

Antrag

**der Abgeordneten Anna-Elisabeth von Treuenfels-Frowein, Carl-Edgar Jarchow,
Michael Kruse, Daniel Oetzel, Dr. Kurt Duwe (FDP) und Fraktion**

**Betr.: Der Einsatz biometrischer Gesichtserkennung bei der Strafverfolgung
erfordert eine spezifische Rechtsgrundlage**

Beginnend mit den circa 100 Terabyte Bild- und Videomaterial, die zur Aufarbeitung der G20-Krawalle erhoben wurden, nutzt die Polizei Hamburg eine „Gesichtserkennungssoftware“ namens „Videmo 360“ zur Aufklärung von Straftaten. Diese spezielle Software kann aus Video- und Bildermaterialsätzen Gesichter automatisch lokalisieren und identifizieren und sodann in Form von maschinenlesbaren Modellen abspeichern, um damit unter anderem vollständige Bewegungsprofile erstellen.

Dadurch hat die Polizei Hamburg die Möglichkeit, verschiedene Bildquellen, die zeitlich und örtlich versetzt aufgenommen wurden, miteinander zu verknüpfen und umfangreiche Rückschlüsse auf das gesamte Tatgeschehen zu erhalten, insbesondere an welchen Orten ein Beschuldigter tätig geworden ist und ob beispielsweise die Kleidung gewechselt wurde. Die Software stellt für die Polizei Hamburg dabei nicht nur eine erhebliche Hilfe bei der Strafverfolgung dar, die über eine konventionelle Datenverarbeitung hinausgeht. Des Weiteren erhält die Polizei Hamburg die technische Möglichkeit zur Erstellung vollständiger Bewegungsprofile von Personen im öffentlichen Raum.

Allerdings muss sichergestellt sein, dass der Einsatz der Software und die technischen Potenziale ihrer Algorithmen rechtsstaatlichen Anforderungen genügen, auch damit in strafrechtlichen Verfahren die Ergebnisse der Gesichtserkennungsanalyse auch als Beweismittel angebracht und anerkannt werden können. Schließlich greift die Polizei bei der Erstellung biometrischer Gesichtsabdrücke und erneut bei deren Abgleich in das Grundrecht auf informationelle Selbstbestimmung einer kaum bestimmbar Menge an Adressaten und Betroffenen ein, da die abgespeicherten individuellen Gesichtsmarkere Personen identifizierbar machen, große Mengen an personenbeziehbar Daten erzeugen und der Polizei vielfältige Nutzungsmöglichkeiten eröffnen, die weit über die Nutzung klassischer Lichtbilder oder Videosequenzen hinausgehen.

Die Polizei Hamburg beruft sich bei der Erstellung und dem Abgleich biometrischer Gesichtsabdrücke auf §§ 161, 163 StPO in Verbindung mit § 48 BDSG. Allerdings stellt diese lediglich eine allgemeine Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten dar, die bei strafrechtlichen Ermittlungen aufgrund eines Anfangsverdachts erlangt wurden. Diese Ermächtigung erfasst aber kaum die hohe Eingriffsintensität des automatisierten Abgleichs biometrischer Daten von zu Anfang noch unbekannt Personen.

Aufgrund der hohen Eingriffsintensität in das Grundrecht auf informationelle Selbstbestimmung ist die Schaffung einer spezifischen Rechtsgrundlage erforderlich, um den Einsatz der Software zur Strafverfolgung unter Abwägung der grundrechtlich geschützten Positionen zu ermöglichen. Der Anwendungsbereich ist auf schwerwiegende Straftaten zu beschränken und muss dem Betroffenen die Möglichkeit bieten, zu erfahren, welche biometrischen Daten von ihm erhoben wurden, ob ein Modell von ihm erstellt wurde und wie und unter welchen Voraussetzungen ein Anspruch auf

Löschung der Daten besteht. Die gesetzlich definierten Tatbestandsmerkmale der Rechtsgrundlage müssen dabei den Maßstäben genügen, die das OVG Hamburg in seiner Entscheidung zu den „Gefahrengebieten“ (Urteil vom 13.05.2015, Az. 4 Bf. 226/12) definiert hat. Dasselbe muss für die vom BVerfG im „BKA-Urteil“ (BVerfG, Urteil des Ersten Senats vom 20. April 2016, 1 BvR 966/09, Rn. 1-29) definierten Bestimmtheitsanforderungen gelten.

Die Bürgerschaft möge beschließen:

Der Senat wird ersucht,

1. sich im Rahmen einer Bundesratsinitiative für die Schaffung einer spezifischen Rechtsgrundlage in der Strafprozessordnung (StPO) zur Nutzung von Gesichtsanalysesoftware durch die Strafverfolgungsbehörden einzusetzen, welche unter Beachtung der Sicherheitsinteressen und der Grundrechte der Betroffenen den automatisierten Abgleich biometrischer Daten legitimiert.
2. der Bürgerschaft bis zum 30.09.2019 zu berichten.