DeutscherAnwaltVerein

Stellungnahme

des Deutschen Anwaltvereins durch den Ausschuss Gefahrenabwehrrecht

zur sog. intelligenten Videoüberwachung

Stellungnahme Nr.: 47/2017 Berlin, im August 2017

Mitglieder des Ausschusses

- Rechtsanwältin Dr. Heide Sandkuhl, Potsdam (Vorsitzende)
- Rechtsanwalt Wilhelm Achelpöhler, Münster (Berichterstatter)
- Rechtsanwältin Dr. Annika Dießner, Berlin
- Rechtsanwalt Dr. Nikolas Gazeas, LL.M., Köln
- Rechtsanwalt Prof. Dr. Björn Gercke, Köln
- Rechtsanwalt Dr. Stefan König, Berlin
- Rechtsanwältin Dr. Regina Michalke, Frankfurt / Main
- Rechtsanwältin Kerstin Oetjen, Freiburg
- Rechtsanwältin Lea Voigt, Bremen (Berichterstatterin)

Zuständig in der DAV-Geschäftsführung

- Rechtsanwalt Max Gröning

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Verteiler

Deutschland

Bundesministerium des Innern
Bundesministerium der Justiz und für Verbraucherschutz

Deutscher Bundestag – Ausschuss für Recht und Verbraucherschutz
Deutscher Bundestag – Innenausschuss

Arbeitsgruppen Inneres der im Deutschen Bundestag vertretenen Parteien
Arbeitsgruppen Recht der im Deutschen Bundestag vertretenen Parteien

Justizministerien und -senatsverwaltungen der Länder
Landesministerien und Senatsverwaltungen des Innern
Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Landesdatenschutzbeauftragte
Innenausschüsse der Landtage
Rechtsausschüsse der Landtage

Europäische Kommission – Vertretung in Deutschland
Bundesrechtsanwaltskammer
Deutscher Richterbund
Bundesverband der Freien Berufe
Gewerkschaft der Polizei (Bundesvorstand)
Deutsche Polizeigewerkschaft im DBB
Verd.di, Recht und Politik
stiftung neue verantwortung e.V.
Deutsches Institut für Menschenrechte
Gesellschaft für Freiheitsrechte

Vorstand und Landesverbände des DAV
Vorsitzende der Gesetzgebungs- und Geschäftsführenden Ausschüsse des DAV
Vorsitzende des FORUM Junge Anwaltschaft des DAV

Presse

Redaktion der Frankfurter Allgemeinen Zeitung
Redaktion der Süddeutschen Zeitung
Redaktion der Berliner Zeitung
Redaktion des Juris Newsletter
JurPC

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit derzeit rund 65.000 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

Anlass für diese Stellungnahme ist der aktuell unter der Schirmherrschaft von Bundespolizei, Bundesinnenministerium und Bundeskriminalamt laufende Probebetrieb eines Systems zur Erkennung von Gesichtern und bestimmten Verhaltensmustern am Berliner Bahnhof Südkreuz. Es wird zunächst auf die aktuelle Rechtslage und die Wirksamkeit herkömmlicher Videoüberwachung eingegangen (1.) und sodann ausgeführt, welche rechtlichen und tatsächlichen Probleme mit der sog. intelligenten Videoüberwachung verbunden sind (2.). Schließlich werden Empfehlungen ausgesprochen (3.).

1.
Der Einsatz von Videoüberwachung ist nach heutiger Rechtslage grundsätzlich für Zwecke der Gefahrenabwehr und zur Strafverfolgungsvorsorge, also der Sammlung von Beweismaterial für spätere Strafverfahren, zulässig. Für Videoüberwachung zum Zwecke der Gefahrenabwehr in Bahnanlagen wie dem Südkreuz besteht die ausschließliche Gesetzgebungskompetenz des Bundes nach Art. 73 Nr. 6a GG (BVerfG, Beschluss vom 28. Januar 1998 – 2 BvF 3/92 –, BVerfGE 97, 198-228, Rn. 99). Geht es um Videoüberwachung zur Strafverfolgungsvorsorge, besteht die Gesetzgebungskompetenz des Bundes im Rahmen der sog. konkurrierenden Gesetzgebung aus Art. 74 Abs. 1 Nr. 1 GG (BVerfG, Urteil vom 27. Juli 2005 – 1 BvR 668/04 –, Rn. 101, juris).

Die Eignung von Videoüberwachung zur Gefahrenabwehr wird zum einen damit begründet, dass allein der Umstand der Videoüberwachung mögliche Täter abschrecke und so Gefahren vorbeuge und zum anderen damit, dass durch die Videoüberwachung ein schnelleres Einschreiten der Polizei möglich sei. Dies ist von je her in der kriminologischen und kriminalpolitischen Diskussion umstritten. Die zur Kriminalprävention vorliegenden Studien

> *„zeigen entweder keine, nur bedingte, d.h. ausschließlich auf Eigentumsdelikte bezogene oder kaum Wirkung von Videoüberwachung. Einige Studien belegten, dass Kriminalität nur verdrängt wurde, andere konnten auch in Nachbarschaftsgebieten ein Kriminalitätsrückgang verzeichnen, wiederum andere fanden beides oder zeigten überhaupt kein signifikante Veränderungen. Am ehesten tritt der Erfolg der Kriminalitätsreduktion bei Eigentumsdelikten und dort auf Parkplätzen ein und vor allem dann, wenn die Videoüberwachung mit verbesserter Beleuchtung verbunden wird. Allerdings sind weniger die technischen Veränderungen (Überwachung und bessere Beleuchtung) für diesen Erfolg ursächlich als vielmehr die Tatsache, dass die Einführung dieser Maßnahmen deutlich macht, dass man sich um dieses Viertel, diesen Stadtteil oder diese Gegend kümmert“*,

so Prof. Dr. Thomas Feltes/Dr. Andreas Ruch, Lehrstuhl für Kriminologie, Kriminalpolitik und Polizeiwissenschaft, Ruhr-Universität Bochum, Stellungnahme zur öffentlichen Anhörung am 06.03.2017 im Innenausschuss des Deutschen Bundestages zum „Videoüberwachungsverbesserungsgesetz“ mit zahlreichen weiteren Nachweisen zu verschiedenen Studien.

Soweit die Videoüberwachung neben den zweifelhaften Abschreckungseffekten ein schnelleres Einschreiten der Polizei ermöglichen soll, setzt dies jedenfalls einen erheblichen personellen Aufwand voraus. Die Videoaufnahmen müssten von sachkundigem Personal laufend ausgewertet werden, um rechtzeitig die erforderlichen Maßnahmen zu treffen, um die Begehung einer Straftat zu verhindern. Diese Personalintensität wirkt sich bisher faktisch begrenzend auf den Einsatz der Videoüberwachung aus, denn es ist stets abzuwägen, ob mit anderen polizeilichen Maßnahmen, z.B. einer größeren Präsenz von Polizeibeamten vor Ort, effektiver die Begehung von Straftaten verhindert werden kann.

2.
Bei der sog. intelligenten Videoüberwachung soll mithilfe entsprechender Software eine vollautomatische Erkennung von Gesichtern, Gegenständen und Verhaltensmustern ermöglicht werden. Hiermit soll das Problem, dass die herkömmliche Videoüberwachung aufgrund des damit verbundenen erheblichen und kaum zu

leistenden Personalaufwandes tatsächlichen Beschränkungen unterliegt, überwunden werden. Ob der Stand der Technik es bereits zulässt, aus Videoüberwachungsaufnahmen die erforderlichen biometrischen Daten zuverlässig zu extrahieren, ist zweifelhaft und wird daher getestet. Unabhängig von dem Ergebnis dieses Tests darf aber unterstellt werden, dass die Schaffung der technischen Voraussetzungen nur eine Frage der Zeit ist. Ebenso zeigt das Pilotprojekt, dass bei Bundesregierung und Polizeibehörden ein starkes Interesse an der sog. intelligenten Videoüberwachung besteht. Im Fokus dieses Interesses steht die Frage der generellen Machbarkeit. Darüber, wozu die Technik eingesetzt werden soll und welche Auswirkungen ihr Einsatz auf die Grundrechte der Bürger haben könnte, ist indes wenig zu hören.

Die automatisierte Auswertung von Bilddaten stellt gegenüber deren Erhebung einen zusätzlichen und ganz erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen dar. Es findet eine fortlaufende Erhebung und Verarbeitung personenbezogener Daten statt. Jedermann, der sich in einem überwachten Bereich bewegt, muss damit rechnen, dass genau registriert wird, von wo nach wo er geht. Damit werden Bewegungsprofile erstellt, deren Informationswert weit über die bloße Videoaufzeichnung hinausgeht. Je nachdem, wie die Datenerfassung und -auswertung ausgestaltet ist, sind viele Weiterungen denkbar: Der Abgleich mit biometrischen Daten der Meldeämter zur Identifizierung; die Feststellung und Identifizierung von Begleitpersonen; die Verknüpfung mit Informationen aus anderen Überwachungsanlagen zur Erstellung ortsübergreifender Bewegungsprofile (etwa Überwachung einer Reise von Hamburg nach München); die Verknüpfung mit Daten aus Polizeidatenbanken etwa in Bezug auf frühere Ermittlungsverfahren; der Abgleich mit Daten aus dem Internet und den sozialen Netzwerken; ein Suchlauf in Hinblick auf bestimmte Personen (Fahndung) in dem Datenbestand einer oder mehrerer Videoüberwachungsanlagen etc.

Diese kursorische Aufzählung zeigt, dass insbesondere die Möglichkeit, die im öffentlichen Raum videografierten Personen automatisch anhand ihrer Biometrie zu identifizieren, erhebliche Grundrechtsrelevanz hat, weil für die Bürgerinnen und Bürger das Risiko besteht, sich nicht mehr anonym in der Öffentlichkeit bewegen zu können. Zusätzlich bereitet die Identifizierung den Weg zu vielfältigen weiteren Datenbeständen.

Im Falle einer Verknüpfung dieser Daten könnten mit überschaubarem Aufwand Bewegungs- und Persönlichkeitsbilder von Personen erstellt werden, die von einer Kamera an einem bestimmten Ort oder etwa mit einer bestimmten Person detektiert wurden. Derartige Datenverarbeitung ist – wenn die Technik so weit ist – sowohl live als auch für auf Vorrat gespeicherte Daten denkbar. Je nach Vorratshaltung könnte auch festgestellt werden, wo und mit wem sich eine Person in der Vergangenheit aufgehalten bzw. bewegt hat. Diese Szenarien machen nicht nur deutlich, dass es sich bei der automatisierten Verarbeitung von Videoaufnahmen um einen eigenen Grundrechtseingriff handelt, der viele weitere nach sich ziehen kann und für den eine eigene Rechtsgrundlage erforderlich ist (so auch der Wissenschaftliche Dienst des Bundestages, http://www.bundestag.de/blob/439670/e2efe42f49749393cc701c7c4f9af7d8/wd-3-202-16-data.pdf). Es wird vor allem klar, dass es einer Grundsatzdebatte über die rechtsstaatlichen Risiken einer „intelligenten“ Videoüberwachung bedarf. Die primäre Orientierung daran, was technisch machbar ist, wird diesen Risiken nicht ansatzweise gerecht und würde jedenfalls mittel- bis langfristig dazu führen, dass mit den technischen Hürden auch alle grundrechtsschützenden Limitierungen entfallen.

Neben der beschriebenen Problematik der automatischen Gesichtserkennung stellen sich bei der Entwicklung von Algorithmen, die auf abweichendes und kriminelles Verhalten schließen sollen, weitere, nicht weniger gewichtige Fragen. Untersuchungen der Personen, die Videoüberwachungsanlagen beaufsichtigen, lassen erkennen, dass diese Personen oftmals Immigranten, junge Frauen oder Nichtsesshafte ins Visier nehmen. Einzelne gesellschaftliche Gruppen werden aufgrund sozialer oder kultureller Vorurteile überwacht, als gefährlich klassifiziert („Nafris“) und Objekt staatlicher Maßnahmen. Eine solche Form sozialen Sortierens kann durch die Automatisierung der Videoüberwachung verstärkt werden. Die Situationseinschätzung ist nicht mehr Sache der konkret die Situation beobachtenden Personen, sondern das Ergebnis eines automatisierten Abgleichs zwischen den Merkmalsprofilen der beobachteten Person und den in das System eingegebenen Regeln. „Vorurteile“, „Vorannahmen“ oder „subjektive Bewertungen“ könnten so anonymisiert und automatisiert werden (vgl. Dragon u. a., Forschungsinitiative Sicherheit der Universität Hannover, Intelligente Videoüberwachung, S. 37). Ist etwa künftig an einem Ort, der als Schwerpunkt von

Drogenkriminalität ausgemacht ist, die Hautfarbe einer beobachteten Person ein Gesichtspunkt, aus dem ein Algorithmus die „Gefährlichkeit“ einer Person herleitet?

Auch die Eignung einer automatisierten Auswertung zur Abwehr terroristischer Anschläge ist zweifelhaft. Für die Annahme, dass sich Terroristen in einer bestimmten Art und Weise verhalten, so dass in Zukunft ein Anschlag Minuten vorher aus Mimik oder ungewöhnlichen Laufwegen von Bombenlegern abgelesen werden kann, gibt es keinen Anhaltspunkt (vgl. Benjamin J. Kees, Algorithmisches Panopticon. Identifikation gesellschaftlicher Probleme automatisierter Videoüberwachung, Münster 2015). Die Absichten von Menschen lassen sich nicht notwendigerweise an ihren Gesten, Mimik oder ihren Handlungen ablesen.

3.
Bevor in eine Debatte über die Ausgestaltung einer Rechtsgrundlage für den Einsatz von Videosystemen mit algorithmischer Mustererkennung eingetreten wird, bedarf es einer umfassenden Aufklärung über das, was die einzusetzenden Videosysteme technisch zu leisten imstande sind, über deren Fehleranfälligkeit, die vorgesehenen Einsatzmöglichkeiten, über den Umfang und Zweck der Datenverarbeitung, deren räumliche und zeitliche Begrenzung sowie über technisch-organisatorische Maßnahmen, die einen Missbrauch der Datenverarbeitung wirksam unterbinden. Soll zum Beispiel (tatsächlich) daran „gearbeitet“ werden, aus 12 Meter Entfernung mittels Videotechnik einen virtuellen Fingerabdruck sowie ein IRIS-Muster zu generieren, müssen die damit verbundenen Gefahren (= Gesicht als Personalausweis) offen gelegt werden. Dazu gehören zum einen die Darlegung der verwendeten Technik sowie die mit deren Einsatz verbundenen Fehlerquellen.

Längst nicht alle technisch möglichen Anwendungsszenarien einer intelligenten Videoüberwachung wären auch verfassungsrechtlich tragfähig. Bereits die massenhafte und anlasslose Überprüfung von Kraftfahrzeugkennzeichen zwecks Abgleich mit einem gesetzlich nicht näher definierten Fahndungsbestand stellt nach der Rechtsprechung des Bundesverfassungsgerichts einen unverhältnismäßigen Eingriff in das Recht auf informationelle Selbstbestimmung dar (BVerfG, Urteil des Ersten Senats vom 11. März 2008 - 1 BvR 2074/05 - Rn. 172 ff.). Für eine Videoüberwachung mit

Gesichtserkennung müssen jedoch noch deutlich strengere Maßstäbe gelten, als für eine automatisierte Kennzeichenerfassung.

Es kann nicht angehen, dass unter Ausnutzung von nicht durchschaubarer Technik mit Bürgern beliebig experimentiert wird (zur fehlendenden Transparenz im Hinblick auf die vollständige Funktion der Transponder, die die Versuchspersonen beim Pilotversuch Südkreuz mit sich tragen: https://digitalcourage.de/blog/2017/gesichtserkennung-am-suedkreuz-bundespolizei-hat-falsch-informiert-wir-fordern-abbruch-des). Zum anderen verbietet sich aber auch von Verfassungswegen, ohne eine breite Diskussion in der Gesellschaft, derartige gravierende Neubewertungen im Hinblick auf von den Bürgern abzuverlangende grundrechtsrelevante Einschränkungen des Persönlichkeitsrechts vorzunehmen. Das Fundament der freiheitlich demokratischen Gesellschaft gerät ins Wanken, wenn sich die Menschen in der Öffentlichkeit nicht mehr frei bewegen können und Gefahr laufen, dass massenhaft über sie biometrische Daten gespeichert und vorgehalten werden. Bevor sich eine freiheitlich demokratische Gesellschaft hierauf einlässt, muss sie wissen, was tatsächlich und technisch auf sie zukommt. Dies aber ist gegenwärtig unklar.