GERRIT HORNUNG / STEPHAN SCHINDLER

Das biometrische Auge der Polizei

Rechtsfragen des Einsatzes von Videoüberwachung mit biometrischer Gesichtserkennung

Intelligente Videoüberwachung
Biometrische Videoauswertung
Biometrische Personensuche
Computergestützte Bildsuche
Verfassungsrechtliche Anforderungen

■ In der Politik wird als Reaktion auf Kriminalität und Terrorismus der Ausbau der Videoüberwachung diskutiert. Der Einsatz von Videoüberwachung wirft zahlreiche Rechtsfragen auf und ist auch jenseits der juristischen Diskussion umstritten. Grundsätzlich können Bildaufnahmen die Polizei bei der Verhinderung und Aufklärung von Straftaten unterstützen. Die „händische" Auswertung der Aufnahmen kann sich allerdings als sehr zeit- und ressourcenintensiv erweisen. Zur Unterstützung der Polizei wird daher verstärkt an computergestützten Verfahren zur Auswertung von Lichtbild- und Videoaufnahmen geforscht. Dies betrifft insbesondere die biometrische Gesichtserkennung. Der vorliegende Beitrag betrachtet anhand dreier exemplarischer Szenarien einige der verfassungsrechtlichen und einfachgesetzlichen Fragestellungen, die mit dieser technischen Weiterentwicklung einhergehen.

■ In politics, the expansion of video surveillance is discussed as a reaction to criminality and terrorism. The use of video surveillance raises multiple legal questions and is also controversial beyond legal discussions. Generally, images can support the police in preventing and solving of crimes. The "manual" analysis of the images can, however, be very time and resource consuming. Thus, to support the police, computer assisted procedures to analyze photos and videos are being researched. In particular, this relates to biometric facial recognition. Using three scenarios as examples, the article at hand will discuss some of the constitutional law and sub-constitutional law issues which are associated with these technical advances.

Lesedauer: 21 Minuten

I. Videoüberwachung: Weit verbreitet und umstritten

1. Aktuelle Gesetzesinitiativen

Mit Blick auf die Anschläge in Ansbach, Würzburg und München hat das *Bundesministerium des Inneren (BMI)* am 11.8.2016 ein Maßnahmenpaket zur Erhöhung der Sicherheit in Deutschland vorgestellt. Demnach bedingt eine „effektive und effiziente Aufgabenwahrnehmung" der Sicherheitsbehörden eine „zeitgemäße Technik", was u.a. die Sicherung öffentlich zugänglicher Räume durch Videoüberwachung sowie den Einsatz „intelligenter Videotechnik"[1] einschließlich der Nutzung biometrischer Gesichtserkennung umfasst.[2] Anfang des Jahres 2017 wurden zwei Gesetzesentwürfe eingebracht, die eine stärkere Berücksichtigung von Sicherheitsbelangen bei der Videoüberwachung öffentlich zugänglicher Räume[3] und den Einsatz körpernah getragener Bild- und Tonaufzeichnungsgeräte (sog. Body Cams) bei der *Bundespolizei*[4] vorsehen. Überdies ist nach Auskunft der *Bundesregierung* ein Pilotprojekt zur Erprobung des Nutzens „intelligenter Videoüberwachung" auf einem „Pilotbahnhof" der *Deutschen Bahn AG* geplant.[5]

2. Einsatz, Ziele und Nutzen von Videoüberwachung

Dieser durch die Politik forcierte Einsatz von Videoüberwachung ist keine neue Erscheinung und lässt sich in Deutschland bis in die 1950er-Jahre zurückverfolgen. Nachdem Videoüberwachung zunächst zur Verkehrsüberwachung eingesetzt wurde, dehnte sich ihr Anwendungsbereich auf die Überwachung von Versammlungen, die Observation verdächtiger Personen sowie die Beobachtung öffentlicher Straßen und Plätze aus.[6] Inzwischen ist Videoüberwachung weit verbreitet und findet sich in den Innenstädten, im öffentlichen Personennahverkehr sowie in Kaufhäusern, Banken oder Supermärkten. Schätzungen gehen von mehreren hunderttausend Überwachungskameras in Deutschland aus.[7]

Videoüberwachung wird sowohl von staatlichen als auch privaten Stellen eingesetzt und dient im Wesentlichen drei Zielen: der Verhinderung und Aufklärung von Straftaten sowie der Stärkung des Sicherheitsgefühls.[8] Zwar können Kameras für sich gesehen keine Straftaten verhindern. Jedoch soll ihre Präsenz potenzielle Straftäter abschrecken. Überdies können Videoaufzeichnungen i.R.d. Strafverfolgung zur Gewinnung von Ermittlungsansätzen, zur Identifizierung von Straftätern sowie als Beweismittel vor Gericht herangezogen werden. Diese Zielsetzungen kommen auch in den aktuellen Gesetzesvorhaben zum Ausdruck.[9]

1 Dies meint regelmäßig die Verwendung fortgeschrittener Verfahren der computergestützten Videoanalyse, z.B. Gesichtserkennung oder Objekt- und Verhaltenserkennung.
2 Meldung des *BMI* v. 11.8.2016 und dazugehöriges Handout, abrufbar unter: https://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2016/08/pressekonferenz-zu-massnahmen-zur-erhoehung-der-sicherheit-in-deutschland.html.
3 Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes – Erhöhung der Sicherheit in öffentlich zugänglichen großflächigen Anlagen und im öffentlichen Personenverkehr durch optisch-elektronische Einrichtungen (Videoüberwachungsverbesserungsgesetz), BT-Drs. 18/10941; die Änderung betrifft § 6b BDSG.
4 Entwurf eines Gesetzes zur Verbesserung der Fahndung bei besonderen Gefahrenlagen und zum Schutz von Beamtinnen und Beamten der Bundespolizei durch den Einsatz von mobiler Videotechnik, BT-Drs. 18/10939; dies betrifft die Einführung von §§ 27a bis 27c BPolG.
5 BT-Drs. 18/10137, S. 5.
6 *Kammerer*, Krim. Journal 2008, 257, 258 ff.
7 *Scholz,* in: Simitis, BDSG, 8. Aufl. 2014, § 6b Rdnr. 7 ff.
8 *Scholz* (o. Fußn. 7), Rdnr. 10; zur praktischen Umsetzung und insb. auch zum Abschreckungseffekt *Hornung/Desoi,* K&R 2011, 153, 153.
9 BT-Drs. 18/10941, S. 1; BT-Drs. 18/10939, S. 1.

Allerdings ist eine dahingehende Wirksamkeit der Videoüberwachung umstritten.[10] Teilweise wird Videoüberwachung schlicht als ein Instrument zur „Inszenierung von Sicherheit" angesehen.[11] Die *Bundesregierung* hat jedenfalls erklärt, dass die bisher verhinderten Anschläge des „islamistisch-terroristischen Spektrums ... nicht maßgeblich aufgrund von Videoüberwachungssystemen vereitelt worden" sind.[12] Das bedeutet aber nicht, dass Videoüberwachung grundsätzlich nutzlos ist. Nachweisbar konnten Videoaufnahmen zur Aufklärung terroristischer Anschläge beitragen.[13] Dies gilt auch für zahlreiche Fälle „normaler" Kriminalität. Die *Bundesregierung* hat dementsprechend im Jahr 2013 erklärt, „dass ein angemessener und zielgerichteter Einsatz von Videotechnik in Kombination mit anderen begleitenden Maßnahmen dazu beitragen kann, der staatlichen Verpflichtung zur Vermeidung und Verfolgung von Straftaten im konkreten Einzelfall nachzukommen."[14] Die eingebrachten Gesetzesentwürfe bestätigen, dass sich diese befürwortende Haltung nicht geändert hat.

II. Videoüberwachung und biometrische Gesichtserkennung

1. Herkömmliche Videoüberwachung

Herkömmliche Videoüberwachung wird entweder im sog. Kamera-Monitor-Verfahren oder (zusätzlich) mit Aufzeichnung der Bildaufnahmen betrieben. Dabei sind – je nach Ausgestaltung und Einsatzzweck – sowohl Nah- als auch Übersichtsaufnahmen möglich.[15] Die Auswertung der Aufnahmen obliegt aber in jedem Fall einem Menschen. Sollen große Mengen an Videodaten unter Zeitdruck gesichtet und interpretiert werden, kann dies einen großen personellen und zeitlichen Aufwand erfordern. Überdies ist die menschliche Aufmerksamkeit begrenzt. Konzentrationsmängel, Müdigkeit und Langeweile können dazu führen, dass relevante Ereignisse oder Personen übersehen werden („Monitorblindheit"[16]), was eine effektive Auswertung der Aufnahmen beeinträchtigen kann.[17]

2. Technische Weiterentwicklung

Nicht zuletzt zur Lösung dieser Probleme wird die Weiterentwicklung der Videotechnik vorangetrieben. Geforscht wird dementsprechend verstärkt an computergestützten Verfahren zur Gesichts-, Verhaltens- und Objekterkennung sowie an Möglichkeiten der Vernetzung moderner Videoüberwachungsanlagen. Diese Entwicklung findet unter Schlagworten wie „Intelligente Videoüberwachung" oder „Smart-CCTV" statt und hat das Ziel, den Menschen bei der Interpretation und Auswertung der Videoaufnahmen zu unterstützen.[18]

Einen hohen Stellenwert nimmt dabei die biometrische Gesichtserkennung[19] ein. In technischer Hinsicht basiert die biometrische Gesichtserkennung im Wesentlichen auf dem computergestützten Abgleich der Bildaufnahmen menschlicher Gesichter. Dementsprechend müssen diese zunächst in den Bild- bzw. Videoaufnahmen aufgefunden werden. Im Anschluss daran werden aus den aufgefundenen Gesichtsaufnahmen die für die Erkennung benötigten Merkmale[20] extrahiert und mit entsprechenden, vorab hinterlegten Referenzdaten[21] auf Übereinstimmung hin abgeglichen. Ein Vergleichswert (Score) zeigt das Maß an Übereinstimmung an.[22] Zur Verbesserung der Erkennungsleistung können vorab Verfahren zur Bildverbesserung durchgeführt werden.

3. Anwendungsmöglichkeiten der Gesichtserkennung

Biometrische Gesichtserkennung eignet sich für unterschiedliche Anwendungen. Dies betrifft zuvorderst Einlass- und Zugangskontrollen zu Gebäuden, Räumen, Sicherheitsbereichen oder Computern, wobei das Gesicht die Funktion eines Schlüssels oder Passworts übernimmt.[23] Vorliegend interessiert aber vor allem die polizeiliche Verwendung biometrischer Gesichtserkennung i.V.m. Videoüberwachung zur Ermittlung von Straftätern. Dazu sollen drei exemplarisch ausgewählte Szenarien betrachtet werden: Wurde eine Straftat auf Video aufgezeichnet, kann Gesichtserkennung die Polizei bei der Sichtung der Aufzeichnungen unterstützen (III.2.b). Ein Abgleich mit Datenbanken erkennungsdienstlich behandelter Personen kann bei der Identifizierung des Täters helfen.[24] Wird dieser schließlich zur Fahndung ausgeschrieben, können Videoüberwachung und Gesichtserkennung dazu beitragen, ihn ausfindig zu machen. Allen drei Szenarien ist gemein, dass am Ende immer ein Mensch über die Folgen einer Erkennung entscheidet.

4. Praxistauglichkeit der Videoüberwachung mit Gesichtserkennung

Diese menschliche Letztentscheidung ist auch damit zu begründen, dass Verfahren der biometrischen Gesichtserkennung derzeit nicht fehlerfrei funktionieren – und dies wahrscheinlich auch in absehbarer Zeit nicht tun werden. Das gilt insbesondere für die Verbindung von Gesichtserkennung mit Videoüberwachung, die häufig mit unzureichender Bildqualität, ungünstigen Lichtverhältnissen (vor allem zur Nachtzeit), Verdeckungen des Gesichts, unterschiedlichen Posen und nicht kooperierenden Betroffenen konfrontiert ist. Diese Probleme wurden von Oktober 2006 bis Januar 2007 i.R.e. Feldversuchs unter Leitung des *BKA* am Hauptbahnhof Mainz eindrucksvoll bestätigt. Die simulierte Fahndung nach freiwilligen Probanden lieferte – insbesondere bei Nacht – eine zu geringe Erkennungsrate.[25]

Mit Blick auf die beständige Verbesserung sowohl der Videotechnik als auch der biometrischen Verfahren ist allerdings davon auszugehen, dass die Technik seitdem Fortschritte erzielt

10 Zur Diskussion z.B. *Müller,* MschrKrim 2002, 33.
11 *Kreutzträger/Osterholz,* in: Zurawski, Sicherheitsdiskurse, 2007, S. 89.
12 BT-Drs. 18/10758, S. 3.
13 BT-Drs. 17/2750, S. 3 unter Verweis auf die Anschläge von Madrid (2004) und London (2005).
14 BT-Drs. 17/13071, S. 3.
15 Z.B. *Lang,* BayVBl 2006, 522 einschließlich grundrechtlicher Würdigung.
16 *Hornung/Desoi*, K&R 2011, 153, 153.
17 *Stutzer/Zehnder,* Vierteljahrshefte zur Wirtschaftsforschung 2009, 119, 129: „Informationsüberflutung"; am Bsp. Großbritannien *Schafer*, DuD 2013, 434, 436.
18 Überblick zu Techniken und Konzepten bei *Kees,* Algorithmisches Panopticon, 2015, S. 38 ff.; aus rechtlicher Sicht *Roßnagel/Desoi/Hornung*, ZD 2012, 459; *Bier/Spiecker gen. Döhmann,* CR 2012, 610; *Hornung/Desoi*, K&R 2011, 153; das Interesse an dieser Weiterentwicklung wird auch durch verschiedene BMBF-Verbundprojekte wie z.B. CamInSens, MuViT, PERFORMANCE oder FLORIDA belegt.
19 Aus dem Griechischen: bios (Leben) und metron (Maß); allgemein bezeichnet Biometrie die Erfassung und Messung von Lebewesen, hier (enger) die automatisierte Messung individueller physiologischer oder verhaltenstypischer Merkmale zur Erkennung und Unterscheidung von Personen, so z.B. der Bericht des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung zu biometrischen Identifikationssystemen, BT-Drs. 14/10005, S. 4; Überblick über verschiedene biometrische Verfahren auch jenseits des Gesichts in *Behrens/Roth,* in: Behrens/Roth, Biometrische Identifikation, 2001, S. 13.
20 Welche Merkmale dies im Einzelnen sind, hängt von den verwendeten Verfahren ab. Dabei kann es um die Abstände einzelner Gesichtspartien zueinander oder deren Oberflächenstruktur gehen.
21 Das erstmalige „Einlernen" in das System wird auch als Enrolment bezeichnet.
22 Zum Ablauf z.B. *Jain/Ross/Nandakumar,* Introduction to Biometrics, 2011, S. 3 ff.
23 Zu Anwendungsfeldern *Behrens/Roth* (o. Fußn. 19), S. 21 ff.; weitere Anwendungen sind die Grenzkontrolle „easyPASS", z.B. MMR-Aktuell 2010, 308790, oder die Durchsetzung von Haus- und Glücksspielverboten, *Hornung,* ZfWG Sonderbeil. 3/2015, 8, 9.
24 Soweit ersichtlich wird beim *BKA* bereits biometrische Gesichtserkennung genutzt, um mit Suchbildern den erkennungsdienstlichen Lichtbildbestand zu durchsuchen, BT-Drs. 17/11299, S. 2 f.; BT-Drs. 17/14714, S. 10.
25 Dazu *BKA,* Forschungsprojekt Gesichtserkennung als Fahndungshilfsmittel: Foto-Fahndung. Abschlussbericht, 2007; s.a. BT-Drs. 18/10137, S. 6; *Kett-Straub,* ZStW 2011, 110, 121; *LfDI Berlin*, Jahresbericht 2007, S. 203.

hat.[26] Daher ist zu erwarten, dass die biometrische Gesichtserkennung i.V.m. Videoüberwachung in absehbarer Zeit praktische Einsatzreife erlangen wird. In anderen Anwendungsbereichen funktioniert biometrische Gesichtserkennung ohnehin bereits deutlich besser. Dies gilt grundsätzlich für alle Bereiche, in denen der Betroffene mit dem System kooperiert, wie dies insbesondere bei Einlass- und Zugangskontrollen der Fall ist.

III. Rechtliche Einordnung

Die Verbindung von Videoüberwachung und biometrischer Gesichtserkennung bringt nicht nur technische, sondern auch rechtliche Herausforderungen mit sich. Bereits die herkömmliche Videoüberwachung ist – nicht nur auf Grund ihrer angezweifelten Wirksamkeit – ein umstrittenes Instrument. Darin spiegelt sich ein breiter gesellschaftspolitischer Streit über den Sinn und Nutzen der Videoüberwachung und anderer Überwachungstechnologien wider.[27] Z.T. wird der Videoüberwachung ein bedrohliches panoptisches Potenzial beigemessen,[28] während solcherlei Kritik nach anderer Auffassung als „rein ideologisch" zurückzuweisen ist.[29]

1. Basis: Rechtsfragen herkömmlicher Videoüberwachung

Einerseits kann Videoüberwachung einen Beitrag zur Verhinderung und Verfolgung von Straftaten leisten. Es entspricht der st. Rspr. des *BVerfG*, dass die Gewährleistung von Sicherheit durch Bekämpfung von Straftaten eine Aufgabe von großer verfassungsrechtlicher Bedeutung darstellt.[30] Für den *EGMR* steht es dabei „außer Frage, dass der Kampf gegen das Verbrechen ... weitgehend vom Einsatz moderner wissenschaftlicher Techniken der Ermittlung und Identifizierung abhängt".[31] Ein solches modernes Instrument kann auch die Videoüberwachung darstellen. Andererseits kann diese verfassungsrechtlich gewährleistete Grundrechte in schwerwiegender Weise beeinträchtigen. Dieser Umstand wird durch die erweiterten Möglichkeiten biometrischer Gesichtserkennung verschärft. I.E. ist also zwischen den beeinträchtigten Grundrechten und dem Interesse an der Verhinderung und Verfolgung von Straftaten abzuwägen.

Videoüberwachung kann insbesondere das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG)[32] beeinträchtigen, wenn Videoaufnahmen z.B. Informationen über das Aussehen, die Kleidung oder das Verhalten identifizierbar aufgenommener Personen enthalten. Dies gilt sowohl für das Beobachten im Kamera-Monitor-Verfahren als auch die Aufzeichnung der Aufnahmen (Erhebung und Speicherung).[33] Betroffen sind daneben das Recht am eigenen Bild[34] sowie je nach erfasstem Verhalten weitere spezielle Grundrechte, etwa die Versammlungsfreiheit des Art. 8 GG.[35]

Auf Grund des mit der Videoüberwachung einhergehenden Grundrechtseingriffs bedarf der Einsatz von Videoüberwachung durch die Polizei gesetzlicher Regelungen (Vorbehalt des Gesetzes), die den Anforderungen an Bestimmtheit und Verhältnismäßigkeit entsprechen. Diese wiederum sind von dem Gewicht des Eingriffs abhängig, das „von der Art der erfassten Informationen, dem Anlass und den Umständen ihrer Erhebung, dem betroffenen Personenkreis und der Art der Verwertung der Daten" bestimmt wird.[36]

Videoüberwachung ermöglicht Eingriffe von unterschiedlichem Gewicht: Die anlassbezogene Videoüberwachung des Rechtsbrechers im öffentlichen Raum, etwa bei Geschwindigkeitsüberschreitungen, weist kein besonders hohes Eingriffsgewicht auf.[37] Anders kann sich dies bei einer heimlichen, länger andauernden Observation darstellen. Insbesondere aber die – häufig kriminalpräventiv ausgerichtete – Videoüberwachung öffentlicher Straßen und Plätze kann schwerwiegende Grundrechtseingriffe hervorrufen, weil sie grundsätzlich alle Personen erfasst, die sich in dem überwachten Bereich aufhalten, auch wenn diese für die Maßnahme keinen Anlass (etwa durch strafbares Verhalten) gegeben haben. Solche anlasslosen Maßnahmen mit großer Streubreite können überdies Einschüchterungseffekte bewirken. Das Gewicht des Eingriffs wird ferner durch die Folgemaßnahmen, die vielfältigen Möglichkeiten der Auswertung der Aufzeichnungen und die Verknüpfung des Bildmaterials mit anderen Informationen vertieft. Ein heimliches Vorgehen erhöht das Eingriffsgewicht zusätzlich.[38]

Wegen des regelmäßig hohen Eingriffsgewichts sind an Bestimmtheit und Verhältnismäßigkeit der Ermächtigungsgrundlagen hohe Anforderungen zu stellen. Ein Rückgriff auf Generalklauseln ist deshalb grundsätzlich nicht zulässig.[39] Regelungen bestehen inzwischen in den Polizeigesetzen des Bundes und der Länder (z.B. § 27 BPolG, § 14 Abs. 3 HSOG), in der Strafprozessordnung (§ 100h Abs. 1 Satz 1 Nr. 1 StPO) und in den Datenschutzgesetzen (z.B. § 6b BDSG). Diese sind zwar nicht unumstritten; sie sind aber grundsätzlich anerkannt und werden angewandt.

2. Neue Rechtsfragen auf Grund der technischen Weiterentwicklung

Daran anknüpfend wirft die Verbindung herkömmlicher Videoüberwachung mit Verfahren zur biometrischen Gesichtserkennung neue rechtliche Fragen auf.[40]

a) Verfassungsrechtliche Problematik

Problematisch an der biometrischen Gesichtserkennung ist nicht so sehr die Nutzung des menschlichen Gesichts als solches. Menschen besitzen von Natur aus die Fähigkeit, ihresgleichen anhand des Gesichts zu erkennen, ohne dass damit rechtliche Probleme verbunden sind.

■ Eingriffsgewicht

Allerdings ist die Nutzung des menschlichen Gesichts im Rahmen polizeilicher biometrischer Gesichtserkennung grundsätzlich – neben der Erhebung und Speicherung der Bilddaten bei Anfertigung der Videoaufnahmen – als ein weiterer Eingriff in

26 So auch die Einschätzung der *Bundesregierung*, BT-Drs. 18/10137, S. 6.
27 Hierzu z.B. die Beiträge in *Zurawski*, Surveillance Studies, 2007.
28 *Schmitt Glaeser,* BayVBl 2002, 584, 585.
29 *Wendt,* in: Gaycken/Kurz, 1984.exe, 2008, S. 127.
30 Z.B. BVerfGE 100, 313, 388 f.
31 *EGMR* NJOZ 2010, 696, 701.
32 Anerkannt seit BVerfGE 65, 1.
33 Für das Kamera-Monitor-Verfahren ohne Aufzeichnung war dies umstritten, kann inzwischen aber als anerkannt gelten, z.B. *VGH Mannheim* MMR 2004, 198 m. Anm. *v. Stechow/v. Foerster*; *Lang,* BayVBl 2006, 522; zum Grundrechtseingriff auch *BVerfG* NVwZ 2007, 688, 690.
34 Dieses wird bei staatlicher Videoüberwachung allerdings kaum diskutiert und regelmäßig nur auf die informationelle Selbstbestimmung abgestellt.
35 Z.B. *VG Berlin* NVwZ 2010, 1442.
36 BVerfGE 120, 378, 401 ff. = MMR 2008, 308 m.w.Nw.
37 *BVerfG* DuD 2010, 788, 790; der Eingriff entfällt aber nicht dadurch, dass Verhaltensweisen im öffentlichen Raum erfasst werden, *BVerfG* NVwZ 2007, 688, 690.
38 Zu diesen Kriterien zur Bestimmung des Eingriffsgewichts s. z.B. BVerfGE 120, 378, 401 ff. = MMR 2008, 308 m.w.Nw.; zur Entwicklung *Hornung*, Grundrechtsinnovationen, 2015, S. 309 ff.; speziell zur Videoüberwachung *BVerfG* NVwZ 2007, 688, 691.
39 S. *BVerfG* NVwZ 2007, 688, 691 für Art. 16, 17 BayDSG.
40 Hierzu z.B. *Held*, Intelligente Videoüberwachung, 2014; *Bier/Spiecker gen. Döhmann*, CR 2012, 612; *Roßnagel/Desoi/Hornung*, ZD 2012, 459; *Hornung/Desoi*, K&R 2011, 153. Zu § 27 BPolG *Wissenschaftliche Dienste des Deutschen Bundestages,* Rechtsgrundlage für den Einsatz sog. intelligenter Videoüberwachung durch die Bundespolizei, 2016. Die Rspr. hat sich bisher nicht eingehend mit diesen Fragen beschäftigt; kurz *OVG Hamburg* MMR 2011, 128, 131: „automatisierten Auswertung des Bildmaterials ausgeschlossen".

das Recht auf informationelle Selbstbestimmung[41] zu qualifizieren, der zusätzliche Informationen über den Betroffenen offenbaren und als Grundlage für weitere Maßnahmen dienen kann.[42] Dabei gehen von der biometrischen Gesichtserkennung, insbesondere im Zusammenwirken mit Videoüberwachung, spezifische Gefahren für die Persönlichkeitsrechte betroffener Personen aus, die zu schwerwiegenden Grundrechtseingriffen führen können.[43]

Biometrische Gesichtserkennung erhöht die Möglichkeiten der Auswertung von Videoaufnahmen, indem sie die automatisierte Erkennung von Personen, den automatisierten Abgleich mit Lichtbilddatenbanken sowie – eine Vernetzung der Kamerasysteme vorausgesetzt – die automatisierte Verfolgung von Personen über mehrere Videokameras hinweg gestattet. Dies wiederum erleichtert die Erstellung von Verhaltens- und Bewegungsprofilen,[44] aus denen weitere Rückschlüsse gezogen werden können. Da biometrische Charakteristika – hier das Gesicht – nicht einfach austauschbar sind, ist es auch nicht ohne weiteres möglich, sich dieser Form der Überwachung zu entziehen.

Zwar ist eine solche Form der Überwachung auch ohne biometrische Gesichtserkennung möglich. Letztere kann diese aber maßgeblich erleichtern und so Auswertemöglichkeiten schaffen, die ansonsten zwar theoretisch, nicht aber praktisch realisierbar sind. Insofern kann die Schlagkraft herkömmlicher Videoüberwachung deutlich verstärkt werden. Hinzu tritt, dass mittels Videoüberwachung grundsätzlich eine Beobachtung und Erkennung aus der Ferne und ohne Kenntnis des Betroffenen möglich ist. Von einem solchen Überwachungsinstrument können überdies Einschüchterungseffekte ausgehen, die durch die – aus Sicht des Betroffenen bestehende – Komplexität und Undurchschaubarkeit der Technik noch verstärkt werden.

Schließlich ist das Risiko von Fehlerkennungen auf Grund technischer Unzulänglichkeiten in Betracht zu ziehen, welches ggf. Maßnahmen gegen Unbeteiligte bzw. unschuldige Personen nach sich ziehen kann. In den hier untersuchten Szenarien wird sich dies wegen der menschlichen Begleitung aber regelmäßig nicht auswirken.

Keine Unzulässigkeit per se

Obwohl also Gesichtserkennung i.V.m. Videoüberwachung schwerwiegende Grundrechtseingriffe hervorrufen kann, werden diese aber regelmäßig nicht so weit reichen, dass sie von vornherein verfassungsrechtlich unzulässig sind. Dies gilt insbesondere für Verstöße gegen die Menschenwürde (Art. 1 Abs. 1 GG), die ein „Schutzschild gegen ganz große Bedrohungen des Menschseins" darstellt und auch im Zusammenhang mit Biometrie nicht zur „kleinen Münze" geschlagen werden sollte.[45] Die staatliche Beobachtung von Menschen, auch die heimliche, stellt grundsätzlich weder die Subjektqualität der Betroffenen in Frage,[46] noch beeinträchtigt sie, jedenfalls solange sie im öffentlichen Raum stattfindet, den Kernbereich privater Lebensgestaltung (Art. 2 Abs. 1 i.V.m. 1 Abs. 1 i.V.m. 19 Abs. 2 GG).[47]

Überdies führt das videotechnische Erfassen und Auswerten menschlicher Gesichter grundsätzlich nicht zu einer menschenwürdewidrigen Registrierung und Katalogisierung der Betroffenen. Dies kann sich ggf. anders darstellen, wenn der menschliche Körper in seiner Gänze durch biometrische Verfahren erfasst und ausgewertet wird.[48] Jedenfalls unzulässig wäre aber eine Verbindung von Videoüberwachung und biometrischer Gesichtserkennung dergestalt, dass eine flächendeckende Videoüberwachung, wie sie z.B. in London[49], nicht aber in Deutschland Realität sein mag, mit zentralen, die Gesichtsdaten aller Bürger umfassenden Datenbanken gekoppelt wird, um jeden jederzeit erkennen und verfolgen zu können.[50] Dies würde eine nahezu vollständige „Rundumüberwachung"[51] aller Verhaltens- und Lebensvorgänge im öffentlichen Raum ermöglichen und damit der verfassungsrechtlichen Identität der Bundesrepublik Deutschland widersprechen, nach der „die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf"[52].

b) Zulässigkeit von Einsatzszenarien

Mit Blick auf das unterschiedliche, in manchen Szenarien aber jedenfalls hohe Eingriffsgewicht (s.o. III.2.a) lässt sich nicht pauschal beantworten, ob und inwieweit biometrische Gesichtserkennung auf bestehende Rechtsgrundlagen gestützt werden kann. Dies ist von der jeweiligen Ausgestaltung und Nutzung der Technik abhängig.[53] Daher wird in den drei folgenden Szenarien der Frage nachgegangen, ob für die dort vorgestellten Anwendungsmöglichkeiten Rechtsgrundlagen bestehen oder ob hierfür neue Regelungen zu schaffen sind.

Gesetzliche Regelungen, die ausdrücklich den Einsatz von Videoüberwachung i.V.m. biometrischer Gesichtserkennung zulassen, existieren derzeit nicht.[54] Dies bedeutet allerdings nicht zwingend, dass die Heranziehung bestehender Regelungen unzulässig ist, da in einem gewissen Umfang die Einbeziehung „kriminaltechnischer Neuerungen" in den Anwendungsbereich bestehender Regelungen gestattet ist.[55] Eine Grenze bilden hierfür aber sowohl der Wortlaut der Normen als auch die Anforderungen an Bestimmtheit und Verhältnismäßigkeit.

Sichtung von Videoaufzeichnungen

Zunächst kann biometrische Gesichtserkennung als ein bloßes Hilfsmittel für die Sichtung von Videoaufzeichnungen herangezogen werden. Wurde eine Straftat begangen, können vorhandene Videoaufzeichnungen des Tatorts helfen, den Tathergang zu rekonstruieren und verdächtige Personen aufzufinden. Die Sichtung der Aufzeichnungen kann allerdings nicht nur einen großen zeitlichen Aufwand mit sich bringen, sondern ist auf Grund der begrenzten Aufmerksamkeit menschlicher Betrachter auch mit dem Risiko verbunden, entscheidende Stellen zu übersehen.

In Verbindung mit einem leistungsfähigen Videomanagementsystem kann es biometrische Gesichtserkennung ermöglichen, den Aufwand der Auswertung deutlich zu reduzieren. Z.B. kann

---

41 Auf weitere ggf. betroffene Grundrechte wird an dieser Stelle nicht eingegangen. Bestimmte Formen intelligenter Videoüberwachung können insb. hinsichtlich Art. 3 GG problematisch werden, z.B. *Hornung/Desoi,* K&R 2011, 153, 156.
42 Zum Datenabgleich als Eingriff BVerfGE 100, 313, 366; 115, 320, 344 = MMR 2006, 531.
43 Allg. zu den rechtlichen Risiken biometrischer Erkennung *Biermann/Bromba/Busch/Hornung/Meints/Quiring-Kock,* White Paper zum Datenschutz in der Biometrie, 2008, S. 10 ff.
44 Zur Profilbildung *Hornung,* Die digitale Identität, 2005, S. 159 ff.
45 *Roßnagel,* in: Schaar, Biometrie und Datenschutz – Der vermessene Mensch, 2006, S. 59.
46 BVerfGE 109, 279, 313 = MMR 2004, 302 zur akustischen Wohnraumüberwachung.
47 *BVerfG* ZD 2011, 177 zu Videoaufzeichnungen von Verkehrsverstößen; zur Entwicklung der Kernbereichsfigur *Hornung* (o. Fußn. 38), S. 319 ff.
48 *Hornung* (o. Fußn. 44), S. 170; zur unzulässigen Registrierung und Katalogisierung BVerfGE 27, 1, 6; 65, 1, 53.
49 Großbritannien gilt als das Land mit der am stärksten ausgebauten Videoüberwachung weltweit, z.B. *House of Lords,* Surveillance: Citizens and the State, Volume I: Report, 2009, S. 20.
50 *Hornung* (o. Fußn. 44), S. 170 f.
51 Zur unzulässigen Rundumüberwachung BVerfGE 109, 279, 323 = MMR 2004, 302; BVerfGE 112, 304, 319 = MMR 2005, 371.
52 BVerfGE 125, 260, 324 = MMR 2010, 356.
53 So auch die *Bundesregierung* zur der Frage, ob der Einsatz „intelligenter Videoüberwachungssysteme" eine „verfassungsrechtliche Neubewertung" erfordert, BT-Drs. 18/10137, S. 7.
54 Der Gesetzgeber erwähnt den Einsatz biometrischer Erkennung i.V.m. Videoüberwachung im Bereich des § 6b Abs. 3 BDSG in BT-Drs. 14/5793, S. 62.
55 BVerfGE 112, 304, 316 = MMR 2005, 371; zur „Technikoffenheit" strafprozessualer Regelungen *Roggan,* NJW 2015, 1995.

der mit der Sichtung beauftragte Beamte eine in der Videoaufzeichnung auftretende Person markieren, woraufhin das Programm die Gesichtsinformationen der markierten Person ausliest und mit allen in der Aufnahme auftretenden Personen abgleicht. Im Trefferfall wird angezeigt, an welchen Stellen die markierte Person in der Videoaufnahme noch auffindbar ist. Dadurch können Leersequenzen oder anderweitig nicht interessierende Sequenzen in der Videoaufnahme übersprungen werden, was die für die Sichtung des Videos benötigte Zeit reduziert.

Eine solche Vorgehensweise erscheint nach derzeitiger Rechtslage zulässig. Erlauben gesetzliche Regelungen z.B., dass „Bildaufnahmen hergestellt" (§ 100h Abs. 1 Satz 1 Nr. 1 StPO) werden,[56] umfasst dies auch die Befugnis, das rechtmäßig aufgenommene Bildmaterial zur gesetzlichen Aufgabenerfüllung zu sichten.[57] Dies kann mittels analoger Videorecorder und einem Fernsehbildschirm oder mittels digitaler Bildwiedergabeprogramme an einem Computer erfolgen. Hieran knüpft die biometrische Gesichtserkennung an und bietet ein zusätzliches computergestütztes Hilfsmittel zur Sichtung der Aufzeichnungen.[58] Es ist nicht erkennbar, dass mit einer solchen Vorgehensweise erhebliche zusätzliche Gefährdungen des Rechts auf informationelle Selbstbestimmung einhergehen, die nicht schon durch die Regelungen zur Herstellung der Aufnahmen abgedeckt sind. Zwar mag der mit der Gesichtserkennung verbundene Abgleich der Gesichter innerhalb der Videoaufnahme einen zusätzlichen Grundrechtseingriff darstellen. Dieser ist aber nur von geringem Gewicht, da hierdurch keine Informationen gewonnen werden, die nicht bereits auf dem zur Verfügung stehenden Video festgehalten sind.

Zwar ist grundsätzlich erhebliche Zurückhaltung hinsichtlich der Annahme geboten, ein elaboriertes technisches Verarbeitungsverfahren sei „nur" eine technische Arbeitshilfe und rechtlich deshalb nicht anders zu bewerten als manuelle Verfahren.[59] Im vorliegenden Fall spricht aber alles dafür, dass es sich bei dieser Nutzung der biometrischen Gesichtserkennung letztlich um eine fortschrittliche Form des Vor- und Zurückspulens handelt, deren zusätzliches Eingriffsgewicht so geringfügig ist, dass sie keiner spezifischen Rechtsgrundlage bedarf, sondern auf die Regelungen zur Anfertigung der Aufnahme gestützt werden kann. Dies gilt zumindest, solange keine Verknüpfung mit Informationen aus anderen, mit den auszuwertenden Aufnahmen nicht im Zusammenhang stehenden Quellen stattfindet.

Identitätsfeststellung

Eine weiteres Szenario besteht darin, im Fall einer auf Video aufgenommenen Straftat zu versuchen, die Identität des mutmaßlichen Straftäters durch einen Abgleich mit polizeilichen Datenbeständen, insbesondere erkennungsdienstlichen Lichtbildsammlungen, zu ermitteln.

Ein solcher Datenabgleich kann nicht mehr auf die Ermächtigung zur Anfertigung der Videoaufnahmen gestützt werden. Möglich erscheint aber ein Rückgriff auf die Regelungen zum Datenabgleich. Gem. § 98c StPO[60] dürfen zur Aufklärung einer Straftat personenbezogene Daten aus einem Strafverfahren mit anderen zur Strafverfolgung oder Strafvollstreckung oder zur Gefahrenabwehr gespeicherten Daten maschinell abgeglichen werden. Zwar werden Bildaufnahmen weder in der Norm noch in der Begründung[61] explizit erwähnt. Die Norm erfasst aber allgemein personenbezogene Daten und damit auch Videoaufnahmen, wenn diese solche enthalten. Zu den Daten, mit denen abgeglichen werden kann, gehören auch erkennungsdienstliche Lichtbildsammlungen.[62]

Es ließe sich zwar einwenden, dass die Regelung nur geringe Eingriffsvoraussetzungen (Tatverdacht) aufweist und sehr allgemein gefasst ist. Allerdings ist der Datenabgleich von vergleichsweise geringem Eingriffsgewicht. Es werden i.R.e. Strafverfahrens aus konkretem Anlass nur Daten miteinander abgeglichen, die sich bereits auf Grundlage anderer gesetzlicher Ermächtigungen in der Verfügungsgewalt der staatlichen Behörden befinden. Für diese Form des Datenabgleichs ist keine über die Voraussetzungen des § 98c StPO hinausgehende Rechtsgrundlage erforderlich.

Personenfahndung

Der Charakter der Maßnahme wandelt sich hingegen beim dritten Szenario, der Fahndung nach gesuchten Personen. Hierzu könnten im öffentlichen Raum, z.B. an belebten Plätzen, Bahnhöfen oder Flughäfen, befindliche Videokameras mit einer Fahndungsdatenbank und einem Gesichtserkennungssystem verbunden werden. Die Gesichter aller von der Kamera erfassten Personen würden beständig in Echtzeit mit den in der Datenbank hinterlegten Gesichtern gesuchter Personen abgeglichen. Im Falle einer Übereinstimmung (Trefferfall) würde eine Treffermeldung ausgegeben, an die sich weitere Maßnahmen anschließen können.

Diese Vorgehensweise weist starke Parallelen zur automatisierten Kennzeichenerkennung auf. Dazu werden Kfz-Kennzeichen von einer Videokamera optisch erfasst, ihre Buchstaben- und Zahlenfolgen durch eine Software ausgelesen und mit den Einträgen in polizeilichen Fahndungsdateien abgeglichen.[63] Mittels der mobil oder stationär eingesetzten Systeme können auf diese Weise alle Fahrzeuge kontrolliert werden, die den überwachten Straßenabschnitt passieren.

Im Jahr 2008 hat sich das *BVerfG* eingehend mit der rechtlichen Bewertung dieser Technik auseinandergesetzt.[64] Wesentliche Gedanken dieser Rechtsprechung erscheinen auf die biometrische Personenfahndung übertragbar: Da biometrische Gesichtsdaten durch den Bezug zum menschlichen Körper und die Stabilität über einen langen Zeitraum eine höhere Persönlichkeitsrelevanz haben als Kfz-Kennzeichen, können die Eingriffsvoraussetzungen bei Ersteren auf keinen Fall niedriger sein.

Die Nutzung von Videoüberwachung i.V.m. Gesichtserkennung knüpft unmittelbar an die Videoüberwachung im öffentlichen Raum an, die bereits für sich gesehen schwerwiegende Grundrechtseingriffe hervorbringen kann. Erfasst und überprüft werden alle Personen, die sich im überwachten Bereich aufhalten, ohne dass diese in ihrer ganz überwiegenden Mehrzahl hierfür einen Anlass gegeben haben oder auch nur konkrete Erkenntnisse dafür vorliegen, dass sich die gesuchten Personen unter ihnen befinden könnten. Derartige anlasslose Maßnahmen mit großer Streubreite können Einschüchterungseffekte hervorrufen und sind nach der st. Rspr. des *BVerfG* bereits aus diesem Grund von hohem Gewicht.[65] Hinzu treten die vielfältigen Auswertemöglichkeiten dieser Form biometrischer Videoüberwachung. Im Trefferfall können zunächst unmittelbare Maßnah-

56 In einem Gefahrenabwehrszenario gilt Entsprechendes, wenn Regelungen wie § 14 Abs. 3 HSOG gestatten, „öffentlich zugängliche Orte mittels Bildübertragung offen [zu] beobachten und auf[zu]zeichnen".
57 So auch *Held* (o. Fußn. 40), S. 185 zur „herkömmliche[n] Auswertung mit dem bloßen Auge".
58 Wenn mit dem Auswertevorgang das Anlegen von Dateien verbunden ist, kann dies durch § 483 StPO abgedeckt werden.
59 Klassisches Bsp.: Eine Videokamera ist rechtlich anders zu bewerten als ein Streifenpolizist, der an derselben Stelle denselben Vorgang visuell wahrnimmt.
60 Zu § 98c StPO als verfassungskonform auszulegender Eingriffstatbestand *Günther,* in: MüKoStPO, 2014, § 98c Rdnr. 7 f.
61 BT-Drs. 12/989, S. 38.
62 S. *Greven,* in: Karlsruher Komm., StPO, 7. Aufl. 2013, § 98c Rdnr. 1 f.: z.B. Personenfahndungsdatei, Erkennungsdienstdatei, Daktyloskopiedatei.
63 Zur Funktionsweise BVerfGE 120, 378, 379 f. = MMR 2008, 308.
64 BVerfGE 120, 378 = MMR 2008, 308; s. ferner *BVerwG* NVwZ 2015, 906 sowie aus der Lit. z.B. *Roßnagel*, Kennzeichenscanning – Umsetzung der Vorgaben des Bundesverfassungsgerichts, 2009; *Kauß*, DuD 2014, 627; *Ziebarth*, CR 2015, 687.
65 Zur Videoüberwachung *BVerfG* NVwZ 2007, 688, 691; zur Kennzeichenerkennung BVerfGE 120, 378, 402 = MMR 2008, 308.

men wie etwa die Festnahme der gesuchten Person veranlasst werden. Darüber hinaus kann diese Form der Videoüberwachung aber auch genutzt werden, um zusätzliche Informationen zu erlangen. Sind Ort und Zeit einer Treffermeldung feststellbar, ermöglicht dies Rückschlüsse auf das Verhalten einer Person, was z.B. den Besuch bestimmter politischer, sportlicher oder kultureller Veranstaltungen betreffen kann. Werden so über einen längeren Zeitraum zahlreiche Treffermeldungen zusammengetragen, können Bewegungsprofile erstellt werden, die wiederum auf das Verhalten und die Interessen des Betroffenen schließen lassen.[66] Dies alles kann automatisiert und heimlich geschehen, ohne dass der Betroffene das Ausmaß der Datensammlung und -auswertung zu überblicken und sich dagegen gerichtlich zu wehren vermag.

Auf diese Weise wird ein Überwachungsmittel eigener Art geschaffen, welches in seiner Eingriffsintensität weit über die herkömmliche Videoüberwachung hinausgehen kann. Die Automatisierung der Personenerkennung ermöglicht durch die „Vervielfachung der Zahl der möglichen Erfassungsvorgänge gegenüber den bisherigen technischen und personellen Möglichkeiten der Polizei" eine „besondere Schlagkraft" und schafft neue Möglichkeiten der (heimlichen) Datenerfassung und -auswertung.[67]

Der polizeiliche Einsatz eines solchen Instruments bedarf einer expliziten gesetzlichen Regelung und kann nicht auf bereits vorhandene Regelungen zur Videoüberwachung gestützt werden. Für § 100h Abs. 1 Satz 1 Nr. 1 StPO folgt das schon aus dem Wortlaut, der das „Herstellen" von Bildaufnahmen erlaubt.[68] Dies umfasst keinesfalls den beständigen Abgleich aller aufgenommenen Videodaten mit – ggf. umfangreichen – Fahndungsbeständen.[69] Ebenso wenig kann diese Form der Nutzung biometrischer Gesichtserkennung auf die gesetzlichen Regeln zum Datenabgleich (hier § 98c StPO) gestützt werden.[70] Die vergleichsweise unbestimmten Regelungen zum Datenabgleich werden dem schwerwiegenden Grundrechtseingriff nicht gerecht. Überdies würde durch die Heranziehung dieser Regelung ein einheitlicher Vorgang, also das Erheben und sofortige Abgleichen der erhobenen Informationen, auf künstliche Weise auseinandergerissen und auf unterschiedliche Rechtsgrundlagen verteilt.

Vielmehr erfordern der Vorbehalt des Gesetzes und das damit im Zusammenhang stehende Bestimmtheitsgebot eine klare gesetzliche Aussage des demokratisch legitimierten Gesetzgebers, die der Exekutive ihre Befugnisse vorgibt und betroffene Personen das Ausmaß der Datenerhebung und -verarbeitung erkennen lässt. Insbesondere sind der Anlass und Verwendungszweck sowie die Grenzen der Datenerhebung und -verarbeitung bereichsspezifisch und präzise zu regeln[71] und Eingriffe auszuschließen, die außer Verhältnis zur Bedeutung der sie rechtfertigenden Gründe stehen.[72]

Grundsätzlich darf der Gesetzgeber den Einsatz von Videoüberwachung i.V.m. Gesichtserkennung zur Personenfahndung nur unter sehr engen Voraussetzungen zulassen. Die verfassungsrechtlich geforderten Eingriffsvoraussetzungen können auf unterschiedliche Weise normiert werden.[73] Um eine angemessene Eingriffsschwelle zu gewährleisten, ist der Einsatz auf die Aufklärung schwerer oder schwerster Straftaten zu beschränken.[74] Damit korrespondiert eine Eingrenzung des heranziehbaren Fahndungsbestands auf Personen, die solcher Straftaten verdächtig oder überführt sind. Des Weiteren ist der Einsatz in räumlicher Hinsicht zu begrenzen und auf Orte zu beschränken, an denen tatsächlich mit einem Auffinden der gesuchten Personen zu rechnen ist. Dafür bieten sich insbesondere Flughäfen oder Bahnhöfe an, die auch jetzt schon mannigfaltig überwacht werden. Auf jeden Fall ist eine flächendeckende Nutzung sowie eine anlasslose Ermittlung „ins Blaue hinein" auszuschließen.[75]

Überdies ist die weitere Verwendung der erlangten Informationen einzuschränken. Eine Verwendung zu Zwecken, die nicht eine der Verfolgung schwerer Straftaten gleichwertige Bedeutung aufweisen, ist auszuschließen. Da die Erstellung von Bewegungs- und Verhaltensprofilen einen besonders schweren Grundrechtseingriff darstellt, ist diese entweder vollständig zu untersagen oder zumindest auf eng umgrenzte Ausnahmen zu beschränken. Soll die biometrische Gesichtserkennung i.V.m. Videoüberwachung als ein Instrument polizeilicher Beobachtung (z.B. § 163e StPO) genutzt werden, ist dies explizit zu regeln und das besondere Gewicht einer solchen Maßnahme in Rechnung zu stellen.

Schließlich muss eine gesetzliche Regelung auch technisch-organisatorische sowie verfahrensrechtliche Vorkehrungen umfassen, um einen ausreichenden Grundrechtsschutz zu gewährleisten.[76] Dies bedingt ein hohes Maß an Datensicherheit[77] und kann weiterhin Dokumentationspflichten, um eine missbräuchliche Verwendung zu erschweren, einen Richtervorbehalt[78] sowie parlamentarische Berichtspflichten umfassen.[79] Wenn technisch-organisatorische Maßnahmen in Form von Privacy-Enhancing Technologies[80] vorgegeben werden, kann dies überdies das Eingriffsgewicht substanziell reduzieren und damit auf der Ebene der Verhältnismäßigkeit über die Zulässigkeit mitentscheiden. Dies kann etwa eine „gestufte" Überwachung umfassen, die sich zunächst auf eine Beobachtung ohne Aufzeichnung beschränkt und nur bei Auffälligkeiten die betreffenden Personen näher verfolgt, beweissichernd aufzeichnet und ggf. Maßnahmen zur (biometrischen) Identifizierung durchführt.[81] Freilich kommen solche Beschränkungen mit den sicherheitsbehördlichen Interessen in Konflikt, möglichst viele Aufnahmen guter Qualität zu erheben und für einen gewissen Zeitraum zu speichern. Eine solche Speicherung, die bei hergebrachter Videoüberwachung inzwischen weithin üblich ist, steht auch einer unmittelbaren Löschung der „Nichttrefferfälle" entgegen, bei der nach umstrittener Ansicht des *BVerfG* der Grundrechtseingriff entfällt.[82] Verzichtet man auf eine solche technisch gesicherte sofortige Löschung, muss man sich allerdings bewusst sein, dass ein erheblicher Eingriff für eine Vielzahl Unbeteiligter bestehen bleibt, der sich nur schwer rechtfertigen lässt.

66 BVerfGE 120, 378, 403 ff. = MMR 2008, 308 zum Eingriffsgewicht der Kennzeichenerkennung.
67 BVerfGE 120, 378, 407 = MMR 2008, 308 zur Kennzeichenerkennung.
68 Entsprechend für ein Präventionsszenario z.B. § 14 Abs. 3 HSOG: „beobachten und aufzeichnen".
69 In diesem Sinne ist wohl auch *OVG Hamburg* MMR 2011, 128, 131 zu verstehen.
70 *Petri,* in: Lisken/Denninger, Hdb. des Polizeirechts, 2012, Kap. G Rdnr. 519 verwirft entsprechend die Möglichkeit, die automatisierte Kennzeichenerkennung auf die Regeln zum Datenabgleich zu stützen.
71 BVerfGE 120, 378, 408 = MMR 2008, 308.
72 BVerfGE 120, 378, 428 = MMR 2008, 308.
73 Zur präventiven Kennzeichenerkennung BVerfGE 120, 378, 432 f. = MMR 2008, 308.
74 Dem entspräche im Gefahrenabwehrbereich eine Begrenzung auf die Abwehr von (konkreten) Gefahren für hochrangige Rechtsgüter.
75 BVerfGE 120, 378, 430 = MMR 2008, 308 zur Kennzeichenerkennung.
76 Zu organisatorischen und verfahrensrechtlichen Vorkehrungen bereits BVerfGE 65, 1, 44.
77 Zu den strengen Anforderungen bei der Vorratsdatenspeicherung BVerfGE 125, 260, 325 ff. = MMR 2010, 356.
78 Zum Richtervorbehalt z.B. BVerfGE 109, 279, 357 f. = MMR 2004, 302.
79 So z.B. § 31 Abs. 2 Satz 5 BbgPolG zur polizeilichen Videoüberwachung öffentlicher Straßen und Plätze und § 36a Abs. 3 BbgPolG zur Kennzeichenerkennung.
80 Grundlegend *Borking,* DuD 2001, 607; vor dem Hintergrund der Datenschutzreform *Hornung,* ZD 2011, 51.
81 Zu einem „Drei-Stufen-Modell" *Roßnagel/Desoi/Hornung,* DuD 2011, 694; zu software-basierten „Privacy Filtern", z.B. Verpixelung, *Stechow,* Datenschutz durch Technik, 2005, S. 53 ff.
82 BVerfGE 120, 378, 399 = MMR 2008, 308; krit. zu dieser Rspr. z.B. *Breyer,* NVwZ 2008, 824, 824 f.; als Vorgabe zur Technikgestaltung *Roßnagel,* NJW 2008, 2547, 2548.

I.E. ist nach derzeitiger Rechtslage eine Verbindung von Videoüberwachung und biometrischer Gesichtserkennung in der hier dargestellten Art und Weise zur Personenfahndung auf Grund fehlender gesetzlicher Ermächtigungen unzulässig. Bei entsprechender Ausgestaltung ist die Schaffung geeigneter Rechtsgrundlagen zwar grundsätzlich, aber nur unter sehr engen Voraussetzungen und keinesfalls flächendeckend und anlasslos möglich.

IV. Ausblick

Die Kombination verbesserter Kameratechnik mit biometrischer Gesichtserkennung ist ein Beispiel dafür, dass die Weiterentwicklung von Überwachungs- und Kontrolltechnologien nicht nur bestehende Rechtsfragen verschärft, sondern auch ganz neue Probleme aufwirft. Einige dieser Fragen und einige neue Einsatzszenarien kann das geltende Recht angemessen verarbeiten, wesentliche Änderungen der Technologien und ihrer Einsatzzwecke bedürfen aber einer Entscheidung des demokratischen Gesetzgebers. Insoweit ist sowohl vor Technikgläubigkeit als auch vor normativen Schnellschüssen zu warnen: Erforderlich ist schon aus verfassungsrechtlicher Sicht eine sorgfältige Analyse der tatsächlichen Wirksamkeit zur Kriminalitätsbekämpfung und sodann auch und gerade bei wirksamen Technologien eine grundrechtsschonende Umsetzung in der Praxis, um Szenarien der Massenüberwachung vorzubeugen, die nicht nur den Einzelnen betreffen, sondern auch die demokratische Gesellschaft insgesamt.[83]

83 S. schon BVerfGE 65, 1, 42 f.

Prof. Dr. Gerrit Hornung, LL.M.
ist Professor für Öffentliches Recht, IT-Recht und Umweltrecht an der Universität Kassel und Direktor im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) sowie Mitglied des Wissenschaftsbeirats der ZD.

Stephan Schindler
ist Wissenschaftlicher Mitarbeiter am Lehrstuhl für Öffentliches Recht, IT-Recht und Umweltrecht an der Universität Kassel und am Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG).

Der Beitrag ist im Zusammenhang mit dem BMBF-Projekt PERFORMANCE – Kooperative Systemplattform für Videoupload, Bewertung, teilautomatisierte Analyse und Archivierung, FKZ 13N14030, entstanden.