

STRAFRECHT

Verwendung von Gesichtserkennungssoftware als Beweismittel im Strafverfahren

von RAin Diana Nadeborn, FAin für Strafrecht, Berlin, IT-Strafrecht Blog:
www.iww.de/s2188

| Computer kann man nicht nur nutzen, um Straftaten zu begehen, sondern auch, um solche zu verfolgen. Software zur Auswertung riesiger Mengen von Bildern und Videos, für die Polizeibeamte Jahre brauchen würden, steht zur Verfügung. Allein, es fehlt an der gesetzlichen Grundlage. Die Polizei in Hamburg preschte vor und setzt seit 2018 eine Gesichtserkennungssoftware ein, bevor der Gesetzgeber ein spezielles Gesetz dafür geschaffen hat. Was die Software kann und was gegen ihren Einsatz spricht, wird im Folgenden diskutiert. |

Täteridentifizierung mittels Software

Zur Aufklärung von Straftaten während des G20-Gipfels in Hamburg am 7.7.17 und 8.7.17, bei dem die rund 31.000 eingesetzten Polizisten Ausschreitungen nicht verhinderten, wurde in Hamburg die Sonderkommission „Schwarzer Block“ ins Leben gerufen. Sie führte Anfang 2019 mehr als 3.500 Ermittlungsverfahren, unter anderem wegen Landfriedensbruch, Körperverletzung und Sachbeschädigung (www.iww.de/s2933). Mit der Gesichtserkennungssoftware „Videmo 360“ wollte die Polizei ganz neue Wege beschreiten. Sie wollte neben eigenem Material insbesondere Videos von acht S-Bahnhöfen auswerten lassen, indem zunächst – im Vorfeld strafrechtlicher Ermittlungen – individuelle Gesichts-IDs (Templates) erstellt wurden. Im Anschluss daran gleicht die Polizei bis heute Gesichts-IDs mit den Bildern einzelner Tatverdächtiger ab, die im Rahmen von erkennungsdienstlichen Maßnahmen während des G20-Gipfels erhoben wurden.

Anders als bei dem Bildabgleich in Echtzeit, welcher im Testbetrieb am Bahnhof Berlin-Südkreuz erfolgte, baute die Hamburgische Polizei mit der Gesichtserkennungssoftware dauerhaft eine Datenbank mit betroffenen Personen auf, gegen die zunächst kein Tatverdacht besteht. Damit führte in Hamburg allein die Benutzung bestimmter S-Bahnen und die Teilnahme an Demonstrationen zur Erfassung des Gesichtsprofils, welches dann analysiert und für die Strafverfolgung bereitgehalten wird. Die Sonderkommission will auf diese Weise

- das Verhalten eines Beschuldigten in der Vor- und Nachtatphase ermitteln,
- dem Beschuldigten noch weitere bis dato unbekannte Straftaten zuordnen,
- bekannte Taten aus anderen Blickwinkeln feststellen,
- ggf. entlastende Informationen bezüglich eines Beschuldigten gewinnen,
- unbekannte Tatverdächtige identifizieren (www.iww.de/s2934).

Die mittels Software abgeglichenen Bilder werden zudem für Fahndungsausschreibungen verwendet und zur Begründung von Anträgen auf Strafverfolgungsmaßnahmen wie Durchsuchungen oder Haftbefehle verwendet.

Ein Fall von Vorratsdatenspeicherung

Der Hamburgische Datenschutzbeauftragte Caspar ordnete jedoch im Dezember 2018 die Löschung der biometrischen Datenbank zum Gesichtsabgleich an. Die Begründung entspricht den wesentlichen Kritikpunkten an der Vorratsdatenspeicherung (Speicherung von Verkehrsdaten durch die Telekommunikationsdienstleister zur späteren Erhebung durch die Strafverfolgungsbehörden), denn auch hier sollen Daten tausender unbeteiligter Personen zunächst auf Vorrat zum Zwecke der späteren Verwendung im Strafverfahren erfasst werden:

- Die Datenerfassung erfolgt unterschieds- und anlasslos.
- Sie betrifft massenhaft Personen, die nicht tatverdächtig sind.
- Die Datenerhebung geschieht ohne Kenntnis der Betroffenen.
- Sie ermöglicht den Strafverfolgungsbehörden die Erstellung von Persönlichkeitsprofilen (www.iww.de/s2934).

Umstritten ist, ob die Hamburgische Polizei für die Verarbeitung polizeifremder Daten mit einer biometrischen Datenbank, die einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt, eine Rechtsgrundlage hat. Nach Auslegung der geltenden Eingriffsbefugnisse spricht Folgendes dagegen:

- Erkennungsdienstliche Maßnahmen gemäß § 81b StPO dürfen sich nur gegen einen Beschuldigten richten.
- Auf die Ermittlungsgeneralklausel gemäß §§ 161, 163 StPO dürfen nur Maßnahmen mit geringem Grundrechtseingriff gestützt werden.
- Der maschinelle Abgleich mit vorhandenen Daten gemäß § 98c StPO setzt eine rechtmäßige Erhebung und Speicherung personenbezogener Daten voraus.
- Die Datenverarbeitung für Zwecke des Strafverfahrens gemäß § 483 StPO setzt einen Anfangsverdacht in einem konkreten Strafverfahren voraus.
- Für die Datenverarbeitung für Zwecke künftiger Strafverfahren gemäß § 484 StPO dürfen nur Daten verwendet werden, die bereits Gegenstand eines gegen einen Beschuldigten geführten Strafverfahrens waren.

Nach Auffassung des Datenschutzbeauftragten müsste eine (zu schaffende) Rechtsgrundlage zudem einen Richtervorbehalt und die Kontrolle der Datenbank durch unabhängige Stellen enthalten.

Der Senat für Inneres und Sport ist die Aufsichtsbehörde der Polizei Hamburg und Adressatin der Löschanordnung des Datenschutzbeauftragten. Der Senat hat gegen die Löschanordnung Klage beim VG Hamburg (17 K 203/19) erhoben. Die mündliche Verhandlung wird voraussichtlich Ende Oktober 2019 stattfinden. Bis zu einer gerichtlichen Entscheidung darf die Hamburgische Polizei die Software weiter in Ermittlungsverfahren einsetzen. Eine geplante Nutzung der biometrischen Datenbank durch das Landeskriminalamt Hamburg zur Aufarbeitung von Großereignissen ist derzeit ausgesetzt. Letztlich muss der Gesetzgeber und damit der Wähler entscheiden, ob für eine effektivere Strafverfolgung Datenbanken aufgebaut werden sollen, um den Preis, dass z.B. Demonstrationsteilnehmer die Erstellung biometrischer Profile befürchten müssen und dann womöglich lieber gleich auf die auf die Kundgebung verzichten.