Der Hamburgische Beauftragte für

Datenschutz und Informationsfreiheit

Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg

Inhalt

I. Sachverhalt

Die Polizei Hamburg setzt derzeit die Gesichtserkennungssoftware „Videmo 360“ (im Folgenden: GAS) für die Analyse von Bild- und Videomaterial im Rahmen der Ermittlungstätigkeit der SoKo „Schwarzer Block“ im Zusammenhang mit den strafrechtlich relevanten Ereignissen während des G20-Gipfels ein, der im Juni 2017 in Hamburg stattgefunden hat. Diese Gesichtserkennungssoftware kann Video- und Bilddateien unterschiedlicher Formate verarbeiten. In dem System findet eine automatisierte Analyse von menschlichen Gesichtern und deren Abgleich statt. Dabei erstellt das System zunächst mathematische Modelle menschlicher Gesichter her (sog. Templates) und ermöglicht im nächsten Schritt die Abgleichung individueller Gesichter, die dann auf Anordnung der Staatsanwaltschaft durch die Polizei erfolgte, untereinander.

Die Anschaffung der GAS beruht auf alleiniger Entscheidung der Polizei Hamburg. Eine „Grundanordnung“ dergestalt, dass die Staatsanwaltschaft Hamburg den Einsatz dieser Software zur Analyse von Gesichtern und das Anlegen von Abgleichdatenbanken zum Zweck des späteren Abgleichs angeordnete hätte, besteht nach vorliegenden Informationen nicht.

Bei Nutzung der GAS werden laut Benutzerhandbuch zunächst folgende Teilfunktionen vorgenommen: *Detektion* und *Identifikation*. Während unter Detektion das reine Lokalisieren (Auffinden) der Gesichter in einer Bild- oder Videosequenz zu verstehen ist, werden im Rahmen der Identifikation auch sog. „Gesichtstemplates“ gebildet; laut Benutzerhandbuch kann diese Funktion jedoch („*z.B. aus Gründen des Datenschutzes*“) deaktiviert werden. Unter „Gesichtstemplates“ 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 etc.). Die erfassten Punkte werden für jedes Gesicht in einer mathematischen Form abgespeichert (sog. Templates). Die Templates werden dann samt Fundstelle (d.h. Name des Videos, Chipkartennummer, Clip-Nr., Zeitstempel) in einer Datenbank hinterlegt. Die eingelesenen Videodaten können durch „Videmo 360“ nicht verändert werden. Diese Datenbank dient „Videmo 360“ später als Basis für den Vorgang des

Abgleichens und der Wiedererkennung der einzelnen Templates. 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.

Am 23.11.2017 begann die Polizei Hamburg mit dem Prozess der Lokalisierung und Identifikation durch Einspielung von Rohdaten in die Software. Dieser Prozess dauerte 8 Wochen.

Nach Angaben der Polizei mit Stand vom 6. August 2018 liegen der SoKo „Schwarzer Block“ insgesamt 100 TB Bild- und Videomaterial vor. Das davon für „Videmo 360“ genutzte Rohmaterial umfasste ca. 17 TB und setzte sich zusammen aus polizeieigenem sowie polizeifremden Bild- und Videomaterial. Das polizeifremde Material wiederum fügt sich zusammen aus Material aus 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:

- Königsstraße: 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)

Das Material wurde vor Einspielung nicht durch einen menschlichen Bearbeiter der Polizei Hamburg gesichtet oder aussortiert, sondern zeitlich lückenlos in das System 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 „Videmo 360“-Server eingespielt. Als Grund dafür gibt die Polizei technischen 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.

Das Hinweisportal „Boston Infrastruktur“ war im Zeitraum vom 08.07.17 (03:00 Uhr) bis 17.07.17 (23:45 Uhr) der Öffentlichkeit freigegeben worden. 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 werden auf den Servern des BKA entgegengenommen und per VPN-Verbindung aus Hamburg abgerufen. Die hochgeladenen Dateien werden nur von der Polizei Hamburg genutzt.

Über das Hinweisportal gingen 10.588 einzelne Hinweise ein, die insgesamt 14.334 Dateien enthielten. Über 4.500 dieser Dateien sortierte die Polizei im Rahmen einer ersten manuellen Sichtung aus, weil sie erkennbar keine Relevanz für die G20-Ereignisse hatten (z.B. Videos mit pornographischem Inhalt) und löschte sie. Die Polizei Hamburg legte gegenüber dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit dar, dass sämtliche von Bürgern hochgeladenen Dateien auf G20-Relevanz untersucht und bei erkennbarem Nichtvorliegen der Relevanz aussortiert wurden. Eine G20-Relevanz sei nach Ausführungen der Polizei Hamburg immer dann gegeben, wenn die Bild- und Videosequenzen einen örtlichen und zeitlichen Zusammenhang zu den Ausschreitungen in Hamburg vor und während des Gipfels aufwiesen. Dateien, die zwar örtlich und zeitlich in den „G20-Rahmen“ passen, aber keine Straftaten abbilden, wurden nicht aussortiert. Auch wenn auf den Bildern keine Straftat abgebildet sei und z.B. nur Passanten gezeigt würden, können diese Bilder nach Auffassung der Polizei für die Identifizierung von Tatverdächtigen notwendig sein.

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 von 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 Polizei führt aus, dass die Anzahl der Dateien auf dem „Videmo 360“-Server schwankend und tendenziell anwachsend sei.

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.

Eine Feststellung der Zahl der Gesichtstemplates oder der Anzahl der Personen, die von dem auszuwertenden Bildmaterial erfasst wurden, ist von der Software nicht vorgesehen. Der Aufbau des Netzwerks wurde dem HmbBfDI in der Besprechung am 28.02.2018 auf Nachfrage grob skizziert. Die Polizei Hamburg nutzte die Voreinstellung

der Software (sog. Default-Einstellung) des Herstellers. Neben den Templates erstellt die Software in der Default-Einstellung auch einen Konfidenzwert über die Wahrscheinlichkeit, dass das vermeintlich gefundene Gesicht wirklich ein menschliches Gesicht ist und über die nach Angaben der Polizei jedoch unzuverlässige und daher nicht weiter genutzte Schätzung über Geschlecht und Alter des Gesichts. Die Polizei Hamburg bekam auf die nachträgliche Anfrage bei der zuständigen Softwarefirma eine Version zur Verfügung gestellt, die keine automatische Altersschätzung mehr durchführt. Über den Einsatz dieser neuen Version bzw. Ersetzung der alten Software im Rahmen der Bearbeitung liegen keine Auskünfte vor.

In einem gesonderten bzw. parallel laufenden Schritt zu der automatischen Lokalisierung und Vermessung von Gesichtern durch die Gesichtserkennungssoftware „Videmo 360“ wird das Material, das die Polizei selbst erstellt hat, von den Bildauswertern der Sonderkommission „Schwarzer Block“ manuell gesichtet. Die Auswertung erfolgt mittels Wiedererkennungsvermögen und Gedächtnisleistung des einzelnen Auswerters sowie über Rechercheunterlagen und über die Crime-Datei „Schwarzer Block“, welche anlässlich der Ereignisse während des G20-Gipfels errichtet wurde. Durch eine ebenfalls durchgeführte Geolokalisierung des Bild- und Videodatenmaterials (VIDoGIS) des Datenbestandes wird die Recherche im kompletten Datenbestand nach den genannten Parametern „Zeit“ und „Ort“ ermöglicht. Die manuellen Bildauswerter der Sonderkommission 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 Templates-Datenbank 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 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, so dass die Aufklärungsarbeit nicht auf die G20-ED-Bilder beschränkt werden muss. Auf Nachfrage teilte die Polizei mit, dass keine Lichtbilder aus sog. „Gefährderdateien“ herangezogen würden. Voraussetzung für die Einleitung eines Abgleichverfahrens sei stets ein konkreter Tatverdacht. Die Staatsanwaltschaft genehmigt(e) die Recherche in „Videmo 360“ auf der Grundlage von §§ 161, 163 i.V.m. § 98 c StPO (vgl. dem HmbBfDI durch die Polizei überreichte beispielhafte Verfügung der Staatsanwaltschaft vom 20.06.2018).

Seit dem 01.03.2018 (und andauernd) werden die ggf. mehreren zu einer „Identität“ verknüpften Gesichtern mit sämtlichen zuvor erstellten Gesichtstemplates, die sich in der Datenbank 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. vgl. oben), auf dem Rechercherechner aufgelistet. Der Videoauswerter muss sodann die Gesichter aus dem Suchergebnis manuell herausfiltern, die tatsächlich mit dem gesuchten Gesicht übereinstimmen. Dann werden alle bis dahin manuell zugeordneten Treffer 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.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat sich zweimal (11.10.2017 und 28.02.2018) mit Vertretern der Polizei und einem Vertreter der Staatsanwaltschaft bezüglich des Einsatzes der GAS getroffen. Im Rahmen beider Treffen äußerten die Polizei und die Staatsanwaltschaft, dass durch die dargestellte Nutzung der Software sich u.a. versprochen wird, in der Lage sein zu können, das Verhalten eines Beschuldigten in der Vor- und Nachtatphase zu ermitteln, einem Beschuldigten noch weitere bis dato unbekannte Straftaten zu zuordnen und bekannte

Taten aus anderen Blickwinkeln festzustellen, aber auch entlastende Informationen bezüglich des Beschuldigten zu gewinnen. Bei unbekannten Tatverdächtigen werde „Videmo 360“ ebenfalls genutzt um eine Identifizierung zu ermöglichen. Im Rahmen des Termins am 11.10.2017 gab die Polizei zunächst auf Nachfrage an, dass Videodateien ohne aufgezeichnete strafbare Handlung für die „SOKO Schwarzer Block“ uninteressant seien und keine Anwendung im Rahmen von „Videmo 360“ fänden. Beim Treffen am 28.02.2018 wurde eine derartige Einschränkung nicht mehr vorgenommen. Auf Nachfrage des HmbBfDI wurde wiederholt § 161 StPO und § 98 c StPO als einschlägige Rechtsgrundlagen für den Einsatz von „Videmo 360“ genannt.

Der Hamburgische Polizeipräsident hat die Vorgehensweise der Polizei durch Einsatz eines Hinweisportals und deren 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. Juli 2018 - gerichtet an Hamburgischen Polizeipräsidenten - hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit die Auffassung vertreten, dass die Analyse von Gesichtsmerkmalen aus Bild- und Videosequenzen und deren Nutzung zur Erstellung von sog. Templates durch den Einsatz von „Videmo 360“ rechtswidrig sei. Hierzu wurde eine rechtliche Beurteilung auf Basis der bis dahin durchgeführten Untersuchungen vorgelegt. Die Polizei Hamburg wurde um fristgebundene Stellungnahme gebeten.

Mit Schreiben vom 18. Juli 2018 hat die Generalstaatsanwaltschaft Hamburg zunächst zum Schreiben des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit Stellung genommen. Dabei wurde im Wesentlichen ausgeführt, dass die Bildung der sog. Templates schon kein eigenständiger Eingriff in das Grundrecht auf informationelle Selbstbestimmung sei. Es handele sich um einen integralen Bestandteil des gesamten Auswertungsvorganges. Das gesamte Verfahren – Analyse und Vermessung von Gesichtern, Erstellung der Templates und anschließender Abgleich dieser Templates untereinander – sei ein vergleichsweise niedrigschwelliger Eingriff in das Grundrecht. Durch den Einsatz der Software werde die Dauer des Eingriffs verkürzt. Als Ermächtigungsgrundlage für diesen gesamten Vorgang sei daher die Ermittlungsgeneralklausel nach § 161 Abs. 1 StPO - wahlweise auch § 483 StPO - ausreichend. Dies folge aus der Entscheidung des Bundesverfassungsgerichts zur Abfrage von Kreditkartendateien von Verdächtigen im

strafrechtlichen Ermittlungsverfahren (BVerfG, Beschluss v. 17.02.2009 – 2 BvR 1372, 1745/07), sowie aus den Erwägungen des BGH aus dem Jahre 1975 im Zusammenhang mit dem Recht am eigenen Bild und der Herstellung von Fotographien eines Demonstrationszuges (BGH, Urteil v. 12.08.1975 – 1 StR 42/75).

Mit Schreiben vom 23.07.2018 hat die Polizei Hamburg zum Schreiben des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit Stellung genommen. Sie vertritt die Ansicht, dass es sich bei sämtlichen der beschriebenen Tätigkeiten im Rahmen des Einsatzes von „Videmo 360 um solche der Strafverfolgung handele. Die Polizei Hamburg gab nun an, dass das gesamte polizeieigene Bild- und Videomaterial, das als Rohdaten in „Videmo 360“ eingespielt worden sei, anlassbezogen und aufgrund eines Anfangsverdacht bezüglich einer Straftat nach § 100h StPO erhoben worden sei. Bild- und Videoaufzeichnungen, die aufgrund einer Gefährdungslage bei Veranstaltungen, Ansammlungen oder Versammlungen durch die Polizei nach Landesrecht erhoben werden dürften, seien demnach nicht in „Videmo 360“ eingespeist worden. Bei dem polizeifremden Material handele es sich ebenfalls allesamt um strafrechtliche Beweismittel, die formlos sichergestellt worden seien. Die erstellten mathematischen Modelle von menschlichen Gesichtern könne man bereits nicht als personenbezogenes Datum qualifizieren. Bei der Analyse von Gesichtsmerkmalen, der Erstellung von Templates und der Speicherung dieser Templates handele es sich nicht um eigenständige Eingriffe in das Recht auf informationelle Selbstbestimmung, es bedarf daher keiner gesonderten Ermächtigungsgrundlage. Biometrische Analysen und deren spätere Nutzung zum automatisierten Abgleich seien nur Hilfsmittel zur Sichtung des Materials und daher mit der Beobachtung und Sichtung durch einen Polizeibeamten gleichzusetzen. Dieser gesamte Vorgang sei daher bereits von der Ermittlungsgeneralklausel (§§ 161, 163 StPO) gedeckt, darüber hinaus folgt die Zulässigkeit der Auswertung von GAS bereits aus der Norm, die der Polizei die Anfertigung von Videoaufnahmen gestattet (§ 100 h StPO), § 48 BDSG bilde den Prüfungsmaßstab, § 98c StPO sei nicht einschlägig. Die Speicherung der Templates erfolge auf Grundlage des § 483 StPO. Die Recherche in „Videmo 360“ sei im Rahmen der Verhältnismäßigkeit die mildere Eingriffsmaßnahme gegenüber der Öffentlichkeitsfahndung.

Auf eine kleine schriftliche Anfrage der Abgeordneten Christiane Schneider und Cansu Özdemir (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 soll auch künftig dort zu

diesem Zweck genutzt werden. Aktuell werde die Gesichtserkennungssoftware vom LKA nicht genutzt (Drucksache 21/13939 vom 10.08.2018: Antwort zu Frage Nr. 12).

Auf eine telefonische Anfrage des HmbBfDI vom 2. August 2018 teilte die Justizbehörde am 24. August 2018 mit, über den Einsatz der Gesichtserkennungssoftware durch die Staatsanwaltschaft am 6. März 2018 informiert worden zu sein.

II. Rechtliche Stellungnahme

Die ausnahmslose und verdachtsunabhängige Erfassung und Vermessung von allen, auf den fraglichen Video- bzw. Bildmaterial zu sehenden menschlichen Gesichtern, die Erstellung von mathematischen Modellen („Templates“) dieser Gesichter und die Speicherung dieser Modelle in umfangreichen Referenzdatenbanken zum Zwecke eines späteren Abgleichs dieser Modelle untereinander sind bereits rechtswidrig. Daraus folgt auch die Unzulässigkeit des – hier nicht weiter untersuchten – zeitlich nachfolgenden Abgleichs dieser Templates untereinander. Die Polizei Hamburg als verantwortliche Stelle hat daher die Datenbank gem. § 75 Abs. 2 BDSG zu löschen.

Die durchgeführte biometrische Analyse von Gesichtsmerkmalen und die Erstellung von sog. Gesichtstemplates sowie deren Speicherung sind eigenständige Datenverarbeitungsschritte, die zusätzlich zur vorherigen Bild- und Videoerhebung durch Kameraaufnahmen, deren Speicherung und der folgenden Abgleichmaßnahme 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 eingreifen, und daher einer hinreichend bestimmten Ermächtigungsgrundlage bedürfen.

An einer klaren gesetzlichen Grundlage im Sinne einer verfassungsmäßigen Schranke, die die Voraussetzungen für derartige intensive Eingriffe normiert und erkennbar regelt, fehlt es nach geltendem Recht. Aus der Rechtmäßigkeit der Erhebung von Bild- und Videoaufnahmen folgt nicht die Zulässigkeit der weiteren biometrischen Verarbeitung zu individuellen Gesichtsprofilen. Zwar vermögen auch technische Erneuerungen und Weiterentwicklungen von Aufklärungsmethoden vom Wortlaut bestehender (Ermittlungs-)Normen gedeckt sein, ein Auswertungssystem, das bislang nicht bekannte Dimensionen staatlicher Kontrolle über den Aufenthaltsort und das Verhalten von Personen in kürzester Zeit ermöglicht und - in Bezug auf den ganz überwiegenden Teil der Betroffen - anlasslos Gesichtsmerkmale ausliest und maschinenlesbar abspeichert, fällt nicht mehr darunter. Insbesondere kann eine biometrische Aufbereitung von

Abbildungen menschlicher Gesichter nicht mit der einfachen Sichtung des Materials gleichgestellt werden. Eine solche Technologie verschiebt mit seiner Eingriffsintensität die gesetzlich austarierte Balance zwischen informationeller Selbstbestimmung und staatlicher Eingriffsbefugnis zur Strafverfolgung massiv zu Lasten der Wahrung der Privatsphäre.

Nur durch eine hinreichende gesetzgeberische Entscheidung kann sichergestellt werden, dass sowohl die Betroffenen als auch die Handelnden den Inhalt und die Grenzen von derartigen Auswertungssystemen klar erkennen und ihr Verhalten danach ausrichten können. Für die Nutzung von großen Datenmengen durch automatisierte Analyseverfahren bedarf es zunächst klarer Regelungen, um gerade Unsicherheiten bezüglich der Anwendbarkeit der Norm, Voraussetzungen, des Umfanges und der Reichweite solcher Maßnahmen zu beseitigen, die durch die immer leistungsfähiger werdende modernen Datenverarbeitung und fortschreitenden technischen Möglichkeiten entstehen können.

Die momentanen Ermächtigungsnormen für polizeiliches Handeln erfüllen diese Anforderungen nicht:

Zunächst stützen Polizei und Staatsanwaltschaft den Einsatz von GAS stets auf die Ermächtigungsgeneralklausel (§§161, 163 StPO) i.V.m. § 98c StPO. Nunmehr, im Rahmen der erfolgten Stellungnahmen, wird seitens der Generalstaatsanwaltschaft lediglich §§ 161, 163 StPO oder wahlweise § 483 StPO als Ermächtigungsgrundlage herangezogen. Während die Polizei nunmehr zwischen polizeifremden (dann §§161, 163 StPO) und polizeieigenem (dann § 100h StPO) Material zu differenzieren scheint, wird § 98c StPO - weder von der Staatsanwaltschaft noch der Polizei, die nunmehr erklärt § 98c StPO sei nicht anwendbar - als einschlägig gesehen.

Die Generalermächtigungsklausel (§§ 160, 163 StPO) ist aber zu unbestimmt um derartige Eingriffe zu rechtfertigen. Selbst wenn man - aufgrund der hohen Anforderungen, die § 100h StPO für grundrechtliche Eingriffe aufstellt - mit der Polizei Hamburg annehmen sollte, dass eine Ermächtigung zu Video- und Bildaufnahmen auch deren biometrische Bearbeitung (mit) abdeckt, kann aufgrund der Vermengung zum Zweck des späteren Abgleichs mit den übrigen Templates dies im vorliegenden Fall nicht bejaht werden. Weiter Ermächtigungsgrundlagen sind ebenfalls nicht einschlägig.

Dazu im Einzelnen:

1. Nutzung des „polizeifremden“ Materials

Die Nutzung einer Technologie zur biometrischen Analyse von menschlichen Gesichtern, Erstellung von mathematischen Modelle dieser Gesichter und Speicherung dieser Modelle zum Zwecke des späteren Abgleich aus privaten Video- und Bildmaterialien durch die Polizei Hamburg erfolgte jeweils ohne hinreichend bestimmte Ermächtigungsgrundlage.

a. § 81b StPO

§ 81b StPO vermag die Analyse von Gesichtsmerkmalen und die Speicherung von mathematischen Modellen von menschlichen Gesichtern aus dem der Polizei Hamburg zustehenden Rohmaterial durch die GAS nicht zu rechtfertigen. § 81b StPO erlaubt zum Zwecke der Durchführung des Strafverfahrens oder für die Zwecke des Erkennungsdienstes die Vornahme von „Messungen“ und ähnliche Maßnahmen gegen den Willen eines Beschuldigten. Es kann schon bezweifelt werden, dass die erlaubten „Messungen“ auch das vorliegend zu beurteilende Herausfiltern und Abspeichern von Gesichtstemplates beinhalten. Dies kann allerdings im Ergebnis offen bleiben, weil die Anwendbarkeit der Norm daran scheitert, dass die Betroffenen der Maßnahmen zumindest ganz überwiegend zum Zeitpunkt der Maßnahme keine Beschuldigten waren. Dies wäre aber Voraussetzung für eine Maßnahme nach § 81b StPO (vgl. OVG Hamburg, Urteil v. 11.04.2013 – 4 Bf 141/11 Rn. 31 ff.). Beschuldigter i.S.d Norm ist nicht derjenige, der in einen vagen Tatverdacht gerät. Vielmehr müssen tatsächliche Anhaltspunkte gem. § 152 Abs. 2 StPO für die Begehung einer Straftat durch den Betroffenen vorliegen (KK-StPO/Senge, 7. Auflage 2013, § 81b Rn. 2). Eine vorherige Einordnung der Betroffenen als Beschuldigte war aber zum Zeitpunkt der Anwendung von „Videmo 360“ nicht gegeben. Im vorliegenden Fall wurden sämtliche technisch lokalisierbaren Abbildungen von menschlichen Gesichtern erfasst und analysiert. Viele Betroffene wurden dabei nur zufällig von der GAS erfasst, kategorisiert und als mathematisches Modell abgespeichert, weil sie sich zu einem bestimmten Zeitpunkt an einem bestimmten Ort (z.B. auf einem S-Bahnhof in der Zeit vom 06.07.2017 bis 10.07.2017) aufgehalten hatten und von einer Kamera aufgezeichnet wurden.

b. § 483 Abs. 1 StPO

Ebenso scheidet § 483 Abs. 1 StPO als Ermächtigungsgrundlage aus.

Die Norm erlaubt gemäß Absatz 1 die Speicherung, Veränderung und Nutzung von personenbezogenen Daten nachdem die Daten aufgrund einer gesonderten Ermächtigungsgrundlage erhoben worden sind (KK-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/Graf, 29. Ed. 01.01.2018, § 483 Rn. 1). Dies folgt aus § 483 Abs. 2 StPO, denn dieser erlaubt ausdrücklich die Nutzung der Daten des 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/Graf, 29. Ed. 01.01.2018, § 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 i.S. eines Anfangsverdachts soll - nach Angaben der Polizei Hamburg - vielmehr den Vorgang des Abgleichens mit der Templatedatenbank einleiten; zu diesem Zeitpunkt sind aber bereits alle Gesichter ausgewertet und deren Modelle abgespeichert worden.

c. § 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 (KK-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.

d. §§ 161, 163 StPO i.V.m. § 48 BDSG

Nach Angaben der Polizei handelt es sich bei sämtlichen Bild- und Videosequenzen aus dem öffentlichen Nahverkehr sowie aus dem Hinweisportal des BKA um sog. formlos sichergestellte Beweismittel gem. § 94 Abs. 1 StPO, da sie allein aufgrund ihrer zeitlichen und örtlichen Einordnung in den von der Polizei Hamburg festgelegten G20-Rahmen eine potentielle Beweisbedeutung besäßen.

Eine Auswertung dieser sichergestellten Daten durch Inaugenscheinnahme könne neben dem menschlichen Betrachter auch durch das – allein unterstützend wirkende „Hilfsmittel“ – „Videmo 360“ erfolgen. Dieser „Inaugenscheinnahme“ von Daten (wobei die Polizei dabei nicht zwischen biometrischer Analyse, Templateerstellung und späteren Abgleich unterscheidet) stelle keinen tiefgreifenden Eingriff in das Recht auf informationelle Selbstbestimmung dar. Der gesamte Vorgang, also die Analyse/Herausfilterung von Gesichtsmerkmalen aller auf dem Material enthaltenen beliebig vielen Personen, die Erstellung des mathematischen Modells dieser Merkmale und der Abgleich dieser Modelle bedürfe daher keiner über § 161 Abs. 1 StPO hinausgehenden Spezialermächtigung. Den Prüfungsmaßstab für biometrische Daten stelle § 48 BDSG dar.

Dem kann nicht gefolgt werden. Die Ermittlungsgeneralklauseln der StPO scheiden als Ermächtigungsgrundlage für die Analyse von Gesichtern und Erstellung von mathematischen Modellen aus Gesichtsmerkmalen aus. Diese allgemeinen Regelungen sind zu unspezifisch, um massenhafte Eingriffe in besondere Kategorien personenbezogener Daten von tausenden unbeteiligter Personen, deren biometrische Daten zunächst auf Vorrat erhoben werden, zu legitimieren. Bei §§ 161,163 StPO handelt es sich um Ermittlungsgeneralklauseln, auf die nur solche Ermittlungsverfahren gestützt werden können, die mit keinen oder 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, 29. Ed., § 161 Rn. 4).

Daran ändert auch der nun anwendbare § 48 BDSG im Rahmen der Generalklauseln nichts (vgl. Referentenentwurf des Bundesministeriums für Justiz und für Verbraucherschutz: *Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die VO EU) 2016/679*. Nach diesem Entwurf soll künftig bereits in § 161 Abs. 2 StPO auf § 48 BDSG zur *Klarstellung* verwiesen werden (S. 66)). § 161 Abs. 2 – StPO-E lautet: „*Zu*

den in § 160 bezeichneten Zwecken dürfen besondere Kategorien personenbezogener Daten nach Maßgabe des § 48 des Bundesdatenschutzgesetzes verarbeitet werden" (S. 8). Stand 23.04.2018).

§ 48 BDSG dient zwar zunächst der Umsetzung der Richtlinie (EU) 2016/680 und schafft für öffentliche Stellen im Rahmen der Strafverfolgung (und Gefahrenabwehr) eine Rechtsgrundlage für die Verarbeitung besonderer Kategorien 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 aber ebenfalls um eine unspezifische Generalklausel (so ausdrücklich Kühling/Buchner/Schwichtenberg, DSGVO/BDSG, 2. Auflage 2018, § 48 BDSG, Rn. 7), die intensive Grundrechtseingriffe mit derart hoher Streubreite nicht zu rechtfertigen vermag. Eine biometrische Massendatenerhebung kann daher nicht auf diese Rechtsgrundlage gestützt werden.

aa. Grundrechtseingriff durch biometrische Analyse

Bereits die hier vorliegende biometrische Analyse von Lichtbildern von zum großen Teil unbeteiligten Personen zur Erstellung mathematischer Modelle zum Zweck des späteren Abgleichs 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 dar.

Entgegen dem Verständnis der Polizei und der Generalstaatsanwaltschaft handelt es sich dabei insbesondere rechtlich nicht bloß um „*integrale Bestandteile des gesamten Auswertungsvorganges*", sondern um weitere - neben der Anfertigung des Video- und Bildmaterials und des späteren Abgleichs - eigenständige Datenverarbeitungsschritte mit eigener Eingriffsqualität, die auf eine Erlaubnisgrundlage zu stützen sind (Jandt, ZRP 2018, 16 (18), die genannte Autorin befasst sich überwiegend mit Systemen, bei denen Videoüberwachung mit biometrischer Gesichtserkennung kombiniert wird (sog. Intelligente Videoüberwachung), dennoch werden die einzelnen Schritte datenschutzrechtlich gesondert untersucht.).

Zwar regelt der Gesetzgeber datenschutzrechtlich zu unterscheidende Eingriffe oftmals - aus Gründen der Praktikabilität - zusammen (z.B. die Aufzeichnung und Speicherung von Videoaufnahmen), eine rechtliche Einheit stellen sie dennoch nicht dar. Eine Erlaubnis zur Erhebung von Daten impliziert nicht gleichzeitig deren Speicherung. Eine Erlaubnis zur Speicherung von personenbezogenen Daten erlaubt nicht jegliche Form deren weiteren Verarbeitung. Vielmehr ist jeder Schritt der Datenverarbeitung von

personenbezogenen Daten zu beachten und auf deren Zulässigkeit zu untersuchen. So handelt es sich vorliegend bei der Speicherung und Erhebung des Video- und Bildmaterials zunächst um unspezifische Abbildungen von Personen, die erst aufgrund eines weiteren Verarbeitungsschritts mittels der GAS zu biometrischen Gesichtstemplates, die automatisiert ausgewertet werden können, umgewandelt werden.

Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG schützt den Bürger zunächst gegen jede Art der staatlichen Erhebung, Speicherung und Verwendung seiner persönlichen Daten, also auf ihn bezogene, individualisierte oder individualisierbare Informationen. 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 die grundrechtlich geschützten 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).

Durch die Analyse bzw. das Herausfiltern von biometrischen Merkmalen und das Erstellen von mathematischen Modellen liegen selbstständige Eingriffe in das Grundrecht vor. Der polizeilichen Einschätzung, dass es sich bei den hier vorliegenden biometrischen Geschichtstemplates bereits nicht um personenbezogene Daten handelt bzw. kein eigenständiger Eingriff in das Grundrecht auf informationelle Selbstbestimmung vorliegt, kann nicht gefolgt werden.

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dabei ist eine natürliche Person identifizierbar, die direkt oder indirekt, insbesondere mittels Zuordnung zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Bei biometrischen Daten handelt es sich um mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu

den physiologischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen (Art. 3 Nr. 1 und 13 der Richtlinie (EU) 2016/680).

Gesichtsbilder von Personen sind dabei bereits unstreitig personenbezogene Daten, weil sie Rückschlüsse auf die Identität einer Person sowie über deren zeitlichen Aufenthaltsort zulassen (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 und sich auf zumindest identifizierbare Personen beziehen (Schwenke NJW 2018, 823 (824)). 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 Modellen abgespeichert (Thiel ZRP 2016, 218 (219 ff.)) Nicht das Videomaterial selbst, sondern die aus diesem extrahierten Merkmale stellen biometrische Daten dar (Jandt, ZRP 2018, 16 (18)). Aus einzelnen Abbildungen von menschlichen Gesichtern werden mit Hilfe von speziellen technischen Verfahren Informationen zusammengetragen und Nutzungen erschlossen, die ein gewöhnliches Lichtbild – und damit auch die Abbildung in einer Videosequenz – nicht preisgeben.

Die gespeicherten Templates weisen ebenfalls einen Personenbezug auf, weil sie dazu bestimmt sind, eine Person identifizierbar zu machen. So lässt sich aus der Antwort des Senats zur Kleinen schriftlichen Anfrage entnehmen, dass die SoKo „Schwarzer Block“ die GAS „Videmo 360“ unter anderem gerade einsetzt, um bei unbekannten Personen gegebenenfalls geeigneteres Bildmaterial für weitere Ermittlungen zu deren Identifizierung zu erlangen. Viel mehr gelang es „*mit Hilfe der biometrischen Gesichtserkennung durch Recherchen mit der GAS „Videmo 360“ bislang drei Personen namentlich* (zu) *identifizieren*“ (Drucksache 21/13939: Antwort zu Frage Nr. 10).

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)). Die Merkmale des menschlichen Körpers werden dabei „maschinenlesbar gemacht, wodurch sich vielfältige Nutzungsmöglichkeiten erschließen (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 werden.

So führt das Bundesverfassungsgericht in seiner Entscheidung zur automatisierten Erfassung von Autokennzeichen 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 gegebenenfalls 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.). Dies muss insbesondere auch dann gelten, wenn Gesichtsmerkmale analysiert werden, mathematische Modelle von Gesichtern erstellt werden und diese - nicht die eigentlichen Lichtbilder - als Grundlage für einen späteren Abgleich benutzt werden. Vollständigkeitshalber sei erwähnt, dass im Ergebnis das Gericht den Eingriff in den Schutzbereich des Grundrecht nur deshalb verneint hat, weil der „*Abgleich mit dem Fahndungsbestand unverzüglich vorgenommen wird und negativ ausfällt, sowie rechtlich und technisch gesichert ist, dass die Daten anonym bleiben und sofort spurlos und ohne die Möglichkeit, einen Personenbezug herzustellen gelöscht werden*“ (Rn. 68). So liegt die Sache hier jedoch nicht, da die personenbezogenen Daten von tausenden von Menschen im Nichttrefferfall gerade nicht nach einer „ergebnislosen Suche“ automatisch gelöscht werden, sondern über Monate in der Datenbank gespeichert werden.

Durch die Analyse von Gesichtsmerkmalen und die Erstellung von maschinenlesbaren Modellen mag es sich zunächst grob betrachtet nur um ein Mittel zur Vorbereitung für den späteren Zweck des Abgleichs handeln. Der Eingriff liegt aber gleichwohl darin, dass dadurch die Informationen für den Staat in einer Weise verfüg- und nutzbar gemacht werden, die bloße Lichtbilder und konventionelle Datenverarbeitung durch manuelle Durchsicht nicht ermöglichen.

So können u.a. das Verhalten (z.B. Kleidungswechsel) und die räumliche Veränderung von Beschuldigten (durch Verknüpfung mit Geodaten) in der Vor- bzw. Nachtatphase ermittelt werden. Dabei können Bewegungsprofile, Verhaltensweisen, Teilnahme an Versammlungen und zwischenmenschliche Kontakte auf dem Hamburger Stadtgebiet über einen Zeitraum von maximal 5 Tagen detailliert rekonstruiert werden. Das Recht auf informationelle Selbstbestimmung schützt aber gerade auch das Interesse des Einzelnen in der Öffentlichkeit, dass die damit verbundenen personenbezogenen Informationen nicht im Zuge automatischer Informationserhebungen zur Speicherung

mit der Möglichkeit der Weiterverwertung erfasst werden (BVerfG Urteil v. 11.03.2008 – 1 BvR 1254/07 Rn. 67).

bb. Keine Rechtfertigung durch Gesetz

Aufgrund der Intensität des hier vorliegenden Eingriffes kann entgegen der Ansicht der Polizei Hamburg von einer (eventuellen) Zulässigkeit der Sicherstellung und Speicherung von Videos und Bildern nicht auf die Zulässigkeit eine weiter biometrische Verarbeitung dieser Bildsequenzen geschlossen werden.

Dabei ist bereits die hier vorliegende umfangreiche formlose Sicherstellung von Bildern und Videosequenzen als potentiell strafrechtliche Beweismittel nach § 94 StPO mehr als zweifelhaft, da sie aus ganz unterschiedlichen privaten Quellen stammen und – außer einer nicht weiter substantiierten groben zeitlichen und örtlichen Zuordnung – keiner weiteren Vorauswahl oder Eingrenzung unterlagen.

Selbst wenn man die Zulässigkeit der formlosen Sicherstellung aller dieser Dateien annehmen würdet, weil es sich um potentielle Beweismittel handelt, die für die Untersuchung von Bedeutung sein können (§ 94 Abs. 1 StPO), kann der Argumentation, dass der Einsatz der GAS eine allgemeine Ermittlungshandlung nach §§ 161, 163 StPO darstellt (vgl. Stellungnahme der Polizei vom 23.07.2018 S. 10) und lediglich ein bloßes Hilfsmittel für die visuelle Auswertung von Videoaufzeichnungen ist (vgl. Stellungnahme der Polizei 23.07.2018 S. 8), nicht gefolgt werden.

§§ 161, 163 StPO i.V.m § 48 BDSG stellen zwar Rechtsgrundlagen für die Verarbeitung von besonderen Kategorien personenbezogener Daten dar, sie sind aber zu unbestimmt, um derartig intensive Eingriffe in das Grundrecht auf informationelle Selbstbestimmung zu rechtfertigen. Der Einsatz von GAS ist nicht mit einer visuellen Auswertung durch einen menschlichen Beobachter gleichzustellen. Es handelt sich um eine neue Technologie, deren Einsatz eine neue Eingriffsqualität darstellt, indem sie eine Auswertung von menschlichen Merkmalen und eine staatliche Kontrolle über den Aufenthaltsort und das Verhalten von Personen automatisiert ermöglicht, die nicht mehr der Informationsgewinnung durch das menschliche Auge entspricht. Die erstellten Templates werden beliebig verwendbar, ohne dass der Betroffe dieses überblicken kann, überhaupt nur Kenntnis erhält oder irgendwie – z.B. durch Antrag auf Löschung – beeinflussen könnte. Nach ständiger Rechtsprechung des Bundesverfassungsgerichts sind Einschränkungen des Grundrechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse insbesondere auch im Rahmen der Strafverfolgung zulässig. Der Verhinderung und Aufklärung von Straftaten kommt insoweit 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 (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 (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 ist dabei der zu verlangende Grad der Bestimmtheit. Das Bundesverfassungsgericht hat dafür mittlerweile gefestigte Kriterien entwickelt. Relevant sind danach:

- Die Gestaltung der Eingriffsschwelle
- Die Anzahl der Betroffenen (sog. „Streubreite“)
- Individuelle Beeinträchtigung.

Dies bedeutet insbesondere, dass verdachtslose Eingriffe mit großer Streubreite, bei denen zahlreiche Personen in den Wirkungskreis einer Maßnahme einbezogen werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff nicht veranlasst haben, eine hohe Eingriffsintensität aufweisen (BVerfG, Beschluss v. 23.02.2007 – 1 BvR 2368/06, Rn. 51 zur Videoaufzeichnung).

Bereits die Videoaufzeichnung an sich stellt einen intensiven Eingriff dar, der aber durch die biometrische Analyse und das Erstellen von mathematischen Modellen von menschlichen Gesichtern sowohl qualitativ als auch quantitativ erheblich intensiviert wird.

Durch Videoaufzeichnungen werden die Daten für eine weitere Auswertung zur Verfügung gestellt. Es werden meist verdachtslose und mit großer Streubreite massenhaft unbeteiligte Personen einbezogen, die den Eingriff nicht veranlasst haben. Daher kann bereits die Videoaufzeichnung an sich nicht auf allgemeine Regeln für die Datenerhebung durch staatliche Stellen gestützt werden (BVerfG, Beschluss v. 23.02.2007 – 1 BvR 2368/06 Rn. 45). Durch die biometrische Analyse wird eine umfangreiche Datenbank eines Teils der Bevölkerung mit Gesichstemplates durch die Polizei erstellt, die wesentliche weitreichende Nutzungsmöglichkeiten und Folgeeingriffe ermöglicht, ohne dass viele der Betroffenen dafür Anlass gegeben hätte, weil der

Großteil der erfassten Betroffenen in keiner Beziehung zu einem Fehlverhalten steht. Wenn lediglich der Aufenthalt im öffentlichen Raum, z.B. bei der Benutzung einer S-Bahnlinie oder der Teilnahme an einer Demonstration ausreicht, dass das individuelle Gesichtsprofil des Einzelnen erstellt über einen unbefristeten Zeitraum in einer polizeilichen Datenbank gespeichert wird, dann liegt hierin ein erheblicher Eingriff in das Grundrecht der informationellen Selbstbestimmung, der auch für die Wahrnehmung des Grundrechts auf Versammlungsfreiheit prohibitive Wirkung hat.

Betroffen wurden von der Maßnahme eine hohe Anzahl von Personen, wobei sich nicht klären ließ, wie viele sog. Identitäten und Gesichtstemplates durch den Einsatz von „Videmo 360“ durch die Polizei erstellt wurden. Denn nicht nur das Betreten eines Bahnsteiges, sondern auch die Tatsache, dass eine weitere Privatperson die Entscheidung getroffen hat, ein Video auf einen Server des BKAs zu laden und dieses Video lediglich nach polizeilicher Einschätzung grob darauf geprüft wurde, ob dies „örtlich und zeitlich in den G20-Rahmen“ passt, führt zur biometrischen Auslese, unabhängig davon, ob strafrechtlich relevantes Verhalten, ein Tatort oder eben nur eine Gruppe Passanten auf dem Video bzw. Bild zu sehen ist.

Das Bundesverfassungsgericht sieht es bereits anlässlich von einer Datenverarbeitung ohne biometrischen Bezug als gegeben an, dass 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).

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 (vgl. zur Videoüberwachung: BVerfG, Beschluss v. 23.02.2007 – BvR 2368/06Rn. 52; BVerfG, Urteil v. 11.03.2008 – 1 BvR 2074/05 Rn. 79).

Das macht auch der europäische Gesetzgeber deutlich. Er stellt in der Richtlinie (EU) 2016/680 fest, 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. Oder 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 (vgl. Erwägungsgrund 51 der Richtlinie).

Der europäische Gesetzgeber erwähnt in seiner 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 die biometrischen Daten von einer hohen Zahl von Menschen ausliest und den durch Videoaufzeichnungen bereits intensiven Eingriff nochmals u.a. durch die Verknüpfungs- und Nutzungsmöglichkeiten deutlich vertieft (s.o.).

Das Bestimmtheitsgebot verlangt daher für die vorliegende Fallkonstellation vom Gesetzgeber, 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, unter denen die umfassende Erstellung von Templates zulässigerweise angeordnet werden kann. Zu den gesetzlich zu regelnden Voraussetzungen 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.

Zwar mögen gewisse technische Erneuerungen/Weiterentwicklungen vom Wortlaut einer Norm gedeckt sein. Das gilt jedoch nicht im Ausgangsfall. 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 Abgleich vorrätig hält, fällt aufgrund seiner enormen Streubreite und seiner Eigenschaft als Grundstein für weitere dadurch möglich werdende Nutzungsmöglichkeiten (z.B. Erstellung von Bewegungs- und Verhaltensprofile) nicht in den Bereich dieser Norm. Vielmehr stellt es einen in seiner Qualität gänzlich neuen Eingriff zur Straftatenermittlung dar, der in den Schutzbereich des Grundrechts auf informationelle Selbstbestimmung erheblich eingreift und deshalb einer eigenständigen gesetzlichen Regelung bedarf.

Dass es sich dabei auch nach Einschätzung der Polizei Hamburg nicht nur - wie nun in der erfolgten Stellungnahme behauptet - um ein „*bloßes Hilfsmittel für die visuelle Auswertung*“ handelt, lässt sich auch aus den Aussagen des Polizeipräsidenten sowie des Leiters der SoKo „Schwarzer Block“ entnehmen, die von einer „*konzeptionellen Weiterentwicklung von nicht unerheblichen Ausmaß*“ bzw. einem „*völlig neuen Standard*

der Beweisführung“ im Zusammenhang mit der Auswertung des Videomaterials sprechen (vgl. Wortprotokoll Nr. 21/12 der öffentlichen Sitzung des Sonderausschusses „Gewalttätige Ausschreitungen rund um G20 – Gipfel in Hamburg“ vom 28. Juni 2018).

Soweit die Polizei in diesem Zusammenhang eine abweichende Rechtsauffassung vertritt und sich dazu auf eine Stimme in der Literatur stützt und ausführt, dass die hier fragliche Maßnahme als verfassungsrechtlich zulässig bewertet wird (vgl. Stellungnahme der Polizei vom 23.07.2018 S. 9), wird verkannt, dass auch der zitierte Autor - entgegen der Ansicht der Polizei Hamburg - zunächst feststellt, dass „*in einer biometrischen Analyse sicherlich ein intensiver Eingriff in das Persönlichkeitsrechte der Betroffenen*“ zu sehen ist (Hornung, InTeR 2015 8 (11)). Folgerichtig geht auch dieser Autor (wohl) nicht davon aus, dass ein solcher Eingriff auf die Ermächtigungsgeneralklausel der StPO gestützt werden kann. Vielmehr ist zu entnehmen, dass im Ergebnis die Ansicht vertreten wird, dass die (hohen) Anforderungen des § 100 h StPO, die die Polizei zu ursprüngliche Videoaufzeichnungen von Tatverdächtigen ermächtigen, auch bestimmt genug seien eine biometrische Analyse durchzuführen, da „*diese Normen relativ hohe Anforderungen statuiert und § 101 StPO verfahrens- und organisationsrechtliche Absicherungen enthält*“ (InTeR 2015 8 (11) vgl. auch Hornung/Schindler ZD 2017 S. 203 (206): wo diese Frage im Rahmen von § 100h StPO erörtert wird). Diese Absicherungen liegen aber gerade bei §§ 161, 163 StPO nicht vor.

Der Einsatz der Technik ist missbrauchsanfällig und kann ohne klare Vorgaben als Instrument einer flächendeckenden staatlichen Überwachung der Bürgerinnen und Bürger eingesetzt werden. Wird, wie im vorliegenden Fall, durchgehendes Videomaterial von beispielsweise 103,5 Stunden (vgl. S-Bahnstation Königsstraße) ohne vorherige Selektion in das System eingespielt, biometrisch erfasst, weist diese Vorgehensweise erhebliche Parallelen zu der sog. Intelligenten Videoüberwachungen auf, die Videoüberwachung mit Gesichtserkennung verknüpfen und an belebten Plätzen die Gesichter aller von der Kamera erfassten Personen automatisch biometrisch verarbeitet und in Echtzeit mit Fahndungsdateien abgleicht (vgl. zum Sachstand: Wissenschaftlicher Dienst des Bundestages „Rechtsgrundlage Einsatz sog. Intelligenter Videoüberwachung durch die Bundespolizei“ WD 3 – 3000 – 202/16). Für den Einsatz solcher Systeme wird im Schrifttum ganz überwiegend vertreten, dass nach derzeitigem Stand dafür keine Ermächtigungsgrundlage besteht. Es bestehen jedoch qualitativ und quantitativ keine relevanten Unterschiede mehr zu dem Fall, dass Personen über einen einem Zeitraum von mehreren Tagen erfasst werden und die Auswertung des Bildmaterials nicht in Echtzeit, sondern erst nachträglich erfolgt.

Diese Überlegung wird dadurch gestützt, dass die Polizei über weitere 159 externe Festplatten des öffentliche Nahverkehrs verfügt, die nur aufgrund von technischen Gegebenheiten (noch) nicht in das System importiert werden. Aufgrund der Aussage der Polizei, dass die Größe der importierten Dateien tendenziell anwachsend sei, ist aber mit einer immer weiteren Ausdehnung zu rechnen. Es widerspricht rechtsstaatlichen Grundsätzen, wenn allein das technisch Mögliche Ausmaß und Intensität der Eingriffe in Grundrechte Betroffener bestimmt.

Auch vermag die von der Generalstaatsanwaltschaft in ihrer Stellungnahme aufgeführte Rechtsprechung zu keiner anderen Beurteilung verhelfen. Weder die Rechtsprechung des Bundesverfassungsgerichts zur Abfrage von Kreditkartendaten bei Kreditkartenunternehmen (BVerfG, Beschluss v. 17.02.2009 – 2 BvR 1372, 1745/07) noch die genannte Entscheidung des Bundesgerichtshofs bezüglich der Verbreitung von Fotographien nach dem Kunsturhebergesetz (BGH, Urteil v. 12.08.1975 – 1 StR 42/75) lassen sich als Argumente für die Anwendbarkeit der Ermittlungsgeneralklausel bei derartigen Eingriffen heranziehen. Vielmehr ist das Gegenteil der Fall:

Wenn die Generalstaatsanwaltschaft ihre Argumentation auf die o.g. Entscheidung des Bundesverfassungsgerichts stützt und daraus ableiten will, dass die Generalklausel auch für den vorliegenden Fall bestimmt genug sei, wird verkannt, dass die Feststellung des Gerichts - dass nur eine „*Maßnahme mit geringer Eingriffsintensität*“ vorlag und die Generalklausel daher Anwendung findet - gerade darauf fußte, dass die Maßnahme gegenüber den Betroffen aufgrund „*konkreter Tatumstände“* erfolgte. Auskünfte wurden nur von Personen „*gegen die auf Grund dieser Umstände ein zureichender Tatverdacht bestand*“ erfragt. Durch den dort behandelten Datenverarbeitungsschritt war nur ein „*eng begrenzter und präzise beschriebener Personenkreis, der nach dem damaligen Ermittlungsstand durch sein Verhalten den Tatverdacht begründet hatte*“, betroffen (Rn. 29 d. Entscheidung). Diese Voraussetzungen liegen ersichtlich gerade nicht vor, da massenhaft biometrische Templates erstellt werden, gerade ohne das ein Verhalten einen Tatverdacht gegen diese Personen begründet hätte. Zudem stellt das Gericht gerade in dieser Entscheidung klar, dass maßgeblich für die Frage, ob eine hohe Eingriffstiefe vorliegt und welche Anforderungen an eine Ermächtigungsgrundlage zu stellen ist, sich danach richtet, ob die Maßnahme verdachtslos erfolgt und durch eine große Streubreite gekennzeichnet ist, „*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*“ (Rn. 29 d. Entscheidung). Insoweit ist ein Rückgriff auf die Generalklausel der

StPO in dem hier vorliegenden Fall der biometrischen Massendatenerhebung nicht möglich.

Fehl geht auch die Schlussfolgerung der Generalstaatsanwaltschaft, dass aus der Rechtsprechung des Bundesgerichtshofs zum Kunsturhebergesetz die Geringfügigkeit des Eingriffs folgt. Entgegen dem Verständnis der Generalstaatsanwaltschaft ist das Recht am eigenen Bild als Ausprägung des allgemeinen Persönlichkeitsrechts nicht abschließend im Kunsturhebergesetz geregelt. Zunächst regelt das KunstUrhG allein die Verbreitung und das öffentliche zur Schau stellen, § 22 KunstUrhG. Weder über die Erhebung noch über die Zulässigkeit einer biometrische Analyse trifft dieses Gesetz eine Aussage. Das Kunsturhebergesetz regelt schon keine Rechtfertigungsgrundlage für die Verarbeitung von personenbezogenen Daten durch die Polizei. Lichtbilder und biometrische Merkmale sind personenbezogene Daten. Deren Verarbeitung greift in das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Recht auf informationelle Selbstbestimmung ein (s.o.). Das informationelle Selbstbestimmungsrecht ist erst aus einer verfassungsgerichtlichen Rechtsfortbildung anlässlich des Volkszählungsurteil von 1983 – also acht Jahre nach der zitierten Entscheidung des BGH – entstanden (BVerfG, Urteil v. 15.12.1983 – 1 BvR 209/83 u.a.).

Letztlich sei auch auf die Rechtsprechung des OVG Hamburg verwiesen, dass in Bezug auf die speziellen Befugnisnormen des HmbPolDVG zu Bildaufzeichnungen im öffentlichen Raum im Rahmen der Gefahrenabwehr 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: ausdrücklich zu § 8 Abs. 3 S. 1 HmbPolDVG). Vermag also eine Rechtsgrundlage (im präventiven Bereich), die ausdrücklich zur Erhebung von Bild- und Videoaufnahmen durch die Polizei ermächtigt, schon keinen Einsatz von Analysesystemen mit abdecken, muss dies insbesondere für Generalklauseln gelten, die von vorneherein nur zu geringfügigeren Eingriffen herangezogen werden können.

e. § 98c StPO

Entgegen der ursprünglichen Ansicht von Polizei und Staatsanwaltschaft kann auch die anlasslose Auslese und Speicherung von biometrischen Daten tausender Personen durch die Polizei Hamburg zum Zwecke des späteren Abgleichs nicht auf § 98c StPO gestützt 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 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, 1 Ed. 01.01.2018, § 98c Rn. 1).

Darüber hinaus ist die Norm materiell weitgehend und formell vollständig voraussetzungslos (BeckOK StPO/Gerhold, a.a.O § 98c Rn.1). Sie enthält weder eine Konkretisierung des Tatverdachts noch eine Beschränkung auf bestimmte Straftatbestände oder eine Subsidiaritätsklausel (MüKo StPO/Günther, a.a.O, § 98c Rn. 2), weshalb sie ohnehin nur zu geringfügigen Grundrechtseingriffen berechtigt (BeckOK StPO/Gerhold, a.a.O. § 98c Rn. 1).

2. Nutzung des „polizeieigenen“ Materials

Nach Angaben der Polizei handelt es sich bei sämtlichen von GAS verwendeten Video- und Bildsequenzen um solche, die auf Grundlage von § 100 h Abs. 1, Abs. 2 Nr. 1 und Abs. 3 StPO erstellt wurden. Dabei erlaube § 100h StPO nicht nur die Erhebung und Speicherung der personenbezogenen Daten, sondern auch die anschließende Verwendung zur manuellen und technikunterstützten Auswertung (Stellungnahme der Polizei vom 23.07.2018 S. 8), da der hier vorliegende Einsatz von GAS keinen eigenständigen Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstelle.

§ 100h Abs. 1 Nr. 1, Abs. 2 Nr. 1 und Abs. 3 StPO stellt aber keine hinreichende Ermächtigungsgrundlage für die biometrische Analyse und die Erstellung von Templates von allen auf den Bild- und Videoaufnahmen abgebildeten Personen dar. Diese Vorschrift erlaubt nur die Erhebung von Bild- und Videoaufnahmen bezüglicher einer konkreten Zielperson als „Beschuldigter“. Andere Personen dürfen gem. § 100h Abs. 3 StPO nur betroffen sein, wenn dies unvermeidbar ist.

Zwar entspricht die Norm den hohen Bestimmtheitsanforderungen die an einen Grundrechtseingriff durch Bild- bzw. Videoaufzeichnungen zu stellen sind, die weitere -

grundrechtsintensive automatisierte - Verarbeitung von personenbezogenen Daten deckt sie jedoch nicht (mit) ab:

Es erscheint bereits fraglich, ob sämtliche nun verwendeten Bild- und Videoaufnahmen aus Anlass einer Verdachtslage - wie § 100h StPO dies voraussetzt - erstellt wurden. Selbst wenn dies der Fall wäre, kann von der Zulässigkeit der Erhebung und Speicherung von Videos und Bildern über eine mögliche Straftat nicht auch auf eine zulässige Verarbeitung der Bilder durch ein vollkommen neues Auswertungsinstrument mit der bereits dargelegten Eingriffsintensität 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). Die hier vorliegende biometrische Analyse und Erstellung von Gesichtstemplates zum Zweck des späteren Abgleichs ist jedoch nicht mehr von dieser Norm gedeckt. Es handelt sich - entgegen der Ansicht der Polizei Hamburg - bei „Videmo 360“ nicht nur um ein „*bloßes Hilfsmittel für die visuelle Auswertung*“, sondern um einen eigenständigen intensiven Eingriff in das Grundrecht auf informationelle Selbstbestimmung, der in seiner Qualität nicht mit einer Sichtung zu vergleichen ist (vgl. unter I. 1. d)

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 (DSK): Einsatz von Videokameras zur biometrischen Gesichtserkennung birgt erhebliche Risiken 30.03.2017). Eine Beschränkung der DSK auf einzelne Kamerasysteme mit bereits integrierter biometrischen Analyse kann der Entschließung nicht entnommen werden. Insofern markiert der Einsatz der Gesichtserkennung eine neue Qualität der Eingriffsbefugnis, indem sie neue technische Wege bei der Fahndung und Überwachung von Personen über eine Fülle von Bildmaterial ermöglicht, dass weit über die Fähigkeiten einer Auswertung durch das menschliche Auge reicht. Wenn künftig 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 künftig zu einer nie gekannten Kontrollmacht staatlicher Stellen gegenüber den Bürgern.

Selbst wenn man annimmt, dass auf der Grundlage von § 100h StPO die biometrische Gesichtserkennung gedeckt sein könne, um mithilfe von vorhandenen

Videoaufzeichnungen eines Tatorts einen Tathergang zu rekonstruieren und „*Leersequenzen oder anderweitig nicht interessante Sequenzen in einer Videoaufnahme zu überspringen (*so der Vorschlag zu § 100h StPO von Hornung/Schindler ZD 2017 S. 203 (207))*,* betrifft das nicht den hier vorliegenden Einsatz der GAS.

Anders als der Zugriff und die Durchsicht einzelner Videos oder Bilder eines Tatortes handelt es sich hier um ein vollkommen neues Instrument staatlicher Überwachung in einem bisher nicht zulässigen Ausmaß. Die hier vorliegende biometrische Analyse setzt den Grundstein für die Rekonstruktion von Bewegungsprofilen von einzelnen Personen über längere Zeiträume, durch sie können die Beziehungen zu anderen Menschen dokumentiert und rekonstruiert werden. Verhaltensmuster, Teilnahme an Versammlungen, Präferenzen und religiöses/politische Engagement kann über Tage auf großen Teilen des Hamburger Stadtgebiets herausgelesen werden. Dies hat eine vollkommen andere Qualität als die Sichtung und das Vor- und Zurückspulen von einzelnen Tatortvideos durch einen Ermittler der Polizei.

3. Verhältnismäßigkeit

Selbst wenn man, der Rechtsauffassung der Polizei Hamburg folgend, hinreichend bestimmte gesetzliche Eingriffsnormen für die Herstellung von biometrischen Gesichtsprofilen in den genannten Vorschriften sehen möchte, bestünden dennoch aus dem rechtsstaatlichen Grundsatz der Verhältnismäßigkeit erhebliche Zweifel an den durchgeführten Maßnahme zur massenhaften Erhebung, Speicherung und Verarbeitung von biometrischen Profilen tausender unbeteiligter Personen zum Zweck der Verfolgung von Straftaten anlässlich der G20 Ausschreitungen.

Dabei mag dahinstehen, ob die eher geringe Erfolgsquote bei der Ermittlung nach Tätern die Erforderlichkeit der Maßnahme nicht bereits grundsätzlich in Frage stellt (vgl. Drucksache 21/13939, Antwort zu Frage Nr. 10 wonach es „*mit Hilfe der biometrischen Gesichtserkennung durch Recherchen mit der GAS „Videmo 360“ bislang drei Personen namentlich (zu) identifizieren*“ gelang). Immerhin ist zu erwarten, dass die Aufklärungsquote sich bei technischer Weiterentwicklung der Software und erweiterten Speicherkapazitäten durch eine noch intensivere flächendeckende Heranziehung und Auswertung von Bildmaterial verbessern dürfte. Hingegen steht die Verhältnismäßigkeit der umfassenden biometrischen Vermessung von Gesichtern zum Ziel der Strafverfolgung von Delikten (wie z.B. Landfriedensbruch oder Körperverletzungsdelikte) mit den Eingriffen in die informationelle Selbstbestimmung

einer Vielzahl Unbeteiligter erheblich in Frage. Das Anlegen von Datenbank mit Gesichtsmodellen von Bürgerinnen und Bürgern, die in zeitlicher und örtlicher Hinsicht zu den zu verfolgenden Straftaten keinen direkten Zusammenhang mehr aufweisen, stellt einen weit reichenden Eingriff in Grundrechtspositionen tausender unbescholtener Menschen dar, der auch nicht mit dem Ziel einer flächendeckenden und umfassenden Täterermittlung zur Strafverfolgung zu rechtfertigen ist. Die Persönlichkeitsrelevanz der gewonnenen Informationen kann sich noch erhöhen, wenn nicht nur Aufschlüsse unmittelbar über das Bewegungsverhalten, sondern mittelbar auch über sonstiges Verhalten ermöglicht. Die Maßnahme kann sich unter Umständen auch als funktionales Äquivalent eines grundrechtlichen Eingriffs in andere grundrechtliche Freiheiten darstellen, wenn z.B. die Teilnahme an Versammlungen rekonstruiert werden kann (BVerfG, Urteil v. 11.03.2008 – 2 BvR 1345/03 Rn. 87 ff. zur automatisierten Erfassung von Kennzeichen). Dies kann nach Ausführungen des Bundesverfassungsgerichts schon dann der Fall sein, wenn aus der „*Erfassung der Fahrzeuge auf den Zufahrtswegen die Vermutung abgeleitet werden, dass der Fahrer* (…) *eine Versammlung aufsucht*“. Dies muss insbesondere gelten, wenn große Mengen an Bild- und Videomaterial von Privaten mit örtlichem und zeitlichem Bezug zum G20-Rahmen verwertet werden. Es muss darauf geschlossen werden, dass neben gewalttätigen Ausschreitungen auch viele Aufnahmen von friedlichen Versammlungszügen unter diesen Dateien sind.

Das Verfahren der Gesichtserkennung, bei dem biometrische Merkmale der Bevölkerung über einen unbestimmten Zeitraum gespeichert werden, um bei einzelnen Straftätern die Tatbegehung von Delikten wie Landfriedensbruch oder Sachbeschädigung nachzuweisen, käme künftig für alle Formen von in der Öffentlichkeit begangenen Alltagskriminalität in Betracht. Ausdrücklich wird eine Ausweitung des Eingriffsbereichs von der Polizei Hamburg beabsichtigt. Die Folge wäre eine flächendeckende Verknüpfung und Auswertung von Videoaufzeichnungen aus gänzlich unterschiedlichen Quellen in den Händen der Strafverfolgungsbehörden. Eine Strafverfolgung um jeden Preis, die in die Grundrechte einer unbestimmten Vielzahl von Personen eingreift und eine umfassende Kontrolle von Menschen durch Profilbildung ermöglicht, ist jedoch mit Blick auf den Grundsatz der Verhältnismäßigkeit, insbesondere auf Grundlage von unspezifischen strafprozessualen Generalermächtigungen, nicht zulässig. Letztlich ist dabei auf § 48 BDSG zu verweisen, wonach die Verarbeitung besonderer Kategorien personenbezogener Daten nur zulässig ist, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist. Damit reicht somit nicht nur die Einhaltung des datenschutzrechtlichen Erforderlichkeitsgrundsatzes aus, die Verarbeitung muss auch zwingend erforderlich sein (Auerhammer/Greve,

DSGVO/BDSG, 2. Auflage 2018 § 48 Rn. 11). Daher gilt zu klären, ob nicht auch ein weniger eingriffsintensives Verfahren zum Einsatz gebracht werden kann. Weniger invasiv wäre ein Verfahren, das z.B. vermeidet, dass die Templates betroffener Personen gespeichert werden, indem ein Abgleich des Fahndungsbestands direkt anhand der Referenzdatenbank erfolgt. Werden die Gesichter unbeteiligter Personen nur für eine logische Sekunde abgeglichen und für den Nichttrefferfall gelöscht, könnte bereits fraglich sein, ob - nach den Grundsätzen der Rechtsprechung über die Kennzeichenerfassung - dann überhaupt ein Eingriff in das informationelle Selbstbestimmungsrecht vorliegt (vgl. dazu die Ausführung des BVerfG zur Kennzeichenerfassung a.a.O.). Dies wiederum erscheint fraglich, da die auch kurzfristige Erstellung von biometrischen Templates in der Intensität weit über das Speichern von Kfz-Kennzeichen hinausgeht.

Dabei mag hier offen bleiben, ob und inwieweit ein durch den Gesetzgeber geschaffener Regelungsrahmen zum Einsatz biometrischer Massenverfahren überhaupt für bestimmte, klar definierte Anlasstaten mit verfahrensmäßigen Sicherungen von Rechten und Freiheiten Betroffener dem Grundsatz der Verhältnismäßigkeit künftig genügen kann. Vorliegend fehlt es bereits an einer solchen Grundlage, die eine Anordnung der hier durchgeführten Maßnahmen in einem angemessenen Rahmen legitimieren könnte.

III. Verantwortlichkeit der Polizei

Die Polizei Hamburg ist Verantwortliche Stelle. „Verantwortlicher“ im Sinne der Richtlinie (EU) 2016/680 ist die zuständige Behörde, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, Art. 3 Nr. 8 der Richtlinie. Die Anschaffung der GAS „Videmo 360“ erfolgte nach Kenntnisstand des HmbBfDI eigenverantwortlich und nach alleiniger Entscheidung durch die Polizei Hamburg, um zunächst zum Zwecke des Anlegens von umfangreichen Referenzdatenbanken mathematische Modelle von menschlichen Gesichtern zu erstellen. Daran ändert auch die spätere Nutzung von „Videmo 360“ zum Abgleich der zuvor erstellten Templates auf konkreter Anordnung der Staatsanwaltschaft nichts.

Die einzelnen Datenverarbeitungsschritte sind – wie dargelegt – nämlich gesondert nach ihrer Zulässigkeit zu überprüfen. Für die Verantwortlichkeit der Polizei und nicht auch der Staatsanwaltschaft spricht zudem, dass die Justizbehörde erst über den Einsatz der GAS durch die Staatsanwaltschaft am 06. März 2018 informiert worden ist. Ab März begann jedoch erst der Abgleich auf Grund der jeweiligen Genehmigung der

Staatsanwaltschaft. Die biometrische Analyse und die Erstellung der Templates erfolgte jedoch bereits Ende November 2017.

Darüber hinaus erscheint es bereits fraglich, ob es sich bei sämtlichen Video- und Bildaufzeichnungen um strafrechtliche Beweismittel handelt. Sollte dies nicht der Fall sein, handelt es sich ohnehin um eine Datenverarbeitung im Vorfeld von strafrechtlichen Ermittlungen, die die technischen Bedingungen herstellt, die einen späteren Abgleich einzelner, nach Durchsicht des Videomaterials strafrechtlich verdächtiger Personen gegenüber der dann aufgebauten Referenzdatenbank ermöglicht.

IV. Ergebnis

Nach alledem fehlt für die biometrische Verarbeitung von Daten im Rahmen der Erstellung von Gesichtstemplates aller Personen auf dem umfänglichen Bildmaterial, das die Polizei anlässlich der Ermittlungen von G20-Straftaten herangezogen hat, eine tragfähige Rechtsgrundlage.

Die Erstellung von Gesichtstemplates aus einer durch Strafverfolgungs- bzw. Ordnungsbehörden zusammengezogenen Vielzahl von ganz unterschiedlich zustande gekommenen Videosequenzen für eine unbestimmte Zahl von Personen, die durch eigenes Verhalten staatliche Untersuchungen bzw. Ermittlungen weder veranlasst noch zurechenbar verursacht haben, stellt einen schwerwiegenden Eingriff in das informationelle Selbstbestimmungsrecht dar. Dies gilt umso mehr, als diese Personen über die Verarbeitung ihrer persönlichen Daten regelmäßig weder informiert werden noch Auskünfte darüber einholen können. Ohne davon zu erfahren, dass ihre biometrischen Daten von Behörden erstellt und für eine weitere Verarbeitung über einen unbestimmten Zeitraum vorgehalten werden, können diese ihre weitergehenden Datenschutzrechte insbesondere auf Löschung weder gerichtlich noch durch Beschwerde bei unabhängigen Stellen durchsetzen. Insoweit bedarf es für derartige Eingriffe rechtsstaatlicher Vorgaben für eine Erzeugung und Nutzung von Gesichtstemplates, die eine Kontrolle der Einhaltung dieser Vorgaben durch eine unabhängige Stelle als Kompensation für den individuellen Rechtsschutz vorsehen (vgl. BVerfG, Urteil v. 20.04.2016 – 1 BvR 966/09 Rn. 135). Nur so kann sicherstellt werden, dass die Betroffenen, potenziell jede Bürgerin bez. jeder Bürger, sowie die Verantwortlichen den Inhalt und die Grenzen des Eingriffsbereichs der Norm jeweils klar erkennen können (vgl. etwa BVerfG, Urteil v. 12.04.2005 – 2 BvR 581/01 Rn. 49). Dies gilt auch, wenn die Betroffenen - anders als bei der offenen Videoüberwachung - sich einem derartigen Eingriff naturgemäß nicht entziehen können, da über die Verwendung

der Bilder zur biometrischen Analyse zumeist erst im Nachhinein entschieden wird. Die Situation ist hier durchaus ähnlich wie bei einem maschinellen-automatisierten Datenabgleich im Rahmen einer Rasterfahndung nach § 98a StPO. Diesen hat der Gesetzgeber im Hinblick auf Anlass, Betroffene und Verfahren in einer eigenen Bestimmung geregelt. Solange der Gesetzgeber davon absieht, Vorgaben für den Einsatz solcher Technologien zu formulieren, können entsprechende Maßnahmen nicht auf eine unspezifische Auffangkompetenz von Generalklausel gestützt werden und sind zu unterlassen

Damit ist auch der Abgleich von Daten zur Wiedererkennung von einzelnen Gesichtstemplates mit der Referenzdatenbank von massenhaft erzeugten Templates unbeteiligter Personen nicht zulässig. Selbst wenn man annimmt, dass der Einsatz von GAS auf polizeieigenen Video- bzw. Bilddateien durch § 100h StPO (mit) abgedeckt wäre, führte die Zusammenführung mit einer Datenflut von Aufnahmen aus dem Privatbereich im Ergebnis zur Unzulässigkeit der Anwendung von „Videmo 360“. Wie dargelegt, wurde ein Großteil der Bild- und Videosequenzen von Privaten „zur Verfügung gestellt und nicht aufgrund von § 100h StPO erhoben. Hohe Anforderungen wie gerade § 100h StPO sie an staatliche Eingriffe stellt, und verfahrens- und organisatorische Absicherungen, wie § 101 StPO sie im Falle von § 100h festschreibt, liegen gerade nicht vor.

Ohne eine spezielle gesetzliche Regelung ist ein derartiger Eingriff durch Erstellung biometrischer Gesichtstemplates verfassungsrechtlich nicht zulässig. Die verantwortliche Stelle hat die Datenbank daher gem. § 75 BDSG unverzüglich zu löschen.