Der Hamburgische Beauftragte für
Datenschutz und Informationsfreiheit

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Ludwig-Erhard-Str. 22, 20459 Hamburg

Hamburgisches Oberverwaltungsgericht
Lübeckertordamm 4
20099 Hamburg

Ludwig-Erhard-Str. 22, 7. OG
20459 Hamburg
Telefon: 040 - 428 54 – 4040 Zentrale - 40 40
E-Fax: 040 - 428 54 – 4000
Ansprechpartner:

E-Mail*:

Az.: J / 11.03-13

Hamburg, 13.3.2020

Antrag auf Zulassung der Berufung §§ 124, 124a VwGO
Az. 5 Bf 46/20.Z - Begründung des Antrags vom 6.2.2020

In der Verwaltungsrechtssache

der Freien und Hansestadt Hamburg, vertreten durch die Behörde für Inneres und Sport, Amt für Innere Verwaltung und Planung, Johanniswall 4, 20095 Hamburg,

./.

den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, Ludwig-Erhard-Straße 22, 20459 Hamburg,

führt der Beklagte zur Begründung des Antrags, die Berufung gegen das Urteil des Verwaltungsgerichts Hamburg vom 23.10.2019, Az. 17 K 203/19, zugestellt am 24.01.2020, zuzulassen, Folgendes aus:

I.

Das Verwaltungsgericht Hamburg hat der Klage der Freien und Hansestadt Hamburg, vertreten durch die Behörde für Inneres und Sport – Polizei -, gegen die Anordnung des Beklagten vom 18.12.2018 (Bl. 1385 d. Akte) stattgegeben.

Mit der genannten Anordnung hat der Beklagte auf Grundlage von § 6 des Hamburgischen Gesetzes zur Aufsicht über die Anwendung der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften (HmbRLUmsG) i.V.m. § 43 Abs. 1 Satz 5 des Hamburgischen Justizvollzugsdatenschutzgesetz (HmbJVollzDSG) die Löschung einer von der Klägerin erstellten sog. Referenzdatenbank mit biometrisch bearbeitetem Bildmaterial verfügt. Zur Erstellung dieser Referenzdatenbank wurde im Rahmen der strafrechtlichen Aufarbeitung der Geschehnisse rund um den im Juni 2017 in Hamburg stattgefundenen G20-Gipel durch die Klägerin die Gesichtserkennungssoftware Videmo 360 (im Folgenden als „Videmo“ bezeichnet) eingesetzt. Dabei hat die Klägerin Videmo genutzt um in umfangreichem Video- und Bildmaterial (ca. 17 TB an Rohdaten) menschliche Gesichter zu lokalisieren, deren Gesichtszüge zu vermessen und zu berechnen sowie diese in der streitgegenständlichen Referenzdatenbank in maschinenlesbarer und abgleichbarer Form (sog. Gesichtstemplates) zum Zweck des späteren Abgleichs zu speichern. Das von der Klägerin verarbeitete Material setzt sich zusammen aus Bild- und Videoaufzeichnungen, welche die Klägerin selbst hergestellt hat sowie aus Bild- und Videoaufzeichnungen, die aus externen Quellen stammen. Letztere bestehen aus Aufzeichnungen aus Überwachungskameras, S-Bahnhöfen, Material des Hinweisportals „Boston Infrastruktur“ des Bundeskriminalamtes sowie aus dem Internet und sonstigen Medien.

Die Erstellung dieser Referenzdatenbank wurde zunächst vom Beklagten im September 2018 nach § 6 HmbRLUmsG i.V.m. § 43 Abs. 1 Satz 1 HmbJVollzDSG beanstandet (Bl. 1013 d. Akte). Am 18.12.2018 ordnete der Beklagte die Löschung der Datenbank an. Das Verwaltungsgericht Hamburg hat der Klage der Klägerin stattgegeben und entschieden, dass der Beklagte nicht - wie nach § 43 Abs. 1 S. 1 HmbJVollzDSG erforderlich - einen Verstoß gegen Vorschriften über den Datenschutz bei der tatsächlichen Verarbeitung personenbezogener Daten festgestellt, sondern sich auf eine fiktive Datenverarbeitung gestützt habe (VG Hamburg, Urteil v. 23.10.2019, Az. 17 K 203/19, Seite 16 ff.). Der Beklagte habe sich dabei allein auf die Errichtung der Referenzdatenbank fokussiert, vorgelagerte und zeitlich nachgelagerte Datenverarbeitungsschritte von seiner Prüfung ausgenommen und dadurch den Verfahrensgegenstand – nach Ansicht des Gerichts in unzulässiger Weise – fragmentiert (VG Hamburg, a.a.O. Seite. 18 ff.).

Das Verwaltungsgericht Hamburg befand weiterhin, dass § 48 Abs. 1 BDSG eine zutreffende Ermächtigungsgrundlage für die Maßnahme der Klägerin darstelle, der Beklagte jedoch zu Unrecht die Tatbestandsvoraussetzungen als nicht erfüllt angesehen habe (VG Hamburg, a.a.O., Seite 22 ff.). Zudem bestehe in der vom Beklagten behaupteten mangelnden Bestimmtheit des § 48 BDSG als Ermächtigungsgrundlage kein Verstoß der Klägerin gegen § 43 Abs. 1 S. 1 HmbJVollzDSG (VG Hamburg, a.a.O., Seite 23). Der Beklagte sei zudem nicht befugt, die verfassungsrechtliche Eignung des § 48 BDSG als rechtliche Grundlage für

die Verarbeitung der von der Klägerin erhobenen personenbezogenen Daten in Frage zu stellen und den Anspruch des Gesetzes, die rechtliche Grundlage für sämtliche Fallgestaltungen der einschlägigen Verarbeitung personenbezogener Daten zu bilden, zu verneinen (VG Hamburg, a.a.O. Seite 24 - 30).

Schließlich sei die Anordnung des Beklagten auch ermessensfehlerhaft, da dieser das Vorliegen der Tatbestandsvoraussetzungen nicht festgestellt und sein Auswahlermessen bezüglich der vorzunehmenden Maßnahmen nicht richtig ausgeübt habe (VG Hamburg, a.a.O., Seite 31 ff.). Nach Ansicht des Verwaltungsgerichts Hamburg hätte der Beklagte festgestellte Verstöße durch Auflagen gegenüber der Klägerin beseitigen lassen müssen (VG Hamburg, a.a.O., Seite 32 ff.).

II.

Die Berufung gegen das Urteil vom 23.10.2019 ist gem. § 124a Abs. 5 Satz 2 VwGO i.V.m. § 124 Abs. 2 VwGO zuzulassen.

Es bestehen:

1. **Ernstliche Zweifel an der Richtigkeit des Urteils nach § 124 Abs. 2 Nr. 1 VwGO.**
2. **Die Rechtssache weist besondere rechtliche Schwierigkeiten i.S.v. § 124 Abs. 2 Nr. 2 VwGO auf.**
3. **Die Rechtssache ist darüber hinaus i.S.d. § 124 Abs. 2 Nr. 3 VwGO von grundsätzlicher Bedeutung**

Zu den einzelnen Berufungszulassungsgründen wird wie folgt ausgeführt:

1. Ernstliche Zweifel an der Richtigkeit des Urteils, § 124 Abs. 2 Nr. 1 VwGO

Es bestehen ernstliche Zweifel an der Richtigkeit des Urteils i.S.v. § 124 Abs. 2 Nr. 1 VwGO. Das in Rede stehende Urteil ist in seiner Begründung und in seinem Ergebnis unrichtig. Die vom Verwaltungsgericht Hamburg auf der Grundlage der tatrichterlichen Feststellung getroffenen rechtlichen Wertungen sind in mehrfacher Hinsicht fehlerhaft. Entgegen der Ansicht des Gerichts lagen die Voraussetzungen für eine Löschungsanordnung durch den Beklagten gegen die Klägerin vor. Der Beklagte hat einen tatsächlichen und konkreten Verstoß gegen Vorschriften über den Datenschutz festgestellt.

Die Löschungsanordnung des Beklagten vom 18.12.2018 ist – entgegen der Auffassung des Verwaltungsgerichts – rechtmäßig, weil die Voraussetzungen des § 6 HmbRLUmsG i.V.m. § 43 Abs. 1 Satz 5 HmbJVollzDSG vorliegen. Danach kann der Beklagte gegenüber der jeweiligen Aufsichtsbehörde der öffentlichen Stellen der Freien und Hansestadt Hamburg, deren Tätigkeit der Richtlinie (EU) 2016/680 des europäischen Parlaments und des Rates vom 24. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (JI-Richtlinie) unterfällt, geeignete Maßnahmen anordnen, wenn Verstöße gegen Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten durch diese öffentlichen Stellen trotz Beanstandung nach § 6 HmbRLUmsG i.V.m. § 43 Abs. 1 Satz. 1 HmbJVollzDSG fortbestehen und dies zur Beseitigung eines erheblichen Verstoßes gegen datenschutzrechtliche Vorschriften erforderlich ist. Diese Voraussetzungen liegen hier – entgegen der Auffassung des Verwaltungsgerichts – vor.

Die Errichtung der streitgegenständlichen biometrischen Referenzdatenbank durch die Klägerin stellt einen Verstoß gegen Vorschriften über den Datenschutz bei der Verarbeitung oder Nutzung von personenbezogenen Daten i.S.d. § 43 HmbJVollzDSG dar, da es an einer tauglichen Rechtsgrundlage für die Errichtung fehlt. Diesen Verstoß hat der Beklagte auch konkret festgestellt **(a.)**. Selbst wenn man der Auffassung des Verwaltungsgerichts Hamburg folgen wollte, dass § 48 BDSG als Ermächtigungsgrundlage für die Datenverarbeitung der Klägerin in Betracht käme, lägen die tatbestandlichen Voraussetzungen der Norm nicht vor, da das Tatbestandsmerkmal der unbedingten Erforderlichkeit nicht erfüllt ist **(b.)**. Folglich hat der Beklagte von seiner Befugnis in rechtmäßiger Weise und in Ausübung seines pflichtgemäßen Ermessens Gebrauch gemacht **(c.)**. Die Klage hätte daher abgewiesen werden müssen.

a. Feststellung des Vorliegens eines Verstoßes gegen Vorschriften über den Datenschutz durch den Beklagten bei der Datenverarbeitung durch die Polizei Hamburg i.S.d. § 43 Abs. 1 HmbJVollzDSG

Der Beklagte als zuständige datenschutzrechtliche Aufsichtsbehörde gem. § 4 Abs. 1 i.V.m. § 2 Abs. 1 HmbRLUmsG hat seine Anordnung nach § 43 Abs. 1 Satz 5 HmbJVollzDSG auf einen zuvor festgestellten und beanstandeten Verstoß gegen Vorschriften über den Datenschutz bei der Datenverarbeitung gestützt. Der festgestellte Verstoß besteht dabei in der Verarbeitung personenbezogener Daten durch die Klägerin ohne ausreichende Ermächtigungsgrundlage.

Die Verarbeitung personenbezogener Daten durch die Klägerin muss nach dem Grundsatz der Rechtmäßigkeit, wie er sich aus § 47 Nr. 1 1. Alt. BDSG ergibt und aus dem Sekundär- (Art. 4 Abs. 1 lit. a 1. Alt. JI-Richtlinie) und Primärrecht (Art. 8 der Charta der Grundrechte der Europäischen Union (GRCh)) der EU folgt, auf einer legitimen und somit verhältnismäßigen Rechtsgrundlage beruhen **(aa.)**. Entgegen der Auffassung des Verwaltungsgerichts Hamburg stellt § 48 BDSG für die konkret in Rede stehende Verarbeitung keine solche Rechtsgrundlage dar; die Ausführungen des Verwaltungsgerichts Hamburg, dass der Beklagte im Rahmen dieser Beurteilung einen nicht vom Gesetz vorgesehenen Verfahrensgegenstand bewertet habe und auf Nutzungen abstellen würde, die nicht dem tatsächlichen Gebrauch der Daten entsprechen, sondern von ihm lediglich für möglich gehalten werden („*fiktive Verarbeitung und Nutzung*“ vgl. VG Hamburg, a.a.O., Seite 17), sind unrichtig **(bb.)** Gleiches gilt für die Ausführungen des Verwaltungsgerichts, dass der Beklagte mit der Löschungsanordnung den vom Gesetz vorgegebenen Prüfungsrahmen verlassen habe, weil diese nicht von seiner Anordnungskompetenz gedeckt sei (VG Hamburg, a.a.O., Seiten 20 und 23 ff.) **(cc.)**.

aa. Nichtvorliegen einer legitimen Rechtsgrundlage als Verstoß gegen Bestimmungen gegen Vorschriften über den Datenschutz

Das Nichtvorliegen einer legitimen Ermächtigungsgrundlage für eine gegenständliche Verarbeitung stellt, entgegen der Ansicht des Verwaltungsgerichts Hamburg (VG Hamburg, a.a.O., Seiten 16 und 25), einen konkreten Verstoß gegen Vorschriften über den Datenschutz i.S.d. § 43 HmbJVollzDSG dar.

Bei dem Tatbestandsmerkmal *„Verstöße […] gegen Vorschriften über den Datenschutz“* des § 43 Abs. 1 Satz 1 HmbJVollzDSG ist nicht ausdrücklich definiert, welche Vorschriften des Datenschutzes als solche zu verstehen sind. Bei verständiger Auslegung fallen sämtliche Normen darunter, die – wie auch § 43 HmbJVollzDSG i.V.m. § 6 HmbRLUmsG selbst – der Umsetzung der JI-Richtlinie dienen.

Dies trifft auch auf § 47 BDSG zu, der die in Art. 4 JI-Richtlinie enthaltenen „*Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten*“ nahezu wortgleich in deutsches Recht umsetzt (s. auch Paal/Pauly-Frenzel, DS-GVO BDSG, 2. Aufl. 2018, § 47 BDSG Rn. 1). Nach § 47 Nr. 1 BDSG müssen personenbezogene Daten auf rechtmäßige Weise verarbeitet werden. Der unionsrechtlich determinierte, unbestimmte Rechtsbegriff der Rechtmäßigkeit ist – wie auch der gleichlautende Grundsatz in Art. 5 Abs. 1 lit. a DSGVO (Kühling/Buchner-Herbst, DS-GVO BDSG, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 8; Simits/Hornung/Spiecker-Roßnagel, Datenschutzrecht, 2019, Art. 5 Rn.34) – dahingehend auszulegen, dass eine Verarbeitung personenbezogener Daten nur zulässig ist, wenn eine

entsprechende Rechtsgrundlage diese erlaubt (Kühling/Buchner-Schwichtenberg, DS-GVO BDSG, 2. Aufl. 2018, § 47 BDSG Rn. 2; Paal/Pauly-Frenzel, DS-GVO BDSG, 2. Aufl. 2018, § 47 BDSG Rn. 2).

Dies bedeutet im Hinblick auf die Beurteilung der Rechtmäßigkeit, dass für die betreffende Verarbeitung eine ausreichende Rechtsgrundlage entweder im Unionsrecht oder im Recht des Mitgliedstaates bestehen muss (Kühling/Buchner-Herbst, DS-GVO BDSG, 2. Aufl. 2018, Art. 5 DS-GVO, Rn. 8). Dieses Verständnis unterstreicht auch ErwGr. 26 JI-Richtlinie, Danach dürfen personenbezogene Daten nur für bestimmte, durch Rechtsvorschriften geregelte Zwecke verarbeitet werden (engl.: *„legitimate basis, laid down by law“*).

Insofern setzt § 47 BDSG i.V.m. Art. 4 JI-Richtlinie, wie auch Art. 5 DSGVO, die Anforderung des Grundrechts auf Datenschutz nach Art. 8 GRCh um, wonach personenbezogene Daten nur *„mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden“* dürfen (so auch Streinz, EUV/AEUV Kommentar, 3. Aufl. 2018, EU-GRCh Art. 8 Rn. 9; Meyer/Hölscheidt-Bernsdorff, Charta der Grundrechte der EU Kommentar, 5. Aufl. 2019, Art. 8 Rn. 28 f.; Simits/Hornung/Spiecker-Roßnagel, Datenschutzrecht, 2019, Art. 5 Rn. 31 f.; Auernhammer-Kramer, DSGVO BDSG, 6. Aufl. 2018, DSGVO Art. 5 Rn. 10). Das Merkmal der Legitimität konkretisiert die allgemeine Schrankenregelung des Art. 52 Abs. 1 GRCh und ist mit dieser dahingehend auszulegen, dass verlangt wird, dass die gesetzliche Grundlage den Anforderungen des Grundsatzes der Verhältnismäßigkeit genügt (Calliess/Ruffert-Kingreen, EUV/AEUV Kommentar, 5. Aufl. 2016, Art. 8 GRCh Rn. 14-16; Streinz, EUV/AEUV Kommentar, 3. Aufl. 2018, EU-GRCh Art. 8 Rn. 11).

Gleiches gilt auch für nationales Verfassungsrecht. Das allgemeine Persönlichkeitsrecht in seiner Ausformung als Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs.1 i.V.m. Art. 1 Abs. 1 GG schützt das Recht des Einzelnen grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Dieses Grundrecht wird jedoch nicht schrankenlos gewährt. Es verlangt laut ständiger Rechtsprechung des Bundesverfassungsgerichts nach einer verfassungsmäßigen gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkung klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht (BVerfG, Urteil v. 15.12.1983 – 1 BvR 209/83, Rn. 149 - *Volkszählungsurteil*).

Das Fehlen einer legitimen Rechtsgrundlage an sich stellt somit bereits einen Verstoß gegen Vorschriften über den Datenschutz dar.

bb. Keine solche legitime Rechtsgrundlage für die streitgegenständliche Verarbeitung

Für die konkrete streitgegenständliche Datenverarbeitung, das Auslesen von Gesichtsmerkmalen einer unbegrenzten Anzahl von Personen aus gesammeltem Videomaterial, die Erstellung von maschinenlesbaren Gesichtstemplates und deren Speicherung in einer Referenzdatenbank durch die Klägerin zu Ermittlungszwecken, fehlt es, entgegen der Auffassung des Verwaltungsgerichts (VG Hamburg, a.a.O., Seite 21 ff.), an einer solchen nach Unionsrecht und nationalem Verfassungsrecht erforderlichen legitimen Rechtsgrundlage.

Es besteht für die streitgegenständliche Verarbeitung biometrischer personenbezogener Daten i.S.d. § 46 Nr. 1 und Nr. 12 BDSG (vgl. Anordnung des Beklagten vom 18.12.2018 Seite 8.) weder eine einschlägige spezialgesetzliche Regelung im bereichsspezifischen Fachrecht **(1.)**, noch kann – entgegen der Ansicht des Verwaltungsgerichts (VG Hamburg, a.a.O., Seite 22) – davon ausgegangen werden, dass mit der Generalklausel des § 48 BDSG eine Rechtsgrundlage für die streitgegenständliche Verarbeitung besteht. Diese Norm erfüllt im vorliegenden Fall nicht die Anforderungen des dargelegten Grundsatzes der Rechtmäßigkeit nach § 47 Nr. 1 BDSG und Art. 8 Abs. 2 GRCh **(2.).**

(1). Keine Regelung im bereichsspezifischen Fachrecht

Die Klägerin ist in Bezug auf die Verarbeitung personenbezogener biometrischer Daten im Rahmen der Ermittlungstätigkeit tätig geworden. Die allgemeinen Regelungen des dritten Teils des BDSG (§§ 45 ff. BDSG), zu dem auch § 48 BDSG zählt und die der Umsetzung der JI-Richtlinie dienen, sollen zunächst im Rahmen von Ermittlungstätigkeiten ergänzend neben die eigenen, nicht abschließenden Datenschutzregelungen der Strafprozessordnung (StPO) treten (Gesetzesentwurf BR, BT-Drs. 19/4671, S. 44). Dies bedeutet, dass sich beispielsweise die Zulässigkeit von molekulargenetischen Untersuchungen, wobei ebenfalls besondere Kategorien von personenbezogenen Daten im Sinne von § 46 Ziff. 14 BDSG verarbeitet werden, im strafrechtlichen Ermittlungsverfahren weiterhin nach § 81 e StPO und nicht nach § 48 BDSG richtet (Kühling/Buchner-Schwichtenberg, 2. Aufl. 2018, BDSG § 48 Rn. 7). In der StPO, findet sich aber, anders als für molekulargenetische Untersuchungen, keine Norm, die die Verarbeitung von biometrischen Daten ausdrücklich regelt. Lediglich § 81 b StPO, der zu „*Messungen*“ an Beschuldigten ermächtigt, kommt auch für eine biometrische Verarbeitung in Betracht (so wohl Meyer-Großner-Schmitt, 61. Auflage 2018, § 81 b StPO Rn. 8; Petri, GSZ 2018, 144 (144)). Dieser Tatbestand scheitert jedenfalls im konkreten Fall an der mangelnden Beschuldigteneigenschaft der Betroffenen der Maßnahme (Anordnung des Beklagten vom 18.12.2018, Seite 11). Dem hat sich das Gericht zunächst insoweit angeschlossen, als im Ergebnis – ohne weitere Ausführungen – keine

Rechtsgrundlage aus dem Bereich der StPO als einschlägig angesehen wurde (VG Hamburg, a.a.O., Seite 22).

(2). § 48 BDSG ist keine ausreichende Rechtsgrundlage

Entgegen der Ansicht des Gerichts (VG Hamburg, a.a.O., Seite. 22) kann die streitgegenständliche Datenverarbeitung nicht auf die Generalklausel des § 48 BDSG gestützt werden. § 48 BDSG ist als Generalklausel nicht hinreichend bestimmt, um die durch die Klägerin durchgeführten Maßnahmen zu legitimieren **(a)**. Bei der Frage der Eingriffstiefe der Maßnahmen der Klägerin verkennt das Gericht dabei datenschutzrechtliche Grundsätze sowie die Rechtsprechung des Gerichtshofs der EU (EuGH) bzw. BVerfG **(b).**

(a). Keine hinreichende Bestimmtheit von § 48 BDSG

Wie bereits oben (II.1.a.aa.) festgestellt, muss eine Rechtsgrundlage, die staatliche Stellen zum Eingriff in die betroffenen Grundrechte ermächtigt, nicht nur rein formell bestehen, sondern muss auch legitim sein. Dies ergibt sich nicht nur aus dem Grundsatz der Rechtmäßigkeit nach § 47 Nr. 1 BDSG i.V.m. Art. 4 Abs. 1 lit. a JI-Richtlinie, sondern folgt auch aus Art. 8 Abs. 2 GRCh (s.o.). Die Rechtsgrundlage muss also in einer Art und Weise angewandt werden, die den Anforderungen des Grundsatzes der Verhältnismäßigkeit genügt. Insoweit greifen die Anforderungen, die der EuGH und das BVerfG bezüglich der Bestimmtheit von Rechtsgrundlagen herausgebildet haben, die mit Eingriffen in das Recht auf Datenschutz nach Art. 8 GRCh, bzw. das Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verbunden sind.

Diese Anforderungen sind jedoch im vorliegenden Fall nicht erfüllt, wie der Beklagte bereits in seiner Anordnung ausgeführt hat (Anordnung des Beklagten vom 18.12.2018, Seite 11 ff.). Soweit das Verwaltungsgericht unterstellt, dass § 48 BDSG *„explizit eine rechtliche Grundlage für eine bestimmte Datenverarbeitung enthält“* (VG Hamburg, a.a.O., Seite 25), ist dem daher nicht zu folgen. Es handelt sich, wie das Verwaltungsgericht selbst feststellt, lediglich um eine Generalklausel für die Verarbeitung besonderer Kategorien personenbezogener Daten. Solche Generalklauseln stellen aber gerade keine konkreten Vorgaben bezüglich des Einsatzes der von der Klägerin verwendeten automatisierten Gesichtserkennungssoftware auf. Diese unspezifische Generalklausel (Kühling/Buchner-Schwichtenberg, BDSG § 48 Rn. 7.; Gola/Heckmann-Braun, 13. Aufl. 2019, BDSG § 48 Rn. 1 - 3) ist für die hier vorliegende besonders eingriffsintensive Verarbeitungsform von besonderen Kategorien personenbezogener Daten – hier biometrische – nach den von höchstrichterlich entwickelten Maßstäben Grundsätzen zu unbestimmt gefasst.

Um den Anforderungen des Grundsatzes der Verhältnismäßigkeit zu genügen und dadurch gerechtfertigt zu sein, muss eine gesetzliche Grundlage nach der Rechtsprechung des EuGH klare und präzise Regeln für die Tragweite und die Anwendung der fraglichen Maßnahme vorsehen und Mindestanforderungen aufstellen, sodass die Personen, deren Daten verarbeitet werden über ausreichende Garantien verfügen, die einen wirksamen Schutz vor Missbrauchsrisiken ermöglichen (EuGH, verb. Rs. C-293/12 und C-594/12 Digital Rights Ireland u.a., Rn. 54; verb. Rs. C-203/15 und C-698/15 Tele 2 Sverige, Rn. 109). Auch nach der Rechtsprechung des BVerfG muss der parlamentarische Gesetzgeber in „*grundlegenden normativen Bereichen, zumal im Bereich der Grundrechtsausübung, soweit diese staatlicher Regelung zugänglich ist, alle wesentlichen Entscheidungen selbst*“ treffen (BVerfG, Urt. v. 28.10.2008 – 2 BvC 3, 4/07, Rn. 132 m.w.N.). Dies betrifft nicht allein die Frage, ob es einer gesetzlichen Regelung bedarf, sondern auch, wie weit diese Regelung im Einzelnen zu gehen hat (BVerfGE, Urt. V. 6.7.1999 – 2 BvF 3/90, Rn. 124 m.w.N.). Dabei muss eine Norm hinreichend bestimmt sein (BVerfG, Urt. V. 28.10.2008 – 2 BvC 34/07 Rn. 132 m.w.N.). Bei Eingriffen in das Recht auf informationelle Selbstbestimmung dient der Bestimmtheitsgrundsatz auch dazu, den Anlass der Maßnahme zu umgrenzen und die möglichen Verwendungszwecke der betroffenen Daten sicherzustellen (BVerfGE, Urt. v. 11.3.2008 – 1 BvR 2074/05, Rn. 96 m.w.N.). Im Einzelfall hängen die Anforderungen an die Bestimmtheit einer Norm jedoch von dem Regelungsgegenstand und der Intensität der Maßnahme ab, wobei höhere Anforderungen an den Bestimmtheitsgrad zu stellen sind, wenn sie mit intensiveren Eingriffen in grundrechtlich geschützte Rechtspositionen einhergehen (BVerfGE Beschluss v. 8.1.1981 – 2 BvL 3, 9/77, NJW 1981, 1311 m.w.N.). Das Maß der gebotenen Bestimmtheit richtet sich u.a. nach der Grundrechtsrelevanz, insbesondere Art und Schwere des mit der Maßnahme verbundenen Eingriffs (vgl. insb. BVerfGE, Urt. v. 11.3.2008 – 1 BvR 2074/05, Rn. 95 m.w.N.). Der EuGH geht davon aus, dass ein schwerer Eingriff in die betroffenen Grundrechte vorliegt, wenn eine Maßnahme eine große Anzahl von Personen betrifft und diese auch nach Beendigung der Maßnahme nicht über ihre Durchführung informiert werden (EuGH, verb. Rs. C-293/12 und C-594/12 Digital Rights Ireland u.a., Rn. 37; verb. Rs. C-203/15 und C-698/15 Tele 2 Sverige, Rn. 100). Nach der Rechtsprechung des BVerfG weisen Grundrechtseingriffe insbesondere dann eine hohe Eingriffsintensität auf, wenn sie sowohl durch Verdachtslosigkeit als auch durch eine große Streubreite gekennzeichnet sind, wenn also zahlreiche Personen in den Wirkungskreis einer Maßnahme einbezogen werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben (BVerfG, Beschluss v. 23.2.2007 – 1 BvR 2368/06 Rn. 51 zur Videoüberwachung; BVerfG, Urteil v. 14.7.1999 – 1 BvR 2226/94, Rn. 270).

So liegt es hier. Die streitgegenständlichen Maßnahmen, also das Erstellen der Referenzdatenbank durch biometrische Analyse von Gesichtsmerkmalen, weisen eine hohe

Eingriffsintensität auf. Dies folgt zum einen daraus, dass es sich bei den erzeugten Templates um einzigartige Informationen über das eigene Gesicht als dem zentralem biometrischem Merkmal handelt und biometrische Daten im Datenschutz als besondere Kategorien von Daten unter einen herausgehobenen Schutz gestellt sind (vgl. Art. 10 JI-Richtlinie, ErwGr. 51 JI-Richtlinie). Zum anderen wurden die Maßnahmen sowohl für die Betroffenen unerkannt durchgeführt und sind gerade durch Verdachtslosigkeit als auch durch eine große Streubreite gekennzeichnet. Die weit überwiegende Zahl der Betroffenen wurde ohne eigenes Zutun, bzw. ohne einen Anlass dafür zu geben, in die Referenzdatenbank aufgenommen (Anordnung des Beklagten vom 18.12.2018, Seite 14 ff.) und haben möglicherweise keinerlei Kenntnis darüber, ob ein Gesichtstemplate von ihnen in der Referenzdatenbank zu finden ist. Dies schränkt jedoch auch ihre Möglichkeit ein, die in Rede stehenden Maßnahmen zu überprüfen. Erfasst wurden sämtliche Personen, die sich auf dem Video- bzw. Bildmaterial befanden. Eine Einordnung als Beschuldigter war gerade nicht Voraussetzung für die Maßnahmen der Klägerin.

Soweit das Verwaltungsgericht die Parallelen zur Rechtsprechung des BVerfG zur Kennzeichenerkennung (BVerfG, Beschluss v. 18.12.2018 – 1 BvR 142/15 Rn. 42) im vorliegenden Fall in diesem Zusammenhang verneint (VG Hamburg, a.a.O., Seite 30), wenn es ausführt, dass nur der vom Bundesverfassungsgericht zu entscheidende Sachverhalt an ein (eingriffsteigerndes) Alltagsverhalten anknüpft, ist dies unzutreffend. Entgegen den Ausführungen des Gerichts, die vermuten lassen, dass es davon ausgeht, dass sämtliche der erfassten Personen Anlass zu der Datenverarbeitung gegeben hätten, da sie sich durch Teilnahme an einer Demonstration oder die bloße Nutzung des öffentlichen Nahverkehrs in „*die* (beabsichtigte) *räumliche Nähe zu zahlreichen und teils außerordentlich schwerwiegenden Straftaten*“ (VG Hamburg, a.a.O., Seite 30) begeben hätte, ist dies fehlerhaft. Wie in der Anordnung ausführlich dargelegt, hat der weitaus größte Teil der Betroffenen zu der biometrischen Gesichtsanalyse, der Erhebung, Abspeicherung und der Bereithaltung gerade keinen Anlass gegeben, weil die Personen weder in einer Beziehung zu einem strafrechtlichen oder ansonsten rechtlich relevantem Fehlverhalten standen. Das Gericht hat sich dabei weder mit der Herkunft noch mit Umfang oder der (unzureichenden) Vorauswahl des Materials hinreichend auseinandergesetzt. Die streitgegenständliche Gesichtsanalyse knüpft an die Nutzung des öffentlichen Nahverkehrs in einem bestimmten Zeitrahmen oder der Demonstrationsteilnahme an, aber auch daran, dass private Personen sich entschieden haben, Bild- oder Videomaterial an einen Server des BKA zu übermitteln, wobei es nach polizeilicher Einschätzung alleine ausreichte, dass die angefertigten Aufnahmen „*örtlich und zeitlich in den G20-Rahmen*“ passten (vgl. Anordnung des Beklagten vom 18.12.2018 , Seite15 ff.).

Auch die Ausführungen des Verwaltungsgerichts im Rahmen der Frage des Eingriffs, dass gerade – im Gegensatz zur Kfz-Kennzeichenerfassungs-Rechtsprechung des Bundesverfassungsgerichts – hier keine „*Überwachungsstruktur installiert wurde, welche zu Einschüchterungen und (…) zu Beeinträchtigungen bei der Ausübungen von Grundrechten führe*“ (VG Hamburg, a.a.O., Seite 29) sind ebenfalls nicht zutreffend. Gerade im vorliegenden Fall ist es ein Aspekt, der den Eingriff und damit die Anforderungen an eine Eingriffsnorm substantiell erhöht, weil zukünftig Bürger davon ausgehen müssen, von Gesichtserkennung betroffen zu sein, wenn im Umfeld der Versammlung Straftaten begangen werden könnten. Dabei dürfte es sich gerade um eine Verhaltenssteuerung handeln, wenn stets mit dem Erstellen einer umfangreichen biometrischen Datenverarbeitung gerechnet werden muss (vgl. Mysegades, 2020 NVwZ, in Erscheinung). Die Polizei Hamburg hat darüber hinaus bereits mehrfach in Aussicht gestellt, die Gesichtserkennungssoftware auch bei anderen Großereignissen - wie z.B. einem Fußballderby - ggf. einsetzen zu wollen (Bericht aus dem Innenausschuss, Bü-Drs. 21/15080 – Seite 11).

Entgegen der Auffassung des Verwaltungsgerichts können auf § 48 BDSG derart intensive Nutzungsformen wie die Vorliegende nicht gestützt werden. Das Bestimmtheitsgebot verlangt für die vorliegende Fallkonstellation vom Gesetzgeber zumindest, dass er beim Einsatz der Gesichtserkennungssoftware zur Verfolgung von Straftaten die technischen Eingriffsinstrumente zur biometrischen Erstellung wie auch die Voraussetzungen zu deren Einsatz genau benennt und an einschränkende Bedingungen knüpft, unter denen die umfassende Erstellung von Templates zulässigerweise angeordnet werden kann. Zu den gesetzlichen Mindestvoraussetzungen zählen nicht nur die Anlassstraftaten für einen derartigen Einsatz, sondern auch Art und Umfang des herangezogenen Videomaterials sowie der Zeitraum, für den Videosequenzen ausgewertet und Templates daraus erstellt werden dürfen. Ferner sind spezifische prozedurale Vorgaben, wie ein Richtervorbehalt oder die Kontrolle entsprechender Datenbanken durch unabhängige Stellen erforderlich, die eine Kompensation der Rechte Betroffener, denen die Verarbeitung ihrer Daten regelmäßig nicht bekannt sein wird, bezweckt (vgl. zur Kompensationsfunktion der aufsichtsrechtlichen Kontrolle für schwach ausgestalteten Individualrechtsschutz BVerfG, Urteil v. 24.4.2013 – 1 BvR 1215/07, Rn. 213 ff.). Diese Anforderungen erfüllt § 48 BDSG nicht.

§ 48 BDSG dient zwar der Umsetzung von Art. 10 JI-Richtlinie, der geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen bei der Verarbeitung von besonderer Kategorie von personenbezogenen Daten fordert. § 48 Abs. 2 BDSG nennt aber nur beispielhaft einige mögliche Maßnahmen der Datensicherheit zur Gewährleistung geeigneter Garantien. Wann und wie diese Maßnahmen in welchem Umfang bei welcher Art der Datenverarbeitung umzusetzen sind, ist der Regelung gerade nicht zu entnehmen. Als

Beispielsfall dafür, wie eine Umsetzung im Bereich der Verarbeitung von besonderen Kategorien personenbezogener Daten erfolgen muss, kann in dem bereits erwähnten § 81 e StPO gesehen werden (s.o., obwohl dieser älter ist als die JI-Richtlinie). Dabei kann das Erfordernis einer richterlichen Anordnung nach § 81 f Abs. 1 StPO als geeignete Garantie i.S.d § 48 Abs. 2 BDSG verstanden werden. Der Anwendungsbereich des § 48 BDSG ist daher von vorneherein begrenzt und bleibt damit eine unspezifische Generalklausel. (Kühling/Buchner-Schwichtenberg, DSGVO/BDSG, 2. Auflage 2018, § 48 BDSG Rn. 7). Die praktische Bedeutung dieser allgemeinen Regelungen wird daher als „*überschaubar*“ (Gola/Heckmann-Braun, 13. Auflage 2019, BDSG § 45 Rn. 3) bezeichnet. Insofern bedarf es, ähnlich wie für die molekulargenetische Untersuchung nach § 81 e StPO (vgl. unter II.a.bb.(1)), einer speziellen fachgesetzlichen Regelung.

§ 48 BDSG kann die gegenständliche biometrische Datenverarbeitung nicht legitimieren. Der europäische Gesetzgeber erwähnt in der JI-Richtlinie ausdrücklich, dass die Verarbeitung von personenbezogenen Daten stets in einer für die betroffene Person nachvollziehbaren Weise erfolgen muss. Dies stehe zwar Maßnahmen wie z.B. der Videoüberwachung zur Verfolgung von Straftaten nicht entgegen, sie dürfen aber nur getroffen werden, sofern sie durch Rechtsvorschriften geregelt sind (ErwGr. 26 JI-Richtlinie) Dies muss gerade für ein biometrisches Auswertungssystem gelten, das verdachtslos tausende Betroffene betrifft und den bereits intensiven Eingriff gegenüber Videoaufzeichnungen nochmals u.a. durch die Verknüpfungs- und Nutzungsmöglichkeiten deutlich vertieft (Anordnung des Beklagten vom 18.12.2018, Seite 16).

Es ist allenfalls davon auszugehen, dass die Generalklausel des § 48 BDSG z.B. zu Speicherungen ermächtigt, wenn diese an eine auf Grundlage bereichsspezifischer Ermächtigung rechtmäßige Datenerhebung anknüpfen. Eine solche Speicherung von besonderen Kategorien von personenbezogenen Daten die auf § 48 BDSG gestützt werden könnte, erfolgt bei der Polizei etwa bei personengebunden Hinweisen, die besonderen Kategorien von Daten unterfallen (Gola/Heckmann-Braun, 13. Aufl. 2019, BDSG § 48 Rn. 3). Gleiches gilt für Ermittlungen in deren Verlauf die Verarbeitung von sensiblen Daten eine Rolle spielen kann. Das kann etwa der Fall sein, wenn im Rahmen einer Ermittlung die Feststellung getroffen wird, dass ein Augenzeuge eine erhebliche Sehschwäche hat, wodurch auch Gesundheitsdaten verarbeitet werden. Vorliegend geht es jedoch um ein zielgerichtet eingesetztes Verfahren, dass gerade auf die Erhebung und Verarbeitung von besonders sensiblen Daten, nämlich der biometrische Gesichtsabdruck von tausenden von Personen, abzielt.

(b). Der Beklagte hat die Eingriffstiefe auch anhand konkreter Feststellungen getroffen

Der Beklagte hat sich bei der Prüfung der Eingriffstiefe der Datenverarbeitungen der Klägerin – entgegen der Ansicht des Verwaltungsgerichts (VG Hamburg, a.a.O., Seite 16 ff. u. 21) – auch nicht auf mögliche Szenarien in der Zukunft bezogen, sondern anhand der konkret durch die Klägerin vorgenommenen Datenverarbeitungen die Schwere des in dieser Verarbeitung bestehenden Eingriffs festgestellt und ist zu dem Ergebnis gelangt, dass ein Rückgriff auf eine Generalklausel ausgeschlossen ist. Dabei hat der Beklagte die Datenverarbeitungsschritte auch nicht - entgegen der Ausführungen des Gerichts (VG Hamburg, a.a.O., Seite 18) - in unzulässiger Weise fragmentiert.

Wenn das Gericht in seinem Urteil ausführt, dass „*beabsichtigte Datenvorgänge*“ fälschlicherweise vom Beklagten herangezogenen wurden (VG Hamburg, a.a.O., Seite 16 ff.) verkennt das Gericht die datenschutzrechtliche Dogmatik. Mit dieser Würdigung des Verfahrensgegenstands stellt es sich sowohl den Anforderungen des nationalen Verfassungsrechts, als auch des EU-Rechts entgegen. Die Beurteilung der Risiken/Gefährdungen, die einer Datenverarbeitung inhärent sind, ist notwendiger Bestandteil jeglicher Überprüfung der Rechtmäßigkeit eines konkreten Verarbeitungsvorgangs. Diese Tatsache ist nicht zuletzt auch dem Umstand geschuldet, dass es sich bei dem Allgemeinen Persönlichkeitsrecht, das durch Vorgaben des Datenschutzrechts geschützt werden soll, um ein unterstützendes Grundrecht handelt, das seinem Inhaber vor allem auch die Ausübung anderer Grundrechte ermöglichen soll. Der Beklagte beurteilt daher umfassend den von ihm zu beurteilenden Einzelfall, der, wie das Verwaltungsgericht zutreffend ausgeführt hat, die konkreten Umstände der Verarbeitung in den Blick nehmen muss. Entgegen der Auffassung des Verwaltungsgerichts fallen darunter jedoch auch die konkreten Risiken für die Rechte und Freiheiten der von einem konkreten Verarbeitungsvorgang betroffenen Personen.

Sowohl dem Schutz des Art. 8 GRCh als auch dem Grundrecht auf informationelle Selbstbestimmung ist immanent, dass die Risiken/Gefahren der (modernen) konkreten Datenverarbeitung zu beurteilen sind. Es geht dabei aus der Missbrauchsperspektive heraus um die Gefahr der totalen Registrierung und Katalogisierung (Maunz/Dürig/*Di Fabio* Art. 2 GG, Rn. 173). Der EuGH geht davon aus, dass für das Recht auf Datenschutz ein hohes Schutzniveau gewährleistet werden muss, weshalb Eingriffe auf das absolut notwendige Maß beschränkt und Maßnahmen zum Schutz gegen die Risiken etwaigen Missbrauchs definiert werden müssen (EuGH, verb. Rs. C-293/12 und C-594/12 Digital Rights Ireland u.a., Rn. 54; EuGH, Avis 1/15, Gutachten vom 26.7.2016, Rn. 134, 139-141). Das BVerfG hat erstmals im sog. Volkszählungsurteil (BVerfG, Urteil v. 15.12.1983 – 1 BvR 209/83 u.a.) das Recht auf informationelle Selbstbestimmung entwickelt und festgelegt, dass damit Gefährdungen und Verletzungen der Persönlichkeit Rechnung getragen wird, die sich für

den Einzelnen insbesondere unter den Bedingungen moderner Datenverarbeitungen, aus informationsbezogenen Maßnahmen ergeben. Es flankiert und erweitert den grundrechtlichen Schutz von Verhaltensfreiheit und Privatheit und lässt ihn damit schon auf der Stufe der Persönlichkeitsgefährdung beginnen (st. Rechtsprechung des BVerfG Beschluss v. 18.12.2018, 1 BvR 142/15 – Rn. 37 m.w.N; so auch OVG Hamburg, Urteil v. 22.6.2010 – 4 Bf 276/07 Rn. 61). Im Rahmen der automatisierten Verarbeitung personenbezogener Daten wird von der verfassungsgerichtlichen Rechtsprechung immer wieder auf die verschiedenen Verarbeitungsmöglichkeiten abgestellt. Gerade diese führen nach Ansicht des BVerfG zu den spezifischen Gefahren für die Freiheitsrechte des Einzelnen (BVerfG, Urteil v. 15.12.1983 – 1 BvR 209/83, Rn. 149; Urteil v. 11.3.2008 – 1 BvR 2074/05, Rn. 64, BVerfG, Urt. V. 18.12.2018 – 1 BvR 142/15, Rn. 37: „*Der mit solchen technischen Möglichkeiten einhergehenden gesteigerten Gefährdung entspricht der hierauf bezogene Grundrechtsschutz*“). Dabei führt das BVerfG bereits in seiner ersten Entscheidung zur automatischen Erfassung von Kfz-Kennzeichen ausdrücklich aus, dass es zu einem Eingriff in das Grundrecht auf informationelle Selbstbestimmung bereits dann kommt, wenn ein erfasstes Kennzeichen in einem Speicher festgehalten wird und dadurch Grundlage für weitere Maßnahmen werden kann. Es steht ab diesem Zeitpunkt zur Auswertung durch staatliche Stellen zur Verfügung und es beginnt die spezifische Persönlichkeitsgefährdung durch die Beeinträchtigung der Verhaltens- - und Privatfreiheit, die den Schutz des Grundrechts auf informationelle Selbstbestimmung auslöst (BVerfG Urteil v. 11.3.2008 – 1 BvR 1254/07, Rn. 69 ff.). Im Rahmen der Datenverarbeitung nimmt die Schwere des Eingriffs darüber hinaus zu mit der Möglichkeit der Nutzung der Daten für Folgeeingriffe sowie mit der Möglichkeit der Verknüpfung mit anderen Daten, die wiederrum Folgemaßnahmen auslösen können (zur Videoüberwachung: BVerfG, Beschluss v. 23.2.2007 – BvR 2368/06, Rn. 52; BVerfG, Urteil v. 11.3.2008 – 1 BvR 2074/05, Rn. 79).

Auf fachgesetzlicher Ebene ist in der JI-Richtlinie der sog. risikobasierten Ansatz verankert (vgl. ErwGr. 50-54 JI-Richtlinie, Art. 19, 27 JI-Richtlinie). Dabei sind im Rahmen einer Gefahrenanalyse – einem durch die JI-Richtlinie, die den Begriff des Risikos verwendet, unionsrechtlich determiniertem Begriff, der sich nicht mit dem Gefahrenbegriff des deutschen Verwaltungsrechts deckt – Risiken für die Rechte der betroffenen Personen zu beurteilen. Dieser Begriff des Risikos für die Rechte betroffener Personen umfasst notwendigerweise auch die Grundrechte der von der Datenverarbeitung betroffenen Personen (s. dazu detailliert Bieker/Bremert, ZD 2020, 7 (8)), da die JI-Richtlinie ausweislich ihres Art. 1 Abs. 2 lit. a dazu dient, die Grundrechte natürlicher Personen, insbesondere ihr Grundrecht auf Datenschutz, zu schützen.

Fehlerhaft sind auch die Ausführungen des Gerichts in diesem Zusammenhang, dass der Beklagte den Verfahrensgegenstand in unzulässiger Weise fragmentiere (VG Hamburg,

a.a.O. Seite 18 ff.), indem er bei der Frage der Eingriffstiefe nur die Erstellung der Referenzdatenbank beurteile, und den zeitlich davorliegenden Schritt der Errichtung der Grunddatei und den nachfolgenden Schritt der einzelnen Suchläufe bei der Beurteilung außer Acht lasse. Die Ausführung des Gerichts, dass der Beklagte die Eingriffstiefe daher anhand der „*entscheidenden dritten Stufe*“ (VG Hamburg, a.a.O., Seite 29), also der Suchläufe, hätte festmachen müssen, widerspricht dabei ebenfalls der datenschutzrechtlichen Dogmatik.

Jeder Datenverarbeitungsschritt ist vielmehr gesondert zu betrachten. Die Auslese von charakteristischen Gesichtsmerkmalen, die Templateerstellung und deren Speicherung in eine Referenzdatenbank sind neben der vorherigen Bild- und Videoerhebung/Speicherung (erste Stufe) und der Erstellung der Templates folgenden Abgleichmaßnahmen (dritte Stufe) eigenständige Datenverarbeitungsschritte (vgl. Jandt, ZPR 2018, 16 (18)) und stellen damit eigene Grundrechtseingriffe dar (zum Erfassen und Abgleich von Daten bei der automatisierten Kfz-Kennzeichenkontrolle: BVerfG, Beschluss v. 18.12.2018 – 1 BvR 142/15 Rn. 42). Für jeden Grundrechtseingriff bestehen (eigene) Gefahren und Missbrauchsrisiken denen somit durch (hinreichend bestimmte) Ermächtigungsgrundlagen mit entsprechenden Verfahrenssicherungen Rechnung getragen werden muss. Aus diesem Grund verlangt das Bundesverfassungsgericht bestimmte und normenklare Ermächtigungsgrundlagen für jeden Akt der automatisierten Datenverarbeitung (BVerfG, Urteil v. 15.12.1983 – 1 BvR 209/83, Rn. 149; Urteil v. 11.3.2008 – 1 BvR 2074/05, Rn. 64).

Die Eingriffstiefe war somit – wie vom Beklagten in der Anordnung vorgenommen – anhand der aus Erstellung der Referenzdatenbank ergebenden Risiken und Gefahren im konkreten Fall zu beurteilen. Dabei wurde den Vorgaben der höchstrichterlichen Rechtsprechung zum gefährdungs-, bzw. risikobasierten Ansatz entsprechend eine erhebliche Eingriffstiefe festgestellt, die nicht nur aus der bereits dargelegten Streubreite und Anlasslosigkeit folgt. Es ist ein erheblicher Unterschied, ob die Strafverfolgungsbehörde lediglich Bilddaten von Personen speichert oder diese mittels einer Software biometrisch auswertet und hierfür jeder einzelnen Person eine unverwechselbare Gesichts-ID zuordnet. Die Analyse und Speicherung von mathematischen Modellen menschlicher Gesichter macht Informationen über Personen in zeitlicher und örtlicher Hinsicht in unbegrenzte Weise auf Vorrat verfüg- und nutzbar, wie dies bloße Lichtbilder und konventionelle Datenverarbeitung durch manuelle Durchsicht nicht ermöglichen. So kann u.a. das Verhalten und die räumliche Veränderung von Personen ermittelt werden. Bewegungsprofile und Verhaltensweisen können detailliert erkannt werden. Diese Form der Datenverarbeitung eröffnet vielfältige Nutzungsmöglichkeiten (Anordnung des Beklagten vom 18.12.2018, Seite 15 ff.). Das während der einzelnen Suchläufe, also im Rahmen der sog. dritten Stufe, die biometrischen Daten der Vielzahl Unverdächtiger gerade „*unterdrückt*“ werden (VG Hamburg, a.a.O., Seite

29) mindert die Eingriffstiefe der hier gegenständlichen zweiten Stufe – entgegen der Auffassung des Gerichts – somit nicht.

cc. Durch Feststellung dieses Verstoßes verlässt der Beklagte auch nicht den ihm durch § 43 HmbJVollzDSG vorgegebenen Prüfungsrahmen.

Die Ausführungen des Verwaltungsgerichts, dass der Beklagte mit der Anordnung den ihm durch das Gesetz vorgegebenen Prüfungsrahmen verließ (VG Hamburg, a.a.O., Seite. 20 u. 23 ff.), weil der Beklagte zur Prüfung der grundrechtlichen Implikationen nicht befugt sei (VG Hamburg, a.a.O., Seite 20) und auch nicht prüfen dürfe, ob § 48 Abs. 1 BDSG eine hinreichend konkrete Ermächtigungsgrundlage für das Handeln der Polizei darstellt (VG Hamburg, a.a.O., Seite 24), sind fehlerhaft. Dabei kann dem Beklagten insbesondere kein Verstoß gegen den Grundsatz des Vorrangs des Gesetzes vorgeworfen werden (VG Hamburg, a.a.O., Seite 26). Der Beklagte prüft vielmehr, wie es nach § 43 Abs. 1 HmbJVollzDSG seinem gesetzlichen Auftrag entspricht, ob die von der Klägerin vorgenommene Datenverarbeitung gegen Vorschriften über den Datenschutz verstößt. Das Fehlen einer legitimen Rechtsgrundlage stellt einen solchen Verstoß dar (s.o.). Das Verwaltungsgericht verkennt in seiner Entscheidung insbesondere den unions- und verfassungsrechtlichen vorgegebenen Auftrag und die Stellung des Beklagten.

Art. 8 Abs. 3 GRCh sieht eine unabhängige institutionelle Datenschutzkontrolle vor. Die Einrichtung und insbesondere die Unabhängigkeit der Datenschutzaufsicht gehören zu den tragenden Grundsätzen des europäischen Datenschutzrechts. Nach der ausdrücklichen Rechtsprechung des EuGH sind die Aufsichtsbehörden die Hüter der den Datenschutz betreffenden Grundrechte aus Art. 7 und 8 GRCh (EuGH, Rs. C-518/07 Kommission./. Deutschland, Urt. v. 9.3.2010, Rn. 23 f.). Nach Art. 8 Abs. 2 GRCh dürfen personenbezogene Daten nur mit Einwilligung der betroffenen Person oder auf einer gesetzlich geregelten legitimen Grundlage verarbeitet werden. Die umfassende Kontrollbefugnis der in Art. 8 Abs. 3 GRCh genannten Stellen, und damit des Beklagten, erstreckt sich nach Art. 8 Abs. 3 GRCh auf „*diese Vorschriften*“. Dieser Verweis bezieht sich dabei zunächst auf die Vorgaben des Art. 8 GRCh selbst und darüber hinaus auf die in Art. 8 Abs. 2 GRCh genannten legitimen gesetzlichen Grundlagen, d.h. auf alle Normen, die den Eingriff in das Recht auf Datenschutz rechtfertigen. Soweit die Grundrechtsbindung greift, muss die Kontrolle greifen (Pechstein/Nowak/Häde-Wolff, Frankfurter Kommentar zu EUV, GRC, AEUV, Art. 8 GRC Rn. 57 ff.). Der Beklagte hat daher zu prüfen, ob die gegenständliche Datenverarbeitung auf einer gesetzlich geregelten legitimen Grundlage basiert.

Nach der Rechtsprechung des BVerfG flankiert die aufsichtsrechtliche Kontrolle die subjektivrechtliche Kontrolle durch die Gerichte. Sie dient – neben administrativen Zwecken – eben auch der Gewährleistung der Gesetzmäßigkeit der Verwaltung insgesamt und schließt dabei den Schutz der subjektiven Rechte der Betroffenen ein. Eingriffe in das Recht auf informationelle Selbstbestimmung können deshalb auch dann unverhältnismäßig sein, wenn sie nicht durch ein hinreichend wirksames aufsichtsrechtliches Kontrollregime flankiert sind. Dies hat umso größeres Gewicht, je weniger eine subjektivrechtliche Kontrolle sichergestellt werden kann (BVerfG, Urteil v. 24.4.2013 - 1 BvR 1215/07, Rn. 207). Auf einfachgesetzlicher Ebene sind diese Grundsätze zunächst in der JI-Richtlinie niedergelegt, wonach die unabhängigen Aufsichtsbehörden ein wesentlicher Bestandteil des Schutzes natürlicher Personen bei der Datenverarbeitung sind (ErwGr. 75 JI-Richtlinie). Sie sind daher auch im Anwendungsbereich der JI-Richtlinie von den Mitgliedstaaten nach Art. 47 Abs. 1 JI-Richtlinie mit wirksamen Untersuchungsbefugnissen auszustatten. Dies ist erforderlich um ihre Aufgaben, die nach Art. 46 Abs. 1 lit. a JI-Richtlinie auch in der Überwachung der Anwendung der datenschutzrechtlichen Vorschriften bestehen, effektiv erfüllen zu können. Diese Vorschriften sind wiederum in Kapitel 3 BDSG umgesetzt, der explizit auch den Grundsatz der Rechtmäßigkeit umfasst. Da es nach Art. 1 Abs. 2 lit. a JI-Richtlinie gerade Zweck dieser Vorschriften ist, die Grundrechte der betroffenen Personen zu schützen (s.o.).

Aus dieser vom Unionsgesetzgeber und der höchstrichterlichen Rechtsprechung vorgegebenen Stellung und verlangten Effektivität der datenschutzrechtlichen Aufsicht wäre es nicht vereinbar, wenn diese gerade beim stärksten vorstellbaren Verstoß gegen den Datenschutz durch öffentliche Stellen – eine Verarbeitung, die nicht auf eine Ermächtigungsgrundlage gestützt werden kann – nicht wirksam handeln könnte. Dabei disponiert der Beklagte mit seiner Anordnung auch nicht wie vom Verwaltungsgericht angedeutet über den Geltungsanspruch eines Parlamentsgesetzes (VG Hamburg, a.a.O., Seite 26). Der Beklagte hat weder die Kompetenz noch den Willen, die Regelung des § 48 BDSG „*außer Kraft*“ (VG Hamburg, a.a.O., Seite 27) zu setzen. Die Geltung der Norm ist von dem Erlass der streitgegenständlichen Anordnung – eines Verwaltungsaktes – auch nicht beeinträchtigt.

Der Beklagte ist aufgrund des Vorbehalts des Gesetzes und seiner Stellung vielmehr verpflichtet, zu prüfen, ob für die Datenverarbeitung der Polizei eine ausreichende Rechtsgrundlage besteht. Wie bereits dargelegt, erfordert sowohl Art. 8 GRCh als auch das allgemeine Persönlichkeitsrecht in seiner Ausformung als Recht auf informationelle Selbstbestimmung eine legitime Rechtsgrundlage beim Eingriff in das Grundrecht. Dieser Vorbehalt des Gesetzes wird durch § 48 BDSG im vorliegenden Fall aber nicht erfüllt (s.o.). Die Eingriffsverwaltung kann ihren Eingriff nicht auf diese Grundlage stützen. Dies muss der Beklagte als Aufsichtsbehörde auch prüfen. Hierdurch wird nicht in den Geltungsanspruch

eines Parlamentsgesetzes eingegriffen, sondern der Vorbehalt des Gesetzes gerade geschützt, indem überprüft wird, ob für das Handeln der Exekutive eine gesetzliche Grundlage besteht. Zum Vergleich kann auf eine Widerspruchsbehörde verwiesen werden, die bei ihrer Prüfung des Ausgangsbescheids selbstverständlich auch zu prüfen hat, ob dieser auf einer ausreichenden Ermächtigungsgrundlage beruht (vgl. dazu ausführlich Mysegades, NVwZ 2020, im Erscheinen).

Es ist insoweit unrichtig wenn das Gericht feststellt, der Beklagte habe gegen den Grundsatz des Vorranges des Gesetzes verstoßen, vielmehr hat er gerade die in Betracht kommenden Eingriffsgrundlagen überprüft. Die Prüfung der Rechtmäßigkeit der Datenverarbeitung gehört zu den zentralen Aufgaben der Datenschutzaufsichtsbehörden. Das gilt gerade auch für das Bestehen einer Rechtsgrundlage, als verfassungsrechtliche Voraussetzung für eine zulässige Datenverarbeitung Die Prüfung des § 48 BDSG sowie anderer möglicher Eingriffsgrundlagen im spezifischen Fachrecht führte in keiner Weise – wie das Gericht unterstellt – zum Ergebnis der Verfassungswidrigkeit dieser Normen. Vielmehr hat der Beklagte die Bestimmungen des § 48 BDSG, wie auch der anderen in Betracht kommenden Rechtsgrundlagen, als mögliche Eingriffsgrundlagen überprüft und im Ergebnis abgelehnt.

In diesem Zusammenhang verkennt das Gericht, dass der Prozess der Normenauslegung und Prüfung naturgemäß verfassungsrechtliche Aspekte wie den Bestimmtheitsgrundsatz und der Verhältnismäßigkeit zu berücksichtigen hat (s.o.). Es ist offenbar die Auffassung des Gerichts, dass eine Kontrolle der Anwendbarkeit des § 48 BDSG aufgrund des überaus weiten und nicht näher eingegrenzten Wortlauts durch die Aufsichtsbehörde gar nicht möglich ist. Auch hat der Beklagte die unstreitig erfolgte Überprüfung der unbedingten Erforderlichkeit gem. § 48 Abs. 1 BDSG vorgenommen, sodass sich schon aus dieser Tatsache die Annahme eines Verstoßes gegen den Vorrang des Gesetzes verbietet.

dd. Zwischenergebnis

Folglich besteht in Form der konkret festgestellten Datenverarbeitung der Klägerin ein Verstoß gegen Bestimmungen des Datenschutzes i.S.d. § 43 HmbJVollzDG, da keine ausreichende Rechtsgrundlage für eine solche eingriffsintensive Verarbeitung vorliegt und damit den Anforderungen des datenschutzrechtlichen Grundsatzes der Rechtmäßigkeit nicht genügt wird. Aufgrund dessen konnte der Beklagte von seinen Abhilfebefugnissen Gebrauch machen.

b. Nichtvorliegen des Tatbestandsmerkmals der unbedingten Erforderlichkeit gem. § 48 BDSG

Selbst wenn unterstellt würde, dass § 48 BDSG bei der streitgegenständlichen Datenverarbeitung grundsätzlich Anwendung finden könnte, ist die Beurteilung des Gerichts, dass das Tatbestandsmerkmal der „*unbedingten Erforderlichkeit*“ gem. § 48 BDSG im vorliegenden Fall erfüllt sei (VG Hamburg, a.a.O., Seite 23), fehlerhaft. Das Verwaltungsgericht definiert den Zweck der Verarbeitung in einer Art und Weise, die mit dem Grundsatz der Zweckbindung nach § 47 Ziff. 2 BDSG unvereinbar ist **(aa.).** Im Rahmen der für die Bestimmung der unbedingten Erforderlichkeit vorzunehmenden Abwägung verwendet das Verwaltungsgericht einen verkürzten Begriff, der dazu führt, dass es das Tatbestandsmerkmal der unbedingten Erforderlichkeit fehlerhaft als die „*ermittlungstaktisch sinnvoll*(e)“ Nutzung der Gesamtdatei (VG Hamburg, a.a.O., Seite 23) definiert und bejaht wird **(bb.)**.

aa. Zweck der Datenverarbeitung durch die Klägerin

Obwohl das Verwaltungsgericht zunächst dem Beklagten fehlerhaft vorhält, er würde den Verfahrensgegenstand in unzulässiger Weise fragmentieren (VG Hamburg, a.a.O., Seite 18; s.o.), nimmt es selbst bei der Bestimmung der Frage ob eine unbedingte Erforderlichkeit der Verarbeitung i.S.d. Norm vorliegt, eine verkürzte und verfehlte Definition des Verarbeitungszwecks vor. Nach Ansicht des Verwaltungsgerichts besteht der Zweck der Nutzung der Referenzdatenbank in der (effektiven) Nutzung der Grunddatei (VG Hamburg, a.a.O., Seite 23). Die Nutzung einer Datei durch die Polizei ist jedoch kein festgelegter eindeutiger Zweck i.S.v. § 47 Ziff. 2 BDSG und kann daher nicht für die Ausfüllung des Begriffs der unbedingten Erforderlichkeit herangezogen werden. Der Zweck der Nutzung der Referenzdatenbank kann vielmehr nur die Ausübung eigener Kompetenzen der Klägerin sein, also im Anwendungsbereich der JI-Richtlinie zu Zwecken der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung (Wolff/Brink-Hertfelder, BeckOK Datenschutzrecht, 30. Edition, § 47 BDSG Rn. 12). Als Zweck der Datenverarbeitung durch die Klägerin ist daher – anders als vom Verwaltungsgericht angenommen – allein die Nutzung der Referenzdatenbank zur Unterstützung der Ermittlung von Personen, die im Rahmen der Demonstrationen gegen den G20-Gipfel womöglich Straftaten verübt haben, anzusehen.

bb. Definition des Tatbestandsmerkmals

Nach § 48 Abs. 1 BDSG ist vorausgesetzt, dass die Verarbeitung besonderer Kategorien personenbezogener Daten durch Polizei und/oder Justiz zu den in § 45 BDSG genannten Zwecken unbedingt erforderlich ist. Diese Anforderung gibt Art. 10 JI-Richtlinie vor, sie ist dadurch europarechtlich determiniert und kann nicht durch Rückgriff auf ein Verständnis des Begriffs im deutschen Recht interpretiert werden (vgl. EuGH, Rs. C-524/06 Huber./. Bundesrepublik Deutschland, Urt. v. 16.12.2008, Rn. 52; und bereits in der Anordnung, S. 12 ff.).

Das Merkmal, dass eine Verarbeitung unbedingt erforderlich (engl. „*strictly necessary*“) sein muss, entstammt der Rechtsprechung des EuGH, der unter diesem Maßstab eine strenge Erforderlichkeitsprüfung durchführt (vgl. bereits Anordnung des Beklagten vom 18.12.2018, Seite 22 ff.; EuGH, verb. Rs. C-293/12 und C-594/12 Digital Rights Ireland u.a., Rn. 52 f.). Davon weicht die Begründung des Verwaltungsgerichts, ohne sich mit dieser Rechtsprechung auseinanderzusetzen, ab. Stattdessen reduziert das Verwaltungsgericht das Tatbestandsmerkmal auf alle Maßnahmen, die „*ermittlungstaktisch sinnvoll*“ erscheinen (VG Hamburg, Seite 23). Dadurch erweitert sich die Zulässigkeit von Datenverarbeitung gegenüber der vom EuGH vorgenommenen Prüfung deutlich, sodass das Verwaltungsgericht zu dem fehlerhaften Ergebnis gelangt, dass das Merkmal der unbedingten Erforderlichkeit erfüllt sei.

Folgt man der Rechtsprechung des EuGH erhöhen sich folglich die Anforderungen an die Durchführung der Datenverarbeitung, um den mit ihr angestrebten Zweck zu erreichen. Die Erstellung der Referenzdatenbank greift in die Grundrechte der in den verwendeten Videoaufzeichnungen abgebildeten Personen auf Datenschutz, informationelle Selbstbestimmung und auch das Recht zur friedlichen Teilnahme an Demonstrationen ein. Um deren Gesichter mit den Gesichtstemplates der von der Polizei einer Straftat verdächtigten Personen abgleichen zu können, sind in der Referenzdatenbank auch eine Vielzahl von Gesichtstemplates gänzlich unbeteiligter Personen oder Personen, die an einer Demonstration teilgenommen haben, enthalten. Aufgrund des besonderen Umfangs des gesicherten Videomaterials hat der Beklagte diese Positionen abgewogen und in seiner Anordnung begründet, warum diese als nicht unbedingt erforderlich angesehen werden kann (Anordnung des Beklagten vom 18.12.2018, Seite 23).

c. Ermessensausübung

Entgegen der Auffassung des Verwaltungsgerichts (VG Hamburg, a.a.O., Seite 31 ff.) ist die Löschungsanordnung zur Wiederherstellung datenschutzkonformer Zustände auch ermessensfehlerfrei. Da die tatbestandlichen Voraussetzungen des § 6 HmbRLUmsG i.V.m.

§ 43 Abs. 1 Satz 5 HmbJVollzDSG vorlagen, durfte der Beklagte die Löschung der Referenzdatenbank als geeignete Maßnahmen anordnen, da dies zur Beseitigung des erheblichen Verstoßes gegen datenschutzrechtliche Vorschriften erforderlich war. Von diesem durch § 43 Abs. 1 Satz 5 HmbJVollzDSG eingeräumten Ermessen hat der Beklagte pflichtgemäß Gebrauch gemacht.

Dies gilt, entgegen der Ansicht des Verwaltungsgerichts, sowohl bezüglich des Entschließungs- **(aa.),** als auch des Auswahlermessens **(bb.).**

aa. Entschließungsermessen

In Anbetracht dessen, dass der Beklagte zu Recht davon ausging, dass die Tatbestandsvoraussetzungen des § 43 Abs. 1 Satz 5 HmbJVollzDSG vorliegen, hat er, indem er sich entschloss gegen die Klägerin vorzugehen, auch sein Entschließungsermessen nicht überschritten.

bb. Auswahlermessen

Innerhalb des Auswahlermessens ist es der Entscheidung der Behörde überlassen, welche rechtmäßige sowie sachgerechte und zweckmäßige Auswahl von mehreren zulässigen Maßnahmen sie trifft. Bezüglich der Auswahl der konkreten Maßnahme zur Beseitigung des festgestellten und fortbestehenden Verstoßes, der in der Verarbeitung personenbezogener Daten ohne Rechtsgrundlage entgegen § 47 Nr. 1 BDSG besteht, hat der Beklagte pflichtgemäß und dezidiert die Geeignetheit, Erforderlichkeit und Angemessenheit der Löschungsanordnung geprüft (Anordnung des Beklagten vom 18.12.2018, Seite 25 ff.). Insbesondere hat der Beklagte mildere Mittel, wie etwa eine Verwarnung auszusprechen oder die Versuche eine außergerichtliche Einigung zu bewirken, in Betracht gezogen, diese hatten sich jedoch nicht als ebenso wirksam, wie die schließlich erlassene Löschungsanordnung erwiesen (Anordnung des Beklagten vom 18.12.2018, Seite 26 ff.).

Die Ausführungen des Gerichts, dass ein Ermessensfehler vorliegt, weil der Beklagte als milderes Mittel „*normenkonkretisierende Auflagen*“ hätte erlassen können, ist fehlerhaft. Die Frage der Rechtmäßigkeit einer Verarbeitung betrifft im vorliegenden Fall die Frage, ob personenbezogene Daten überhaupt von der Polizei Hamburg durch den Einsatz der Gesichtserkennungssoftware verarbeitet werden durften (s.o.). Die Frage, ob eine Rechtsgrundlage besteht, ist notwendigerweise der Frage nach dem „Wie“ der Verarbeitung, also unter welchen Bedingungen und unter Umsetzung welcher konkreten technischen und organisatorischen Maßnahmen personenbezogene Daten verarbeitet werden dürfen, vorgelagert. Da der festgestellte Verstoß im vorliegenden Fall den Grundsatz der

Rechtmäßigkeit nach § 47 Nr. 1 BDSG betrifft, musste der Beklagte nicht noch weitere, zusätzliche Verstöße auf der Ebene des „Wie“ feststellen. Die Frage, ob etwa eine hinreichende Protokollierung erfolgt (vgl. VG Hamburg, a.a.O., Seite. 33), stellt sich zwangsläufig erst dann, wenn die grundsätzliche Verarbeitung von biometrischen Daten durch eine legitime Rechtsgrundlage gestattet ist. Da es bereits an einer Rechtsgrundlage mangelt, an der die Rechtmäßigkeit der Maßnahme gemessen werden kann, ist der Beklagte auch gar nicht in der Lage, konkrete Verstöße gegen eine solche Rechtsgrundlage festzustellen und dementsprechend Auflagen zu erlassen, die einen Verstoß kompensieren könnten (Korte, ZD-Aktuell 2020, 06955).

2. Besondere Schwierigkeiten der Rechtssache, § 124 Abs. 2 Nr. 2 VwGO

Die Rechtssache weist besondere Schwierigkeiten in tatsächlicher und rechtlicher Hinsicht i.S.d. § 124 Abs. 2 Nr. 2 VwGO auf. Nach Ansicht des OVG Hamburg sind besondere – tatsächliche und rechtliche – Schwierigkeiten solche die das Maß des in verwaltungsrechtlichen Streitigkeiten Üblichen erheblich übersteigen (OVG Hamburg, Beschluss v. 16.4.1999 – 5 Bs 71/99; vgl. auch OVG Lüneburg, Beschluss v. 12.9.2011 – 11 LA 209/11).

Der vorliegende Rechtstreit stellt an den entscheidenden Richter deutlich höhere Anforderungen als der Normalfall (vgl. OVG Hamburg, Beschluss v. 26.7.1999 – 3 Bf 92/99).

Aufgrund des komplexen, dem Fall zugrundeliegenden Datenverarbeitungsvorgangs bestehen besondere tatsächliche **(a.)** und rechtliche Schwierigkeiten, insbesondere im Hinblick auf die Stellung und die Befugnisse des Beklagten und des dabei heranzuziehenden Normengefüges **(b.)**.

a. Komplexer Datenverarbeitungsvorgang

Die Rechtssache weist besondere tatsächliche Schwierigkeiten i.S.d. § 124 Abs. 2 Nr. 2 VwGO auf. Der der Entscheidung zugrundeliegende Sachverhalt weist eine überdurchschnittliche Komplexität auf. Der Sachverhalt betrifft eine Technologie, die – soweit ersichtlich – noch nicht Gegenstand verwaltungsprozessualer Rechtsprechung war. Der Einsatz biometrische Gesichtserkennung durch die Polizei bei Massenveranstaltungen und das Anlegen großer biometrischer Datenbanken unter Zuhilfenahme von Daten, die durch Bürger bereitgestellt werden, stellen neuartige Entwicklungen dar, die bislang nur theoretisch behandelt wurden. Für den Einsatz in der Praxis bestehen daher noch keine gesicherten Erfahrungswerte.

Die von der Klägerin eingesetzte Gesichtsanalysesoftware führt eine komplexe Datenverarbeitung mit mehreren Abschnitten durch. Dabei ist zwischen den einzelnen Phasen der Verarbeitung, von der Erstellung der Grunddatei, der Erstellung der Referenzdatenbank und ihrer Nutzung zu unterscheiden. Auch diese einzelnen Phasen weisen verschiedene Verarbeitungsvorgänge auf, die bezüglich der streitgegenständlichen Verarbeitungsphase der Erstellung der Referenzdatenbank wiederum aus mehreren Abschnitten besteht. So werden, damit die Referenzdatenbank zum Abgleich mit den von der Klägerin erstellten Gesichtstemplates verdächtiger Personen genutzt werden kann, zunächst von allen auf den Bild- und Videoaufnahmen von der Gesichtsanalysesoftware automatisiert als Gesichter identifiziert und diese in Templates umgewandelt, um einen solchen Abgleich überhaupt zu ermöglichen. Diese komplexen technischen Abläufe führen dazu, dass die Beurteilung der zugrundeliegenden Datenverarbeitung das in verwaltungsrechtlichen Streitigkeiten das übliche Maß erheblich übersteigt.

b. Befugnisse des Beklagten nach § 43 HmbJVollzDSG

Auch die Frage der Ausübung und des Umfangs der Befugnisse des Beklagten nach § 43 HmbJVollzDSG gegenüber anderen öffentlichen Stellen stellt deutlich höhere Anforderungen als ein normaler verwaltungsgerichtlicher Rechtstreit.

Dies folgt daraus, dass Aufsichtsbehörden nicht zur kontrollierenden Verwaltungstätigkeit im traditionellen Sinne gehören (vgl. Petri/Tinnefeld, MMR 2010, S. 157 (157)). Der Beklagte hat - wie unter II.1.a.cc.) dargelegt - als datenschutzrechtliche Aufsichtsbehörde eine vom primären Europarecht garantierte unabhängige Sonderstellung mit dem Auftrag der institutionellen Datenschutzkontrolle inne. Teilweise wird daher vertreten, dass datenschutzrechtliche Aufsichtsbehörden, als unabhängigen Kontrollinstanzen für die Datenverarbeitung sowohl privater, als auch staatlicher Stellen nicht mehr als Teil von Legislative, Exekutive oder Judikative einzuordnen wären, sondern vielmehr als Kontrollorgane sui generis zu qualifizieren sind (Kühling/Buchner-Boehm, DS-GVO BDSG Kommentar, 2. Aufl. 2018, Art. 51 DS-GVO Rn. 10). Diese Sonderstellung hat sich auch in Art. 60a der Hamburgischen Verfassung niedergeschlagen, nach der der Beklagte unabhängig und nur dem Gesetz unterworfen ist. Der HmbBfDI findet aufgrund seiner unions- und verfassungsrechtlichen bedingten Sonderstellung folgerichtig auch keinerlei Erwähnung im Hamburgischen Gesetz über Verwaltungsbehörden. Diese Sonderstellung ist dem deutschen Verfassungs- und Verwaltungsrecht weitestgehend unbekannt. Der Umfang der Befugnisse der Aufsichtsbehörde, die hier entscheidungserheblich sind, können dabei nicht ohne weiteres einfach dem HmbJVollzDSG oder der bereits dazu ergangenen Rechtsprechung entnommen werden. Im Gegensatz zu einer Ordnungsbehörde im traditionellen Sinne muss die Frage, ob der Beklagte auch Maßnahmen anordnen kann,

wenn die Datenverarbeitung der Klägerin gegen die Verfassung verstößt, sowohl anhand des einschlägigen europäischen primär- und Sekundärrechts, als auch den nationalen Vorschriften und im Lichte der Rechtsprechung des EuGH und BVerfG bestimmt werden (s.o.). Dies stellt erhöhte Anforderungen an das Gericht im Normalfall. Hinzu tritt, dass die auf der JI-Richtlinie beruhenden hier heranzuziehenden Normen erst seit Mai 2018 Wirkung entfalten und es sich damit um ein junges Normengefüge handelt.

3. Grundsätzliche Bedeutung, § 124 Abs. 2 Nr. 3 VwGO

Die Rechtssache ist ferner von grundsätzlicher Bedeutung i.S.d. § 124 Abs. 2 Nr. 3 VwGO.

Eine grundsätzliche Bedeutung liegt vor, wenn der Rechtsstreit eine entscheidungserhebliche, bisher höchstrichterlich oder obergerichtlich nicht beantwortete Rechts – oder Tatfrage von allgemeiner Bedeutung aufwirft, die sich in dem erstrebten Rechtsmittelverfahren stellen würde und die im Interesse der Einheitlichkeit der Rechtsprechung oder der Fortentwicklung des Rechts einer obergerichtlichen Klärung in einem Berufungsverfahren bedarf (vgl. OVG Berlin-Brandenburg, Beschluss v. 12.1.2018 – OVG 11 N 119/17, Rn. 2).

Von grundsätzlicher Bedeutung i.S.d. Definition ist vorliegend die Frage des Umfangs der Befugniswahrnehmung des Beklagten gegenüber einer anderen öffentlichen Stelle **(a)**. Es besteht darüber hinaus Vereinheitlichungsbedarf bezüglich der Auslegung der Reichweite des Grundsatzes der Rechtmäßigkeit in § 47 BDSG **(b)**. und der Frage der Anwendbarkeit des § 48 BDSG auf Maßnahmen der biometrischen Gesichtserkennung **(c)**.

a. Befugniswahrnehmung durch datenschutzrechtliche Aufsichtsbehörden nach § 43 HmbJVollzDSG

Die entscheidungserhebliche Frage, ob der Beklagte auch von seinen Abhilfebefugnissen nach § 43 HmbJVollzDSG Gebrauch machen kann, wenn behördliches Handeln gegen die Verfassung oder das Unionsrecht verstößt, ist von grundsätzlicher Bedeutung. An der obergerichtlichen Klärung besteht auch ein über diesen konkreten Einzelfall hinausgehendes allgemeines Interesse.

§ 43 Abs. 1 Satz 5 HmbJVollzDSG ist erst seit Mai 2018 in Kraft und dient der Umsetzung des Art. 47 Abs. 2 Nr. b JI-Richtlinie, der nationalen Gesetzgebern der Mitgliedstaaten aufgibt, durch Rechtsvorschriften vorzusehen, dass jede (datenschutzrechtliche) Aufsichtsbehörde über wirksame Abhilfebefugnisse verfügt, die ihr z.B. gestatten den Verantwortlichen anzuweisen, Verarbeitungsvorgänge, gegebenenfalls auf bestimmte Weise

und innerhalb eines bestimmten Zeitraums, mit den nach der Richtlinie erlassenen Vorschriften in Einklang zu bringen, insbesondere durch die Anordnung der Berichtigung und Löschung personenbezogener Daten.

Die Umsetzung des Art. 47 Abs. 2 JI-Richtlinie in § 43 Abs. 1 Satz 5 HmbJVollzDSG eröffnet erstmalig die Möglichkeit für den Beklagten, überhaupt eine Anordnung gegenüber anderen öffentlichen Stellen zu erlassen. Vorliegend handelt es sich – soweit ersichtlich - dabei nicht nur um die erste Anordnung des Beklagten aufgrund von § 43 Abs. 1 S. 5 HmbJVollzDSG, sondern auch um die erste Anordnung des Beklagten – oder einer anderen (deutschen) datenschutzrechtlichen Aufsichtsbehörde – gegenüber einer anderen öffentlichen Stelle im Allgemeinen. Nach bisheriger Rechtslage stand dem Beklagten - und anderen nationalen Aufsichtsbehörden - allenfalls die Möglichkeit der Beanstandung gegenüber öffentlichen Stellen zu (vgl. § 25 HmbDSG a.F., § 25 BDSG a.F.). Dabei wurde ganz überwiegend vertreten, dass eine datenschutzrechtliche Beanstandung über keine Verwaltungsaktqualität verfügt (BVerwG, Beschluss v. 5.2.1992 – 7 B 15/92). Dies hatte zur Folge, dass eine gerichtliche Überprüfung von Abhilfebefugnissen gegenüber anderen öffentlichen Stellen nicht stattfand. Die Frage, was unter „*Verstöße gegen Vorschriften über den Datenschutz*“ zu verstehen ist und inwieweit eine datenschutzrechtliche Kontrollbefugnis der unabhängigen Datenschutzbehörden reicht und der Beklagte auch von seinen Abhilfebefugnissen Gebrauch machen kann, wenn behördliches Handeln gegen die Verfassung verstößt, ist vor dem Hintergrund des vorliegenden Urteils damit nicht geklärt. Diese Frage stellt sich dabei nicht nur im Bereich der im gesamten Bundesgebiet umzusetzenden JI-Richtlinie, sondern auch gegenüber öffentlichen Stellen die nicht dem Anwendungsbereich der JI-Richtlinie unterfallen, sondern in den Geltungsbereich der DSGVO (vgl. Art. 58 Abs. 2 DSGVO). Im Anwendungsbereich der DSGVO, der den eingriffsintensiven Bereich der Strafverfolgung und straftatbezogenen Gefahrenabwehr ausnimmt, steht dem Beklagten gegenüber anderen öffentlichen Stellen eine Reihe von Abhilfebefugnissen zu. Insbesondere kann der Beklagte nach Art. 58 Abs. 2 lit. g DSGVO auch gegenüber anderen öffentlichen Stellen die Löschung personenbezogener Daten anordnen.

b. Reichweite des Grundsatzes der Rechtmäßigkeit nach § 47 Ziff. 1 BDSG

Entscheidungserheblich ist die Frage der Reichweite des Grundsatzes der Rechtmäßigkeit. In § 47 Ziff. 1 BDSG ist nunmehr explizit der Grundsatz der Rechtmäßigkeit, wie er in Art. 4 Abs. 1 lit. a JI-Richtlinie enthalten ist, umgesetzt (s.o.). Dabei ist bei der Auslegung des Grundsatzes auch das europäische Primärrecht, insbesondere die Vorschrift des Art. 8 GRCh zu beachten. Es liegt bisher keine höchstrichterliche Rechtsprechung zu Auslegung und Reichweite dieses für das Datenschutzrecht zentralen Grundsatzes vor. Für den vorliegenden Rechtstreit ist dabei insbesondere erheblich, inwieweit die Anforderungen, die

EuGH und BVerfG bezüglich der Bestimmtheit gesetzlicher Vorschriften entwickelt haben, auch im Rahmen des Grundsatzes der Rechtmäßigkeit zu beurteilen sind. Aufgrund der speziellen Stellung und Aufgaben bezüglich des Grundrechtsschutzes von betroffenen Personen (wie bereits dargestellt) stellt sich diese Frage vor dem Hintergrund der streitgegenständlichen Anordnung.

c. Biometrische Gesichtserkennung aufgrund von § 48 BDSG

Von grundsätzlicher Bedeutung sind ferner die entscheidungserheblichen Fragen der Rechtmäßigkeit der biometrischen Gesichtserkennung aufgrund von § 48 BDSG (s.o.) und das Verhältnis zum bereichsspezifischen Fachrecht. Die damit einhergehende Frage der Eingriffstiefe derartiger Maßnahmen und die damit korrespondierende Frage, welche Anforderungen an die Regelungsdicht von Ermächtigungsnormen zu stellen sind, sind bisher überhaupt noch nicht richterlich entschieden worden. Es handelt sich beim vorliegenden Urteil auch um das erste Urteil zu § 48 BDSG und dessen Anwendungsbereich sowie bezüglich des dritten Teils des BDSG. Die Frage hat über diesen Rechtsstreit hinaus gehende Bedeutung und bedarf im Interesse der Rechtssicherheit bzw. Rechtseinheit einer obergerichtlichen Klärung.

Die vorliegende Thematik weist zudem besondere praktische Bedeutung über den Einzelfall hinaus für die Handhabung zukünftige Gesichtserkennungstechnologien auf. Die Klägerin hat wiederholt gegenüber dem Beklagten, als auch in der Öffentlichkeit angekündigt ggf. im Rahmen von erwarteten Krawallen bei Fußballspielen die Gesichtserkennungssoftware wieder einsetzen zu wollen (vgl. Bericht des Innenausschuss, Bü-Drs. 21/15080, S. 11). Aufgrund von fortschreitenden technischen Entwicklungen und Möglichkeiten ist aber insbesondere bei allen Strafverfolgungsbehörden im Bundesgebiet mit dem vermehrten Bedürfnis zu rechnen, derartige kriminaltechnische Erneuerungen einzusetzen. Dies nicht zuletzt, weil Hersteller wie Clearview AI Inc. sich auf Gesichtserkennungssoftware spezialisiert haben und ihr Angebot direkt an Strafverfolgungsbehörden richten (https://clearview.ai/: *„Clearview is a new research tool used by law enforcement agencies to identify perpetrators and victims of crimes“).* Die Bundespolizei hat bereits im Jahr 2017 Tests mit einer sog. intelligenten Videoüberwachung im Bahnhof Berlin Südkreuz durchgeführt, bei der eine biometrische Gesichtserkennung mit einer Videoüberwachungsanlage verbunden war. Dabei dürfte es sich im Gegensatz zu der gegenständlichen Maßnahme noch um eine eingriffsmildere Variante handeln, weil bei der intelligenten Videoüberwachung im Nichttrefferfall die personenbezogenen Daten der abgeglichenen Personen umgehend wieder gelöscht werden. Anders beim Einsatz der Klägerin, die die Templates aller betroffenen Personen auf unbestimmte Zeit in der Referenzdatenbank vorhält. Dieser Einsatz traf dabei auf bestehende umfangreiche fachliche

Diskussionen über die Zulässigkeit solcher Maßnahmen, die die biometrische Verarbeitung von Gesichtsmerkmalen zu Zwecken der Strafverfolgung zum Gegenstand haben (vgl. Hornung/Schindler, ZD 2017, 203 ff.; Jandt, ZRP 2018, 16 ff. m.w.N.). Dabei ist streitig welche Anforderungen an Normen zu stellen sind, die zu derartigen Maßnahmen ermächtigten könnten. Es geht nicht zuletzt aber auch um die Frage, inwieweit technische Neuerungen oder Auswertungsmethoden noch von bestehenden Normen gedeckt sind (ablehnend zur automatisierten Auswertung von Videoaufzeichnungen aufgrund bestehender Befugnisnormen zur Videoüberwachung : OVG Hamburg, Urteil v. 22.6.2010 – 4 Bf 276/07, Rn. 102) oder es einer ausdrücklichen Entscheidung des Gesetzgebers bedarf (vgl. zum Streitstand: Wissenschaftlicher Dienst des Bundestages – WD 3 – 3000 - 202/16). Aufgrund der bestehenden Unsicherheit, inwieweit und unter welchen Voraussetzungen der Einsatz von Gesichtserkennungssoftware und damit korrespondierende weite Grundrechtseingriff (s.o.) durch den Gesetzgeber geregelt werden kann, wurde zuletzt von der Schaffung einer Rechtsgrundlage zumindest auf Bundesebene abgesehen (vgl. https://www.zeit.de/politik/deutschland/2020-01/bundespolizeigesetz-gesichtserkennung-verzicht-horst-seehofer). Bemerkenswert ist insoweit, dass nach Auffassung des Bundesinnenministers jedenfalls für die angesprochene intelligente Videoüberwachung eine Rechtsgrundlage in jedem Fall erforderlich ist.

III.

Nach alledem ist die Berufung zuzulassen.