF-Terroristin erfolgreich ermittelten und dadurch die Strafverfolgungsbehörden in die Lage versetzten, die gesuchte Person festzunehmen.[66]

Staatliche Akteure nutzen die biometrische Gesichtserkennung, um die **öffentliche Sicherheit** zu erhöhen, da die Technologie es ermöglicht, Personen in Echtzeit zu identifizieren oder zu überwachen. An öffentlichen Orten wie Bahnhöfen, Flughäfen oder Stadien könnte die Gesichtserkennung folglich dazu beitragen, potenzielle Gefahren frühzei-

62 Bundeskriminalamt, Gesichtserkennungssystem (GES), https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Erkennungsdienst/erkennungsdienst_node.html, [11.06.2024].

63 Amazon.com, Inc., Amazon Rekognition, https://aws.amazon.com/de/rekognition/, [11.06.2024]

64 Facebook AI Research, DeepFace: Closing the Gap to Human-Level Performance in Face Verification, 2014, abrufbar unter research.facebook.com [12.06.2024].

65 Apple Inc., About Face ID Advanced technology, support.apple.com/en-us/102381 [12.06.2024]

66 Verfassungsblog.de, PimEyes User auf den Spuren der RAF, verfassungsblog.de/pimeyes-user-auf-raf-spuren [12.06.2024].

tig zu erkennen und gegebenenfalls zu verhindern. Ebenso könnte Gesichtserkennungstechnologie z.B. die Verfahren an Grenzübergängen beschleunigen, indem Reisende automatisch identifiziert werden und manuelle Kontrollen verringert werden. Des Weiteren könnte die Gesichtserkennung die Strafverfolgung **unterstützen**, da Verdächtige schneller identifiziert oder aufgespürt werden würden. **Unternehmen** hingegen nutzen Gesichtserkennungssoftware zur **Sicherung ihrer Einrichtungen**, indem die Software bei der Zugangskontrolle zu sensiblen Bereichen verwendet wird. Vorstellbar ist ebenso, dass der Einsatz von Gesichtserkennungssoftware es Unternehmen ermöglicht **Geschäftsprozesse zu optimieren**, indem Kunden analysiert werden, um personalisierte Angebote zu erstellen und das Einkaufserlebnis zu verbessern. Ferner wird durch die Verwendung von Gesichtserkennung potentiell Kundenzufriedenheit generiert, da sichere, schnelle und unkomplizierte Lösungen zur Identifikation bei Transaktionen geschaffen werden können. Bei weiterer Forschung im Bereich biometrischer Gesichtserkennung sind so weitere Potentiale für zukünftige Anwendungen zu erwarten, wovon sowohl staatliche als auch private Akteure profitieren würden.

Der Verwendung biometrischer Gesichtserkennung werden aber auch **Gefahren und Risiken** für Bürgerinnen und Bürger zugeschrieben. Gesichter in Echtzeit oder ex-post zu erkennen und über Kameras zu verfolgen, könnte eine weitere **Ausleuchtung der Privatsphäre** bedeuten, da die so überwachten Personen ohne ihr Wissen oder Zustimmung überwacht und deren sensiblen personenbezogenen Daten in Form von Gesichtsmerkmalen gespeichert und verarbeitet werden.[67] Weiterhin wird darauf hingewiesen, dass Gesichtserkennungssysteme aufgrund einer unzureichenden Basis an Trainingsdaten zu **diskriminierenden Ergebnissen** führen könnten. Das National Institute of Standards and Technology (NIST) fand in seiner Studie „Face Recognition Vendor Test (FRVT)" heraus, dass die Fehlerquoten je nach ethnischer Herkunft und Geschlecht stark variieren. Eine Vielzahl an überprüften Systemen zeigten höhere **Fehlerquoten** bei der Identifikation von Personen mit dunkler Hautfarbe im Vergleich zu Personen mit helleren Hauttönen.[68]

67 IEEE Transactions on Information Forensics and Security, Privacy–Enhancing Face Biometrics: A Comprehensive Survey, 2021

68 NIST Interagency/Internal Report (NISTIR) – 8280, 2019, www.nist.gov/publications/face-recognition-vendor-test-part-3-demographic-effects [13.06.2024].

II. Fortgang der Prüfung anhand einer gedachten Verbotsnorm

Mit ihrem Koalitionsvertrag haben sich die regierungstragenden Parteien zur Aufgabe gemacht, die biometrische Gesichtserkennung im öffentlichen Raum sowie zu Überwachungszwecken auszuschließen. Hieran ansetzend könnte eine **denkbare Verbotsnorm** könnte lauten:

> *„Biometrische Gesichtserkennung im öffentlichen Raum sowie zur Überwachung ist verboten.“*

Um die für den Bundesgesetzgeber bestehenden europa- und verfassungsrechtlichen Grenzen hervortreten zu lassen, wird im Folgenden geprüft, ob und unter welchen Voraussetzungen und Modifikationen eine solche gedachte, die Zielsetzung des Koalitionsvertrags ausschöpfende Verbotsnorm mit den europa- (dazu III) und verfassungsrechtlichen (dazu IV) Vorgaben vereinbar wäre.

Dabei ist auf folgende **begriffliche Differenzierung** hinzuweisen, die sich im Fortgang als strukturbildenden und auch rechtssystematisch als zentral erweist. So setzt die vorstehende Verbotsnorm an der biometrischen Gesichtserkennung im Sinne einer *Tätigkeit* an. Im Vergleich dazu knüpft die KI-VO im Sinne einer Technikregulierung vorrangig an Systemen, also an *Mitteln oder Instrumenten* an, erweitert ihren Bezugspunkt aber auch auf den Umgang bzw. die Tätigkeit mit diesen Mitteln (vgl. Art. 1 lit. a KI-VO: „Inverkehrbringen, Inbetriebnahme und Verwendung von Systemen“). Das Datenschutzrecht wiederum knüpft in erster Linie an Daten, in diesem Sinne also an die *Ergebnisse* oder den *Gegenstand* einer Tätigkeit an, bezieht dabei aber regulativ ebenfalls die Tätigkeit mit ein (vgl. Art. 1 Abs. 1 DSGVO: „Verarbeitung personenbezogener Daten“).

III. Europarechtliche Grenzen zur Regulierung durch den Mitgliedstaat

Zu prüfen ist zunächst, ob eine bundesgesetzliche Verbotsregelung europarechtliche Grenzen verletzen würde. Solche Grenzen können sich zum einen in Hinblick auf die Regelungskompetenz der Mitgliedstaaten ergeben (dazu 1), zum anderen in Hinblick auf die Verletzung europarechtlicher Grundfreiheiten und Grundrechte (dazu 2).

1. Regulierungskompetenz der Mitgliedstaaten

Die Regelung einer Verbotsnorm durch den Bundesgesetzgeber scheitert nicht daran, dass den Mitgliedstaaten europarechtlich keine Kompetenz (mehr) zur Regelung der biometrischen Gesichtserkennung zustünde. Die Regelungskompetenz der Bundesrepublik Deutschland als Mitgliedstaat gründet sich im Ausgangspunkt auf deren **staatliche Souveränität**, wird allerdings in dem Maße eingeschränkt, in dem sie gem. Art. 23 Abs. 1 S. 2 u. 3 GG Hoheitsrechte auf die EU überträgt. In der Folge laufen die deutschen Regulierungskompetenzen leer, soweit die **EU von den ihr übertragenen Kompetenzen durch Regelungen Gebrauch gemacht hat**, die (wie etwa EU-Verordnungen nach Art. 288 Abs. 2 AEUV) in den Mitgliedstaaten unmittelbar gelten.[69] Jedenfalls gehen die europarechtlichen den mitgliedstaatlichen Regelungen in der Anwendung vor, soweit letztere über die Grenzen hinausgehen, die die europarechtlichen Regeln den Mitgliedstaaten ziehen.[70]

Soweit ersichtlich, hat die EU keine spezifischen Regelungen zur biometrischen Gesichts*erkennung*, mit der **DSGVO** und der Richtlinie (EU) 2016/680 – sog. **JI-RL** – sehr wohl aber Regelungen zur Verarbeitung *biometrischer Daten* erlassen. Zudem hat sie jüngst auf Grundlage von Art. 114 und Art. 16 Abs. 2 AEUV die **KI-VO** erlassen und dort konkrete Vorschriften zum Umgang mit Systemen Künstlicher Intelligenz (KI-Systeme) statuiert, die auch *KI-Systeme* zur Erstellung von Datenbanken zur Gesichtserkennung sowie *KI-Systeme* zur biometrischen Fernidentifizierung erfassen, soweit diese insbesondere in öffentlich zugänglichen Räumen und in Echtzeit für Zwecke der Strafverfolgung eingesetzt werden sollen (vgl. insbes. Art. 5 Abs. 1 lit. e u. h, Abs. 2 bis 7 KI-VO). Indem sie so von den ihr zustehenden Kompetenzen wirksam[71] Gebrauch gemacht hat, hat sie

69 Rozek; in: v. Mangoldt/Klein/Starck (Hrsg.), GG (Kommentar), 7. Aufl. 2018, Art. 70 Rn. 10; Jarass/Pieroth, Art. 70 Rn. 11.

70 Zur Unterscheidung von Anwendungs- und Geltungsvorrang des EU-Recht s. Rozek; in: v. Mangoldt/Klein/Starck (Hrsg.), GG (Kommentar), 7. Aufl. 2018, Art. 23 Rn. 47.

71 Es werden allerdings Bedenken angemeldet, dass die EU die ihr übertragenen Kompetenzen beim Erlass der KI-VO überschritten habe. Gemäß Artikel 114 AEUV steht der EU die Kompetenz zu, Maßnahmen für die Errichtung und das Funktionieren des Binnenmarkts vorzusehen. Zudem begründet Artikel 16 Abs. 2 AEUV die Kompetenz der EU, Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten zu erlassen, die in den Anwendungsbereich des Unionsrechts fallen. Für die sich vorliegend stellende Frage der verbleibenden Regulierungskompetenz wirken sich die Bedenken allerdings nicht aus, solange sie nicht zur Rechtsunwirksamkeit der KI-VO führen.

notwendig in einem gewissen Maße auch die biometrische Gesichtserkennung geregelt und die Mitgliedstaaten in ihrer diesbezüglichen Regulierungskompetenz spiegelbildlich eingeschränkt. Die insoweit zentralen Grenzziehungen für die verbleibende mitgliedstaatliche Regulierungskompetenz folgen vor allem aus Art. 5 KI-VO (dazu a und b) und Art. 6 ff. KI-VO (dazu c) sowie aus den Vorschriften der DSGVO und der JI-RL (dazu d). Sie belassen den Mitgliedstaaten eine Kompetenz für die (weitere) regulative Ausgestaltung der biometrischen Gesichtserkennung, die – wie nachfolgend ausgeführt wird – auch die Möglichkeit eines weitgehenden Verbotes tragen würde.

a. Grenzen des Art. 5 Abs. 1 lit. d KI-VO

Art. 5 KI-VO nimmt den Mitgliedstaaten nicht die Kompetenz, den Einsatz biometrischer Gesichtserkennung unter Beachtung seiner Festlegungen weiter zu regulieren. Art. 5 KI-VO verbietet bestimmte Praktiken im Bereich der Künstlichen Intelligenz und ist als Verbotsnorm mit Ausnahmen ausgestaltet, die den Spielraum des nationalen Gesetzgebers zwar beschränkt, aber nicht ausschließt. Insbesondere ein an den nationalen Gesetzgeber gerichtetes Gebot für den Einsatz bestimmter KI-Systeme – oder umgekehrt ein Verbot, solche Systeme zu verbieten – kann Art. 5 KI-VO nicht entnommen werden.

Ähnlich wie die JI-RL verfolgt auch die KI-VO einen risikobasierten Ansatz. Auf der höchsten Risikostufe stehen hierbei die in **Art. 5 Abs. 1** lit. a bis d KI-VO beschriebenen **Praktiken**, die wegen der mit ihnen einhergehenden unvertretbaren Risikos **grundsätzlich verboten** sind. Zu diesen gehört gem. **lit. d** auch die Verwendung biometrischer Fernidentifizierungssysteme, sofern diese in Echtzeit in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken erfolgt. Allerdings sieht lit. d unter i bis iii Ausnahmen von diesem Verbot vor. Soweit das so konturierte Verbot reicht, ist die Regulierungskompetenz der BRD als Mitgliedstaat und damit auch des Bundes entsprechend ausgeschlossen.

aa. Biometrische Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen

Der Begriff der **Strafverfolgung** in Art. 5 Abs. 1 lit. d KI-VO ist weit zu verstehen und umfasst nicht nur die repressivpolizeiliche Tätigkeit, sondern **auch die Gefahrenabwehr** im Sinne des deutschen Polizeirechts. Dies zeigt nicht nur die Begriffsbestimmung in Art.

3 Abs. 46 KI-VO, sondern auch Art. 5 Abs. 1 lit. d. iii KI-VO, der als Zulässigkeitsvoraussetzung die Abwendung einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder eines Terroranschlags und damit eine klassische präventivpolizeiliche Tätigkeit normiert. Dem entspricht die systematische Nähe der KI-VO zur JI-RL, der ebenfalls und unstrittig ein weiter Strafverfolgungsbegriff zu Grunde liegt.

Den Begriff der **Fernidentifizierung in Echtzeit** i.S.v. Art. 5 Abs. 1 lit. d KI-VO regelt Art. 3 Nr. 37 KI-VO. Ein biometrisches Echtzeit-Fernidentifizierungssystem ist hiernach ein biometrisches Fernidentifizierungssystem, bei dem die Erfassung biometrischer Daten, der Abgleich und die Identifizierung ohne erhebliche Verzögerung erfolgen, wobei dies zur Vermeidung einer Umgehung der Vorschriften nicht nur die sofortige Identifizierung umfasst, sondern auch eine Identifizierung mit begrenzten kurzen Verzögerungen.

Unter einem **öffentlich zugänglichen Raum** i.S.v. Art. 5 Abs. 1 lit. d KI-VO ist schließlich gemäß Art. 3 Nr. 39 KI-VO ein der Öffentlichkeit zugänglicher physischen Ort zu verstehen, unabhängig davon, ob für ihn bestimmte Zugangsbedingungen gelten.

bb. Ausnahmen vom grundsätzlichen Verbot

Die in Art. 5 Abs. 1 lit. d i bis iii KI-VO normierten Fälle sind als Ausnahmen vom grundsätzlichen Verbot des Art. 5 Abs. 1 lit. d KI-VO zu lesen und beziehen sich auf Fälle, in denen das **öffentliche Interesse an einer effizienten Strafverfolgung bzw. Gefahrenabwehr** das Interesse der von einer Maßnahme gem. Art 5 Abs. 1 lit. d KI-VO möglicherweise betroffenen Personen am Schutz ihrer Rechte **überwiegt**.

Aus diesen Ausnahmen vom grundsätzlichen Verbot des Art. 5 Abs. 1 lit. d KI-VO lässt sich jedoch **kein** an die Mitgliedstaaten gerichtetes **Gebot** ableiten, Systeme der biometrischen Gesichtserkennung in den von den Ausnahmen umfassten Fällen auch **einzusetzen**. Der mit Art. 5 Abs. 1 KI-VO in engem Zusammenhang zu lesende Abs. 4 zeigt verdeutlicht, dass die KI-VO den Mitgliedstaaten lediglich die Möglichkeit gewährt, eine vollständige oder teilweise Genehmigung der Verwendung biometrischer Echtzeit-Identifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken innerhalb der in Art. 5 Abs. 1 lit. d, Abs. 2 und Abs. 3 KI-VO aufgeführten Grenzen und unter den dort genannten Bedingungen vorzusehen.

d. Grenzen des Art. 5 Abs. 1 lit. e KI-VO

Entsprechend wird die Regulierungskompetenz der Mitgliedstaaten durch Art. 5 Abs. 1 lit e KI-VO eingeschränkt, aber nicht ausgeschlossen. Danach sind die Möglichkeiten **Privater** beim Einsatz von Systemen biometrischer Gesichtserkennung europarechtlich beschränkt worden. Unzulässig ist es, **ungezielt** Gesichtsbilder aus dem Internet oder aus Videoüberwachungsaufnahmen auszulesen (sog. Image-Scraping). Europarechtlich ungeregelt blieb dagegen beispielsweise die Fernidentifikation mittels anderer physischer, physiologischer und verhaltensbezogener menschlicher Merkmale erfolgen, wie etwa die Augenbewegungen (vgl. ErwGr. 15), ebenso das **gezielte** Auslesen von Gesichtsbildern.

c. Grenzen des Art. 6 ff. KI-VO

Auch Art. 6 ff. KI-VO verschließt den Mitgliedstaaten nicht die Kompetenz, den Einsatz biometrischer Gesichtserkennung in dem vorgegebenen Rahmen zu regulieren, insbesondere auch weitgehend zu verbieten. Die Vorschriften enthalten vor allem **Anforderungen für KI-Systeme**. Ein an den nationalen Gesetzgeber gerichtetes Gebot, derartige Systeme zuzulassen, ist auch hier nicht enthalten.

Art. 6 ff. KI-VO regeln die sog. **Hochrisiko-KI-Systeme**, die sich im Vergleich zu den verbotenen Praktiken des Art. 5 KI-VO als weniger eingriffsintensiv darstellen und sich somit auf der zweiten Stufe der Risikopyramide befinden. Für sie gelten vor allem die in **Art. 8 bis 51 KI-VO statuierten Anforderungen und Regularien**. Dementsprechend wird die Regelungskompetenz der Mitgliedstaaten begrenzt, soweit diese europarechtlichen Vorschriften reichen. Dies hängt maßgeblich davon ab, was unter einem Hochrisiko-KI-System zu verstehen ist und ob und inwieweit Systeme der biometrischen Gesichtserkennung darunter zu fassen sind.

Die KI-VO enthält allerdings **keine Definition** des Hochrisiko-Systems, sondern arbeitet mit Konkretisierungen in Form von Listen. Gemäß Art. 6 Abs. 2 i.V.m. Anhang III Nr. 1 lit. a KI-VO gelten auch Systeme als Hochrisiko-Systeme, die im Bereich der biometrischen Identifizierung und Kategorisierung natürlicher Personen verwendet werden. Hierunter sind Systeme zu verstehen, die bestimmungsgemäß für die **biometrische Echtzeit-Fernidentifizierung und nachträgliche biometrische Fernidentifizierung** natürlicher

Personen verwendet werden sollen. Daraus folgt, dass biometrische Fernidentifizierungssysteme, die die Verbotsnorm des Art. 5 Abs. 1 lit. d KI-VO nicht erfüllen, als Hochrisiko-KI-Systeme zu qualifizieren sind und etwa den Anforderungen der Art. 8 ff. KI-VO unterliegen (z.B. im Hinblick auf die Einrichtung eines Risikomanagementsystems, die Daten-Governance oder Dokumentations- und Transparenzpflichten).

d. Grenzen der DSGVO bzw. der JI-RL

Die mitgliedsstaatliche Kompetenz zur Regulierung biometrischer Gesichtserkennung wird darüber hinaus auch nicht durch andere europarechtliche Vorschriften eingeschränkt, insbesondere nicht durch Vorschriften der DSGVO und der JI-RL. So regeln insbesondere Art. 9 DSGVO und die entsprechende Parallelnorm des Art. 10 JI-RL grundsätzliche **Verbote zur Verarbeitung biometrischer Daten** sowie spezifische Verbotsausnahmen. Da bei Systemen der biometrischen Gesichtserkennung biometrische Daten verarbeitet werden, sind diese Vorschriften in ihrem jeweiligen Anwendungsbereich von sich aus zu berücksichtigen. Eine Einschränkung der Kompetenz der Mitgliedstaaten zur Regelung der biometrischen Gesichtserkennung folgt daraus nicht. Dies wird durch **Art. 9 Abs. 4 DSGVO** und **Art. 1 Abs. 3 JI-RL** bestätigt.

2. Verletzung von europäischen Grundfreiheiten und -rechten

Eine bundesgesetzliche Vorschrift zum Verbot biometrischer Gesichtserkennung verletzt keine europarechtlichen Grundfreiheiten oder Grundrechte der Grundrechte-Charta (GrCH). Solange das Verbot insbesondere inländische wie ausländische Produkte gleichermaßen betreffen würde, dürfte es insbesondere nicht die **Warenverkehrsfreiheit** (Art. 28 bis 37 AEUV) verletzen. Mitgliedstaatliche Einschränkungen oder Regelungen der Marktfreiheit sind zulässig, wenn sie – wie vorliegend das angedachte Verbot – alle Marktteilnehmer, die ihre Tätigkeit in Deutschland ausüben, gleichermaßen betreffen sowie wenn die Verkaufsmodalitäten die inländischen Produkte sowie Produkte aus anderen EU-Ländern (ehemals EG-Ländern) rechtlich wie tatsächlich in gleicher Weise betreffen.[72]

72 Siehe hierzu EuGH, Urt. v. 24. November 1993, Rs. C-267/91 u. C-268/91 – Keck und Mithouard.

IV. Verfassungsrechtliche Grenzen zur Regulierung durch Bundesgesetz

Zu prüfen ist, inwieweit eine bundesgesetzliche Verbotsregelung verfassungsrechtliche Grenzen verletzen würde. Zu wahren sind insbesondere die Grenzen der Gesetzgebungskompetenzen (dazu 1) und die Grundrechte (dazu 2). Zudem könnte eingebracht werden, dass ein weitgehendes Verbot im Widerspruch zur Aufgabe des Staates steht, die Sicherheit zu gewährleisten (dazu 3).

1. Grenzen der Gesetzgebungskompetenzen

Die Verankerung des angedachten Verbots des Einsatzes biometrischer Gesichtserkennung im BDSG als Bundesgesetz setzt voraus, dass innerhalb der bundesstaatlichen Ordnung dem Bundesgesetzgeber die dafür notwendige Gesetzgebungskompetenz zusteht. Dies richtet sich nicht nach den Art. 30, 70 ff. GG, die auch für die gesetzliche Ausfüllung von Regelungsspielräumen gelten, die dem Mitgliedstaat zur Ausfüllung in Folge der Übertragung von Hoheitsrechten auf die EU verbleiben (s. vorstehend III.1).[73] Danach steht dem Bund für das hier in Rede stehende Verbot der biometrischen Gesichtserkennung eine Gesetzgebungskompetenz nur zu, **soweit sich das Verbot auf die** in den Art. 73 Abs. 1 Nr. 1 bis 14 GG und Art. 74 Abs. 1 Nr. 1 bis 33 GG genannten **Materien stützen lässt**. Soweit das Verbot die Verarbeitung biometrischer Daten erfasst, kann sich der Bund auf seine Annexkompetenzen zu den verschiedenen Sachmaterien stützen, wie dies für den Datenschutz allgemein anerkannt ist, also für die Verarbeitung im privaten Bereich vor allem auf Art. 74 Abs. 1 Nr. 1, 11 und 12 GG und für die Verarbeitung in einem Teil des öffentlichen Bereichs etwa auf die Art. 73 Abs. 1 Nr. 5 GG und Art. 74 Abs. 1 Nr. 1, 72 GG. Im Übrigen fällt den Ländern die Gesetzgebung zu (Art. 70 GG). Dies gilt insbesondere für die allgemeine und polizeiliche Gefahrenabwehr. Entsprechendes dürfte gelten, soweit das hier in Rede stehende Verbot nicht nur die Verarbeitung biometrischer Daten, also die Tätigkeit der und die Ergebnisse von Gesichtserkennung, sondern auch die dabei eingesetzten Mittel, insbesondere KI-gestützte Informationstechnik, miterfasst.

73 Rozek; in: v. Mangoldt/Klein/Starck (Hrsg.), GG (Kommentar), 7. Aufl. 2018, Art. 70 Rn. 10.

2. Grundrechtliche Grenzen

Ein Verbot würde keine Grundrechte verletzen. Auf Grund des technischen Potenzials der biometrischen Gesichtserkennung und der prinzipiell vielfältigen Einsatzmöglichkeiten in unterschiedlichen Lebensbereichen dürfe ein Verbot in einzelne Grundrechte, jedenfalls aber in die allgemeine Handlungsfreiheit nach Art. 2 Abs. 1 GG **eingreifen**. Von den besonderen Grundrechten gilt dies insbesondere für die Unternehmerfreiheit nach Art. 12 GG, weil ein weitgehendes Verbot biometrischer Gesichtserkennung das Wirtschaften mit entsprechenden Techniken und Dienstleistungen stark, wenn nicht weitgehend vollständig einschränken dürfte. Gemäß der vom BVerfG zu Art. 12 GG verwendeten sog. Drei-Stufen-Theorie dürfte ein generelles Verbot des Inverkehrbringens, der Inbetriebnahme bzw. der Verwendung von biometrischen KI-Systemen auf der dritten und höchsten Intensitätsstufe der Eingriffe (objektive Zulassungsschranke) einzuordnen sein. Auch soweit Unternehmen erwägen, beispielsweise die Kontrolle der Leistungserbringung ihrer Beschäftigten auch mittels biometrischer Gesichtserkennung zu organisieren, würde deren Verbot die unternehmerische Freiheit insoweit einschränken.

Soweit demnach einem Verbot biometrischer Gesichtserkennung ein grundrechtliches Eingriffsgewicht zufällt, ist es allerdings gleich durch **mehrere gewichtige Schutzgüter gerechtfertigt**, selbst wenn man speziell in Bezug auf Art. 12 GG entsprechend der sog. Drei-Stufen-Theorie vorliegend Beschränkungen ausschließlich zur Abwendung einer nachweislichen oder höchstwahrscheinlichen Gefahr für ein überragend wichtiges Gemeinschaftsgut verlangen würde.

aa. Mit der biometrischen Gesichtserkennung verbinden sich besondere Gefährdungen der grundrechtlich durch Art. 2 Abs. 1 GG i.V.m. Art. 2 Abs. 1 GG geschützten **informationellen Selbstbestimmung**. Der Grund hierfür liegt in der besonderen Bedeutung höchstpersönlicher Merkmale wie das Gesicht[74] und anderer biometrischer Daten für Individualität, Privatheit und Intimität und damit letztlich für den innersten Kern menschlicher Persönlichkeitsentfaltung (vgl. auch Art. 9 Abs. 1 DSGVO und Art. 10 JI-RL).[75] Soweit zu ihrer Erzeugung und Verarbeitung zudem wirkmächtige Technologien wie etwa

74 Vgl. BVerfG v. 18.12.2018 – 1 BvR 142/15, Rn. 53.

75 Vgl. BVerfG v. 16.2.2023 – 1 BvR 1547/19, 1BvR 2634/20, Rn. 87.

KI-basierte Software eingesetzt werden, verstärken sich die Grundrechtsgefährdungen und drohen sich zu Bewegungs- und Persönlichkeitsprofilen auszuweiten, die der Preisgabe und Verwendung der persönlichsten Daten die Selbstbestimmung nehmen und zu einer verdichteten Überwachung, jedenfalls aber doch zu einem stetigen Gefühl des **Überwachtwerdens** führen können. Hinzu kommt, dass mit der zwangsläufigen Ausweitung biometrischer Datenbestände die Gefahr des **Missbrauchs** durch privat und staatliche Akteure wachsen dürfte. Schließlich entfalten Instrumente der biometrischen Gesichtserkennung regelmäßig eine hohe **Streubreite**, betreffen also viele Menschen, und zwar auch dann, wenn sie hierfür keinen spezifischen Anlass bilden.[76]

bb. Über die Gefährdung der informationellen Selbstbestimmung hinaus können sich biometrische Identifizierungsinstrumente erheblich auf das Verhalten von Menschen auswirken und sie von der Wahrnehmung und Ausübung grundrechtlicher Freiheiten abhalten, etwa ihre Religion auszuüben (Art. 4 Abs. 2 GG), ihre Meinung zu äußern (Art. 5 Abs. 1 S. 1 GG), sich künstlerisch oder wissenschaftlich zu betätigen (Art. 5 Abs. 3 S. 1 GG), an Versammlungen teilzunehmen (Art. 8 Abs. 1 GG) oder an Vereinigungen mitzuwirken (Art. 9 Abs. 1 GG). Solche **einschüchterungsbedingten Grundrechtsgefährdungen** beeinträchtigen nicht nur die individuellen Entfaltungschancen des Einzelnen, sondern auch das **Gemeinwohl**, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.[77]

cc. Mit den Möglichkeiten biometrischer Gesichtserkennung verbinden sich zudem besondere Gefahren der **Diskriminierung**, also von Ungleichbehandlungen wegen des Geschlechtes, der Abstammung, der Rasse, der Sprache, der Heimat und Herkunft, des Glaubens, der religiösen oder politischen Anschauungen von Menschen, wie dies durch Art. 3 Abs. 3 GG gerade absolut auszuschließen ist. So wurde bereits darauf hingewiesen, dass Gesichtserkennungssysteme aufgrund einer unzureichenden Basis an Trainingsdaten zu diskriminierenden Ergebnissen führen könnten (s. vorstehend I.).

76 Vgl. hierzu BVerfG v. 18.12.2018 – 1 BvR 142/15, Rn. 51.

77 Vgl. bereits BVerfG v. 15.12.1983 – 1 BvR 209/83, Rn. 146.

dd. Die grundrechtliche Gefährdungslage vertieft sich weiter, wenn man einbezieht, dass die biometrische Gesichtserkennung auch entscheidungsassistierend fungieren kann, etwa indem sie Risikoprofile oder Prognosen erstellt, die auch - soweit sie diskriminierend sind – **Anlass und Grund für weitergehende Handlungen und Maßnahmen** sein können (s. hierzu auch § 54 BDSG).

3. Grenzen der staatlichen Aufgabe zur Gewährleistung der inneren Sicherheit

Soweit der Staat, insbesondere die Sicherheitsbehörden, die Möglichkeiten der biometrischen Gesichtserkennung einsetzen oder einzusetzen erwägen, könnte gegen ein weitgehendes Verbot biometrischer Gesichtserkennung vorgebracht werden, dass es im Widerspruch zur Aufgabe des Staates steht, die Sicherheit zu gewährleisten.

Die Gewährleistung der inneren Sicherheit, also vor allem von Gefahrenabwehr und Strafverfolgung wird verbreitet als notwendige **Staatsaufgabe** angesehen.[78] Auch wenn sie im Grundgesetz nicht explizit und speziell geregelt, kommt sie in verschiedenen staatsorganisationsrechtlichen Regelungen zum Ausdruck (etwa Art. 35 Abs. 2 S. 1, 73 Abs. 1 Nr. 10 lit. b, 87 Abs. 1 S. 2 u. 91 GG). Zur **verfassungsrechtlichen Begründung** tragen aber vor allem die Grundrechte bei, soweit ihnen – z.B. Art. 2 Abs. 2 S. 1 u. 2 GG – nicht nur ein subjektives Recht des Einzelnen auf Abwehr staatlicher Eingriffe, sondern auch eine (objektivrechtliche) Pflicht des Staates zum Schutz des Einzelnen vor Beeinträchtigung entnommen wird. Verletzt der Staat seine Schutzpflicht, so verletzt er grundsätzlich auch das betroffene subjektive Grundrecht.[79] Dem Staat obliegt es nicht nur, Eingriffe Dritter in grundrechtlich geschützte Positionen – etwa mithilfe des Strafrechts – gesetzlich zu verbieten, sondern auch, die gesetzlichen Eingriffsverbote – typischerweise mithilfe des Gefahrenabwehrrechts – effektiv durchzusetzen.

Bei der **Wahl der Mittel**, die dem Staat und insbesondere auch den Exekutivorganen wie der Polizei zur Gewährleistung der inneren Sicherheit zur Verfügung gestellt werden, fällt dem Gesetzgeber allerdings ein sehr **weitreichender Gestaltungsspielraum** zu, der nur in seinen äußersten Grenzen verfassungsrechtlich angeleitet ist. Diese Grenze findet sich

78 Vgl. etwa Schoch/Kießling, in: Schoch/Eifert, Besonderes Verwaltungsrecht, 2. Aufl. 2023, Kap. 1 Rn. 66 ff.

79 Vgl. etwa BVerfGE 77, 170 (214).

insbesondere dort, wo sich ganz bestimmte Mittel als erforderlich zum Schutz des Schutzguts erweisen oder wo die Verfassung bestimmte Mittel des Schutzes vorschreibt (etwa gerichtlicher Rechtsschutz gegen Eingriffe Dritter als Gebot des Rechtsstaatsprinzips). Der Gesetzgeber überschreitet seine Grenzen, wenn er völlig untätig bleibt, eindeutig zu wenig zum Schutz unternimmt oder Vorkehrungen zum Schutz der Grundrechte trifft, die gänzlich ungeeignet oder völlig unzulänglich sind.[80] Selbst wenn man die biometrische Gesichtserkennung – trotz der dargelegten, derzeitigen Fehleranfälligkeit (s. oben I) – grundsätzlich als geeignet ansieht, zur Erfüllung staatlicher Aufgaben, insbesondere zur Gewährleistung der inneren Sicherheit beizutragen, würde die verfassungsrechtlichen Grenzen in Anbetracht der zahlreichen alternativen Mittel nicht überschritten, wenn der Gesetzgeber ein weitgehendes Verbot biometrischer Gesichtserkennung normieren würde.

V. Bedarf und verfassungsrechtliche Gebotenheit eines gesetzlichen Verbots

In den aufgezeigten Grenzen obliegt es der **Einschätzung des Gesetzgebers**, ob eine Regelung eines gesetzlichen Verbots zweckmäßig ist. Dies ist eine Frage des rechtspolitischen Bedarfs, nicht der verfassungsrechtlichen Gebotenheit. Insbesondere aus den Grundrechten folgt keine zwingende Notwendigkeit, biometrische Gesichtserkennung einfachgesetzlich zu verbieten. Allerdings ist zu berücksichtigen, dass das BVerfG in einer Reihe von Entscheidungen die erhebliche grundrechtliche Eingriffstiefe und die **Menschenwürde- (Art. 1 Abs. 1 GG) und Diskriminierungsrelevanz (Art. 3 Abs. 3 GG)** der automatisierten Verarbeitung persönlicher und insbesondere auch biometrischer Daten sowie des Einsatzes digitaler Instrumente hervorgehoben hat, die etwa darin deutlich werden, dass sie etwa mit dem Schutz besonders gewichtiger Rechtsgüter vor zumindest hinreichend konkretisierten Gefahren gerechtfertigt werden müssen.[81]

Bei genauer Betrachtung muss allerdings festgestellt werden, dass jedenfalls den staatlichen Stellen schon nach der jetzigen Rechtslage die biometrische Gesichtserkennung in dem Sinne verboten ist, als sie durch den Gesetzgeber nicht erlaubt wurde. Nach dem

80 Vgl. BVerfGE 46, 160 (164 f.); 77, 170 (214 f.).

81 Vgl. nur beispielhaft BVerfG, Beschl. v. 4.4.2006 – 1 BvR 518/02, NJW 2006, 1939, Rn. 117 f.; BVerfGE 156, 11 (Rn. 39 f, 73); BVerfG v. 16.2.2023 – 1 BvR 1547/19, 1BvR 2634/20.

aus dem Gesetzmäßigkeitsprinzip (Art. 20 Abs. 3 GG) und den Grundrechten abgeleiteten **Vorbehalt des Gesetzes** sind grundrechtswesentliche Tätigkeiten nicht zulässig, solange und soweit sie nicht durch Gesetz (positiv) zugelassen wurden. Dies hat allerdings die Praxis nicht davon abgehalten, biometrische Gesichtserkennung durchführen (s. oben I), obwohl sie sich dafür allenfalls auf gesetzliche Befugnisse berufen kann (vgl. etwa §§ 98c, 100h i.V.m. 98a, 163f StPO sowie § 48 BDSG), die kaum hinreichend sind, um die dargelegte Eingriffsintensität biometrischer Gesichtserkennung zu rechtfertigen. Insoweit könnte die Einführung eines ausdrücklichen Verbots dazu beitragen oder sogar angezeigt sein, um die Bindung an Recht und Gesetz nach Art. 20 Abs. 3 GG – im Sinne des **Vorrangs des Gesetzes** – und deren zentrale Bedeutung für die rechtsstaatliche Demokratie zu verdeutlichen.

VI. Ergebnis und Vorschlag einer Regelung für das BDSG

Das Europa- und Verfassungsrecht steht einem bundesgesetzlichen Verbot der biometrischen Gesichtserkennung durch staatliche und private Akteure nicht grundsätzlich entgegen, gebietet ein solches Verbot aber auch nicht. Es obliegt der Einschätzung des Gesetzgebers, der dabei den Vorrang der bereits europarechtlich geregelten Aspekte zu beachten hat (insbes. Art. 5 lit. d u. e, Art. 6 ff. KI-VO).

Ein bundesgesetzliches Verbot darf die biometrische Gesichtserkennung gegenständlich nur soweit erfassen, wie die Gesetzgebungskompetenzen des Bundes reichen. Vom Verbot auszunehmen ist somit insbesondere die allgemeine und polizeiliche Gefahrenabwehr.

Für die Aufnahme des Verbots **in das BDSG** spricht dessen fachgesetzübergreifender und querschnittsartiger Anwendungsbereich, der der beabsichtigten Reichweite des Verbots, insbesondere der grundsätzlichen Erstreckung sowohl auf private als auch staatliche Akteure, sowie den dargelegten Grenzen Rechnung tragen würde (vgl. insbes. § 1 Abs. 1, 4 bis 8 BDSG). Zudem blieben Ausnahmen vom Verbot kraft originärer Gesetzgebungskompetenz der Länder nicht nur durch Landesgesetz (vgl. auch § 1 Abs. 1 S. 1 Nr. 2 BDSG), sondern auch durch Bundesgesetz (vgl. § 1 Abs. 2 BDSG) möglich.

Das Verbot sollte dabei gegenständlich (auch) an der biometrischen Gesichtserkennung anknüpfen, um sowohl die Verarbeitung biometrischer Daten als auch die dafür einge-

setzten Mittel (etwa Echtzeit- und Retrograd-KI-Systeme) zu erfassen (s. oben II). In Hinblick auf seine Grundsätzlichkeit, aber auch zur textsparsamen Umsetzung bietet sich eine Einfügung als allgemeine Vorschrift („vor die Klammer“) an, etwa als neuer **§ 4a BDSG-E**:

> *„Biometrische Gesichtserkennung im öffentlichen Raum oder zur Überwachung und die Verarbeitung diesbezüglicher Daten sind verboten.“*

Soweit das Verbot auch auf die Strafverfolgungstätigkeit der Länder erstreckt werden soll, erscheint wegen des Verweisungsbefehls in § 500 StPO (nur) auf Teil 3 des BDSG zudem eine klarstellende Ergänzung in den §§ 45 ff. BDSG als zweckmäßig, etwa durch die Ergänzung in Form eines neuen **§ 48 Abs. 3 BDSG-E**:

> *„Soweit öffentliche Stellen der Länder im Anwendungsbereich der Strafprozessordnung in der jeweils geltenden Fassung personenbezogene Daten verarbeiten, ist § 4a entsprechend anzuwenden.“*

Prof. Eike Richter