Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Ludwig-Erhard-Str. 22, 7. OG
20459 Hamburg
Telefon: 040 - 428 54 – 40 40
Telefax: 040 - 428 54 - 40 00
Ansprechpartner: Herr Prof. Dr. Caspar
E-Mail*: mailbox@datenschutz.hamburg.de

Az.: 11.03-13

Hamburg, den 18. Dezember 2018

Herrn Senator
Freie und Hansestadt Hamburg
Behörde für Inneres und Sport
Johanniswall 4
20095 Hamburg

Einsatz der Gesichtserkennungssoftware „Videmo 360“ durch die Polizei Hamburg zur Aufklärung von Straftaten im Zusammenhang mit dem in Hamburg stattgefundenen G20-Gipfel

Anordnung gemäß § 6 des Hamburgischen Gesetz zur Aufsicht über die Anwendung der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschrift (HmbRI(EU)2016/680UmsAAG) i.V.m. § 43 Abs. 1 S. 5 Hamburgisches Gesetz zum Schutz personenbezogener Daten im Justizvollzug (HmbJVollzDSG)

Sehr geehrter Herr Senator,

der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) als zuständige Aufsichtsbehörde für den Datenschutz (§§ 4 Abs. 1 i.V.m. 2 Abs. 1 HmbRI(EU)2016/680UmsAAG) ordnet hiermit gegenüber der Behörde für Inneres und Sport, als Aufsichtsbehörde der Polizei Hamburg i.S.d § 6 HmbRI(EU)2016/680UmsAAG i.V.m § 43 HmbJVollzDSG, die folgende Maßnahme an:

> **Die von der Polizei Hamburg durch die Sonderkommission „Schwarzer Block“ im Rahmen der Ermittlungen zur Aufklärung von Straftaten im Zusammenhang mit dem im Juni 2017 in Hamburg stattgefundenen G20-Gipfel ab November 2017 erstellte Referenzdatenbank mit mathematischen Modellen von menschlichen Gesichtern (gem. der Verfahrensbeschreibung vom 18.10.2017) ist zu löschen.**

Begründung

I. Sachverhalt

Die Polizei Hamburg richtete im Juli 2017 für ihre Ermittlungstätigkeiten bezüglich strafrechtlich relevanter Ereignisse im Zusammenhang mit dem im Juni 2017 in Hamburg stattgefundene G20-Gipfel die Sonderkommission „Schwarzer Block“ (Soko „Schwarzer Block“) ein. Die Soko „Schwarzer Block“ setzt derzeit im Rahmen dieser Tätigkeit die Gesichtserkennungssoftware „Videmo 360“ (GAS) für die Verarbeitung von großen Mengen Bild- und Videomaterial ein. Diese GAS lokalisiert menschliche Gesichter auf Bild- und Videoaufzeichnungen, berechnet deren charakteristische Merkmale und erstellt und speichert mathematische Modelle dieser Gesichter (sog. Templates) und ermöglicht den Abgleich dieser Templates untereinander.

Der Soko „Schwarzer Block“ liegen mit Stand vom 6. August 2018 insgesamt 100 TB Bild- und Videomaterial vor. Das davon für die GAS genutzte Rohmaterial umfasste ca. 17 TB. Der Datenbestand auf dem GAS-Server wird in unregelmäßigen Abständen aktualisiert. Nach Angaben der Polizei vom Februar 2018 betrug die Anzahl der Dateien, die im Rahmen der Gesichtserkennungssoftware verarbeitet wurden, ca. 25.000. Mit Stand vom 06. August 2018 hat sich die Anzahl an Dateien auf rund 31.637 erhöht. Dabei handelt es sich um 15.157 Videodateien und 16.480 Bilddateien. Die Anzahl der Dateien auf dem GAS-Server ist schwankend und tendenziell anwachsend. Die von der GAS verarbeiteten Dateien setzen sich zusammen aus Bild- und Videoaufzeichnungen, welche die Polizei Hamburg selbst hergestellt hat (sog. polizeieigenes Material inklusive Bilder von sog. erkennungsdienstlichen Maßnahmen), sowie aus Bild- und Videoaufzeichnen, die von externen Quellen erhoben bzw. zur Verfügung gestellt worden (sog. polizeifremdes Material). Das polizeifremde Material wiederum fügt sich zusammen aus Material von Überwachungskameras von S-Bahnhöfen, Material vom Hinweisportal „Boston Infrastruktur“ des BKA sowie aus dem Internet und von den Medien. Material von acht S-Bahnhöfen wurde in das System eingespielt. Dabei handelte es sich um Videomaterial von folgenden Bahnhöfen und Zeiträumen im Jahr 2017:

* Königstraße: vom 06.07. (12:00) bis 10.07. (19:30)
* Landungsbrücken: 06.07. (12:00) bis 10.07 (19:45)
* Altona: 06.07. (12:00) bis 10.07 (20:15)
* Diebsteich und Stellingen: 06.07 (12:00) bis 07.07. (07:00)
* Eidelstedt: 06.07. (12:00) bis 10.07. (05:00)
* Langenfelde: 06.07 (12:00) bis 10.07. (05:00)
* Reeperbahn: 07.07. (08:30) bis 10.07. (05:00)

Der Inhalt des Materials wurde nicht durch einen menschlichen Bearbeiter der Soko „Schwarzer Block“ gesichtet oder aussortiert, sondern das Material wurde direkt in die GAS eingespielt. Darüber hinausgehendes sichergestelltes ÖPNV-Material, das der Soko „Schwarzer Block“ auf 159 externen Festplatten vorliegt (Daten von Überwachungskameras aus U-Bahnhöfen (83,6 TB), Bild und Videomaterial aus dem Hauptbahnhof (510 GB), Bild- und Videomaterial aus Bussen (1,139 TB), sowie 40 Festplatten aus U-Bahnen), wurde nicht auf den GAS-Server eingespielt. Als Grund dafür gibt die Polizei technische Gegebenheiten (Dauer des Exports der Dateien von den externen Festplatten auf den Server und benötigter Zeitraum für die Analyse der Daten durch die Software sowie Kapazitätsgrenzen) an.
Die zweite große Gruppe von verwendeten polizeifremden Dateien stammt von dem Hinweisportal „Boston Infrastruktur“. Dieses Hinweisportal war im Zeitraum vom 08.07.17 (03:00 Uhr) bis 17.07.17 (23:45 Uhr) der Öffentlichkeit freigegeben. Es ermöglichte der Bevölkerung das Hochladen von Bild- und Videodateien. Das Hinweisportal ist ein Webportal, welches auf den Servern des BKA betrieben wird. Die Daten wurden auf den Servern des BKA entgegengenommen und per VPN-Verbindung aus Hamburg abgerufen. Über das Hinweisportal gingen 10.588 einzelne Hinweise ein, die insgesamt 14.334 Dateien enthielten. Über 4.500 dieser Dateien sortierte die Polizei Hamburg durch eine manuelle Sichtung aus, weil sie keine Relevanz für die G20-Ereignisse hatten (z.B. Videos mit pornographischem Inhalt) und löschte sie. Eine G20-Relevanz lag für die Polizei Hamburg immer dann vor, wenn die Bild- und Videosequenzen einen gewissen örtlichen und zeitlichen Zusammenhang zu den Ausschreitungen in Hamburg vor und während des Gipfels aufwiesen. Die Abbildung von strafrechtlich bedeutsamem Verhalten war nicht Voraussetzung für die Bejahung einer G20-Relevanz und für die Verwendung der Dateien im Rahmen der GAS.

Im Einzelnen stellen sich die Arbeitsabläufe wie folgt dar:

Am 23.11.2017 begann die Soko „Schwarzer Block“ mit dem Anlegen einer sog. Referenzdatenbank durch Einspielung der ca. 17 TB Rohdaten in die Software. Dieser Prozess dauerte acht Wochen. Dabei wurden folgende Teilfunktionen vorgenommen: Detektion und Identifikation. Während unter Detektion das reine Auffinden der Gesichter in einer Bild- oder Videosequenz zu verstehen ist, werden im Rahmen der Identifikation auch die Templates gebildet. Unter Templates sind mathematische Modelle der wesentlichen Merkmale des Gesichts zu verstehen. Dabei wird jedes einzelne Gesicht, das zuvor im Rahmen der Lokalisierung erkannt wurde, analysiert und identifizierbar gemacht. Diese Analyse/Identifikation basiert auf einem festgelegten, standardisierten Verfahren und umfasst markante Punkte des menschlichen Gesichts (z.B. Augenabstände, Nasenform, Ohr-zu-Ohr, Mundwinkel, Haaransatz). Die erfassten Punkte werden für jedes Gesicht in einer

mathematischen Form abgespeichert. Diese mathematischen Formen werden dann samt Fundstelle (d.h. Name des Videos, Chipkartennummer, Clip-Nr., Zeitstempel) in der Referenzdatenbank hinterlegt. Diese Datenbank dient der GAS später als Basis für den Vorgang des Abgleichs und der Wiedererkennung der einzelnen Templates untereinander. Das gesamte Material wurde von der Polizei Hamburg einer nachträglichen örtlichen und zeitlichen Zuordnung unterzogen. Eine örtliche und zeitliche Zuordnung ist jedoch nicht in jedem Fall zweifelsfrei möglich, da die dafür erforderlichen Informationen in vielen Fällen nicht übermittelt worden sind oder ermittelt werden konnten. Die Software erfasst nur Gesichter. Weitere Merkmale einer Person wie z.B. der Gang oder die Kleidung lokalisiert und analysiert die Software nicht. Starke Neigung, Drehung oder Vermummung von Gesichtern können die Identifizierung als Gesicht verhindern. Neben den Templates erstellt die Software auch einen Konfidenzwert über die Wahrscheinlichkeit, dass das vermeintlich gefundene Gesicht wirklich ein menschliches Gesicht ist. Die mögliche Funktion, die eine Schätzung über Alter und Geschlecht vornimmt, wird von der Soko „Schwarzer Block“ derzeit nicht genutzt. Angaben über die Anzahl der erfassten Personen oder der gebildeten Templates liegen nicht vor.

In einem gesonderten und parallel laufenden Schritt zur Erstellung der Referenzdatenbank wird das polizeieigene Material von den Bildauswertern der Soko „Schwarzer Block“ manuell gesichtet. Die Auswertung erfolgt mittels Wiedererkennungsvermögen und Gedächtnisleistung des einzelnen Auswerters sowie über Rechercheunterlagen. Durch eine ebenfalls durchgeführte Geolokalisierung des Bild- und Videodatenmaterials des Datenbestandes wird die Recherche im kompletten Datenbestand nach den genannten Parametern „Zeit“ und „Ort“ ermöglicht. Die manuellen Bildauswerter der Soko „Schwarzer Block“ sind dabei in Teams aufgeteilt, die sich nach Zeit und Ort größeren Ermittlungskomplexen zuordnen lassen. Bei der manuellen Durchsicht gilt die Vorgabe, dass bei Wahrnehmung von tatsächlichen Anhaltspunkten für die Begehung einer Straftat durch eine im Video- oder Bildmaterial aufgenommene Person bei der Staatsanwaltschaft ein Antrag gestellt werden soll, um für diese Person den automatisierten Abgleich mit der Referenzdatenbank vorzunehmen. Wird der Antrag durch die Staatsanwaltschaft genehmigt, werden die Bild- bzw. Videosequenzen von der Person, die im Verdacht steht, eine Straftat begangen zu haben, zunächst manuell durch den Auswerter mit Lichtbildern abgeglichen, die während des G20-Gipfels im Rahmen von erkennungsdienstlichen Maßnahmen (ED-Maßnahmen) erhoben wurden. Bei Vorliegen eines Lichtbildes des Tatverdächtigen, das beispielsweise im Rahmen einer ED-Maßnahme erhoben wurde und nach Einschätzung des manuellen Beobachters dieselbe Person zeigt, die auf der fraglichen Videosequenz zu sehen ist, wird auch dieses Gesicht sodann zur Erstellung einer sog. Identität herangezogen. Eine Identität wird erstellt, indem das aus dem Lichtbild eines Tatverdächtigen, z.B. eines ED-Lichtbildes, extrahierte Gesicht ebenfalls nach dem oben

beschriebenen Verfahren erfasst und mit dem Gesichtstemplate aus der fraglichen Videosequenz verknüpft wird. Die verschiedensten Ermittlungstätigkeiten der Polizei ermöglichen im Einzelfall das Heranziehen der weiteren Vergleichsbilder, sodass die Aufklärungsarbeit nicht auf die G20-ED-Bilder beschränkt werden muss. Lichtbilder aus sog. Gefährderdateien wurden nach Angaben der Polizei bislang nicht herangezogen.

Seit dem 01.03.2018 (und andauernd) werden die ggf. mehreren zu einer Identität verknüpften Gesichter mit sämtlichen zuvor erstellten Gesichtstemplates, die sich in der Referenzdatenbank befinden und vorab automatisch erfasst worden waren, verglichen. Nach einer Dauer von rund zehn Minuten werden alle gefundenen Gesichter mit der genauen Fundstelle, mit der sie hinterlegt wurden (Pfad zum Video, Chipkartennr. Clipnr.), auf dem Rechercherechner aufgelistet. Der Videoauswerter muss sodann die Gesichter aus dem Suchergebnis manuell herausfiltern, die tatsächlich mit dem gesuchten Gesicht übereinstimmen. Alle dieser Treffer werden der Identität ebenfalls zugeordnet und ein weiterer Suchvorgang kann erfolgen. Dies wird in der Regel wiederholt, bis keine neuen Ergebnisse mehr hinzukommen. Die Zahl der zugeordneten Bilder kann sich dabei auf über 2.000 erhöhen. Nach jedem Suchvorgang wird ein sog. „Auswertebericht GAS-Recherche“ vom Durchführenden geschrieben. Sofern Treffer generiert wurden, werden der Pfad der Dateien, die Abspielzeit und eine Bemerkung angegeben. Teilweise wird von der Videofundstelle ein Screenshot ausgedruckt und dem Bericht beigelegt, um den Tatverdächtigen zur Verdeutlichung im Bild anzuzeigen. Dieser Auswertungsbericht wird dem beauftragten Sachbearbeiter der EA-Ermittlungen händisch übergeben. Anschließend erfolgt eine einzelfallbezogene Bewertung des Rechercheergebnisses durch diesen Sachbearbeiter.

Durch die Nutzung der Software wird sich durch die Soko „Schwarzer Block“ versprochen, das Verhalten eines Beschuldigten in der Vor- und Nachtatphase zu ermitteln, einem Beschuldigten noch weitere bis dato unbekannte Straftaten zuzuordnen und bekannte Taten aus anderen Blickwinkeln festzustellen, aber auch entlastende Informationen bezüglich des Beschuldigten zu gewinnen. Bei unbekannten Tatverdächtigen wird die GAS ebenfalls genutzt, um eine Identifizierung zu ermöglichen. Es konnte bereits mehrfach festgestellt werden, dass sich Tatverdächtige an weiteren Straftaten beteiligt haben, Ermittlungsansätze für Personenzusammensetzungen konnten geschaffen werden, Fahndungsbilder generiert und Anträge auf strafprozessuale Maßnahmen und Haftbefehle konnten mit den Ergebnissen des Software-Einsatzes angereichert werden.

Der HmbBfDI hat sich zweimal (11.10.2017 und 28.02.2018) mit Vertretern der Polizei und einem Vertreter der Staatsanwaltschaft bezüglich des Einsatzes einer GAS im Zusammenhang mit den Geschehnissen rund um den G20-Gipfel getroffen.

Der Hamburgische Polizeipräsident hat die Vorgehensweise der Polizei durch Einsatz eines Hinweisportals und dessen Auswertung im Rahmen des G20-Ausschusses als "*konzeptionelle Weiterentwicklung von nicht unerheblichen Ausmaß*" bezeichnet. Der Leiter der Soko "Schwarzer Block" gab im G20-Sonderausschusses in diesem Zusammenhang an, einen "*völlig neuen Standard in der Beweisführung" zu besitzen*" (Wortprotokoll Nr. 21/12 der öffentlichen Sitzung des Sonderausschusses „Gewalttätige Ausschreitungen rund um den G20 – Gipfel in Hamburg" vom 28. Juni 2018, S. 8 ff.).

Mit Schreiben vom 05.07.2018 hat der HmbBfDI gegenüber der Polizei Hamburg darauf hingewiesen, dass die Analyse von Gesichtsmerkmalen aus Bild- und Videosequenzen, deren Nutzung zur Erstellung von Templates und die Speicherung dieser Templates mangels Rechtsgrundlage rechtswidrig seien. Hierzu wurde eine rechtliche Beurteilung auf Basis der bis dahin durchgeführten Untersuchungen mit der Möglichkeit zur Stellungnahme vorgelegt.

Mit Schreiben vom 18.07.2018 hat sich die Generalstaatsanwaltschaft unaufgefordert unter Berufung auf ein beigefügtes Rechtsgutachten vom 13.07.2018 gegenüber dem HmbBfDI dahingehend geäußert, dass der Einsatz der GAS rechtmäßig erfolge. Mit Schreiben vom 23.07.2018 hat die Polizei Hamburg ebenfalls unter Überreichung eines erstellten Gutachtens die Rechtmäßigkeit bekräftigt.

Mit Schreiben vom 30.08.2018 übersendete der HmbBfDI an den Senator der Behörde für Inneres und Sport eine offizielle Beanstandung des Einsatzes der GAS. Dabei wurde auf ein anliegendes Rechtsgutachten des HmbBfDI verwiesen, welches auch unter Berücksichtigung der von Polizei und Generalstaatsanwaltschaft aufgeführten Einschätzungen erneut zu dem Ergebnis gelangt, dass der Einsatz der GAS rechtswidrig erfolge und die Referenzdatenbank daher zu löschen sei.

Mit Schreiben vom 29.09.2018 äußert sich der Senator der Behörde für Inneres und Sport gegenüber dem HmbBfDI dahingehend, dass keine Gesichtspunkte erkennbar seien, die auf eine rechtswidrige Datenverarbeitung durch den Einsatz der GAS schließen ließen. Dies folge aus dem Schreiben beigefügten, durch die Polizei Hamburg erneut erstellten Rechtsgutachten vom 12.09.2018. Eine Löschung der Datenbank sei daher nicht vorzunehmen.

Auf eine kleine schriftliche Anfrage von Abgeordneten der Fraktion DIE LINKE vom 02.08.2018 antwortete der Senat, die in der Soko „Schwarzer Block“ verwendete EDV-Struktur zur systematischen Bild- und Videoauswertung stehe aktuell dem Landeskriminalamt (LKA) Hamburg analog zur Abarbeitung von Großereignissen bereits zur Verfügung und solle auch künftig dort zu diesem Zweck genutzt werden. Aktuell werde die GAS vom LKA nicht genutzt (Drs. 21/13939 vom 10.08.2018: Antwort zu Frage Nr. 12). Diese Ankündigung wurde im Innenausschuss durch den Innensenator bekräftigt (Bericht des Innenausschusses v. 21.11.2018, Drs. 21/15080, S. 2).

II. Formelle Rechtmäßigkeit der Anordnung

Die Zuständigkeit des HmbBfDI für den Erlass dieser Anordnung gegenüber der Aufsichtsbehörde der Polizei Hamburg folgt aus § 4 Abs. 1 i.V.m. § 2 Abs. 1 HmbRI(EU)2016/680UmsAAG. Danach ist der HmbBfDI zuständig für die Aufsicht über die Verarbeitung personenbezogener Daten durch öffentliche Stellen der Freien und Hansestadt Hamburg, soweit deren Tätigkeiten der Richtlinie (EU) 2016/680 unterfallen. In dieser Eigenschaft kann er gem. § 6 HmbRI(EU)2016/680UmsAAG i.V.m § 43 Abs. 1 S. 5 HmbJVollzDSG geeignete Maßnahmen gegenüber der Aufsichtsbehörde der öffentlichen Stelle zur Beseitigung von erheblichen datenschutzrechtlichen Verstößen anordnen.

Bei der Polizei Hamburg handelt es sich um eine öffentliche Stelle der Freien und Hansestadt Hamburg, deren Tätigkeiten der Richtlinie (EU) 2016/680 unterfallen. Nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 RI (EU) 2016/680 gilt die genannte Richtlinie für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Anforderungen an das Verfahren nach § 6 HmbRI(EU)2016/680UmsAAG i.V.m. § 43 Abs. 1 S. 5 HmbJVollzDSG wurden eingehalten. Danach ist gem. § 6 HmbRI(EU)2016/680UmsAAG i.V.m. § 43 Abs. 1 S. 1 HmbJVollzDSG vor Erlass einer Anordnung zur Beseitigung eines erheblichen Verstoßes gegen datenschutzrechtliche Vorschriften die zuständige Aufsichtsbehörde vorerst zu beanstanden und Gelegenheit zur Stellungnahme zu geben. Zu der Beanstandung des HmbBfDI i.S.d. § 6 HmbRI(EU)2016/680UmsAAG i.V.m. § 43 Abs. 1 S. 1 und 3 HmbJVollzDSG erhielt die Behörde für Inneres und Sport mit Schreiben vom 30. August 2018 Gelegenheit zur Äußerung. Von der Möglichkeit zur Äußerung hat die Behörde für Inneres und Sport mit Schreiben vom 29.09.2018 Gebrauch gemacht.

III. Materielle Rechtmäßigkeit

Die Voraussetzungen für den Erlass einer Anordnung gem. § 6 HmbRI(EU)2016/680UmsAAG i.V.m. § 43 Abs. 1 S. 5 HmbJVollzDSG liegen vor. Danach kann der HmbBfDI gegenüber der Aufsichtsbehörde der öffentlichen Stelle der Freien und Hansestadt Hamburg, deren Tätigkeit der Richtlinie (EU) 2016/680 unterfällt, geeignete Maßnahmen anordnen, wenn ein Verstoß bei der Verarbeitung von personenbezogenen Daten durch diese öffentlichen Stellen trotz Beanstandung nach § 6 HmbRI(EU)2016/680UmsAAG i.V.m. § 43 Abs. 1 S. 1 HmbJVollzDSG fortbesteht und dies zur Beseitigung eines erheblichen Verstoßes gegen datenschutzrechtliche Vorschriften erforderlich ist. Die Voraussetzungen hierfür sind gegeben.

1. Personenbezogene Daten

Die mit der GAS ausgelesenen charakteristischen Gesichtsmerkmale von auf Bild- und Videomaterial festgehaltenen Gesichtsbildern von Personen und die daraus erstellten Templates sind personenbezogene biometrische Daten i.S.d. § 46 Nr. 1 und Nr. 12 BDSG. Nach § 46 Nr. 1 BDSG sind personenbezogene Daten zunächst alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie z.B. einem Namen (…), zu Standortdaten (…) oder auch zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen (…) oder sozialen Identität dieser Person sind, identifiziert werden kann. Eine Identifizierung muss dabei zumindest mit weiteren Hilfsmitteln mit noch verhältnismäßigem Aufwand möglich sein (VG Schwerin, Beschluss vom 18. Juni 2015 – 6 B 1637/15 SN, Rn. 15 m.w.N.). Nur wenn es nach allgemeinem Ermessen unwahrscheinlich wäre, dass diese Daten verwendet werden können, um Personen zu identifizieren, ist nicht von einem Personenbezug auszugehen (Schwenke NJW 2018, 823 (824), Erwägungsgrund 21 S. 2 zur RI (EU) 2016/680).

Das von einer Kamera aufgezeichnete Bild einer Person fällt zunächst unter den Begriff der personenbezogenen Daten, sofern es die Identifikation der betroffenen Person ermöglicht (EuGH, Urteil vom 11.12.2014 – C-212/13, Rn. 22). Die von der Software gewonnenen und analysierten Informationen sind ebenfalls personenbezogen, da sie Angaben über äußere Merkmale darstellen. Die gespeicherten Templates sind gerade dazu bestimmt, Personen zu identifizieren (Bericht des Innenausschusses v. 21.11.2018, Drs. 21/15080, S. 2 und 9; Schwenke, NJW 2018, 823 (824)). So lässt sich gerade aus der Antwort des Senats zur schriftlichen kleinen Anfrage entnehmen, dass die SoKo „Schwarzer Block“ die GAS unter anderem einsetzt, um bei unbekannten Personen gegebenenfalls geeigneteres Bildmaterial für weitere Ermittlungen zu deren Identifizierung zu erlangen. Es gelang „*mit Hilfe der biometrischen Gesichtserkennung durch Recherchen mit der GAS „Videmo 360“ bislang drei*

Personen namentlich (zu) *identifizieren*“ (Drs. 21/139339 v. 10.08.2018, Antwort zu Frage Nr. 10; mittlerweile wurden vier Personen auf diese Weise identifiziert (Bericht des Innenausschusses a.a.O., Drs. 21/15080, S. 3)). Dies war u.a. deshalb möglich, weil das polizeieigene Material auch Videosequenzen enthält, die das Abfilmen von Ausweispapieren im Rahmen einer Personenkontrolle zeigt. Die aus dem Videomaterial extrahierten Merkmale stellen auch personenbezogene biometrische Daten dar (vgl. Jandt, ZRP 2018, 16 (18); Thiel, ZRP 2016, 218 (219)). Bei biometrischen Daten i.S.v. § 46 Nr. 12 BDSG handelt es sich um mit einem speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigten. Eine Identifizierung bzw. Detektierung von bestimmten Personen durch die analysierten Gesichtsmerkmale/Templates ist hier nicht nur möglich, sondern gerade der Zweck, der mit dem Einsatz der biometrischen Analysesoftware verfolgt wird. Durch die Lokalisierung und Vermessung der Gesichtsphysiognomie werden die individuellen Gesichtsmerkmale der Betroffenen durch ein spezielles technisches Verfahren erkannt und herausgefiltert und in Form von maschinenlesbaren unverwechselbaren Modellen abgespeichert. Sie wirken sich so unwiderruflich auf die Verbindung von Körper und Identität aus (Art. 29-Datenschutzgruppe, Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien, 2012, S. 4).

2. Verarbeitung von personenbezogenen Daten

Diese personenbezogenen Daten werden auch datenschutzrechtlich i.S.d § 6 HmbRI(EU)2016/680UmsAAG i.V.m. § 43 Abs. 1 S. 1 und 3 HmbJVollzDSG verarbeitet. Unter den Begriff der (Daten-)Verarbeitung nach § 46 Nr. 2 BDSG ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung, die Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verarbeitung oder eine andere Form der Bereitstellung, den Abgleich, die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung zu verstehen. Die charakteristischen Merkmale des menschlichen Gesichts werden automatisch durch die GAS lokalisiert, ausgelesen und in Form von abgleichbaren Templates gespeichert, was unvermeidlich eine Verarbeitung von personenbezogenen biometrischen Daten darstellt (zum Scannen von Gesichtern: Wendt, ZD-Aktuell 2017, 05724). Die Auslese von charakteristischen Gesichtsmerkmalen, die Templateerstellung und deren Speicherung sind neben der vorherigen Bild- und Videoerhebung/Speicherung und der der Erstellung der Templates folgenden Abgleichmaßnahme eigenständige Datenverarbeitungsschritte (vgl. Jandt, ZPR 2018, 16 (18)).

3. Datenschutzrechtlicher Verstoß

Das Auslesen von Gesichtsmerkmalen, die Erstellung der Templates und deren Speicherung in einer umfangreichen Datenbank von einer unbegrenzten Anzahl von Personen zum Zwecke des späteren Abgleichs stellt einen Verstoß gegen datenschutzrechtliche Vorschriften i.S.d. § 6 HmbRI(EU)2016/680UmsAAG i.V.m. § 43 Abs. 1 HmbJVollzDSG dar. Es fehlt an einer Rechtsgrundlage, auf die diese Datenverarbeitungsschritte gestützt werden könnten. Diese Datenverarbeitungsschritte stellen intensive Eingriffe in das durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG geschützte allgemeine Persönlichkeitsrecht der Betroffenen in seiner Ausprägung als Recht auf informationelle Selbstbestimmung bzw. Art. 8 Abs. 1 und 2 Charta der Grundrechte der Europäischen Union dar. Eine hinreichend bestimmte Ermächtigungsgrundlage im Sinne einer verfassungsgemäßen Schranke, die diese Eingriffe erlaubt, fehlt im geltenden Recht.

Es ist an dieser Stelle noch einmal ausdrücklich festzuhalten, dass vorliegend nicht der „erste Schritt“ – die Erhebung des polizeieigenen sowie des polizeifremden Materials – Grund für die Anordnung ist. Vielmehr geht es um den daran anschließenden Datenverarbeitungsschritt, bei dem für alle Gesichter auf dem Bildmaterial ein unverwechselbares biometrisches Template erstellt und gespeichert wird, um es für anschließende Abrufe zu verwenden. Es kann daher offen bleiben, ob die Erhebung der Bildsequenzen auf Bahnhöfen, bei Demonstrationen während des G20-Gipfels und durch das Hochladen privater Videos über die „Boston Infrastructure“, rechtmäßig erfolgte. Vorliegend geht es allein darum, dass für die daran anschließende (Daten)-Verarbeitung durch die Polizei keine Rechtsgrundlage vorliegt. Im Folgenden wird aus Gründen der Übersicht zwischen der Erstellung von Gesichtstemplates aus polizeifremden Bildmaterial und polizeieigenem Material differenziert.

Dazu im Einzelnen:

a. Verarbeitung des polizeifremden Materials

Unabhängig davon, ob es sich bei sämtlichen durch die GAS verwerteten polizeifremden Bild- und Videosequenzen aus dem öffentlichen Nahverkehr sowie aus dem Hinweisportal „Boston Infrastructure“ des BKA um rechtmäßig formlos sichergestellte Beweismittel nach § 94 Abs. 1 StPO handelt (Rechtliches Gutachten der Polizei v. 23.07.2018, S. 10), fehlt für die biometrische Datenverarbeitung dieses Materials eine Rechtsgrundlage:

aa. § 81b StPO

§ 81b StPO vermag die dargelegte Verarbeitung von Gesichtern aus dem der Soko „Schwarzer Block“ zustehenden Rohmaterial durch die GAS nicht zu rechtfertigen. Nach § 81b StPO dürfen Messungen und ähnliche Maßnahmen an einem Beschuldigten auch gegen dessen Willen vorgenommen werden, soweit es für die Zwecke der Durchführung des Strafverfahrens oder für die Zwecke des Erkennungsdienstes notwendig ist.

Diese Voraussetzungen liegen hier aber nicht vor. Es kann im Ergebnis daher offen bleiben, ob unter „Messungen“ überhaupt die automatische biometrische Auslese fällt. Die Anwendbarkeit der Norm scheitert bereits daran, dass die Betroffenen der GAS zum Zeitpunkt der vorliegend zu beurteilenden Maßnahmen keine Beschuldigten waren. Beschuldigter i.S.d. Norm ist nicht derjenige, der in einen vagen Tatverdacht gerät oder gänzlich Unbeteiligter ist. Vielmehr müssen tatsächliche Anhaltspunkte gem. § 152 Abs. 2 StPO für die Begehung einer Straftat durch den Betroffenen vorliegen (Karlsruher Kommentar StPO/Senge, 7. Auflage 2013, § 81b, Rn. 2). Eine vorherige Einordnung als Beschuldigter in diesem Sinne war aber zum Zeitpunkt der Anwendung der GAS nicht gegeben. Es wurden vielmehr sämtliche technisch lokalisierbaren Abbildungen von menschlichen Gesichtern durch die GAS erfasst und vermessen/ausgelesen. Viele Betroffene wurden dabei nur zufällig erfasst, weil sie sich zu einem bestimmten Zeitpunkt an einem bestimmten Ort aufgehalten hatten und von einer Kamera aufgezeichnet wurden bzw. eine Privatperson die Entscheidung getroffen hat, die konkrete Aufnahme auf einen Server des BKA zu laden.

bb. §§ 161,163 StPO i.V.m. § 48 BDSG (i.V.m. § 94 StPO)

Die Ermittlungsgeneralklausel nach §§ 161, 163 StPO i.V.m. § 48 BDSG scheidet als Ermächtigungsgrundlage für die gegenständlichen Datenverarbeitungsschritte ebenfalls aus.
Nach §§ 161, 163 StPO haben die Behörden und Beamten des Polizeidienstes Straftaten zu erforschen. Zu diesem Zweck sind sie befugt, Ermittlungen jeder Art vorzunehmen, soweit nicht andere gesetzliche Vorschriften ihre Befugnisse besonders regeln. § 48 Abs. 1 BDSG erlaubt dabei die Verarbeitung von biometrischen Daten als besondere Kategorie von personenbezogenen Daten (§ 46 Nr. 14 BDSG) im Rahmen der §§ 161, 163 StPO nur, wenn dies zur Aufgabenerfüllung unbedingt erforderlich ist.

§§ 161, 163 StPO sind jedoch bereits zu unspezifisch, um massenhafte Eingriffe in besondere Kategorien personenbezogener Daten von Tausenden unbeteiligter Personen, deren biometrische Daten zunächst auf Vorrat, nämlich zum Zwecke des wiederholten späteren Abgleichs, verarbeitet werden, zu legitimieren. Bei §§ 161,163 StPO handelt es sich um Ermittlungsgeneralklauseln, auf die nur solche Ermittlungsmaßnahmen gestützt werden

können, die mit keinen oder zumindest nicht erheblichen Grundrechtseingriffen verbunden sind und daher keiner speziellen Ermächtigungsgrundlage bedürfen (BVerfG, Beschluss v. 17.02.2009 – 2 BvR 1372, 1745/07, Rn. 26; BeckOK StPO/Sackreuther, 31. Ed. 15.10. 2018, § 161 StPO, Rn. 4).

Dies ist aber vorliegend bei der GAS nicht der Fall. Entgegen der Ansicht der Polizei Hamburg wird der Eingriff, der durch die vorherige formlose Sicherstellung des Materials nach § 94 StPO erfolgt (Rechtliches Gutachten der Polizei v. 23.07.2018, S. 4 ff.), durch die anschließende Datenverarbeitung nochmals erheblich intensiviert. Die Ermächtigungsgeneralklauseln sind deswegen nicht ausreichend, die weiteren Verarbeitungsschritte zur Erstellung von Gesichtsprofilen zu rechtfertigen. Die vorgenommene biometrische Analyse von größtenteils unbeteiligten Personen zur Erstellung mathematischer Modelle zum Zwecke des späteren Abgleichs stellt vielmehr einen eigenständigen intensiven Eingriff in das durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG geschützte allgemeine Persönlichkeitsrecht der Betroffenen in seiner Ausprägung als Recht auf informationelle Selbstbestimmung dar.

Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG schützt den Bürger gegen jede Art der staatlichen Erhebung, Speicherung und Verwendung seiner persönlichen Daten. Das Grundrecht auf informationelle Selbstbestimmung gewährleistet die Befugnis, grundsätzlich selbst über die Preisgabe und eben auch über die Art der Verwendung seiner persönlichen Daten zu bestimmen (BVerfG, Urteil v. 15.12.1983 – 1 BvR 209/83, Rn. 149). Dieses Recht flankiert und erweitert den grundrechtlichen Schutz von Verhaltensfreiheit und Privatheit; es lässt ihn insbesondere im Rahmen der modernen Datenverarbeitung schon auf der Stufe der Persönlichkeitsgefährdung beginnen. Zum einen sind Angaben über Personen in der modernen Datenverarbeitung unbegrenzt speicherbar und jederzeit abrufbar. Zum anderen können sie Grundlage für weitere Maßnahmen werden. Verknüpfungsmöglichkeiten eröffnen vielfältige Nutzungsmöglichkeiten, wodurch wiederum weitere Informationen erzeugt und Schlüsse gezogen werden, die sowohl grundrechtlich geschützte Geheimhaltungsinteressen des Betroffenen beeinträchtigen, als auch anschließende Eingriffe in seine Verhaltensfreiheit nach sich ziehen können (BVerfG, Urteil v. 11.03.2008 – 1 BvR 2074/05, Rn. 64).

Die beschriebene Analyse und Speicherung für den Abgleich benötigter biometrischer Informationen in einer Datenbank greift in das Recht auf informationelle Selbstbestimmung ein, da die angefertigten Bildaufnahmen in abruf- und abgleichbare Informationen umgewandelt werden (Thiel, ZRP 2016, 218 (219 ff.)). Die Merkmale des menschlichen Körpers werden dabei maschinenlesbar gemacht, wodurch sich vielfältige Nutzungsmöglichkeiten ergeben (Art. 29-Datenschutzgruppe, Stellungnahme 3/2012 zu

Entwicklungen im Bereich biometrischer Technologien, 2012 S. 4), die ohne derartige technische Erneuerungen, nur aufgrund von Lichtbildaufnahmen, nicht möglich wären. Bei der Analyse von Gesichtsmerkmalen und der Erstellung von maschinenlesbaren Modellen mag es sich zunächst grob betrachtet nur um ein Mittel zur Vorbereitung für den späteren Zweck des Abgleichs handeln. Der selbständige Eingriff liegt aber gleichwohl darin, dass dadurch Informationen über Personen in zeitlicher und örtlicher Hinsicht in unbegrenzter Weise auf Vorrat verfüg- und nutzbar gemacht werden, wie dies bloße Lichtbilder und konventionelle Datenverarbeitung durch manuelle Durchsicht nicht ermöglichen.

So können u.a. das Verhalten und die räumliche Veränderung von Beschuldigten (durch Verknüpfung mit Geodaten) ermittelt werden. Es werden Bewegungsprofile und Verhaltensweisen, etwa die Teilnahme an Versammlungen sowie soziale Kontakte detailliert rekonstruierbar (Bericht des Innenausschusses a.a.O., Bü.-Drs. 21/15080, S. 4 ff.). Das Bundesverfassungsgericht führt in seiner Entscheidung zur automatisierten 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 für Verhaltensfreiheit und Privatfreiheit, die den Schutz des Grundrechts auf informationelle Selbstbestimmung auslöst (BVerfG Urteil v. 11.03.2008 – 1 BvR 1254/07, Rn. 69 ff.). Mehr noch als für Kfz-Kennzeichen muss dies für biometrische personenbezogene Daten gelten, da diese eine weit höhere Persönlichkeitsrelevanz haben.

Der Vollständigkeit halber sei erwähnt, dass das Bundesverfassungsgericht den Eingriff in den Schutzbereich des Grundrechts nur deshalb im Ergebnis verneinte, weil die Daten ohne Möglichkeit einen Personenbezug herzustellen nach Abgleich mit dem Fahndungsbestand bei Negativanzeige sofort wieder gelöscht werden (BVerfG, Urteil v. 11.03.2008 – 1 BvR 1254/07, Rn. 68). So liegt die Sache hier nicht. Auch im „Nichttrefferfall“ werden die personenbezogenen Daten über Monate in der Datenbank gespeichert. Anders als bei einem Bildabgleich in Echtzeit, wie ihn Bundespolizei, BKA und Deutsche Bahn am Bahnhof Südkreuz in Berlin im Testbetrieb durchführen, kommt es bei der hier praktizierten „retroaktiven“ Gesichtserkennung zum Aufbau einer Datenbank mit betroffenen Personen, gegen die kein Tatverdacht besteht. Das Recht auf informationelle Selbstbestimmung schützt aber gerade das Interesse des Einzelnen, dass die mit seinem Verhalten in der Öffentlichkeit verbundenen personenbezogenen Informationen nicht im Zuge automatischer Informationserhebung zur

Speicherung mit der Möglichkeit der Weiterverwendung und Auswertung durch staatliche Stellen erfasst werden (BVerfG, Urteil v. 11.03.2008 – 1 BvR 1254/07, Rn. 67).

Für derartige Eingriffe in das Grundrecht sind §§ 161, 163 StPO i.V.m. § 48 BDSG als verfassungsmäßige Schranke zu unbestimmt.

Nach ständiger Rechtsprechung des Bundesverfassungsgerichts sind Einschränkungen des Grundrechts auf informationelle Selbstbestimmung zwar im überwiegenden Allgemeininteresse, insbesondere auch im Rahmen der Strafverfolgung, zulässig und der Verhinderung und Aufklärung von Straftaten kommt nach dem Grundgesetz eine hohe Bedeutung zu (BVerfG, Beschluss v. 22.08.2006 – 2 BvR 1345/03, Rn. 72). Der Einzelne muss aber nur solche Beschränkungen seiner Rechte hinnehmen, die auf einer verfassungsgemäßen gesetzlichen Grundlage beruhen und die die Anforderungen erfüllen, die sich aus der Art und Intensität des jeweiligen Grundrechtseingriffs ergeben (st. Rspr., siehe nur BVerfG, Urteil v. 11.03.2008 – 1 BvR 2074/05, Rn. 75). Das Bestimmtheitsgebot soll dabei sicherstellen, dass eine Norm in ihren Voraussetzungen und in ihrer Rechtsfolge so formuliert ist, dass die von ihr Betroffenen die Rechtslage erkennen und ihr Verhalten danach ausrichten können (vgl. für viele: BVerfG, Urteil v. 12.04.2005 – 2 BvR 581/01, Rn. 49). Dabei gilt: Je intensiver der mit der staatlichen Maßnahme verbundene Eingriff ist, desto höher sind die Anforderungen an die Bestimmtheit der Ermächtigungsnorm. Das Bundesverfassungsgericht hat für die Anforderungen an die Ermittlung der Intensität von Eingriffen mittlerweile gefestigte Kriterien entwickelt. Relevant sind danach die Eingriffsschwelle, die Anzahl der Betroffenen, der Anlass sowie die individuelle Beeinträchtigung. Die Eingriffsschwere der Maßnahme ist vorliegend alles andere als gering.

Bereits die Videoaufzeichnung an sich stellt einen intensiven Eingriff dar, der aber durch die biometrische Analyse, das Erstellen von mathematischen Modellen und deren Speicherung noch erheblich intensiviert wird. Schon eine Videoaufzeichnung kann aufgrund des Eingriffscharakters nicht auf die allgemeinen Regeln für die Datenerhebung durch staatliche Stellen gestützt werden, sondern benötigt spezielle Rechtsgrundlagen (BVerfG, Beschluss v. 23.02.2007 – 1 BvR 2368/06, Rn. 45). Dies muss erst recht für den Einsatz der GAS gelten. Aus der enormen Streubreite und weitreichenden Nutzungsmöglichkeiten sowie der Beeinträchtigung für den Einzelnen folgt, dass ein intensiver Grundrechtseingriff vorliegt, der hohe Anforderungen an die Bestimmtheit der Norm stellt. Generalklauseln erfüllen diese Anforderungen nicht.

Grundrechtseingriffe weisen zunächst 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. 23.02.2007 – 1 BvR 2368/06, Rn. 51 zur Videoaufzeichnung; BVerfG, Urteil v. 14.07.1999 – 1 BvR 2226/94, Rn. 270). So liegt es hier. Die überwiegende Zahl der Betroffenen wird ohne eigenes Zutun in die Referenzdatenbank aufgenommen, soweit sich ihr Gesicht auf dem Bildmaterial befindet. Dieses Template wird dann im Rahmen des Referenzdatenbestands wiederholt mit Templates von verdächtigen Personen abgeglichen. Der weitaus größte Teil der Betroffenen hat zu der biometrischen Gesichtsanalyse, der Erhebung, Abspeicherung und der Bereithaltung überhaupt keinen Anlass gegeben, weil die Personen weder in einer Beziehung zu einem strafrechtlich noch ansonsten rechtlich relevantem Fehlverhalten standen. So führte allein die Benutzung einer S-Bahnlinie in der Zeit zwischen dem 06.07. und 10.07. für Passanten zur Erfassung des Gesichtsprofils. Gleiches gilt für die Teilnahme an Demonstrationen oder einfach nur für die Existenz des eigenen Gesichts auf einer Videosequenz, die von einer Privatperson auf einen Server des BKA hochgeladen wurde, wobei es nach polizeilicher Einschätzung allein ausreichte, dass die angefertigten Aufnahmen „örtlich und zeitlich in den G20-Rahmen“ passten. Dabei ist unerheblich, ob es sich um strafrechtlich relevantes Verhalten handelt, ein Tatort oder eben nur eine Gruppe Passanten auf dem Video bzw. Bild zu sehen ist.

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 wiederum Folgemaßnahmen auslösen können (zur Videoüberwachung: BVerfG, Beschluss v. 23.02.2007 – BvR 2368/06, Rn. 52; BVerfG, Urteil v. 11.03.2008 – 1 BvR 2074/05, Rn. 79). Dies ist hier vorliegend ebenfalls der Fall. Die Möglichkeit der Auslese von biometrischen Daten, die Erstellung von abgleichsfähigen Templates sowie deren Speicherung zum Zwecke des späteren Abgleichs eröffnen vielfältige Nutzungsmöglichkeiten, die ein gewöhnliches Lichtbild nicht hergibt. Die in diesem Sinne aus der Schwere des Eingriffs resultierende erhöhten Bestimmtheitsanforderungen sollen aber gerade sicherstellen, dass die Entscheidung über die Grenzen der Freiheit des Bürgers nicht einseitig in das Ermessen der Verwaltung gestellt wird (BVerfG, Urteil v. 27.07.2005 – 1 BvR 668/04, Rn. 118). Dies ist aber der Fall, wenn ein Auswertungssystem vielfach eingesetzt werden kann und mit der Erstellung von maschinenlesbaren, abgleichsfähigen biometrischen Modellen menschlicher Gesichter vielfältige Nutzungsmöglichkeiten eröffnet, deren Vornahme und Einsatzziel eine Begrenzung nur in der eigenen Abwägung der Exekutive findet. Bezeichnend dafür führte der Senatsvertreter im Innenausschuss aus, dass man von bestimmten möglichen Verwendungsmöglichkeiten der GAS Abstand genommen habe, weil „*man die Eingriffstiefe nicht noch weiter treiben wolle*“ bzw. „*wenn man die Fantasie an dieser Stelle laufen lasse, sei alles Mögliche vorstellbar*“ und in diesem Zusammenhang darum bat,

„*Vertrauen in die Strafverfolgungsbehörden zu haben*“ (Bericht des Innenausschusses v. 21.11.2018, Drs. 21/15080, S. 3 und S. 12).

Zudem handelt es sich bei den erzeugten Templates um einzigartige Informationen über das eigene Gesicht als dem zentralen biometrischen Merkmal, das die Unverwechselbarkeit und Identität des Menschen in der Öffentlichkeit ausmacht. Biometrische Daten werden im Datenschutzrecht als besondere Kategorien von Daten unter einen herausgehobenen Schutz gestellt (vgl. Art. 10 der RI (EU) 2016/680). Der europäische Gesetzgeber stellt in der Richtlinie (EU) 2016/680 daher klar, dass insbesondere Risiken aus der Datenverarbeitung hervorgehen können, die zu einem physischen, materiellen oder immateriellen Schaden führen, wenn biometrische Daten das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen und analysieren. Gleiches gilt, wenn diese genutzt werden, um ein persönliches Profil erstellen zu können oder wenn die Verarbeitung eine große Menge personenbezogener Daten oder eine große Anzahl von Personen betrifft (Erwägungsgrund 51 der Richtlinie).

Der europäische Gesetzgeber erwähnt in der Richtlinie daher auch 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 eben nur getroffen werden, sofern sie durch Rechtsvorschriften geregelt sind (vgl. Erwägungsgrund 26 der Richtlinie). Dies muss dann gerade auch für ein biometrisches Auswertungssystem gelten, das verdachtslos Tausende betrifft und den bereits intensiven Eingriff gegenüber Videoaufzeichnungen nochmals u.a. durch die Verknüpfungs- und Nutzungsmöglichkeiten deutlich vertieft (s.o.).

Zudem führt das Bundesverfassungsgericht – bereits bei einer Datenverarbeitung ohne biometrischen Bezug – aus, dass eben eine weitere Besonderheit des Eingriffspotenzials von Maßnahmen der elektronischen Datenverarbeitung in der Menge der verarbeiteten Daten liegt, die auf konventionellem Wege gar nicht bewältigt werden können (BVerfG, Urteil v. 11.03. 2008 – 1 BvR 2074/05, Rn 64). So liegt es auch hier. Entsprechend deutlich macht dies die Stellungnahme der Senatsvertreter in der Innenausschusssitzung vom 25.10. 2018, wonach es allein über 60 Jahre gedauert hätte, das gesamte Videomaterial lediglich zu sichten (Bericht des Innenausschusses v. 21.11.2018 Bü.-Drs. 21/15080, S. 2).

Letztlich bedeutet der Einsatz für den Einzelnen, dass die Berechnungen des individuellen Gesichtsprofils völlig intransparent stattfinden, ohne dass die Person davon etwas bemerkt. Die Betroffenen werden nicht über die hier beschriebene Verarbeitung ihrer Gesichtszüge

informiert. Auch wenn vor Ort eine offene Bilderstellung erfolgt sein sollte, können die Betroffenen nicht sicher davon ausgehen, ob eine biometrische Berechnung ihrer Gesichtsdaten erfolgt, da die Polizei nur ein Teil des gesammelten Materials überhaupt in den Referenzdatenbestand aufnimmt und allein ein örtlicher und zeitlicher Bezug ausreicht. Eine Klärung der Frage, ob und wie die Betroffenen ihre europarechtlich garantierten Auskunftsrechte und Löschungsansprüche bei der Speicherung von personenbezogenen Daten (Art. 12 ff. Rl (EU) 2016/680) durchsetzen können sollen, fehlt gänzlich.

Nicht außer Betracht zu lassen ist auch die realistische Möglichkeit, als Betroffene der GAS fälschlicherweise mit gesuchten Straftätern verwechselt zu werden. Zwar wird die Auswahl der GAS später durch eine manuelle Bearbeitung gefiltert, diese menschliche Bearbeitung wird aber durch die Vorauswahl der GAS induziert. Aufgrund der dargelegten Intransparenz ist dies schwer bis kaum kontrollierbar.

Die Persönlichkeitsrelevanz der gewonnenen Informationen erhöht sich weiter, wenn sich derartige Maßnahmen als funktionales Äquivalent eines Eingriffs in andere grundrechtliche Freiheiten darstellen, z.B. die Teilnahme an Versammlungen rekonstruiert werden kann (BVerfG, Urteil v. 11.03.2008 – 2 BvR 1345/03, Rn. 87 ff.). Dies kann nach Ausführungen des Bundesverfassungsgerichts schon dann der Fall sein, wenn aus der „*Erfassung* (…) *auf den Zufahrtswegen die Vermutung abgeleitet werden* (kann), *dass der Fahrer* (…) *eine Versammlung aufsucht*“. Dies führt dann ggfs. dazu, dass der Einzelne in seiner Entschließungsfreiheit gehemmt ist, da er befürchtet, dass eine (friedliche) Teilnahme an einer Versammlung biometrisch ausgelesen, maschinenlesbar und abgleichbar abgespeichert wird (zur Unsicherheit bei der Wahrnehmung des Grundrechts bei Versammlungen durch Bildaufnahmen durch die Polizei: Nds. OVG, Urteil v. 24.09.2015 – 11 LC 215/14, Rn. 21).

Nach alledem kann der Einsatz der GAS nicht als ein „*bloßes Hilfsmittel für die visuelle Auswertung*“ (Rechtliches Gutachten der Polizei v. 12.09.2018, S. 8) der formlos sichergestellten Bild- und Videodateien nach § 94 StPO gesehen werden. Zwar mögen gewisse technische Erneuerungen/Weiterentwicklungen vom Wortlaut einer Norm gedeckt sein (BVerfG, Beschluss v. 10.11.2004 – 2 BvR 581/01, Rn. 51). Dies gilt jedoch nicht für den vorliegenden Fall. Ein automatisches Auswertungsinstrument, welches tausende von menschlichen Gesichtern nur aufgrund ihres zufälligen örtlichen Aufenthalts biometrisch ausliest, berechnet und als abgleichbares mathematisches Modell in einer Datenbank für einen späteren systematischen Abgleich vorrätig hält, fällt aufgrund seiner enormen Streubreite und seiner Eigenschaft als Grundstein für weitere dadurch ermöglichte Nutzungsmöglichkeiten (z.B. Verhaltensinterpretationen) nicht in den Bereich dieser Norm. Vielmehr stellt es einen in Qualität und Quantität gänzlich neuen Ansatz zur Straftatermittlung

dar. Dies bestätigen nicht zuletzt Aussagen des Hamburgischen Polizeipräsidenten sowie des Leiters der Soko „Schwarzer Block“, die von einer „*konzeptionellen Weiterentwicklung von nicht unerheblichen Ausmaß*“ bzw. einem „*völlig neuen Standard der Beweisführung*“ sprechen (Wortprotokoll Nr. 21/12 der öffentlichen Sitzung des Sonderausschusses „Gewalttätige Ausschreitungen rund um G20-Gipfel in Hamburg“ vom 28.6.2018, S. 8 ff.).

Das Bestimmtheitsgebot verlangt daher für die vorliegende Fallkonstellation vom Gesetzgeber zumindest, dass er beim Einsatz der automatischen Gesichtserkennung 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 gesetzlich zu regelnden 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 bestimmte 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 aufsichtlichen Kontrolle für schwach ausgestalteten Individualrechtsschutz BVerfG, Urt. v. 24.4.2013 – 1 BvR 1215/07, Rn. 213 ff.). Diese Anforderungen erfüllt die Generalklausel jedoch nicht.

Letztlich ändert auch die Vorschrift des § 48 BDSG nichts an der fehlenden Bestimmtheit der Generalklausel für den vorliegenden Sachverhalt. § 48 dient als Rechtsgrundlage für die Verarbeitung besonderer Kategorien von personenbezogener Daten, (Auernhammer/Greve DSGVO/BDSG, 6. Auflage 2018, § 48 BDSG Rn. 1), wozu auch biometrische Daten gem. § 46 Nr. 14 c BDSG gehören. Es handelt sich bei § 48 BDSG ebenfalls um eine unspezifische Generalklausel (Kühling/Buchner/Schwichtenberg, DSGVO/BDSG, 2. Auflage 2018, § 48 BDSG, Rn. 17), die intensive Grundrechtseingriffe mit derart hoher Streubreite nicht zu rechtfertigen vermag. Eine biometrische Massendatenerhebung kann daher jedenfalls nicht auf diese Rechtsgrundlage gestützt werden.

cc. § 98c StPO

Entgegen seinem Wortlaut, der nur den Datenverarbeitungsschritt des Abgleiches regelt, kann auch § 98c StPO als Rechtsgrundlage nicht herangezogen werden. Gem. § 98c StPO dürfen zur Aufklärung einer Straftat, nach der für Zwecke eines Strafverfahrens gefahndet wird, personenbezogene Daten aus einem Strafverfahren mit anderen zur Strafverfolgung oder

Strafvollstreckung oder zur Gefahrenabwehr gespeicherten Daten maschinell abgeglichen werden.

Die Norm bildet lediglich für den Vorgang des Abgleich von personenbezogenen Daten eine Ermächtigungsgrundlage und setzt dabei aber die Rechtmäßigkeit von eigenständigen vorgelagerten Datenverarbeitungsschritten – insbesondere der Erhebung und Speicherung – bezüglich der personenbezogenen Daten bereits voraus (MüKo StPO/Günther, 1. Auflage 2014, § 98c Rn. 7; Hilger, NStZ 1992, 457 (461); BeckOK StPO/Gerhold, 31 Ed. 15.10.2018, § 98c, Rn. 1). Vorliegend geht es jedoch gerade um die Schaffung eines Referenzwertebestandes mit biometrischen Gesichtsmodellen, für die § 98c StPO keine Rechtsgrundlage darstellen kann. Darüber hinaus ist die Norm materiell weitgehend und formell vollständig voraussetzungslos (krit. dazu Körffer, DANA 2014, 146 (148); BeckOK StPO/Gerhold, 31. Ed. 15.10.2018 § 98 c, Rn.1). Sie enthält weder eine Konkretisierung des Tatverdachts noch eine Beschränkung auf bestimmte Straftatbestände oder eine Subsidiaritätsklausel (ebenso MüKo StPO/Günther, a.a.O, § 98c Rn. 2), weshalb sie ohnehin nur zu geringfügigen Grundrechtseingriffen berechtigt (so zutreffend Körffer, DANA 2014, 146 (148) und BeckOK StPO/Gerhold, a.a.O. § 98c, Rn. 1). Geringfügige Grundrechtseingriffe liegen jedoch nicht vor (s.o.).

dd. § 483 Abs. 1 StPO

Ebenso scheidet § 483 Abs. 1 StPO als Ermächtigungsgrundlage aus. Die Norm erlaubt zwar die Speicherung, Veränderung und Nutzung von personenbezogenen Daten, nachdem die Daten aufgrund einer gesonderten Ermächtigungsgrundlage erhoben worden sind (Karlsruher-Kommentar StPO/Gieg, 7. Auflage 2013, § 483, Rn. 2). Allerdings gilt die Erlaubnis nur, soweit dies für Zwecke des Strafverfahrens erforderlich ist. Die Zweckbestimmung des § 483 Abs. 1 StPO bezieht sich lediglich auf das bestimmte Strafverfahren, für das die Daten erhoben worden sind, und nicht bereits auf die Strafverfolgung an sich (BeckOK StPO/Wittig, 31. Ed. 15.10. 2018, § 483, Rn. 1).

Dies folgt aus § 438 Abs. 2 StPO, denn dieser erlaubt ausdrücklich die Nutzung der Daten nach Absatz 1 für andere Strafverfahren. Diese Befugnis wäre überflüssig, wenn der Zweck in Absatz 1 bereits die Strafverfolgung als solche umfasste (Körffer, DANA 2014, 146 (147)). Unter Strafverfahren i.S.d. Norm ist das gesamte Verfahren von Einleitung des Ermittlungsverfahrens bis zum Abschluss des Vollstreckungsverfahrens zu verstehen (BeckOK StPO/Wittig, 31. Ed. 15.10.2018, § 483, Rn. 1). Die Analyse der Abbildungen von Personen durch die GAS erfolgte losgelöst von der Einleitung eines bestimmten Ermittlungsverfahrens. Vielmehr fand die Vermessung und Verarbeitung durch die

Gesichtserkennungssoftware vor bzw. parallel, aber insbesondere in der Sache unabhängig, von der menschlichen Durchsicht des Materials nach strafrechtlich relevantem Verhalten statt. Potenziell strafbewehrtes Verhalten im Sinne eines Anfangsverdachts soll vielmehr den Vorgang des Abgleichens mit der Templatedatenbank (vorgenommen seit 01.03.2018) einleiten; zu diesem Zeitpunkt sind aber bereits alle Gesichter ausgewertet und deren Modelle abgespeichert worden (November 2017 bis einschließlich Januar 2018).

ee. § 484 StPO

§ 484 StPO stellt ebenfalls keine hinreichende Befugnisnorm dar. Zwar erlaubt § 484 StPO die Datenverarbeitung für Zwecke künftiger Strafverfahren, es dürfen jedoch nur Daten verwendet werden, die bereits Gegenstand eines gegen den Beschuldigten geführten Strafverfahrens waren (Karlsruher Kommentar StPO/Gieg, 7. Auflage 2013, § 484, Rn. 2). Bei den verarbeiteten Daten handelt es sich aber gerade nicht um Daten, die bereits Gegenstand eines bestimmten Strafverfahrens waren.

b. Verarbeitung von polizeieigenem Material

Ebenso wie für das polizeifremde Material sieht das geltende Recht auch keine hinreichend bestimmte Ermächtigungsgrundlage für die dargelegte Verarbeitung des von der Polizei Hamburg selbst hergestellten Bild- und Videomaterials vor. Es wird auf III.3.a. verwiesen.

Darüber hinaus kann diese Datenverarbeitung – entgegen der Ansicht der Polizei Hamburg (Rechtliches Gutachten der Polizei v. 23.07.2018, S. 8 ff. und v. 12.09.2018, S. 5 ff.) – auch nicht auf § 100h StPO gestützt werden. Nach § 100h Abs. 1 i.V.m. Abs. 2 StPO wird die Polizei ermächtigt, auch ohne Wissen des Beschuldigten bzw. eines Dritten Bildaufnahmen herzustellen, wenn die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsorts eines Beschuldigten auf andere Weise weniger erfolgsversprechend oder erschwert wäre. Nach Angaben der Polizei Hamburg handelt es sich bei sämtlichen selbst hergestellten und in die GAS eingeführten polizeieigenen Bild- und Videosequenzen um Material, das aufgrund von § 100h StPO erhoben wurde. Damit dürften hiervon auch Aufnahmen von Versammlungen nach Art. 8 Abs. 1 GG umfasst sein. Auch wenn man annimmt, dass die Erhebung der Bild- und Videoaufnahmen insgesamt rechtmäßig aufgrund von § 100h StPO erfolgte, bietet diese Norm keine hinreichende Ermächtigungsgrundlage für die Erstellung und Speicherung von Templates von allen auf den Bild- und Videoaufnahmen abgebildeten Personen. Denn von der Zulässigkeit der Erhebung und Speicherung von Video- und Bildaufnahmen kann nicht auch auf eine zulässige Verarbeitung der Bilder durch ein vollkommen neues Auswertungsinstrument mit den bereits dargelegten Risiken für die informationellen Grundrechte Betroffener geschlossen werden.

Richtig ist, dass aus der Ermächtigung zur Bildaufzeichnung auch die Ermächtigung zur Sichtung – also zur optischen Nutzung – durch den menschlichen Beobachter folgt (so zu § 8 Abs. 3 HmbPolDVG: BVerwG, Urteil v. 25.01.2012 – 6 C 9/11, Rn. 26). Es handelt sich bei der GAS aber nicht um ein „*bloßes Hilfsmittel für die visuelle Auswertung"* (Rechtliches Gutachten der Polizei v. 12.09.2018, S. 8), sondern um einen eigenständigen intensiven Eingriff in das Grundrecht auf informationelle Selbstbestimmung, der eine automatisierte Auswertung in unbegrenztem Umfang ermöglicht und sowohl in Qualität als auch in Qualität nicht mit einer Sichtung durch den menschlichen Beobachter zu vergleichen ist (vgl. III.3.a.bb.).

Bestehende Normen zum Einsatz von Videoüberwachungstechnik erlauben daher nur den Einsatz technischer Mittel für reine Bildaufnahmen oder -aufzeichnungen, nicht hingegen für darüber hinausgehende Datenverarbeitungsvorgänge (Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder v. 30.03.2017: Einsatz von Videokameras zur biometrischen Gesichtserkennung birgt erhebliche Risiken). In diesem Zusammenhang ist auf die Rechtsprechung des OVG Hamburg verwiesen, das in Bezug auf die speziellen (präventiven) Befugnisnormen des HmbPolDVG zu Bildaufzeichnungen im öffentlichen Raum (§ 8 HmbPolDVG) ausführte, dass eine tatbestandliche Beschränkung auf ausschließlich „*optische Nutzung*" der Bildaufnahmen vorliegt. „*Der weiteren Verwendung der Daten sind somit enge Grenzen gesetzt; insbesondere ist jegliche Form der automatisierten Auswertung des Bildmaterials ausgeschlossen*" (OVG Hamburg, Urteil v. 22.06.2010 – 4 Bf 276/07, Rn. 102). Es ist nicht ersichtlich, warum für entsprechende Vorschriften der StPO eine abweichende Bewertung angezeigt sein sollte.

Die hier vorliegende biometrische Analyse setzt den Grundstein für die Rekonstruktion von Bewegungsprofilen von einzelnen Personen über längere Zeiträume auf großen Teilen des hamburgischen Stadtgebiets. Die GAS vermag die Beziehungen zu anderen Menschen dokumentieren und rekonstruieren. Verhaltensmuster, Teilnahme an Versammlungen, Präferenzen und religiöses/politisches Engagement können über einen nicht näher eingegrenzten örtlichen und zeitlichen Kontext hinweg ausgelesen werden. Dies hat eine vollkommen andere Qualität als die Sichtung und das Vor- und Zurückspulen von einzelnen Tatortvideos durch einen Ermittler der Polizei.

Der Einsatz der Gesichtserkennung markiert eine neue Qualität des Eingriffs, indem die GAS neue technische Wege bei der Fahndung und Überwachung von Personen über eine Fülle von Bildmaterial ermöglicht, die bei einer Auswertung durch das menschliche Auge nicht möglich wären. Wenn allein die abstrakte Häufung der Begehung von Straftaten ausreicht, um den Ermittlungsbehörden nicht nur den Zugriff auf Bilddateien, sondern die Auswertung der

biometrischen Identität von Personen zu ermöglichen, wird die Herrschaft über die Bilder zu einer nie gekannten Kontrollmacht staatlicher Stellen gegenüber den Bürgerinnen und Bürgern. Die hierin liegende wesentliche Entscheidung über die informationellen Grundrechte von Bürgerinnen und Bürgern darf nicht allein der Einschätzung von Strafverfolgungsbehörden auf der Basis allgemeiner Grundsätze überlassen bleiben. Es ist vielmehr Sache des Gesetzgebers, für derartige grundrechtssensible Eingriffe durch eingriffsintensive Instrumente klare inhaltliche Vorgaben wie auch Verfahrensgarantien für Betroffene zu formulieren.

4. Keine unbedingte Erforderlichkeit des Einsatzes der GAS i.S.d. § 48 Abs. 1 BDSG

Wenn man mit der Polizei, dem Innensenator und der Generalstaatsanwaltschaft Hamburg dennoch die Auffassung vertritt, dass das geltenden Recht eine Rechtsgrundlage für die Schaffung einer biometrischen Datenbank hergibt, ist der Einsatz der GAS jedoch zumindest im vorliegenden Fall nicht verhältnismäßig.

Biometrische Daten werden wie bereits dargelegt im Datenschutzrecht als besondere Kategorien von Daten unter einen herausgehobenen Schutz gestellt. Nach § 48 Abs. 1 i.V.m. § 45 BDSG ist die Verarbeitung dieser besonderer Kategorien von personenbezogenen Daten, zum Zwecke der Ermittlung, Aufdeckung und Verfolgung von Straftaten durch die zuständige Stelle aber nur zulässig, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist. Dies ist aber vorliegend nicht der Fall.

Die Verarbeitung von biometrischen Daten muss nach dieser Norm zwingend erforderlich sein (Auernhammer/Greve DSGVO/BDSG, 6. Auflage 2018, § 48, Rn. 11). Dies ist zu bejahen, wenn eine Datenverarbeitung beinahe unverzichtbar erscheint (Kühling/Buchner/Schwichtenberg DSGVO/BDSG, 2. Auflage 2018, § 48 BDSG, Rn. 3). Die unbedingte Erforderlichkeit ist dabei eine Verschärfung gegenüber dem allgemeinen Erforderlichkeitskriterium und nicht gleichzusetzen mit dem verfassungsrechtlichen Verständnis im Sinne eines relativ mildesten Mittels (BeckOK BDSG/Albers, 25. Ed. 2018, § 48, Rn. 19). Es handelt sich bei diesem Erforderlichkeitsbegriff vielmehr um einen autonomen Begriff des Gemeinschaftsrechts (EuGH, Urteil v. 16.12.2008 – C 524/06, Rn. 52), der verlangt, das sich die Verarbeitung und damit die Ausnahmen vom Schutz personenbezogener Daten auf „*das absolut Notwendige beschränken muss*“ (EuGH, Urteil v. 04.05.2017 – C-13/16, Rn. 30 zum Begriff der „Erforderlichkeit“ bei der Verarbeitung von personenbezogenen Daten m.w.N.). Daraus folgt im Umkehrschluss, dass die Aufgabe ohne die Verarbeitung der Daten nicht vollständig oder nicht in rechtmäßiger Weise erfolgen kann. Insoweit wird die Verarbeitung hier als *conditio sine qua non* mit Blick auf die Zweckerfüllung konzipiert (BeckOK BDSG/Albers 25. Ed. 2018§ 48, Rn. 23). Dabei ist jedoch zu beachten, dass, „*je ungenauer*

die Ziele einer Normierung und die Anforderungen an die tatsächliche Ausgangslage umschrieben sind, umso schwerer fällt die Beurteilung der Eignung und Erforderlichkeit einer (Überwachungs-)Maßnahme. Vor allem bewirkt die Unbestimmtheit der tatsächlichen Voraussetzungen das Risiko eines unangemessenen Verhältnisses von Gemeinwohlbelangen, zu deren Wahrnehmung in Grundrechte eingegriffen wird, und den Rechtsgütern der Betroffenen" (BVerfG Beschluss v. 03.03.2004 – 1 BvF 3/92, Rn. 111).

So liegt es hier. Eine zwingende Erforderlichkeit des Einsatzes der GAS zur Zweckerreichung in diesem Sinne ist nicht zu erkennen und wurde von der Polizei auch nicht dargelegt. Auch angesichts der unbestrittenen Bedeutung, die eine wirksame Strafverfolgung und damit eine effiziente Aufklärung von Straftaten zur Sicherung des Rechtsfriedens als legitimer Zweck hat, kann weder eine zwingende Notwendigkeit i.S.d. Norm noch eine Angemessenheit der umfassenden Erstellung von biometrischen Profilen aller auf dem umfänglichen Bildmaterial abgebildeten Personen begründen.

Zwar ermöglichen strafprozessuale Ermächtigungen, auch § 161 Abs. 1 StPO, grundsätzlich einen Eingriff in das Recht auf informationelle Selbstbestimmung, sie finden aber ihre Grenzen in der Zweckbindung für das jeweilige Strafverfahren. Voraussetzungen sind zureichende tatsächliche Anhaltspunkte für eine Straftat nach § 152 Abs. 2 StPO. Es besteht insofern eine strenge Begrenzung sämtlicher Ermittlungen und damit auch der Datenerhebung, auf den Zweck der Tataufklärung dahin, dass die Eingriffe in das Recht an den eigenen Daten durch die Strafprozessordnung auf diejenigen begrenzt wird, die für die Strafverfolgung im konkreten Anlassfall von Bedeutung sind (BVerfG, Beschluss v. 17.03.2009 – 2 BvR 1372, Rn. 30 m.w.N.). Angesichts der Masse der Bilder und Videosequenzen von Personen, die biometrisch ausgewertet wurden, vermag eine Identifizierung in nur wenigen Fällen die zwingende Erforderlichkeit für die Erstellung einer biometrischen Datenbank nicht zu rechtfertigen. Hier werden Personen, die sich rechtmäßig in der Öffentlichkeit bewegten, massenhaft zum Zwecke der Strafverfolgung durch die GAS biometrisch ausgelesen unter einer ID gespeichert, ohne aus strafprozessualen zwingenden Erfordernissen.

5. Erheblichkeit des Verstoßes

Der dargelegte Verstoß bei der Verarbeitung von personenbezogenen Daten ist auch erheblich i.S.d. § 6 HmbRI(EU)2016/680UmsAAG i.V.m. § 43 Abs. 1 S. 5 HmbJVollzDSG. Von einem erheblicher Verstoß bei der Verarbeitung von personenbezogenen Daten ist zumindest dann auszugehen, wenn wie im vorliegenden Fall eine große Anzahl von Personen davon betroffen ist, die für derartige Maßnahmen keinen Anlass gegeben haben, sowie durch die Speicherung der Templates weitere Nutzungsmöglichkeiten eröffnet werden, die zu einer

weiteren Gefährdung des Persönlichkeitsrechts des Einzelnen beitragen. Hinzukommt, dass die Polizei Hamburg eine Ausweitung des Einsatzes der GAS auf weitere Fallkonstellation in Zukunft beabsichtigt. Insofern folgt aus der Schwere der (ungerechtfertigten) Eingriffe in das Grundrecht auf informationelle Selbstbestimmung (vgl. III.3.) auch der erhebliche Verstoß bei der Verarbeitung von personenbezogenen Daten.

6. Rechtmäßige Adressatin

Die Behörde für Inneres und Sport ist rechtmäßige Adressatin der Anordnung i.S.d § 6 HmbRL(EU)2016/680UmsAAG i.V.m. § 43 Abs. 1 Satz 5 HmbJVollzDSG. Danach hat die Anordnung von geeigneten Maßnahmen gegenüber der Aufsichtsbehörde der öffentlichen Stelle zu erfolgen, bei der im Rahmen der Datenverarbeitung Verstöße gegen den Datenschutz festgestellt werden. Die Behörde für Inneres und Sport ist Aufsichtsbehörde der Polizei Hamburg, welche hier als datenschutzrechtliche Verantwortliche i.S.d. § 46 Nr. 7 BDSG anzusehen ist. Nach § 46 Nr. 7 BDSG ist datenschutzrechtlicher Verantwortlicher eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

So liegt es hier. Die Polizei entscheidet grundsätzlich über die Mittel und Zwecke von kriminaltechnischen Untersuchungsmitteln und damit im vorliegenden Fall über den konkreten Einsatz und die Ausgestaltung eines Verfahrens zur biometrischen Analyse. Ihr oblag die Entscheidung, welche Daten durch die GAS bearbeitet wurden und auf welche Weise sie diese Templates anschließend in den Referenzdatenbestand aufnimmt. Der Vorgang der biometrischen Analyse und Erstellung der Templates fand auf Rechnern der Polizei statt. Die Polizei hat somit die physische Herrschaft über die Verarbeitungsprozesse. Gemäß dem Dargelegten hat die Polizei Hamburg sich zudem gegenüber dem HmbBfDI stets als (alleinige) Verantwortliche zu erkennen gegeben. Dies tat sie gem. § 9 Abs. 1 Nr. 1 HmbDSG a.F. in ihrer Verfahrensbeschreibung vom 18.10.2017, sowie in der überreichten Risikoanalyse vom 15.02.2018 gem. § 8 Abs. 4 HmbDSG a.F.

Aus dem gesetzlichen Verhältnis von Staatsanwaltschaft und Polizei im Ermittlungsverfahren folgt auch keine gegenteilige datenschutzrechtliche Beurteilung der Stellung der Polizei. Dass die Daten von einzelnen Personen, die auf der dritten Stufe des Verfahrens gegenüber dem Referenzdatenbestand abgeglichen werden, regelmäßig durch die Staatsanwaltschaft benannt werden, rechtfertigt hinsichtlich der datenschutzrechtlichen Verantwortung für die Erstellung und Nutzung einer biometrischen Datenbank mit Referenztemplates keine andere Beurteilung.

Zunächst handelt es sich bei der Erstellung und Speicherung der biometrischen Profile ohnehin um eine Datenverarbeitung im Vorfeld von strafrechtlichen Ermittlungen, die die technischen Bedingungen herstellt, einen späteren Abgleich einzelner, nach manueller Durchsicht des Videomaterials strafrechtlich verdächtiger Personen gegenüber der dann aufgebauten Referenzdatenbank zu ermöglichen. Davon abgesehen orientiert sich die Stellung der Polizei im Ermittlungsverfahren an der zentralen Norm des § 163 StPO. Danach haben Behörden und Beamte des Polizeidienstes Straftaten zu erforschen und alle keinen Aufschub gestatteten Anordnungen zu treffen, um die Verdunkelung der Sache zu verhüten. Daraus folgt, dass die Polizei auch ohne Anordnung der Staatsanwaltschaft selbstständig tätig werden kann („Das Verhältnis von Gericht, Staatsanwaltschaft und Polizei im Ermittlungsverfahren, strafprozessuale Regeln und faktische (Fehl-?) Entwicklungen“ – Große Strafrechtskommission des Deutschen Richterbundes, Ergebnisse der Sitzung 28.07 bis 02.08.2008, S. 130 ff.). Die Polizei Hamburg kann nicht bloß als Auftragsverarbeiterin der Staatsanwaltschaft i.S.d. § 62 BDSG gesehen werden, sondern ist organisatorisch unabhängig.

Nach dem Dargelegten käme bestenfalls eine gemeinsame Verantwortlichkeit von Polizei und Staatsanwaltschaft i.S.d. § 63 BDSG für den Bereich der Referenzdatenbank, basierend auf der grundsätzlichen Sachleitungsbefugnis im Ermittlungsverfahren der Staatsanwaltschaft in Betracht. Aus der Rechtsprechung des EuGH folgt jedoch, dass auch im Rahmen einer gemeinsamen Verantwortlichkeit jeder Verantwortliche den Datenschutzvorschriften unterliegt (EuGH, Urteil v. 10.07.2018 – C-25/17, Rn. 65) und gegen jeden Verantwortlichen vorgegangen werden kann (EuGH, Urteil v. 05.06.2018 – C-210/16).

IV. Ermessen

Angesichts des vorbenannten Verstoßes bei der Verarbeitung von personenbezogenen Daten sind die tatbestandlichen Voraussetzungen des § 6 HmbRI(EU)2016/680UmsAAG i.V.m. § 43 Abs. 1 Satz 5 HmbJVollzDSG erfüllt. Der HmbBfDI kann demnach geeignete Maßnahmen anordnen, wenn dies zur Beseitigung des erheblichen Verstoßes gegen datenschutzrechtliche Vorschriften erforderlich ist. Die Entscheidung über die Anordnung von geeigneten Maßnahmen gegenüber der Aufsichtsbehörde des Verantwortlichen steht demnach im pflichtgemäßen Ermessen des HmbBfDI. Von diesem eingeräumten Ermessen macht der HmbBfDI im vorliegenden Fall in zulässiger Weise Gebrauch, da der festgestellte Verstoß erheblich ist, von der rechtswidrigen Datenverarbeitung durch die GAS eine große Anzahl von Bürgerinnen und Bürgern betroffen ist und die verantwortliche Stelle/bzw. deren Aufsichtsbehörde keine Bereitschaft gezeigt hat, den rechtswidrigen Zustand zu beseitigen.

Die Ermessenserwägungen haben sich dabei vom Zweck der Ermächtigung leiten zu lassen und die gesetzlichen Grenzen des Ermessens zu wahren (§ 40 HmbVwVfG). Dem Zweck der Ermächtigung folgend ist der HmbBfDI gehalten, unter Berücksichtigung der Anforderungen an einen effektiven Datenschutz einerseits und den Grundsätzen der Verhältnismäßigkeit andererseits darüber zu entscheiden, ob die Anordnung geboten ist.

Unter Beachtung dieser Maßgaben waren folgende Ermessenserwägungen für den Erlass der Löschungsanordnung ausschlaggebend: Der Zweck der Ermächtigung liegt in der Wiederherstellung eines datenschutzkonformen Zustands durch die datenschutzrechtliche Aufsichtsbehörde mittels der Anordnung geeigneter Maßnahmen gegenüber der Aufsichtsbehörde des Verantwortlichen, die durch eine rechtswidrige Verarbeitung von personenbezogenen Daten einen datenschutzwidrigen Zustand hergestellt hat. Die Anordnung ist geeignet, diesen Zweck zu erreichen, da durch die Löschung der Referenzdatenbank und der darauf enthaltenen Templates eine rechtswidrige Speicherung von rechtswidrig verarbeiteten personenbezogenen Daten beendet wird.

Die angeordnete Maßnahme ist erforderlich, weil ein milderes Mittel nicht ersichtlich ist, welches den gleichen Erfolg mit der gleichen Sicherheit und einem vergleichbaren Aufwand herbeiführen würde.

Die grundsätzlich zu beachtende Möglichkeit, gem. § 6 HmbRI(EU)2016/680UmsAAG i.V.m. § 43 Abs. 1 S. 4 HmbJVollzDSG lediglich vorab eine Verwahrung auszusprechen, mit der Möglichkeit einer freiwilligen Einstellung, war vom Gesetzgeber zum Zeitpunkt des Beginns des Einsatzes der GAS im November 2017 noch nicht vorgesehen (HmbRI(EU)2016/680UmsAAG sowie das HmbJVollzDSG sind am 18.05.2018 in Kraft getreten).

Der HmbBfDI hat der Verantwortlichen vor Erlass einer offiziellen Beanstandung gegenüber ihrer Aufsichtsbehörde durch Übermittlung einer rechtlichen Stellungnahme vom 05.07.2018 zunächst trotzdem die Möglichkeit eingeräumt, von einer weiteren rechtswidrigen Datenverarbeitung freiwillig Abstand zu nehmen und gleichzeitig auf die Möglichkeit des Erlasses einer Beanstandung und Anordnung hingewiesen.

Die Verantwortliche hat ausdrücklich klargestellt, weder vom Einsatz der GAS absehen noch eine Löschung der gespeicherten Templates vornehmen zu wollen. Zudem wurde angekündigt, das hier eingesetzte Verfahren der automatischen Gesichtserkennung auch auf

andere polizeiliche Einsatzfelder auszudehnen (vgl. Bericht Innenausschuss, v. 21.11.2018, 21/15080, S. 11). Insoweit war eine Reaktion zur Verhinderung des künftigen Einsatzes dieses Verfahrens erforderlich.

Die Anordnung ist auch angemessen, weil das mit ihr verfolgte Ziel in seiner Wertigkeit nicht außer Verhältnis zur Intensität der Löschungsanordnung steht. Der Verhinderung und Aufklärung von Straftaten kommt nach dem Grundgesetz eine hohe Bedeutung zu (ebenso BVerfG, Beschluss v. 22.08.2006 – 2 BvR 1345/03, Rn. 72). Der Einzelne muss aber nur solche Beschränkungen seiner Rechte hinnehmen, die auf einer verfassungsgemäßen, gesetzlichen Grundlage beruhen und die die Anforderungen erfüllen, die sich aus der Art und Intensität des jeweiligen Grundrechtseingriffs ergeben (BVerfG, Urteil v. 11.03.2008 – 1 BvR 2074/05, Rn. 75). Die – einmal unterstellte – Effektivitätssteigerung in der Strafverfolgung durch die GAS kann nicht von der Beachtung rechtsstaatlicher Grundsätze dispensieren.
Die Ausgestaltung von Eingriffsermächtigungen mit besonderer Intensität und dem Schutz vor wesentlichen Eingriffen in Grundrechte liegt in den Händen der Legislative und darf nicht dem Ermessen der Strafverfolgungsbehörden im Rahmen von Generalklauseln überlassen bleiben. Es ist daher zunächst Aufgabe des Gesetzgebers, gegebenenfalls Eingriffsschwelle, Umfang, Verfahrensanforderungen und Grenzen derartiger Eingriffe festzulegen, bevor biometrische Auswertungssysteme im Rahmen der Strafverfolgung eingesetzt werden können. Im Übrigen stellt eine Löschung der Datenbank mit den Gesichtstemplates keinen schweren Eingriff in die stafprozessuale Aufarbeitung des G 20-Gipfel dar. Die Löschung bezieht sich nämlich nicht auf das gesamte Videomaterial, das die Polizei nach wie vor zur Strafverfolgung auswerten kann. Sollte sich daher erweisen, dass der Einsatz der automatisierten Gesichtserkennung entgegen der Rechtsauffassung der Aufsichtsbehörde zulässig war, kann das Material durch Eingabe der Daten in die Software jederzeit wieder hergestellt werden.

Auch soweit hier eine gemeinsame Verantwortlichkeit zwischen Polizei Hamburg und Staatsanwaltschaft Hamburg im datenschutzrechtlichen Sinne vorliegt, ist die Behörde für Inneres und Sport als Aufsichtsbehörde der Polizei Hamburg als Adressat der Anordnung i.S.d § 6 HmbRI(EU)2016/680UmsAAG i.V.m. § 43 Abs. 1 HmbJVollzDSG heranzuziehen, da diese unmittelbar die biometrischen Daten vorhält. Dies folgt sowohl aus den Grundsätzen der datenschutzrechtlichen Verantwortung als auch aus der Überlegung, dass die Polizei Hamburg den datenschutzrechtlichen Verstoß am schnellsten und effektivsten beseitigen kann. Die fragliche Datenbank befindet sich in ihrem tatsächlichen Herrschaftsbereich. Sie hat die Zugänge zur Hardware und ist mit der Bedienung und Gestaltung der Software vertraut. Darüber hinaus liegt keine allgemeine Anordnung der Staatsanwaltschaft zur biometrischen

Analyse, Datenbankerstellung oder überhaupt zur Nutzung der Software in dieser Weise vor, die gegenüber der Polizei aufgehoben werden müsste.

Prof. Dr. Johannes Caspar

Rechtsbehelfsbelehrung:
Gegen diese Anordnung kann innerhalb eines Monats nach Bekanntgabe Klage beim Verwaltungsgericht Hamburg (Lübeckertordamm 4, 20099 Hamburg) erhoben werden.