BÜRO FÜR TECHNIKFOLGEN-ABSCHÄTZUNG
BEIM DEUTSCHEN BUNDESTAG

Claudio Caviezel
Leon Hempel
Christoph Revermann
Saskia Steiger

Beobachtungstechnologien im Bereich der zivilen Sicherheit – Möglichkeiten und Herausforderungen

Endbericht zum TA-Projekt

Juni 2022
Arbeitsbericht Nr. 190

Claudio Caviezel
Leon Hempel
Christoph Revermann
Saskia Steiger

Beobachtungstechnologien im Bereich der zivilen Sicherheit – Möglichkeiten und Herausforderungen

Endbericht zum TA-Projekt

TAB-Arbeitsbericht Nr. 190

Büro für Technikfolgen-Abschätzung
beim Deutschen Bundestag
Neue Schönhauser Straße 10
10178 Berlin

Telefon: +49 30 28491-0
E-Mail: buero@tab-beim-bundestag.de
Web: www.tab-beim-bundestag.de

2022

Umschlagbild: leightwise/123RF

ISSN-Internet: 2364-2602

Das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) berät das Parlament und seine Ausschüsse in Fragen des wissenschaftlich-technischen Wandels. Das TAB wird seit 1990 vom Institut für Technikfolgenabschätzung und Systemanalyse (ITAS) des Karlsruher Instituts für Technologie (KIT) betrieben. Hierbei kooperiert es seit September 2013 mit dem IZT – Institut für Zukunftsstudien und Technologiebewertung gGmbH sowie der VDI/VDE Innovation + Technik GmbH.

Inhalt

Zusammenfassung

Beobachtungstechnologien erweitern das menschliche Wahrnehmungs- und Beurteilungsvermögen für Risiken, Gefahren oder Schäden in vielfältiger Weise. Von ihrer Anwendung können daher sämtliche Aufgabenfelder der zivilen Sicherheit profitieren, angefangen von der Verkehrsüberwachung und dem Umweltmonitoring über den Brand- und Katastrophenschutz, den Rettungsdienst und den Schutz kritischer Infrastrukturen bis hin zur polizeilichen Gefahrenabwehr und Strafverfolgung. Der Einsatz von Beobachtungstechnologien wird in Öffentlichkeit, Wissenschaft und Politik zum Teil allerdings kontrovers diskutiert und es werden Fragen nach dem tatsächlichen Sicherheitsnutzen, den Wirkungen und Folgen sowie nach der Verhältnismäßigkeit von technisierten Beobachtungsmaßnahmen gestellt.

Vor diesem Hintergrund wird mit dem vorliegenden Bericht das Ziel verfolgt, eine fundierte Sachgrundlage für die politische Meinungsbildung bezüglich der erforderlichen Rahmensetzungen für den Einsatz von Beobachtungstechnologien im zivilen Sicherheitsbereich zu erarbeiten. Hierzu werden die relevanten gesellschaftlichen und politischen Fragestellungen, die sich mit der (zunehmenden) Anwendung von Beobachtungstechnologien im zivilen Sicherheitsbereich ergeben, ausführlich reflektiert. Dabei ist es ein besonderes Anliegen, die Vielfalt der (möglichen) Einsatzfelder hinsichtlich ihrer technischen, rechtlichen und sozialen Komplexität zu verdeutlichen, um Chancen und Herausforderungen in ihrer gesamten Breite und Tiefe abzuleiten.

Hinweis zur Aktualität des Berichts

Der Redaktionsschluss für den vorliegenden Bericht war Anfang 2020. Demzufolge konnten jüngere Entwicklungen, veränderte Rahmenbedingungen und neuere Quellen keine Berücksichtigung finden. Dazu gehören insbesondere die rechtlichen Rahmenbedingungen, die sich seit 2021 teilweise erheblich verändert haben, aber auch seither erzielte Fortschritte in der Forschung und Entwicklung oder Veränderungen in den gesellschaftlichen und politischen Diskursen. Aktualisierungen wurden jedoch in Bezug auf die Anwendungspraxis von Beobachtungstechnologien im Bereich der zivilen Sicherheit vorgenommen. Hierzu wurden Daten für die Jahre bis 2020, die erst nach Redaktionsschluss veröffentlicht wurden, entsprechend ergänzt (Stand März 2022).

Thematische und begriffliche Einführung

Im gesellschaftlichen Kontext ist *Beobachtung* Grundvoraussetzung und Mittel für soziale Kontrolle. Damit gemeint sind Prozesse und Strukturen, durch die eine Gesellschaft versucht, bestimmte Normen und ein entsprechendes Verhalten ihrer Mitglieder zu gewährleisten. Soziale Kontrolle verbindet stets beide Aspekte: individuelle Anpassung, aber auch Schutz der Individuen durch die Gesellschaft. Ein gewisses Maß an sozialer Kontrolle und damit an Beobachtung ist für das stabile Funktionieren von Gesellschaften daher unerlässlich. Beobachtung ist zugleich ambivalent, da sie in Form von *Überwachung* ungleiche Machtverhältnisse befördern bzw. verfestigen kann. Gerade *Beobachtungstechnologien* können zur Ambivalenz von Beobachtung beitragen, indem sie die Beobachtung aus der Distanz ermöglichen und so die Wechselseitigkeit der Wahrnehmung, die zwischenmenschlichen Formen der Beobachtung zugrunde liegt, tendenziell aufheben. Für die Bewertung von (technisierten) Beobachtungspraktiken entscheidend sind daher immer der Kontext der Beobachtung, ihr Zweck und Umfang sowie ihre Eingriffstiefe.

Beobachtungstechnologien im Bereich der zivilen Sicherheit

Unser Verständnis von *Sicherheit* ist einem starken Wandel ausgesetzt. Stand noch vor wenigen Jahrzehnten der Schutz der Bevölkerung vor den Auswirkungen zwischenstaatlicher Kriege im Fokus, so sind es heute Konzepte eines umfassenden Risiko- und Krisenmanagements, dessen Ziele von der Kriminalitätsbekämpfung über den Schutz kritischer Infrastrukturen (z. B. Telekommunikationsnetze, Flughäfen, Krankenhäuser, Rechenzentren) bis zur Minimierung von Risiken durch Unfälle, Naturkatastrophen oder Terroranschläge reichen.

Im Konzept der *zivilen Sicherheit* wird Sicherheit entsprechend als eine gesamtgesellschaftliche Aufgabe verstanden, an der sich sämtliche gesellschaftlichen Akteure auch beteiligen. Dazu gehören die Akteure der nichtpolizeilichen Gefahrenabwehr (Brandschutz, Rettungsdienst, Bevölkerungsschutz), die Polizei, nichtstaatliche Sicherheitsakteure (private Hilfsorganisationen, Betreiber von kritischen Infrastrukturen, private Sicherheitsdienstleister z. B. in Einkaufszentren) und nicht zuletzt auch die Bürger/innen selbst (z. B. im Rahmen der spontanen Hilfe während Katastrophenlagen). Weitere zivile Sicherheitsakteure sind die Nachrichtendienste (Aufklärung im In- und Ausland) und die Streitkräfte (im Rahmen der Amts- und Katastrophenhilfe), auf die aber im vorliegenden Bericht nicht weiter eingegangen wird.

Durch die Erweiterung des Gefahrenspektrums im Konzept der zivilen Sicherheit haben sich auch die Anwendungspotenziale für Beobachtungstechnologien massiv vergrößert, sodass heute eine enorme Vielfalt an technischen

Lösungen und Einsatzformen existiert. Die Gliederung des Berichts fußt auf der folgenden Einteilung von Beobachtungstechnologien:

- *Sensorbasierte Beobachtungstechnologien* erfassen bestimmte physikalische oder chemische Eigenschaften der realen Welt und bereiten die Messgrößen in für den Menschen leicht interpretierbare Informationen auf.
- *Datenbasierte Beobachtungstechnologien* erfassen und analysieren Informationen der digitalen Welt. Die *Internetbeobachtung* beschränkt sich hierbei auf öffentlich zugängliche Inhalte im Internet. Zentrale Beobachtungsräume der *informationstechnischen Beobachtung* sind hingegen die Telekommunikation oder Daten in informationstechnischen Endgeräten (PC, Smartphone).

Sensorbasierte Beobachtung

Der Bericht befasst sich mit sensorbasierten Beobachtungstechnologien, die für zivile Sicherheitsaufgaben bereits genutzt werden oder deren Anwendung in naher Zukunft wahrscheinlich ist.

Bildgebende Beobachtungstechnologien

Der Mensch erfasst Informationen aus seiner Umwelt großteils visuell. Entsprechend vielfältig sind die Einsatzmöglichkeiten und der Stellenwert von bildgebenden Beobachtungstechnologien. An der Weiterentwicklung der Technologien und der Erschließung neuer Anwendungsfelder wird – auch maßgeblich durch die zivile Sicherheitsforschung des Bundes unterstützt – intensiv geforscht.

Bodengestützte bildgebende Beobachtungstechnologien

Videokameras gehören zu den am meisten verbreiteten Beobachtungstechnologien. Die notwendige Sensortechnik zur Bildgebung im Bereich des sichtbaren Lichts sowie die Übermittlungs- und Speichertechnik sind ausgereift, kostengünstig und einfach in der Anwendung. Zentrales Einsatzfeld ist die *Videobeobachtung*, deren Einsatzformen in Bezug auf Anwendungskontext, Zielsetzung und beteiligte Akteure eine große Bandbreite aufweisen. Weit verbreitet ist die *offene Videobeobachtung im öffentlich zugänglichen Raum*. Sie wird von der Polizei zum Zweck der Gefahrenabwehr, zum überwiegenden Teil jedoch von privaten Akteuren auch für andere (z. B. unternehmerische) Zwecke eingesetzt. Davon in Zielsetzung und Wirkung grundsätzlich verschieden ist der *verdeckte polizeiliche Einsatz von Videotechnik* für die Beobachtung einzelner Personen zu Zwecken der Gefahrenabwehr oder Strafverfolgung, der an enge rechtliche Voraussetzungen geknüpft ist. Im *nichtpolizeilichen Bereich* werden Videokameras beispielsweise für die automatisierte Waldbrandfrüherkennung oder in Form von trag-

baren Endoskopkameras für die Suche nach Verschütteten bei Gebäudeeinstürzen eingesetzt.

Wärmebildkameras messen die von Objekten emittierte Infrarotstrahlung und ermöglichen die Darstellung von Oberflächentemperaturen. Bei Feuerwehren gehören sie zur Standardausrüstung, um beispielsweise Glutnester zu lokalisieren. Personen lassen sich damit auch bei völliger Dunkelheit beobachten, weswegen Wärmebildkameras oft ein entscheidendes Hilfsmittel für die Vermisstensuche darstellen und auch im Rahmen der Grenzkontrolle eingesetzt werden.

Körperscanner für die Personenkontrolle nutzen für die Bildgebung Millimeterwellen, die Textilien durchdringen. Damit lassen sich unter der Kleidung verborgene Gegenstände aus unterschiedlichen (auch nichtmetallischen) Materialien sichtbar machen, weshalb die an Flughäfen vorhandenen Metalldetektorschleusen derzeit sukzessive durch Körperscanner ersetzt werden. Die Rohbilder stellen auch die Körperkonturen der gescannten Personen und ggf. getragene Prothesen dar. Zum Schutz der Privat- und Intimsphäre erkennen heute gängige Systeme potenziell gefährliche Gegenstände automatisiert und markieren deren Lage in einer schematischen Darstellung des menschlichen Körpers. Nachteilig ist, dass die zu kontrollierenden Personen eine Schleuse durchschreiten und mit Millimeterwellen beleuchtet werden müssen (was Fragen nach möglichen gesundheitsgefährdenden Wirkungen aufwirft). Beide Nachteile entfielen bei Verwendung von Körperscannern auf Basis von Terahertzstrahlung, diese Technik steht aber noch nicht für den Praxiseinsatz bereit.

Röntgengeräte werden standardmäßig zur Durchleuchtung von Gepäck und anderen unbelebten Gegenständen etwa bei Zugangskontrollen oder an Flughäfen sowie zur gezielten Überprüfung von Paket- oder Postsendungen eingesetzt. Größere Geräte, die z. B. Lkw in Gänze durchleuchten, können bei der Suche nach Schmuggelware hilfreich sein. Aus Strahlenschutzgründen dürfen Röntgenstrahlen nicht für Sicherheitskontrollen an Personen verwendet werden.

Luftgestützte bildgebende Beobachtungstechnologien

Videokamerasysteme auf Hubschraubern werden vor allem von der Polizei anlassbezogen zur Lageaufklärung und -beobachtung, zur Vermisstensuche oder zur Verfolgung von Punktzielen eingesetzt. Die Systeme sind meist mit Tageslicht- und Wärmebildkameras ausgestattet. Als Trägersysteme kommen seit rund 10 Jahren zunehmend auch rotorbetriebene *unbemannte Fluggeräte* (Multicopter) zur Anwendung. Die Polizei verwendet sie z. B. für die Tatort- und Beweissicherung oder zur Verkehrsraumbeobachtung. 2018 hat Bayern als erstes Bundesland – nicht unumstrittene – spezielle Ermächtigungsgrundlagen geschaffen, die einen Einsatz auch bei öffentlichen Veranstaltungen oder Ansammlungen erlauben.

Von großem Nutzen können Videokameras auf unbemannten Fluggeräten auch im Brand- und Katastrophenschutz für die schnelle Lageaufklärung bei

komplizierten Einsatzlagen sein. Es besteht allerdings noch ein erheblicher Forschungs- und Entwicklungsbedarf, um entsprechende Systeme speziell für die hier bestehenden Bedürfnisse (lange Flugzeiten, hohe Wetterstabilität etc.) bereitzustellen. Unbemannte Fluggeräte dürfen von Behörden und Organisationen mit Sicherheitsaufgaben (BOS) seit 2017 ohne Sondergenehmigung und nahezu verbotsfrei genutzt werden, sodass künftig von einem verstärkten Einsatz von unbemannten Fluggeräten durch BOS auszugehen ist.

Weltraumgestützte bildgebende Beobachtungstechnologien

Bilddaten von satellitengestützten Beobachtungstechnologien sind bei großräumigen Ereignissen (z. B. Hochwasser, Waldbrände, humanitäre Krisen) von hohem praktischem Nutzen für die Vorbereitung (Risikoanalysen, Gefährdungskartierung), Lagebewältigung (Lagebeurteilung, Planung und Durchführung von Rettungsaktionen) und -wiederherstellung. In den letzten 20 Jahren wurden verschiedene nationale und internationale Dienste entwickelt, mit deren Hilfe Sicherheitsakteure mit bedarfsgerechten Informationsprodukten aus der Erderkundung versorgt werden können. Im Rahmen des europäischen Erdbeobachtungsprogrammes Copernicus beispielsweise können berechtigte Nutzerorganisationen (in Deutschland das Gemeinsame Melde- und Lagezentrum von Bund und Ländern) im Falle von Katastrophen den Dienst zur Notfallkartierung aktivieren, um aktuelle Lagekarten der betroffenen Gebiete zu erhalten. Die Neu- bzw. Weiterentwicklung von Copernicus-Diensten für den öffentlichen Bedarf wird vonseiten der Bundesregierung durch eine Reihe von Förder- und Entwicklungsmaßnahmen unterstützt.

Im polizeilichen Bereich werden aktuelle Satellitenbilder anlassbezogen u. a. zur Objektaufklärung, zur Vorbereitung von Exekutivmaßnahmen, zur Planung von Großereignissen oder zur Aufklärung von Tatorten verwendet. Die Bilder werden vom Zentrum für Satellitengestützte Kriseninformation (ZKI) am Deutschen Zentrum für Luft- und Raumfahrt (DLR) bereitgestellt.

Vertiefung: Videobeobachtung im öffentlich zugänglichen Raum

Von den sensorbasierten Beobachtungstechnologien nimmt im zivilen Sicherheitsbereich die offene Videobeobachtung im öffentlich zugänglichen Raum eine hervorgehobene Rolle ein. Sie wird daher im Bericht vertieft behandelt.

Aktueller Stand: Akteure und rechtliche Grundlagen

Die Videobeobachtung im öffentlich zugänglichen Raum wird von unterschiedlichen Akteuren und in verschiedenen Formen eingesetzt. Die jeweiligen Einsatzformen werden durch ein komplexes Regelungsgefüge aus spezialgesetzlichen und/oder datenschutzrechtlichen Normen auf Bundes-, Landes- und seit dem

25. Mai 2018 auch auf EU-Ebene geregelt. Zu beachten ist insbesondere der Anwendungsvorrang der Datenschutz-Grundverordnung gegenüber nationalen Gesetzen.

Die *polizeiliche Videobeobachtung* richtet sich allein nach nationalen Gesetzen, da die Datenschutz-Grundverordnung keine Anwendung auf Behörden findet, die personenbezogene Daten zu Zwecken der Gefahrenabwehr oder Strafverfolgung verarbeiten (die Regelungen müssen gleichwohl der Richtlinie [EU] 2016/680 genügen). Alle Polizeigesetze der Länder ermöglichen unter bestimmten Bedingungen die offene Videobeobachtung zu Zwecken der Gefahrenabwehr in der Regel

- bei öffentlichen Veranstaltungen,
- an gefährdeten Orten (sogenannte Kriminalitätsschwerpunkte),
- in oder im Umfeld von gefährdeten Objekten
- oder durch Bodycams.

Entsprechende Befugnisse für die Bundespolizei sind auf ihre Aufgabenbereiche bezogen (u. a. Grenzschutz, Bahnpolizei, Schutz der Bundesorgane). Das Strafverfahrensrecht enthält hingegen keine Ermächtigungsgrundlagen für die offene Videobeobachtung im öffentlich zugänglichen Raum.

Für die *Videobeobachtung durch nichtpolizeiliche öffentliche Stellen* (z. B. im Rahmen des Objektschutzes bei Amtsgebäuden oder Kulturgütern) kommt eine Öffnungsklausel der Datenschutz-Grundverordnung in Betracht, die Datenverarbeitungen für Aufgaben im öffentlichen Interesse erlaubt. Die Öffnungsklausel wird durch entsprechende bundes- bzw. landesdatenschutzrechtliche Normen ausgefüllt. Die konkreten Zulässigkeitsvoraussetzungen für den Einsatz offener Videobeobachtung sind uneinheitlich ausformuliert, sehen aber zumeist eine Abwägung mit den schutzwürdigen Interessen der Betroffenen vor.

Die Zulässigkeit der *Videobeobachtung durch nichtöffentliche Stellen* (private Unternehmen und Personen) ist seit Mai 2018 alleine nach den Regelungen der Datenschutz-Grundverordnung zu beurteilen. Nationale Regelungen, wie beispielsweise die 2017 zwecks Erhöhung der Sicherheit eingeführte Erleichterung der privaten Videobeobachtung in hochfrequentierten öffentlichen Räumen nach § 4 Abs. 1 S. 2 Bundesdatenschutzgesetz, finden keine Anwendung mehr.

Der bestehende Rechtsrahmen steht *Kooperationen zwischen polizeilichen und nichtpolizeilichen Akteuren* der Videobeobachtung nicht im Wege. Die datenschutzrechtlichen Regelungen erlauben explizit die Übermittlung von Videomaterial an Polizei- oder Strafverfolgungsbehörden, falls dies zum Zwecke der Gefahrenabwehr oder Strafverfolgung erforderlich ist.

Beispiele aus der aktuellen Einsatzpraxis

Eine eindeutige Zuordnung aktueller Einsatzpraktiken zu den aus rechtlicher Perspektive relevanten Akteursgruppen ist aufgrund vielfältiger Kooperationsfor-

men oft nicht möglich. Auch der aktuelle Umfang des Einsatzes in Deutschland ist unbekannt, da es für den Betrieb von Videobeobachtungsanlagen keine Meldepflicht gibt. Im vorliegenden Bericht werden wichtige Einsatzfelder exemplarisch näher beleuchtet.

Die *polizeiliche Videobeobachtung an gefährdeten Orten* hat nur einen geringen Anteil an der Videobeobachtung im öffentlich zugänglichen Raum. In Nordrhein-Westfalen beispielsweise waren zu diesem Zweck 2018 insgesamt rund 100 Kameras in 7 Städten im Einsatz (zum Vergleich: Alleine die Kölner Verkehrs-Betriebe AG setzte 2015 rund 2.500 Kameras ein). Die Videobilder werden durch Polizeibeamte in Echtzeit ausgewertet und temporär gespeichert. Der Fokus richtet sich auf die Feststellung von Diebstahl-, Betäubungsmittel- und Gewaltdelikten, im Ereignisfall werden Sofortmaßnahmen durch Einsatzkräfte vor Ort eingeleitet. Im Rahmen einer Evaluation bemängelten involvierte Beamte teilweise, dass zu wenig Personal (Videobeobachter, Einsatzkräfte vor Ort) für eine effiziente Nutzung der Videobeobachtung vorhanden sei.

Einen Schwerpunkt polizeilicher Videobeobachtung bildet der *temporäre Einsatz von mobilen Videokameras* im Kontext von öffentlichen Veranstaltungen oder Versammlungen. Über Einsatz und Form (per Hubschrauber, von Dächern, durch Stabkameras etc.) entscheidet die Einsatzleitung. Die Videobilder werden in Echtzeit an die Einsatzleitung übertragen oder aber gespeichert, um sie nach Veranstaltungsende auf mögliche Straftaten hin auszuwerten.

Zum Ausmaß der Videobeobachtung im öffentlich zugänglichen Raum durch *nichtpolizeiliche öffentliche Stellen* sowie durch *private Unternehmen und Personen* gibt es keine aktuellen Schätzungen. Die Zahl der eingesetzten Kameras dürfte sich aber im Millionenbereich bewegen. Die Einsatzformen sind äußerst vielfältig, sowohl in Bezug auf den Einsatzort (z. B. Verkehrsinfrastrukturen, öffentliche Gebäude und Einrichtungen, Einkaufszentren, Sport- und Vergnügungsstätten) als auch auf den Einsatzzweck (z. B. Zugangskontrolle, Sicherheit von Personen, Objektschutz, Diebstahlschutz, Beweissicherung, Kontrolle betrieblicher Abläufe, Analyse des Kundenverhaltens).

Ein zentrales Einsatzfeld ist der *öffentliche Personenverkehr*. Bahnhöfe und Fahrzeuge des *Nahverkehrs* sind oft bereits flächendeckend mit Kameras ausgestattet, wozu in Großstädten Tausende Kameras notwendig sind. Während in Fahrzeugen aufgenommene Videobilder zumeist temporär (z. B. für 48 Stunden) gespeichert werden, wird das Geschehen an Bahnhöfen in der Regel in Echtzeit anlassbezogen (z. B. bei Notrufen) oder anlasslos durch Videobeobachter ausgewertet, um eine schnelle Intervention zu ermöglichen. Der Personalaufwand für eine anlasslose Echtzeitauswertung ist jedoch so hoch, dass meist nur ein kleiner Ausschnitt des gesamten Verkehrsnetzes gleichzeitig beobachtet werden kann. Im *Fernverkehr* setzt die Deutsche Bahn AG aktuell rund 7.000 Videokameras an 1.000 Bahnhöfen ein. Die Videobilder werden durch Bahnmitarbeiter/innen und an großen Bahnhöfen auch durch Beamte der Bundespolizei in Echtzeit ausgewertet.

Stand der Forschung zur Wirksamkeit

Als Instrument der Kriminalitätsbekämpfung verfolgt die offene Videobeobachtung im öffentlich zugänglichen Raum drei wesentliche Zielsetzungen:

- Senkung der Kriminalitätsbelastung durch Prävention,
- Verbesserung der Strafverfolgung durch Beweissicherung,
- Steigerung des Sicherheitsempfindens.

Die *kriminalpräventive Wirkung* fußt auf dem Effekt der Abschreckung: Durch die Videoaufzeichnung erhöht sich für den potenziellen Täter die Wahrscheinlichkeit, durch die Strafverfolgungsbehörden ermittelt und für seine Taten zur Rechenschaft gezogen zu werden. Findet eine Echtzeitauswertung statt, besteht zusätzlich die Möglichkeit, Straftaten durch intervenierendes Handeln ggf. zu verhindern. Die kriminalpräventive Wirkung der offenen Videobeobachtung ist jedoch umstritten. Bisher durchgeführte wissenschaftliche Evaluationen (vor allem aus dem angelsächsischen Raum) zeigten teilweise widersprüchliche und oft hinter den Erwartungen liegende Ergebnisse. Eine Evaluation von 2018 der polizeilichen Videobeobachtung an gefährdeten Orten in Nordrhein-Westfalen bestätigt das heterogene Bild: Zu einer nennenswerten Reduktion des Kriminalitätsaufkommens kam es lediglich in Duisburg. In Essen und Köln ergaben sich allenfalls Tendenzen in diese Richtung und in Dortmund zeigte sich sogar ein gegenteiliger Effekt. Als Ursache werden unterschiedliche Implementierungen der polizeilichen Videobeobachtung an den verschiedenen Standorten vermutet.

Medienberichte, wonach Täter vor allem mithilfe von Videoaufzeichnungen (ggf. in Verbindung mit einer Öffentlichkeitsfahndung) ermittelt wurden, lassen zunächst auf einen hohen *Nutzen der Videobeobachtung für die Strafverfolgung* schließen. Ob es sich bei solchen Ermittlungserfolgen allerdings um die Regel oder eher um Ausnahmefälle handelt, ist schwierig zu bewerten. Der mögliche Nutzen hängt von vielen Faktoren ab (z. B. vom Einsatzkontext, von der Bildqualität und -menge, der praktischen Erfahrung der auswertenden Person). Entsprechend zeigten bisher durchgeführte Evaluationen (vor allem aus dem angelsächsischen Raum) auch hier ein uneinheitliches Bild. In Deutschland hatte die polizeiliche Videobeobachtung an gefährdeten Orten in Nordrhein-Westfalen an allen Standorten einen positiven Effekt auf die Aufklärungsquote. Zu beachten ist allerdings, dass an diesen Orten überdurchschnittlich viele Delikte auftreten und leistungsfähige Videotechnik durch geschulte Polizeibeamten eingesetzt wurde. Ob sich dieser positive Befund auf nichtpolizeiliche Einsatzformen bzw. auf andere Beobachtungsräume übertragen lässt, ist ungewiss und muss weiter untersucht werden.

Auch die *Wirkung der offenen Videobeobachtung auf das Sicherheitsempfinden* ist umstritten. Die Ergebnisse wissenschaftlicher Untersuchungen sprechen dafür, diesen Effekt nicht zu überschätzen. Demnach verstärkt die Videobeobachtung das Sicherheitsgefühl vor allem bei Menschen, die sich ohnehin bereits

sicher fühlen. Auch kann sie negative Stereotype noch verstärken bzw. implizieren, dass an einem bestimmten Ort überhaupt ein Sicherheitsproblem besteht. In Bevölkerungsumfragen gibt etwa die Hälfte der Befragten an, dass Videobeobachtung ihr Sicherheitsgefühl steigere. Anderen Faktoren wird allerdings eine deutlich höhere Bedeutung beigemessen, etwa einer ausreichenden Beleuchtung oder der Anwesenheit von (Sicherheits-)Personal. Falls keine Echtzeitauswertung stattfindet und folglich auch eine schnelle Intervention ausgeschlossen ist, wird ggf. eine Sicherheitserwartung erzeugt, der gar nicht entsprochen werden kann.

Nichtbildgebende Beobachtungstechnologien

Nichtbildgebende Beobachtungstechnologien haben vielfältige Anwendungspotenziale im zivilen Sicherheitsbereich.

Die *akustische Beobachtung* mithilfe von Mikrofonen spielt im polizeilichen Bereich eine wichtige Rolle. Zur Aufklärung von schweren Straftaten sind die Strafverfolgungsbehörden auf richterliche Anordnung hin befugt, Gespräche von Beschuldigten außerhalb von Wohnungen heimlich abzuhören. Abhörmaßnahmen innerhalb von Wohnungen greifen in die Unverletzlichkeit der Wohnung (Artikel 13 Grundgesetz – GG) ein und dürfen nur bei besonders schweren Straftaten erfolgen; sie werden im Schnitt in rund 8 Ermittlungsverfahren pro Jahr eingesetzt. Vergleichbare gefahrenabwehrrechtliche Befugnisse besitzen in ihren jeweiligen Aufgabenbereichen das Bundeskriminalamt, die Bundespolizei sowie die Landespolizeien. Eine wichtige nichtpolizeiliche Anwendung sind akustische Ortungsgeräte, die bei der Bundesanstalt Technisches Hilfswerk (THW) zur Suche nach verschütteten Personen eingesetzt werden. Die Geräte erlauben die Wahrnehmung von leisesten Geräuschen (Klopfen, Hilferufe etc.) innerhalb von Trümmern.

Die Detektion und Analyse von *gefährlichen chemischen, biologischen, radiologischen, nuklearen oder explosiven Stoffen* (CBRNE-Gefahrenstoffe) sind aus offensichtlichen Gründen von herausragender Bedeutung im zivilen Sicherheitsbereich. Hierfür wurde eine Fülle von Mess- und Analyseverfahren entwickelt. Von Nachteil ist allerdings, dass entsprechende Messgeräte in unmittelbare Nähe der verdächtigen Substanzen eingesetzt bzw. Stoffproben für die spätere Analyse genommen werden müssen, was die Einsatzkräfte gefährden kann. Zurzeit wird intensiv an der Entwicklung von Nachweisverfahren gearbeitet, die gefährliche Substanzen am Einsatzort aus einer sicheren Entfernung quasi in Echtzeit detektieren und analysieren können. So ist es durch Miniaturisierung bereits möglich, Messgeräte für chemische oder radiologische Gefahrenstoffe mithilfe ferngesteuerter unbenannter Trägersysteme (Roboter, Drohnen) in die Nähe der verdächtigen Substanzen zu transportieren. Im Vergleich dazu ist die Entwicklung von mobilen Sensorsystemen für biologische Gefahrenstoffe ungleich

schwieriger und befindet sich noch in einem frühen Stadium. Die Forschung und Entwicklung in diesem Feld wird auch durch die zivile Sicherheitsforschung des Bundes vorangetrieben.

Anwendungen von *Ortungstechnologien* wie GPS-Empfänger sind im polizeilichen Bereich die verdeckte Bestimmung des Aufenthaltsorts von verdächtigen Personen oder die elektronische Aufenthaltsüberwachung mittels Fußfesseln. Eine interessante nichtpolizeiliche Anwendung ist das Bioradar, das beim THW zur Ortung von Verschütteten angewendet wird. Hier gelangt die Radartechnik zur Detektion der Bewegungen eines Brustkorbs bei der Atmung oder eines schlagenden Herzens zum Einsatz.

Automatisierte Datenauswertung

Die automatisierte Verarbeitung von Sensordaten zur qualitativen Aufbereitung oder besseren Darstellung der Daten ist ein integraler Bestandteil vieler sensorbasierter Beobachtungstechnologien. An Bedeutung gewinnen jedoch zunehmend algorithmenbasierte Verfahren, deren Ziel darin besteht, den menschlichen Beobachter bei der Analyse und Interpretation der Daten zu unterstützen bzw. solche Aufgaben ganz auf die Beobachtungstechnologie zu übertragen.

Substanzielle Fortschritte konnten in den vergangenen Jahren insbesondere im Bereich der Bildanalyse erzielt werden. Dadurch eröffnen sich auch neue Anwendungsfelder im Bereich der zivilen Sicherheit. Ein Beispiel sind Systeme zum automatisierten Kfz-Kennzeichenabgleich, die bereits seit Mitte der 2000er Jahre durch die Polizeibehörden einiger Bundesländer eingesetzt werden. Aus der Sicherheitsperspektive von großem Interesse sind automatisierte Datenauswertungsverfahren vor allem im Kontext der Videobeobachtung, da die Bewältigung der stetig steigenden Masse an Videodaten durch menschliche Beobachter zunehmend an Grenzen stößt. Einfachere Situations- oder Verhaltensanalysen gehören bereits heute zum Funktionsumfang kommerzieller Videobeobachtungssysteme. Dazu zählen beispielsweise die automatisierte Raumüberwachung (befinden sich Personen in einem festgelegten Bereich?), die Personenzählung (z. B. im Kontext von Veranstaltungen) oder das Erkennen stehengelassener Gegenstände. Soweit bekannt werden solche Systeme im Rahmen der polizeilichen Videobeobachtung bislang noch nicht im Realbetrieb eingesetzt. Der mögliche Nutzen für polizeiliche Zwecke wird seit Juni 2019 im Rahmen des Pilotprojekts »Sicherheitsbahnhof Berlin Südkreuz« durch das Bundesministerium des Innern, für Bau und Heimat, die Bundespolizei, das Bundeskriminalamt und die Deutsche Bahn AG getestet. Zu den hier erprobten Funktionalitäten gehören u. a. die automatisierte Erkennung abgestellter Gegenstände oder liegender (hilfsbedürftiger) Personen.

Verfahren zur Analyse komplexer Verhaltensweisen befinden sich dagegen oft noch in einem frühen Forschungsstadium, allerdings handelt es sich hierbei um ein sehr dynamisches Forschungsfeld. Grundlage hierfür bilden Verhaltens-

modelle, anhand derer Bewegungsinformationen in normales bzw. atypisches Verhalten eingeteilt werden. Dies stellt eine sehr schwierige Aufgabe dar, da menschliches Verhalten enorm vielfältig und meist nicht vorhersehbar ist. Seit Ende 2018 wird ein solches System durch das Polizeipräsidium Mannheim an ausgewählten Kriminalitätsschwerpunkten erprobt.

Vertiefung: automatisierte Videobeobachtung am Beispiel der Gesichtserkennung

Ein weiteres Anwendungsfeld der automatisierten Datenauswertung im zivilen Sicherheitsbereich ist die algorithmenbasierte Gesichtserkennung. Sie wird in Deutschland für polizeiliche Zwecke aktuell im Rahmen der teilautomatisierten Grenzkontrolle (EasyPASS) oder als Hilfsmittel zur retrospektiven Auswertung von gespeichertem Foto- oder Videomaterial einschließlich der Identitätsfeststellung durch den Abgleich mit polizeilichen Lichtbilddatenbanken eingesetzt.

Ein künftiges Anwendungsfeld könnte die Personenfahndung in Echtzeit darstellen. Hierzu wird eine Videobeobachtungsanlage über ein Gesichtserkennungssystem mit einer Fahndungsdatenbank verknüpft. Erkennt das System eine gesuchte Person, wird der Videobeobachter alarmiert, der dann über die weiteren Maßnahmen entscheidet.

Leistungsfähigkeit aktueller Systeme

Gesichtserkennungssysteme arbeiten trotz großer Fortschritte nie fehlerfrei. Generell besteht eine Abhängigkeit zwischen Erkennungsfehlern und Fehlalarmen. Dabei gilt: Je kleiner die Rate der Erkennungsfehler, desto höher die Rate der Fehlalarme und umgekehrt. Wie dieses Verhältnis idealerweise eingestellt wird, hängt von der konkreten Einsatzsituation ab. Dazu ein fiktives Beispiel: Die Videobeobachtungsanlage eines Bahnhofs mit täglich 100.000 Passanten wird durch ein Gesichtserkennungssystem mit dem elektronischen Informationssystem der Polizei (INPOL-Z) verknüpft. Legt man für dieses Szenario die Leistungskennzahlen aktueller Gesichtserkennungssysteme zugrunde, würden bei einer Erkennungsrate von 90 % und einer Fehlalarmrate von 10 % die meisten der anwesenden gesuchten Personen korrekt erkannt werden, gleichzeitig aber würden täglich 10.000 Fehlalarme auftreten. Soll die Zahl der Fehlalarme auf einen noch handhabbaren Wert von ca. 30 pro Tag reduziert werden (Fehlalarmrate von 0,03 %), würde die Erkennungsrate aktueller Systeme auf 72 % sinken.

Unter realen Einsatzbedingungen sind weitere technische und praktische Herausforderungen zu berücksichtigen. Die Aufgabe der Gesichtserkennung in Videoströmen nimmt mit abnehmender Bildqualität, zunehmender Abweichung der Blickrichtung weg von der Kamera und dem Grad der Verdeckung von Gesichtern durch andere Personen, Gegenstände oder bauliche Strukturen an Schwierigkeit zu. Durch bessere Algorithmen, Videotechnik und die Herstellung

geeigneter Beobachtungsbedingungen lässt sich die Erkennungsleistung der Systeme in der Praxis zwar steigern, allerdings nicht beliebig. Denn das Verhalten der zu beobachtenden Personen ist nur schwer beeinflussbar. So könnten diese Personen versuchen, sich der Beobachtung aktiv zu entziehen, indem sie direkte Blicke in Kameras vermeiden oder Gesichtspartien verbergen (z. B. mittels Sonnenbrille oder Hut). Entscheidend für den Nutzen der Maßnahme ist aber die Frage, wie viele der gesuchten Personen die videobeobachteten Bereiche überhaupt betreten. Wählen diese im Wissen um die automatisierte Fahndung verstärkt andere Reiserouten, so nimmt auch die Zahl der Fahndungserfolge im Zeitverlauf ab.

Versuchsprojekte

Zur Personenfahndung in Echtzeit fanden in Deutschland bereits mehrere Versuchsprojekte statt, zuletzt von August 2017 bis Juli 2018 im Rahmen des Pilotprojekts »Sicherheitsbahnhof Berlin Südkreuz«. Auf Grundlage der gemessenen Leistungskennzahlen wurde im Abschlussbericht des Bundespolizeipräsidiums empfohlen, entsprechende Systeme an ausgewählten Bahnhöfen als Unterstützungsinstrument der polizeilichen Fahndung einzusetzen. Die Aussagekraft der erzielten Ergebnisse wurde jedoch teilweise angezweifelt. Einige Experten mutmaßen, dass diese Testergebnisse deshalb erzielt wurden, weil Referenz- und Testbilder am gleichen Ort entstanden waren und somit nicht auf reale Einsatzszenarien in anderen Umgebungen (bzw. mit Referenzbildern aus anderen Quellen) übertragbar seien. Kritisiert wurde außerdem, dass im Abschlussbericht rechtliche Probleme, Kostenfragen oder mögliche Risiken eines realen Einsatzes für unbeteiligte Passanten nicht angesprochen wurden.

Rechtliche Einschätzung

Zur Frage, ob sich die bestehenden Befugnisse zum Einsatz von Videobeobachtung auch auf den Einsatz von Gesichtserkennungssystemen zur nachgelagerten Auswertung des Videomaterials erstrecken, finden sich in der Literatur unterschiedliche Ansichten. Im Kontext einer Personenfahndung in Echtzeit wird jedoch überwiegend argumentiert, dass eine automatisierte gegenüber der manuellen Sichtung von Videodaten ein ganz anderes Auswertungsinstrument darstelle, das in seiner Eingriffsintensität weit über die konventionelle Videobeobachtung hinausgehen könne. Vor einem polizeilichen Einsatz solcher Systeme wären daher eigenständige Rechtsgrundlagen zu schaffen, die Anlass, Zweck und Grenzen der Anwendung klar regelten.

Internetbeobachtung und Ansätze der vorhersehenden Polizeiarbeit

Sicherheitsbehörden und Rettungsorganisationen sind darauf angewiesen, mit veränderten Kommunikationsmustern Schritt zu halten und insofern auch verlässlich über Aktivitäten und Trends im Internet und in den sozialen Medien informiert zu sein. Entsprechend findet die Beobachtung des Internets durch Behörden und Organisationen mit Sicherheitsaufgaben heute verstärkt statt.

Manuelle Internetbeobachtung

Einsatzformen und Zielsetzungen der Internetbeobachtung variieren in Abhängigkeit vom jeweiligen Aufgabenspektrum. Bei Polizeibehörden bereits gängige Praxis ist die manuelle Internetbeobachtung im Vorfeld und während Großveranstaltungen (z. B. bei Demonstrationen oder Risikospielen im Fußball), um lagerelevante Informationen für die Einsatzplanung und -durchführung zu gewinnen. Als Quellen dienen offen zugängliche Bereiche des Internets wie einschlägige Webseiten, Foren, Twitter-Meldungen oder Inhalte sonstiger sozialer Medien.

Aufgabenbedingt steht bei Landeskriminalämtern sowie dem Bundeskriminalamt die Beobachtung der Internetaktivitäten von verdächtigen Personen oder gewaltbereiten Gruppierungen im Vordergrund. Ziel ist die Generierung von Hinweisen auf bevorstehende oder auch bereits begangene Straftaten. Zudem soll die Analyse einschlägiger Internetinhalte und -diskurse zu einem besseren Verständnis von Entwicklungen und Phänomenen wie Links- und Rechtsradikalismus, Salafismus-Dschihadismus und anderen gewaltbereiten Szenen beitragen, indem Einblicke in Radikalisierungspfade und soziale Bedingungen von Gewalt gewonnen werden. Seit 2007 gibt es das Gemeinsame Internetzentrum (GIZ) des Bundeskriminalamts, der Nachrichtendienste des Bundes und der Generalbundesanwaltschaft, dessen Aufgabe vor allem darin besteht, islamistische Propaganda von jihadistischen Gruppierungen und Personen im Internet zu beobachten und im Hinblick auf sicherheitsrelevante Aspekte zu analysieren. Im Herbst 2019 kündigte u. a. das Bundeskriminalamt an, als Reaktion auf mehrere rechtsmotivierte Gewalttaten die Beobachtung rechtsextremistischer Aktivitäten im Internet zu verstärken.

Nutzergenerierte Internetinhalte können für Sicherheits- und Rettungskräfte schließlich auch im Falle von unerwartet eingetretenen Großschadenslagen, Katastrophen oder Terroranschlägen wichtige Informationsquellen sein. Dies gilt insbesondere dann, wenn betroffene Gebiete infolge von Infrastrukturschäden für die Einsatzkräfte schlecht zugänglich sind. Eine generelle Herausforderung stellt jedoch die Einschätzung der Qualität der so gewonnenen Informationen dar, da bei größeren Einsätzen oder Terrorlagen oftmals Gerüchte und Vermutungen im Internet verbreitet werden.

Soweit es sich bei der Internetbeobachtung lediglich um behördliche Recherchen in offenen, allgemein zugänglichen Internetquellen handelt, liegt gemäß Bundesverfassungsgericht kein Eingriff in das allgemeine Persönlichkeitsrecht vor. Entsprechende Maßnahmen bedürfen daher keiner speziellen Ermächtigungsgrundlage und können auf Generalklauseln gestützt werden.

Social Media Intelligence

Die wesentliche Herausforderung bei der manuellen Internetbeobachtung besteht in der Bewältigung und Interpretation der großen Datenmengen. Hilfe könnten hier Softwarelösungen im Rahmen der Social Media Intelligence (SOCMINT) bieten. Primäres Ziel ist, die notwendigen Schritte für die Beobachtung sozialer Medien (und anderer Internetquellen) softwaretechnisch zu unterstützen und dadurch effizienter zu machen. Weiteren Nutzen vor allem für die Früherkennung sicherheitsrelevanter Lagen versprechen sich Sicherheitsakteure von einer zunehmenden Automatisierung der Datenerfassung und -auswertung.

Aktuell verfügbare Softwarelösungen sind allerdings vor allem im Hinblick auf die (teil)automatisierte Datenerfassung und -auswertung noch nicht ausgereift. Sie unterstützen die Arbeit von Analysten bislang vor allem dadurch, dass vorgegebene Webinhalte automatisiert ausgelesen und beispielsweise Verbindungen zwischen Nutzern, Gruppen und Schlagwörtern sichtbar gemacht werden können. Eine Herausforderung stellen die große Heterogenität und Dynamik von Onlineinhalten dar, was die Entwicklung von robusten Softwareanwendungen wesentlich erschwert. An der Weiterentwicklung entsprechender Software und Analysemethoden wird derzeit (auch gefördert durch die zivile Sicherheitsforschung des Bundes) intensiv gearbeitet.

Dementsprechend steht auch die praktische Anwendung solcher Softwarelösungen noch ganz am Anfang. Soweit bekannt erfolgt die Internetbeobachtung durch Polizeibehörden in Deutschland meist noch manuell. Ein Vorreiter ist die hessische Landespolizei, die seit 2017 eine Software testet, die Informationen aus verschiedenen polizeilichen Datenbanken mit Daten aus sozialen Medien verknüpfen soll.

Im Gegensatz zur manuellen Internetbeobachtung wirft der Einsatz von Software des SOCMINT rechtliche Fragen auf. Gemäß Bundesverfassungsgericht liegt ein Eingriff in das Recht auf informationelle Selbstbestimmung vor, wenn im offenen Internet gewonnene Informationen systematisch erhoben und ausgewertet werden. Zudem kann durch Verknüpfung der Daten deren Aussagekraft unter Umständen in solch einem Maße gesteigert werden, dass eigenständige grundrechtliche Risiken für die betroffenen Personen geschaffen werden. In diesem Fall kann der Softwareeinsatz nicht mehr ohne weiteres auf allgemeine Befugnisse zur Verarbeitung personenbezogener Daten gestützt werden.

Ansätze der vorhersehenden Polizeiarbeit

Vorhersehende Polizeiarbeit (Predictive Policing) beschreibt die Anwendung softwarebasierter Methoden, die Wahrscheinlichkeitsaussagen über das zukünftige Auftreten bestimmter Kriminalitätsformen durch automatisierte Datenauswertung treffen. Die Prognosen sollen die polizeiliche Einsatzplanung unterstützen, den effektiven Ressourceneinsatz befördern und geeignete Präventionsstrategien ermöglichen. Weltweit (vor allem in den USA) werden zahlreiche verschiedene Systeme getestet und eingesetzt, die jeweils bestimmte Deliktbereiche adressieren und deren Prognosen auf unterschiedlichen kriminologischen Modellen und Datengrundlagen beruhen.

In Deutschland werden seit einiger Zeit entsprechende Softwarelösungen von verschiedenen Landeskriminalämtern getestet oder angewendet, wobei es sich um kommerzielle Produkte wie auch um Eigenentwicklungen handelt. Das Einsatzfeld ist bislang auf die Bekämpfung des Wohnungseinbruchsdiebstahls beschränkt. Hier basieren die Prognosen auf der Hypothese, dass im unmittelbaren Umfeld eines bereits erfolgten Einbruchs zeitnah mit Folgedelikten zu rechnen ist. In die Analysen fließen in der Regel nur nichtpersonenbezogene Daten (meist polizeiliche Falldaten) ein, lediglich eine Eigenentwicklung des Landeskriminalamts Nordrhein-Westfalen verwendet zusätzlich soziodemografische und gebäudespezifische Daten.

Der polizeiliche Nutzen des Einsatzes von Methoden der vorhersehenden Polizeiarbeit ist noch unklar. Bisher dazu in Deutschland durchgeführte Pilotprojekte zeigten, wenn überhaupt, nur moderate Rückgänge in der Zahl der Wohnungseinbrüche. Wirkungsnachweise sind allerdings schwierig zu führen. Zum Beispiel müssen potenzielle Effekte von zufälligen Schwankungen und externen Einflussfaktoren unterschieden werden. Zudem sind immer auch die an die Prognosen anknüpfenden polizeilichen Präventionsstrategien (z. B. eine erhöhte Streifentätigkeit) im Hinblick auf die Wirksamkeit zu bewerten sowie mögliche Auswirkungen auf die polizeiliche Einsatzpraxis zu analysieren. Hier besteht noch substanzieller Forschungsbedarf.

Die rechtliche Einordnung von Methoden der vorhersehenden Polizeiarbeit ist weitgehend ungelöst. Soweit nur nichtpersonenbezogene Daten einbezogen werden, wird in der Praxis davon ausgegangen, dass sich deren Einsatz außerhalb des grund- und fachrechtlichen Datenschutzes befindet und daher keiner besonderen gesetzlichen Ermächtigung bedarf. Komplexer Datenverarbeitung wohnt allerdings immer das Potenzial inne, dass aus nichtpersonenbezogenen Daten Informationen über einzelne Personen ableitbar sind. Außerdem könnten aus dem Einsatz Diskriminierungsrisiken entstehen, die einen grundrechtlichen Schutzbedarf anzeigen. Sobald auch personenbezogene Daten in die Analyse einfließen, liegt ein Eingriff in das Recht auf informationelle Selbstbestimmung vor, sodass sowohl die Datenerhebung als auch die Datenverarbeitung rechtfertigungs-

bedürftig werden. Welche verfassungsrechtlichen Maßstäbe (z. B. im Hinblick auf die Art der genutzten Daten und den Anlass für deren Verwendung) dieser Rechtfertigung zugrunde zu legen sind, ist bislang jedoch noch ungeklärt.

Informationstechnische Beobachtung

Die informationstechnische Beobachtung richtet sich auf Daten, die eine Person in der berechtigten Erwartung, dass sie vertraulich bleiben, einem informationstechnischen System anvertraut hat. Dazu gehören Inhalte und verbindungsbegleitende Metadaten der Telekommunikation (TK) wie auch sämtliche Daten, die eine Person auf ihren Endgeräten bewusst oder unbewusst speichert.

Informationstechnische Beobachtungsverfahren werden beinahe ausschließlich durch die Polizei- und Strafverfolgungsbehörden und hier in erster Linie zur *verdeckten* Informationsbeschaffung zu Zwecken der Strafverfolgung und Gefahrenabwehr eingesetzt (nachrichtendienstliche Einsatzfelder werden im Bericht nicht behandelt). Die Notwendigkeit dazu ergibt sich u. a. im Kontext der Cyberkriminalität, deren Bekämpfung ohne den Einsatz von informationstechnischen Beobachtungsverfahren kaum möglich ist. Zudem nutzen kriminelle Akteure für die Planung und Durchführung von Straftaten oft den neuesten Stand der Informations- und Kommunikationstechnik (IKT), sodass sich auch das polizeiliche Handeln danach ausrichten muss.

Die Möglichkeiten und Herausforderungen der informationstechnischen Beobachtung sind immer auch vor dem Hintergrund der enormen Dynamik im Bereich der IKT zu betrachten. Beschränkte sich die Fernkommunikation in Deutschland vor 30 Jahren noch weitgehend auf die durch ein staatliches Unternehmen betriebene analoge Sprachtelefonie, so existiert heute eine Vielzahl an funktional unterschiedlichen, vielfach internetbasierten IKT-Diensten, die auf stark fragmentierten und oft weltweit handelnden Anbieter- und Nutzergruppen basieren. Für Polizei- und Strafverfolgungsbehörden ist diese Entwicklung von großer Tragweite. Die im stark wachsenden Umfang anfallenden digitalen Daten können von erheblicher praktischer Bedeutung für die Sicherheitsarbeit sein, zugleich wird der Zugang zu diesen Daten über die meist privaten Diensteanbieter jedoch immer schwieriger.

Verfahren der informationstechnischen Beobachtung

Die unterschiedlichen Verfahren lassen sich danach kategorisieren, an welcher Stelle in der Netzarchitektur die Beobachtung der Daten stattfindet.

Beobachtung während des laufenden Übertragungsvorgangs im TK-Netz

Technisch am einfachsten setzt die Beobachtung beim Betreiber des zur Datenübertragung genutzten TK-Netzes an. Mithilfe standardisierter Schnittstellen wird eine Kopie des fraglichen Datenstroms (Inhalts- und Metadaten) angefertigt und an die nachfragende Polizeibehörde übergeben. Die Betreiber von TK-Netzen sind gesetzlich dazu verpflichtet, technische Einrichtungen zur Umsetzung solcher als Telekommunikationsüberwachung (TKÜ) bezeichneten Maßnahmen vorzuhalten. TKÜ-Maßnahmen beeinträchtigen die Vertraulichkeit der betroffenen Daten, nicht aber deren Integrität (die Daten werden nicht verändert) oder Verfügbarkeit.

Inhalts- und Metadaten der TK können auch ohne Mitwirkung der Netzbetreiber im TK-Netz beobachtet werden. Beim Mobilfunk beispielsweise können sich International-Mobile-Subscriber-Identity-(IMSI-)Catcher als Funkzelle ausgeben und heimlich zwischen Funkmast und Mobilfunkgerät geschalten werden. Je nach Funktionsumfang des Catchers ermöglicht dies die Ermittlung von Rufnummern, die Lokalisierung von Mobilfunkgeräten oder das Mitschneiden der Datenübertragung. Dabei können unter Umständen die Integrität (falls bei der Durchleitung des Funkverkehrs Fehler auftreten) und die Verfügbarkeit (falls der Catcher keine Verbindung zum Mobilfunknetz aufbaut) der betroffenen Daten bzw. Mobilfunkgeräte beeinträchtigt werden.

Beobachtung beim Diensteanbieter

Beim Diensteanbieter können hier ggf. gespeicherte (retrograde) oder in Echtzeit anfallende Inhalts- oder Metadaten erhoben werden. Ob Diensteanbieter *Inhaltsdaten* verarbeiten und (zumindest kurzfristig) speichern, hängt vom jeweiligen Dienst ab. Technisch notwendig ist dies bei zeitversetzten (asynchronen) Diensten wie SMS, E-Mail oder Instant-Messaging. Bei synchron ablaufenden Diensten (z. B. Sprachtelefonie) können die Inhalte auch unmittelbar unter den beteiligten Nutzern über das Internet ausgetauscht werden.

Metadaten werden im Gegensatz dazu immer vom Diensteanbieter verarbeitet und zum Teil (zumindest kurzfristig) auch gespeichert (z. B. für Abrechnungszwecke). Bei klassischen TK-Diensten (Telefondienste, SMS, Internetzugang) werden sie als Verkehrsdaten bezeichnet. Dazu zählen etwa Rufnummern, IP-Adressen oder bei der Mobilfunknutzung die Kennungen der verwendeten Funkzellen. Für Polizei- und Strafverfolgungsbehörden können Verkehrsdaten von hohem praktischem Nutzen sein und stellen bei Straftaten, die per Telefon oder Internet durchgeführt werden (z. B. Trickbetrug, Verbreitung von Kinderpornografie), oftmals die einzigen Ermittlungsansätze dar. In der polizeilichen Praxis haben sich folgende Formen der Verkehrsdatenerhebung herausgebildet:

- Die *individualisierte Verkehrsdatenerhebung* bezieht sich auf einen bestimmten Telefon-, Mobilfunk- oder Internetanschluss. Dies dient etwa der Ermittlung der Nutzer von illegalen Internetforen.
- Bei der *Funkzellenabfrage* werden die Verkehrsdaten aller während eines Zeitraums in einer bestimmten Funkzelle eingebuchten Mobilfunkgeräte erhoben. Dies dient etwa der Ermittlung von Personen, die sich zum Zeitpunkt einer Straftatbegehung in der Nähe des Tatorts aufgehalten haben.
- *Stille SMS* werden von der Zielperson unbemerkt auf ein Mobilfunkgerät verschickt, um Verkehrsdaten aktiv zu erzeugen. Dies ermöglicht beispielsweise die Erstellung von Bewegungsprofilen.

Mit der Vorratsdatenspeicherung werden Diensteanbieter gesetzlich dazu verpflichtet, Verkehrsdaten aller Nutzer für einen bestimmten Zeitraum zu speichern, um sie im Bedarfsfall den Strafverfolgungsbehörden zugänglich zu machen. Die Rechtmäßigkeit der Vorratsdatenspeicherung steht allerdings infrage, weswegen sie zurzeit nicht umgesetzt wird.

Beobachtung auf dem Endgerät

Während des Übergangsvorgangs oder beim Dienstanbieter erhobene Inhaltsdaten haben keinen ermittlungsrelevanten Nutzen, wenn sie verschlüsselt sind. Die Entschlüsselung ist angesichts der heute eingesetzten starken Verschlüsselungsverfahren nur mit einem enormen Zeit- und Ressourcenaufwand oder gar nicht zu leisten. Kommunikationsdienste wie WhatsApp, iMessage oder Facebook Messenger, die eine nutzerseitige Ende-zu-Ende-Verschlüsselung eingebaut haben oder optional anbieten, stellen die Polizei- und Strafverfolgungsbehörden zunehmend vor Probleme, da damit auch Straftäter/innen ihre elektronische Kommunikation wirksam schützen können. Eine Option, um staatlichen Stellen dennoch den Zugriff auf sicherheitsrelevante Kommunikationsinhalte zu ermöglichen, ist die Beobachtung der Daten vor dem Verschlüsselungsvorgang, also noch auf dem Endgerät der Zielperson. Da die Beobachtung an der Quelle der Telekommunikation ansetzt, hat sich die Bezeichnung Quellen-TKÜ etabliert.

Auch die Verschlüsselung von Datenträgern stellt Polizei- und Strafverfolgungsbehörden zunehmend vor Herausforderungen, da beschlagnahmte Endgeräte oft nicht mehr ausgewertet werden können. Die informationstechnische Beobachtung bietet eine Möglichkeit, um bereits vor der Beschlagnahmung heimlich auf die dann ggf. noch unverschlüsselten Daten im Endgerät zuzugreifen. Solche Maßnahmen werden als Onlinedurchsuchung bezeichnet.

Maßnahmen der Quellen-TKÜ oder Onlinedurchsuchung setzen die heimliche Installation einer Beobachtungssoftware auf dem Zielgerät voraus, welche die ermittlungsrelevanten Daten sammelt und an die Polizeibehörden ausleitet. Deren Durchführung ist technisch äußert komplex und mit Risiken für die IT-Sicherheit verbunden, insbesondere dann, wenn zur Installation der Beob-

achtungssoftware Schwachstellen in der auf dem Zielgerät installierten Software ausgenutzt werden. Die Sorge besteht, dass hierfür Zero-Day-Schwachstellen eingesetzt werden könnten, die dem Softwarehersteller noch nicht bekannt sind. Deren Vorteil liegt aus Sicht der Polizeibehörden darin, dass sie über längere Zeit bestehen und damit nutzbar bleiben. Entsteht daraus aber ein Anreiz, die Existenz von Schwachstellen den Herstellern vorzuenthalten, wäre dies zwingend mit hohen Risiken für die IT-Sicherheit verbunden.

Zur Installation der Beobachtungssoftware genügt im Prinzip auch eine vom Hersteller bereits behobene, aber auf dem Zielgerät noch nicht durch ein Softwareupdate geschlossene Schwachstelle. Im Sinne eines Ausgleichs zwischen den Interessen der Gefahrenabwehr und Strafverfolgung einerseits und der IT-Sicherheit andererseits könnte es ein Ansatz sein, die Nutzung von Softwareschwachstellen mit hohem Gefährdungspotenzial für die IT-Sicherheit per Gesetz auszuschließen. Dies würde die Durchführung entsprechender Beobachtungsmaßnahmen zwar erschweren, nicht aber verunmöglichen.

Eingriffsrechtliche Anforderungen

Informationstechnische Beobachtungsverfahren berühren die rechtlich hochgradig sensiblen Felder der grundrechtlichen Privatheitsgarantien. Jeder staatliche Einsatz bedarf daher bestimmter und normenklarer Ermächtigungsgrundlagen, die dem Gewicht des jeweiligen Grundrechtseingriffs Rechnung tragen. An die Durchführung der Maßnahmen werden daher in Anhängigkeit von den betroffenen Grundrechten und der jeweiligen Eingriffstiefe unterschiedlich hohe verfassungsrechtliche Anforderungen gestellt, die im Eingriffsrecht (Strafprozess- und Polizeirecht) konkretisiert sind. Dazu gehören u. a.:

- ein Richtervorbehalt;
- die Abstufung der Eingriffsschwellen je nach Eingriffsintensität der Maßnahme, so etwa bezüglich der Schwere der Straftat (strafprozessual) oder der Gefahrenschwelle (gefahrenabwehrrechtlich);
- Pflichten zur nachträglichen Benachrichtigung von Betroffenen sowie Löschpflichten für erlangte personenbezogene Daten;
- ein Ultima-Ratio-Prinzip für besonders eingriffsintensive Maßnahmen;
- Vorschriften zum Schutz des Kernbereichs privater Lebensgestaltung bei der TKÜ, der Quellen-TKÜ und der Onlinedurchsuchung.

Die Auslegung und die konkrete praktische Anwendung der Eingriffsnormen werfen diverse rechtliche Fragen auf, die im Bericht behandelt werden. Beispielsweise stellt die Behandlung von Kommunikationsdiensten, wie E-Mail oder Instant-Messaging-Dienste, ein noch weitgehend ungelöstes Problem dar. In der Praxis bereitet auch die Abgrenzung zwischen Maßnahmen der Quellen-TKÜ und der Onlinedurchsuchung einige Schwierigkeiten.

Aktuelle Einsatzpraktiken

Öffentlich zugängliche Informationen zur Einsatzpraxis von informationstechnischen Beobachtungsverfahren durch Polizei- und Strafverfolgungsbehörden liegen bis dato nur sehr spärlich vor. Dies gilt für den Bereich der Strafverfolgung, vor allem aber für den Bereich der polizeilichen Gefahrenabwehr.

Anwendungshäufigkeit

In Bezug auf die Anwendungshäufigkeit öffentlich gut dokumentiert sind lediglich der strafprozessuale Einsatz der TKÜ und der individualisierten Verkehrsdatenerhebung, für die es bundesweit gesetzliche Berichtspflichten gibt. Die auf dieser Datenbasis erstellten Übersichten werden seit 2000 für TKÜ-Maßnahmen und seit 2008 für Maßnahmen der Verkehrsdatenerhebung jährlich durch das Bundesamt für Justiz veröffentlicht. Die Anzahl der in Bund und Ländern jährlich angeordneten TKÜ-Maßnahmen erreichte zwischen 2012 und 2014 mit rd. 23.000 Erst- und Verlängerungsanordnungen ein Maximum und nimmt seither tendenziell wieder leicht ab. Auch die Zahl der Ermittlungsverfahren, die davon Gebrauch machten, blieb zwischen 2008 und 2019 vergleichsweise stabil im Bereich von jährlich 5.100 bis 5.900. Daran gemessen werden TKÜ-Maßnahmen nicht häufiger und – im Vergleich zur Gesamtzahl an Ermittlungsverfahren (rd. 5,2 Mio. pro Jahr) – auch eher selten eingesetzt. Im Gegensatz dazu hat sich die Zahl der Ermittlungsverfahren mit Verkehrsdatenerhebung zwischen 2010 und 2019 um 50 % auf knapp über 10.000 Verfahren erhöht (wenngleich seit 2016 auch wieder eine rückläufige Tendenz erkennbar ist). Dies lässt auf eine steigende Bedeutung von Verkehrsdaten für die Strafverfolgung schließen.

Gesonderte Berichtspflichten für strafprozessuale Maßnahmen der TKÜ, Quellen-TKÜ und Onlinedurchsuchung sowie eine Differenzierung der Verkehrsdatenerhebung nach individualisierten Maßnahmen oder Funkzellenabfragen wurden erst mit den Reformen der Strafprozessordnung von 2015 und 2017 verankert. Im Bereich der Gefahrenabwehr wurden ähnliche Berichtspflichten für das Bundeskriminalamt im Zuge der Reform des Bundeskriminalamtsgesetzes von 2017 eingeführt. Die bisher vorliegenden Informationen erlauben noch keine verlässlichen Abschätzungen zur Entwicklung der Anwendungshäufigkeiten.

Da entsprechende amtliche Statistiken bisher (weitgehend) fehlten, wurden für den vorliegenden Bericht verfügbare Informationen aus Parlamentsdokumenten und anderen öffentlichen Quellen zusammengetragen. Allerdings erlauben diese oftmals nur fragmentarische Einblicke in die polizeiliche Einsatzpraxis. Zum Beispiel stuft die Bundesregierung diesbezügliche Auskünfte teilweise als Verschlusssache ein.

Nutzen der Maßnahmen für die Strafverfolgung oder Gefahrenabwehr

In noch geringerem Maße als Angaben zur Anwendungshäufigkeit finden sich Hinweise zur konkreten Durchführung von informationstechnischen Beobachtungsmaßnahmen in der polizeilichen Praxis oder belastbare Informationen zu ihrem Nutzen für die Strafverfolgung oder die polizeiliche Gefahrenabwehr.

Systematische empirische Nutzenuntersuchungen liegen lediglich für strafprozessuale Maßnahmen der TKÜ und der Verkehrsdatenerhebung vor. Im Ergebnis wurde die TKÜ insgesamt als wichtiges und unabdingbares Ermittlungsinstrument eingeschätzt, das vor allem im Bereich der Transaktionskriminalität (kriminelles Verhalten, das sich durch Kommunikation, Handel und Organisation auszeichnet und/oder gewerbs- bzw. bandenmäßig begangen wird) Erfolge erzielt. Die Verkehrsdatenerhebung wurde hingegen als ein nur bedingt erfolgreiches Ermittlungsinstrument bewertet, da die damit verfolgten Ermittlungsziele in rund zwei Dritteln der Fälle nicht erreicht werden konnten. Waren die Maßnahmen allerdings erfolgreich, so konnten wichtige Hinweise erlangt werden. Allerdings handelt es sich hierbei um ältere Untersuchungen. Angesichts des sich kontinuierlich stark ändernden Kommunikationsverhaltens und -aufkommens wären aktuelle Nutzenuntersuchungen dringend notwendig.

Zum Nutzen der anderen informationstechnischen Beobachtungsverfahren für die Strafverfolgung oder die polizeiliche Gefahrenabwehr finden sich keine aussagekräftigen (öffentlich zugänglichen) Aussagen oder Untersuchungen. Die Bundesregierung beispielsweise erachtet ihren Einsatz zwar grundsätzlich als wesentlich, eine darüberhinausgehende Nutzenbewertung sei jedoch in der Regel nicht möglich, da es von Fall zu Fall unterschiedlich sei, welche Maßnahmen zur Aufklärung einer Straftat oder zur Abwehr einer Gefahr beigetragen haben. Dieser Aussage ist nur bedingt zuzustimmen: Wie zuvor erwähnte Untersuchungen zeigten, sind Wirkungsnachweise für einzelne Maßnahmen methodisch zwar komplex, aber durchaus möglich.

Grundlegende regulatorische Fragestellungen

Der Einsatz von Beobachtungstechnologien im zivilen Sicherheitsbereich wirft eine Reihe von grundlegenden regulatorischen Fragestellungen auf. Es handelt sich dabei um neue, teilweise aber auch um bereits bekannte Fragen, die sich infolge des technischen und sozialen Wandels heute verschärft oder anders akzentuiert stellen. Der Bericht greift wichtige Fragestellungen exemplarisch auf. Eine vollständige systematische Erörterung ist aufgrund der Komplexität der rechtlichen Materie nicht möglich.

Vor allem komplexe Beobachtungstechnologien, die die Telekommunikation zum Gegenstand haben oder Methoden der automatisierten Datenauswertung

einsetzen, fordern das bestehende Verfassungs-, Eingriffs- und Datenschutzrecht heraus. Im Folgenden wird dies jeweils an einem Beispiel illustriert.

Verfassungsrecht

Das Grundgesetz schützt die kommunikative Privatheit durch verschiedene Gewährleistungen. Das *Fernmeldegeheimnis* hebt den grundrechtlichen Schutz der Telekommunikation besonders hervor und knüpft staatliche Eingriffe an hohe verfassungsrechtliche Hürden. Einen noch höheren Schutzbedarf markiert das *Grundrecht auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, das persönliche Daten, die in informationstechnischen Systemen verarbeitet oder gespeichert werden, vor staatlichen Zugriffen schützt. Das *Grundrecht auf informationelle Selbstbestimmung*, das dem Einzelnen die Kontrolle über seine personenbezogenen Daten zusichert, bietet hingegen ein vergleichsweise niedriges Schutzniveau.

Der differenzierte Schutzansatz setzt voraus, dass sich die unterschiedlichen Gewährleistungen der Privatheit klar voneinander abgrenzen lassen. Gerade im Kontext moderner Formen der Telekommunikation bereitet dies jedoch zunehmend Schwierigkeiten. So schützt das Fernmeldegeheimnis nach gängiger Doktrin nur die *laufende* Telekommunikation. Während aber die Zuordnung in laufende Vorgänge für hergebrachte Formen der Telekommunikation problemlos möglich ist (ein Telefongespräch beginnt, wenn ein Anruf angenommen wird, und endet, sobald ein Teilnehmer das Gespräch beendet), gilt dies für moderne Kommunikationsdienste wie E-Mail oder Instant-Messaging nicht mehr. Dies führt etwa dazu, dass der Inhalt ein und derselben E-Mail mal stärker, mal schwächer vor staatlichen Zugriffen geschützt wird, je nachdem, ob die E-Mail gerade übertragen wird (hier greift das Fernmeldegeheimnis) oder sich auf dem Endgerät des Empfängers befindet, wo entweder *nur* das niedrige Schutzniveau des Grundrechts auf informationelle Selbstbestimmung (beim Zugriff im Rahmen einer Beschlagnahme) oder das hohe Schutzniveau des Grundrechts auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (beim Zugriff durch eine Onlinedurchsuchung) besteht. Solche Zuordnungs- und Bewertungsprobleme werfen die grundlegende Frage auf, ob der grundrechtliche Schutz der kommunikativen Privatheit ggf. neu zu konzipieren wäre, indem nach technisch und sozial anschlussfähigeren und normativ überzeugenderen Kriterien für die Sensibilität digitaler Inhalte gesucht wird. Bislang fehlt es hierzu jedoch weitgehend an konzeptionellen Vorarbeiten.

Eingriffsrecht (Strafprozess- und Polizeirecht)

Einer kritischen Evaluation bedarf das Eingriffsrecht beispielsweise hinsichtlich des Einsatzes von Beobachtungstechnologien mit automatisierter Datenauswertung. Während sowohl die Polizeigesetze als auch die Strafprozessordnung

zahlreiche und detaillierte Regelungen zur Erhebung und Speicherung von Informationen enthalten, umfassen sie nur wenige Regelungen bezüglich der Auswertung der erhobenen Informationen. Problematisch wird dies, wenn der durch die Datenerhebung gegebene Grundrechtseingriff durch die Datenauswertung erheblich intensiviert wird. In diesem Fall kann die nachgelagerte Auswertung des erhobenen Materials nicht mehr *nur* als logische Folge der Datenerhebung betrachtet werden, die auf die gesetzliche Ermächtigung zu dieser Erhebung gestützt werden könnte.

Es stellt sich die grundlegende Frage, unter welchen Voraussetzungen es ggf. spezieller Ermächtigungsgrundlagen für die nachträgliche Auswertung der erhobenen Daten bedarf. Wird dies grundsätzlich bejaht, müssten die zu schaffenden Regelungen die automatisierte Datenauswertung in sinnvollem Ausmaß ermöglichen und zugleich angemessen begrenzen können. Zudem müsste ein rechtsverträglicher Umgang mit möglichen Fehlern der automatisierten Datenauswertung entwickelt werden. Die Diskussion hierzu steht allerdings noch am Anfang.

Datenschutzrecht

Ein grundsätzliches Problemfeld des hergebrachten Datenschutzrechts ist dessen starre Grenze: Die Verarbeitung personenbezogener Daten unterliegt grundsätzlich vollständig der datenschutzrechtlichen Regulierung, die Verarbeitung nichtpersonenbezogener Daten überhaupt nicht. Der Personenbezug von Daten ist bei Beobachtungstechnologien allerdings oftmals sehr schwierig zu beurteilen. Einerseits ermöglichen es komplexe Datenverarbeitungsverfahren zunehmend, Daten auf einzelne Personen zu beziehen, die früher als anonym gegolten hätten. Zum Beispiel verarbeiten aktuelle Formen der vorhersehenden Polizeiarbeit nur vermeintlich nichtpersonenbezogene Daten. Es scheint aber plausibel, dass in vielen Anwendungsfällen ein Personenbezug durch Hinzuziehen weiterer Informationen aus öffentlichen und nichtöffentlichen Quellen prinzipiell hergestellt werden könnte. Andererseits könnte ein zu weites Verständnis des Personenbezugs den Einsatz von Beobachtungstechnologien ggf. auch unnötig behindern. Beispielsweise lassen sich Geodaten mit entsprechendem Zusatzwissen vielfach auf natürliche Personen zurückführen (z. B. Eigentümer bestimmter Grundstücke). Müssten aber etwa Rettungsorganisationen vor jeder Verarbeitung von Geodaten (z. B. Anfertigung von Luftbildkarten zur Gefährdungskartierung) alle potenziell identifizierbaren Personen benachrichtigen, würde dies die Verarbeitungen solcher Daten massiv erschweren.

In jüngerer Zeit wird daher vermehrt diskutiert, ob der gegenwärtige Grundansatz des Datenschutzrechts (Verbotsprinzip) durch einen neuen Ansatz ersetzt werden sollte, der von den Risiken einer Datenverarbeitung ausgeht. Eine systematische Untersuchung dieser Frage steht allerdings noch aus.

Gesellschaftliche Auswirkungen technisierter Beobachtung

Der Einsatz von Beobachtungstechnologien im Bereich der zivilen Sicherheit ist immer mit gesellschaftlichen Auswirkungen verbunden. Zu den intendierten Wirkungen der jeweiligen Beobachtungspraxis (z. B. die erhoffte abschreckende Wirkung auf potenzielle Straftäter/innen) kommen mögliche unerwünschte psychische und soziale Wirkungen auf Personen, die selbst keinen Anlass für die Beobachtung gegeben haben (z. B. Einschüchterungseffekte). Zu beachten sind darüber hinaus potenzielle Auswirkungen auf die Technologieanwender, also die Sicherheitsakteure und deren Institutionen. In den Debatten um den Einsatz von Beobachtungstechnologien durch Polizeibehörden schließlich bildet das schwierige Spannungsverhältnis zwischen den Werten der Sicherheit und der Freiheit eine herausragende Rolle.

Psychische und soziale Wirkungen

Intuitiv erscheint es naheliegend, dass das Wissen, beobachtet zu werden, sich auf die Psyche und das Verhalten der beobachteten Personen auswirkt. Ein wissenschaftlicher Nachweis solcher möglichen Effekte ist jedoch schwierig. Das Phänomen der Beobachtung ist im gesellschaftlichen Kontext sehr komplex, da auch die mit der Beobachtung verfolgten Zwecke und die Einstellung der Beobachteten zu der beobachtenden Instanz eine wichtige Rolle spielen. Zusätzliche methodische Herausforderung resultieren aus den Beobachtungspraktiken, die ohne Wissen der Beobachteten stattfinden, also beispielsweise Formen der polizeilichen Internet- oder informationstechnischen Beobachtung. Potenziell betroffene Personen können hier kaum nachvollziehen, ob, wann und durch wen sie beobachtet werden – im Bewusstsein bleibt einzig die Möglichkeit, dass man beobachtet werden *könnte*.

Verhältnismäßig gut erforscht sind einzig mögliche psychische Auswirkungen der offenen Videobeobachtung. Demnach kann Videobeobachtung zu einer gesteigerten und ggf. als unangenehm empfundenen Selbstaufmerksamkeit führen. Zudem sind Verhaltensmodifikationen in Form der Vermeidung beobachteter Räume möglich. Der gegenwärtige Forschungsstand legt jedoch auch nahe, diese Wirkungen nicht zu überschätzen. So entstehen Einschüchterungseffekte vermutlich nicht isoliert, sondern nur, wenn zur Beobachtung weitere Faktoren hinzukommen, beispielsweise die Androhung von Sanktionen. Darüber hinaus scheinen sich vergleichsweise schnell Gewöhnungseffekte einzustellen.

Die psychischen und sozialen Auswirkungen der Internet- und/oder informationstechnischen Beobachtung sind bis dato nur unzureichend erforscht. Das mögliche Ausmaß staatlicher Beobachtung im Internet und in der elektronischen Kommunikation ist vor allem durch die Aufdeckung der Aktivitäten einiger Nachrichtendienste der USA und weiterer Staaten durch Edward Snowden im

Jahr 2013 ins Bewusstsein der Öffentlichkeit gedrungen. Entgegen der (damaligen) allgemeinen Empörung darüber haben Befragungen in Deutschland und anderen Staaten gezeigt, dass – zumindest in der eigenen Wahrnehmung – nur ein kleiner Teil der Internetnutzer ihr Onlineverhalten als Reaktion darauf veränderte. Dies kann ggf. darauf zurückgeführt werden, dass ein Teil der Nutzer bereits vor den Enthüllungen umsichtig gehandelt hatte. Eine mögliche Erklärung ist aber auch, dass der Umgang mit staatlichen Beobachtungspraktiken von einer gewissen Passivität und Gleichgültigkeit geleitet ist (oder nach dem Motto »ich habe nichts zu verbergen« oder »für meine Daten interessiert sich der Staat nicht« toleriert werden).

Neben solchen Umfragen, die immer nur subjektive Wahrnehmungen abbilden können, zeigen einige Studien auf Grundlage objektiv messbarer Verhaltensänderungen klare Anhaltspunkte für Chillingeffekte, also für Verhaltensanpassungen oder Einschränkungen der eigenen Handlungen als Folge staatlicher Beobachtung im Internet oder in der elektronischen Kommunikation. Zum Beispiel ließ sich in der Folge der Snowden-Enthüllungen ein Rückgang von Suchanfragen im Internet nach bestimmten politisch oder persönlich sensiblen Begriffen nachweisen. Fraglich bleibt allerdings, ob diese Befunde, die fast ausschließlich im Kontext der Beobachtungspraktiken durch (ausländische) Nachrichtendienste erzielt wurden, sich auch auf polizeiliche Beobachtungspraktiken (in Deutschland) übertragen lassen. Gleichzeitig weisen selbst breit rezipierte Studien oft methodische und konzeptionelle Schwächen auf und generell ist die Forschungslage hinsichtlich ihrer Befunde nicht eindeutig. Auch gibt es empirische Hinweise auf inverse Chillingeffekte, etwa in Form einer gesteigerten Bereitschaft zur Regierungskritik trotz staatlicher Beobachtung.

Es besteht daher noch großer Forschungsbedarf, um die genauen Mechanismen der psychischen Auswirkungen technisierter Beobachtung auf individueller Ebene besser zu verstehen.

Auswirkungen auf Technologieanwender und deren Institutionen

Mögliche Auswirkungen des Einsatzes von Beobachtungstechnologien auf die sie benutzenden Sicherheitsakteure wurden bisher kaum wissenschaftlich erforscht. Sie spielen auch in politischen und öffentlichen Diskursen nur eine untergeordnete Rolle. Dabei zeigt sich in anderen Sicherheitskontexten, dass unerwünschte Wirkungen auf die Technologieanwender das Ziel einer Steigerung von Sicherheit durch Technisierung unter Umständen konterkarieren können.

Aus der Luftfahrt bekannt ist beispielsweise der Complacency-Effekt, der als vom Vertrauen in die Technik überzeugtes Zurücklehnen beschrieben werden kann. Ein übersteigertes Vertrauen in die Funktions- und Leistungsfähigkeit von Sicherheitstechnik ist unerwünscht, da es zu Nachlässigkeit und zur Abnahme des Situationsbewusstseins bei den Anwender/innen führen kann (»Das System

wird mich schon alarmieren, wenn etwas los ist«). Auch Beobachtungstechnologien wird teilweise eine technische Überlegenheit gegenüber menschlichen Beobachtern attestiert, beispielsweise im Kontext der vorhersehenden Polizeiarbeit in Bezug auf das Auffinden neuer, für den Menschen nicht erkennbarer Zusammenhänge in großen Datenmengen. Verlieren Technologieanwender das Bewusstsein für die Grenzen und Limitationen von Beobachtungstechnologien, kann dies aber dazu führen, dass technikbasierte Handlungsempfehlungen akzeptiert werden, ohne sie durch Hinzuziehen anderer Informationsquellen auf ihre Richtigkeit hin zu überprüfen, oder dass sicherheitsrelevante Situationen, die von der Technologie nicht erkannt wurden, auch vom Menschen übersehen werden.

Führt der Einsatz von Beobachtungstechnologien dazu, dass immer mehr Aspekte der Beobachtungs- bzw. Sicherheitsarbeit an technische Systeme abgegebenen werden, während der aktiv handelnde Sicherheitsakteur auf die Aufgabe der Überprüfung von Systemmeldungen verwiesen wird, kann sich dies negativ auf seine Arbeitsmotivation und -leistung auswirken. Zugleich würde dies den Aufbau und Erhalt wichtiger menschlicher Fähigkeiten und Kompetenzen im Sicherheitsbereich beeinträchtigen, die dann ggf. nicht mehr in ausreichendem Maße zur Verfügung stehen, wenn außergewöhnliche Umstände dies erfordern. In diesem Kontext anzuführen wäre beispielweise eine Videobeobachtung in Verbindung mit Gesichtserkennungssystemen zur Personenfahndung in Echtzeit, wie sie künftig an Bahnhöfen zum Einsatz kommen könnte. Da solche Systeme nicht fehlerfrei arbeiten, müssten alle Treffermeldungen durch menschliche Videobeobachter validiert werden. Je nach Anzahl der Fehlalarme könnte diese Aufgabe dauerhaft einen großen Teil der Arbeitszeit von Videobeobachtern in Anspruch nehmen. Auch würden Videobeobachter kaum mehr dieselbe Erfahrung und Intuition für die Erkennung gesuchter Personen oder sicherheitskritischer Situationen aufbauen können, wie dies bei der konventionellen Videobeobachtung möglich und erforderlich ist.

Es sind auch mögliche (negative) Auswirkungen des Technologieeinsatzes auf die Arbeitsprozesse und Organisationsstrukturen in den Blick zu nehmen. Zum Beispiel kann die Erhöhung der Informationsdichte durch luftgestützte Videokamerasysteme die Bewältigung schwieriger Einsatzlagen maßgeblich unterstützen. Die Kehrseite ist jedoch, dass Einsatzleitungen auch immer mehr Informationen zu verarbeiten haben sowie Abstimmungs- und Personalbedarfe zunehmen.

Die Beispiele verdeutlichen, dass der Einsatz von Beobachtungstechnologien in Bezug auf mögliche Auswirkungen auf die Technologieanwender und deren Institutionen vor allem dann zu problematisieren ist, wenn zuverlässig funktionierende Prozesse beeinträchtigt, Fähigkeiten und Erfahrungswissen der Sicherheitsakteure verdrängt oder die motivationalen Voraussetzungen des menschlichen Sicherheitshandeln (negativ) verändert werden. Diesbezüglich sind im Besonderen komplexe Beobachtungstechnologien mit automatisierter Datenaus-

wertung kritisch zu reflektieren. Dies spricht aber nicht generell gegen ihre Einführung und Nutzung. Vielmehr sollten bei Entscheidungen über deren (künftige) Anwendung nicht nur technologische Effizienzkriterien und mögliche Auswirkungen auf die beobachteten Personen betrachtet, sondern auch mögliche Effekte auf die sie benutzenden Sicherheitsakteure adäquat einbezogen werden. Dazu ist es notwendig, Wissen über solche Effekte zu generieren.

Spannungsverhältnis zwischen Sicherheit und Freiheit

Die Herstellung von Sicherheit kann mit Eingriffen in individuelle Freiheitsrechte verbunden sein. Die Verantwortung, staatliches Sicherheitshandeln in ein ausgewogenes Verhältnis von Sicherheit und Freiheit zu bringen, fällt vorrangig dem Gesetzgeber zu, der die hierfür notwendigen gesetzlichen Eingriffsbefugnisse zu schaffen hat. Ein zentrales Instrument hierzu bildet der Grundsatz der Verhältnismäßigkeit, der verlangt, dass der Staat mit jedem Grundrechtseingriff einen legitimen Zweck mit geeigneten, erforderlichen und angemessenen Mitteln verfolgt. Er ist aber nicht nur Verpflichtung, sondern gibt dem Gesetzgeber zugleich ein methodisches Prozedere und Prüfkriterien an die Hand, wie Sicherheit und Freiheit abgewogen werden können, um über die verfassungsrechtliche Konformität staatlicher Sicherheitspraktiken zu entscheiden. Im Kontext polizeilicher Beobachtungsmaßnahmen zu Zwecken der Gefahrenabwehr und Strafverfolgung zeigt sich jedoch, dass diese Prüfkriterien – zumindest nach bisheriger Anwendungspraxis – zum Teil zu vage sind, um über die Verhältnismäßigkeit der Maßnahmen auch nach gesellschaftlichen (z. B. ethischen) Bewertungsmaßstäben entscheiden zu können.

So gilt z. B. ein Mittel im verfassungsrechtlichen Sinne als geeignet, wenn mit seiner Hilfe der gewünschte Erfolg gefördert werden kann. Dabei muss der erstrebte Erfolg nicht in jedem Einzelfall erreicht werden oder erreichbar sein, die abstrakte Möglichkeit der Zweckerreichung genügt. Diese Voraussetzung aber erfüllen polizeiliche Beobachtungsmaßnahmen zumeist quasi automatisch: Solange die technisch-funktionale Leistungsfähigkeit der jeweiligen Beobachtungstechnologie gegeben bzw. nachzuweisen ist, bestehen kaum Zweifel, dass durch ihren Einsatz das verfolgte Ziel zumindest *potenziell* bzw. *in Einzelfällen* erreicht werden kann. Der tatsächliche praktische Nutzen von polizeilichen Beobachtungsmaßnahmen für die Kriminalitätsbekämpfung hängt in den allermeisten Fällen jedoch nicht nur von technisch-funktionalen Kriterien ab, sondern etwa auch von den konkreten sozialen Anwendungskontexten oder von möglichen Effekten und Folgen der Beobachtung auf das Verhalten der beobachteten Personen oder auf die bestehenden polizeilichen Einsatzpraktiken.

Schwierigkeiten bereitet zudem beispielsweise auch die Bestimmung der in der Verhältnismäßigkeitsprüfung zu berücksichtigenden Grundrechtswirkungen. Polizeiliche Beobachtungsmaßnahmen werden in aktuellen Debatten vor allem

im Hinblick auf mögliche Eingriffe in grundrechtlich geschützte Privatheitsgarantien problematisiert. Diese Fokussierung birgt aber unter Umständen die Gefahr, dass Beobachtungspraktiken schon als angemessen betrachtet werden, sobald daraus resultierenden Schutzbedarfen ausreichend Rechnung getragen wurde (z. B. durch Vorkehrungen zum Datenschutz). Polizeiliche Beobachtungsmaßnahmen können aber weitere Grundrechte berühren (z. B. grundrechtliche Diskriminierungsverbote), durch deren Berücksichtigung das Ergebnis der Verhältnismäßigkeitsprüfung sich ggf. anders darstellt.

Diese Beispiele verdeutlichen, dass polizeiliche Beobachtungsmaßnahmen, die im verfassungsrechtlichen Sinne als verhältnismäßig gelten, diese Anforderung nicht notwendigerweise auch nach anderen (z. B. ethischen) Bewertungsdimensionen erfüllen. Hier ergeben sich für den Gesetzgeber Gestaltungsoptionen für eine Erweiterung der Verhältnismäßigkeitsprüfung.

Gestaltungsoptionen

Bei Überlegungen und Entscheidungen zur Entwicklung, zur Implementierung oder zum Einsatz von Beobachtungstechnologien im Bereich der zivilen Sicherheit sollten die im Folgenden angeführten Aspekte Berücksichtigung finden, um einen zielführenden und zugleich gesellschaftlich tragfähigen Umgang mit technisierten Beobachtungspraktiken zu befördern. Die Gestaltungsoptionen richten sich an die Akteure der Forschung und Entwicklung, an den Gesetzgeber sowie an die Akteure der zivilen Sicherheit.

Akteure der Forschung und Entwicklung

Die Erforschung und Entwicklung von Beobachtungstechnologien und deren Einsatzmöglichkeiten im zivilen Sicherheitsbereich werden wesentlich durch öffentliche Gelder gefördert. Durch die entsprechenden Förderstrukturen – hier zu nennen ist insbesondere das Rahmenprogramm »Forschung für die zivile Sicherheit« der Bundesregierung – verfügt die Politik über Einfluss auf Zielrichtungen, inhaltliche Prägungen und Prioritätensetzungen. Das aktuell laufende Forschungsrahmenprogramm verfolgt das Ziel, bei der Entwicklung von Sicherheitslösungen gesellschaftswissenschaftliche Aspekte von Beginn an zu berücksichtigen. Entsprechend werden in der Regel Projektkonsortien aus Technikentwickler/innen und Vertreter/innen aus der Ethik, den Sozialwissenschaften und der Jurisprudenz gefördert. Dieser interdisziplinäre Ansatz ist zu begrüßen und sollte verstärkt und konsequent angewendet werden.

Dies macht jedoch eine gesellschafts- und rechtswissenschaftliche Forschung jenseits von interdisziplinär bearbeiteten Einzelprojekten der Technologieentwicklung nicht überflüssig. Wichtige Forschungsthemen, die programmatisch in den Querschnittsthemen des aktuell laufenden Forschungsrahmenprogramms zu

verorten wären, ergeben sich aus den im Bericht identifizierten Wissenslücken. Dazu gehören im Besonderen:

Psychische und soziale Wirkungen technisierter Beobachtung

Über die psychischen Wirkungen von polizeilichen oder nichtstaatlichen Beobachtungspraktiken bestehen nach wie vor große Wissenslücken. Eine wichtige Forschungsfrage lautet, ob sich mögliche Einschüchterungseffekte nur durch die Angst vor möglichen Sanktionen erklären lassen oder sie zugleich auch eine Folge der im Zuge der Digitalisierung zunehmend allgegenwärtigen Beobachtungsmöglichkeiten durch staatliche und private Akteure sind. Die Mechanismen der psychischen Auswirkungen technisierter Beobachtung müssten wesentlich gründlicher als bislang erforscht werden.

Auswirkungen auf die Technologieanwender und deren Institutionen

Das aktuelle Forschungsrahmenprogramm unterstützt eine bedarfs- und praxisgerechte Entwicklung von Beobachtungstechnologien, indem die (künftigen) Technologieanwender in die jeweiligen Entwicklungsprojekte konsequent eingebunden werden. Dazu ergänzend ist es notwendig, auch solche Auswirkungen in den Blick zu nehmen, die von den jeweilig involvierten Anwender/innen nicht bzw. nur schwer zu antizipieren sind. Hier angesprochen sind insbesondere mögliche handlungspsychologische Effekte der Mensch-Maschine-Interaktion, die in anderen sicherheitsrelevanten Feldern (z. B. in der Luftfahrt) intensiv erforscht werden, im Kontext des Einsatzes von Beobachtungstechnologien aber ein noch weitgehend unbearbeitetes Forschungsfeld darstellen. Hierzu zählen darüber hinaus mögliche Auswirkungen des Technologieeinsatzes auf bestehende Einsatzpraktiken, die Arbeitsorganisation und die jeweiligen Wissensressourcen.

Empirische Wirkungsforschung

Ein wesentliches Ergebnis des Berichts betrifft den in vielen Fällen unbefriedigenden, oft auch veralteten Kenntnisstand zum konkreten sicherheitsrelevanten Nutzen bestehender technisierter Beobachtungspraktiken. Dies bezieht sich vor allem auf polizeiliche Beobachtungsmaßnahmen, angesprochen sind aufgrund der großen Wissenslücken zu den Wirkungen des Technikeinsatzes auf die Technologienanwender aber auch nichtpolizeiliche Einsatzfelder. Die Evaluation des konkreten Nutzens technisierter Beobachtungspraktiken im zivilen Sicherheitsbereich stellt daher fortwährend ein wichtiges Forschungsdesiderat dar.

Aktueller Anwendungsumfang und konkrete Einsatzpraktiken

Die Debatten über das Für und Wider des Einsatzes von Beobachtungstechnologien in der zivilen Sicherheit (und insbesondere im polizeilichen Bereich)

basieren oft auf Vermutungen und spekulativen Annahmen zum aktuellen Umfang der Anwendung und zur konkreten Einsatzpraxis. Wo dies die Datenlage erlaubt, könnten systematische Erhebungen einen wichtigen Beitrag zur Fundierung dieser Debatten liefern.

Grundlegende Fragestellungen

Nicht zuletzt gilt es, auch grundlegende Fragestellungen und Herausforderungen, die sich im Zusammenhang mit staatlichem Sicherheitshandeln stellen, im Rahmen der (öffentlich geförderten) zivilen Sicherheitsforschung zu bearbeiten: Wie sind Sicherheitsrisiken und -bedrohungen im Lichte gestiegener gesellschaftlicher Sicherheitsbedürfnisse zu bewerten? Sind (technikvermittelte) Sicherheitslösungen immer die richtige Antwort auf (neue) Sicherheitsprobleme? Auch wenn solche Fragestellungen über das Thema Beobachtungstechnologien (und damit den Fokus dieses Berichts) weit hinausgehen, so ist deren Einsatz immer als Teil eines Gesamtkonzepts staatlicher Sicherheitsgewährleistung zu sehen. Für die hier notwendig zu führenden gesellschaftlichen und politischen Diskussionen kann die ethische, sozial- und rechtswissenschaftliche Forschung wichtige Beiträge liefern.

Gesetzgeber

Die Gestaltungsoptionen für den Gesetzgeber für eine *Erweiterung* der Verhältnismäßigkeitsprüfung für staatliche Beobachtungspraktiken sind im Folgenden mit Fokus auf polizeiliche Einsatzformen dargestellt.

Methoden und Kriterien für eine adäquate Geeignetheitsüberprüfung entwickeln

Die Überprüfung der Geeignetheit polizeilicher Beobachtungsmaßnahmen zur Kriminalitätsbekämpfung sollte – obwohl im verfassungsrechtlichen Sinne in der Regel ausreichend – nicht allein auf einen Nachweis der technisch-funktionalen Eignung der jeweiligen Beobachtungstechnologien gestützt werden. Sinnvoll bzw. anzustreben wären zusätzliche Bewertungsmethoden und -kriterien, die auf die jeweiligen konkreten Einsatzsituationen anwendbar sind und es ermöglichen, die den jeweiligen technischen, rechtlichen, ethischen und sozialwissenschaftlichen Diskursen entstammenden Bewertungsdimensionen nicht nur im Hinblick auf ihre jeweilige Erfüllung oder Nichterfüllung, sondern auch in ihren Wechselwirkungen integriert zu betrachten.

Dafür notwendige methodische Mindestanforderungen und Bewertungskriterien wären zunächst zu entwickeln, um sie sodann auf die Untersuchungskonzepte von Pilotprojekten zu geplanten bzw. für Evaluationen zu bereits bestehenden polizeilichen Beobachtungsmaßnahmen anwenden zu können.

Handlungsalternativen bedenken

Mit der Prüfung der Erforderlichkeit des Einsatzes einer bestimmten Beobachtungstechnologie zum Zweck der Kriminalitätsbekämpfung verbindet sich stets die Suche nach grundrechtsschonenderen, aber in Bezug auf die Zweckerreichung gleich wirksamen Handlungsalternativen. Neben der Prüfung anderer Beobachtungstechnologie sollten immer auch nichttechnische Handlungsmöglichkeiten mitbedacht werden, die stärker auf die sozialen Ursachen von Kriminalität eingehen. Diese wirken zwar oft nur langfristig, haben aber – im Gegensatz zu Beobachtungstechnologien, die eher der Symptombekämpfung dienen – das Potenzial, die Kriminalitätsprobleme ursächlich eindämmen zu können.

Spektrum der berücksichtigten Folgewirkungen erweitern

Entscheidend für die Bewertung der Angemessenheit polizeilicher Beobachtungspraktiken ist, diese nicht nur auf naheliegende Grundrechtswirkungen zu beschränken. Neben Privatheitsfragen können weitere Grundrechte berührt werden, etwa wenn mögliche Einschüchterungseffekte die Bereitschaft zur freien Meinungsäußerung mindern oder Diskriminierungsrisiken für bestimmte Personengruppen entstehen. Eine adäquate Verhältnismäßigkeitsprüfung sollte stets das gesamte Spektrum der Auswirkungen und (grundrechtsrelevanten) Folgen für die Betroffenen berücksichtigen. Dies unterstreicht die Notwendigkeit, den diesbezüglichen Wissensstand durch eine Stärkung der (Folgen-)Forschung auszubauen.

Kontinuierliche Verhältnismäßigkeitsüberprüfungen

Die Bewertung der Verhältnismäßigkeit von polizeilichen Beobachtungspraktiken hängt von den jeweiligen technischen und sozialen Rahmenbedingungen ab, die jedoch einem kontinuierlichen und zum Teil starken Wandel unterliegen. Der Gesetzgeber sollte die Überprüfung der Verhältnismäßigkeit staatlicher Beobachtungspraktiken daher nicht nur als einmalige Verpflichtung während des Gesetzgebungsverfahrens, sondern als eine fortwährende Aufgabe verstehen.

Überprüfung der Verhältnismäßigkeit im Gesamtkontext aller polizeilichen Beobachtungmaßnahmen

Die Überprüfung der Verhältnismäßigkeit polizeilicher Beobachtungspraktiken erfolgt jeweils isoliert für einzelne Maßnahmen. Aus der Verhältnismäßigkeit jeder einzelnen Maßnahme kann jedoch nicht auf die Verhältnismäßigkeit der Summe der Einzelmaßnahmen geschlossen werden, da die Wirkungen und Folgen in komplexer Weise miteinander wechselwirken können. Die äußert schwierige, aber notwendige Aufgabe besteht also darin, die Verhältnismäßigkeit

polizeilicher Beobachtung jeweils unter Betrachtung des Gesamtkontextes aller Beobachtungsmaßnahmen zu überprüfen.

Akteure der zivilen Sicherheit

Gestaltungsmöglichkeiten zur Förderung eines gesellschaftlich tragfähigen Umgangs mit Beobachtungstechnologien bestehen schließlich für Akteure, die die Technologien im Rahmen ihrer jeweiligen Aufgaben und Befugnisse in der Praxis anwenden.

Evaluation bestehender Beobachtungspraktiken

Die Aufgabe, den Erkenntnisstand zu den Wirkungen und Folgen bestehender Beobachtungspraktiken im zivilen Sicherheitsbereich auszubauen, richtet sich nicht nur an die Forschung oder an den Gesetzgeber, sondern auch an die Anwender/innen (z. B. Behörden und Organisationen mit Sicherheitsaufgaben, Ministerien). Gerade hier bieten sich gute Voraussetzungen, um den Ressourceneinsatz und damit die Wirtschaftlichkeit der Beobachtungsmaßnahmen zu bewerten, mögliche nichtintendierte Wirkungen der Technologieanwendung zu erkennen und die Fragen zu klären, ob die aufgewendeten Mittel im Verhältnis zu den erlangten Erkenntnissen stehen bzw. ob eine konventionelle Sicherheitsarbeit im Rahmen der vorhandenen Ressourcen bessere Wirkungen entfalten könnte.

Kompetenzaufbau bei Technologieanwendern und darüber hinaus

Angesichts der steigenden Komplexität vieler Beobachtungstechnologien ist Sorge zu tragen, dass die Aus- und Fortbildung der Anwender/innen der Entwicklung nicht hinterherhinkt. Insbesondere der (geplante) Einsatz von Beobachtungstechnologien mit automatisierter Datenauswertung (automatisierte Videobeobachtung, Social Media Intelligence, Methoden der vorhersehenden Polizeiarbeit etc.) erfordert spezielle Fähigkeiten, um eine sinnvolle Interpretationsarbeit an den Datenquellen und Analyseergebnissen zu leisten. Zur Ausbildung muss auch die Sensibilisierung für die Begrenzungen von Beobachtungstechnologien gehören, da anderenfalls die Gefahr besteht, dass deren Funktions- und Leistungsfähigkeit überschätzt wird oder unrealistische Nutzenerwartungen entstehen.

Kompetenzaufbau und Sensibilisierung sollten nicht nur auf die unmittelbaren Technologieanwender beschränkt bleiben, sondern alle Akteure mit einschließen, deren Tätigkeit mit dem Einsatz von Beobachtungstechnologien im Zusammenhang steht (z. B. Staatsanwälte, Richter, Behörden-/Abteilungsleitungen).

Umgang mit automatisierten Beobachtungstechnologien

Der (geplanten) Einsatz von Beobachtungstechnologien mit automatisierter Datenauswertung ist mit weiteren Herausforderungen verbunden. Ein zentrales Problem stellt die Frage der Verantwortungszuschreibung dar: Obschon als Systeme zur Entscheidungsunterstützung ausgelegt, motivieren verschiedene Gründe die Sorge, dass das Prinzip der menschlichen Letztverantwortung durch solche Beobachtungstechnologien zunehmend untergraben werden könnte. Die individuelle Verantwortungszuschreibung ist aber gerade im Sicherheitskontext von essenzieller Bedeutung. Wie in anderen Anwendungsfeldern der künstlichen Intelligenz bleibt auch hier die schwierige Frage zu diskutieren, wie eine geteilte Verantwortung zwischen Menschen und technischen Systemen genau aussehen könnte.

Vertrauensbildende und transparenzfördernde Maßnahmen

Obgleich der empirische Forschungsstand zu den psychischen Wirkungen technisierter Beobachtung noch sehr lückenhaft ist, lässt sich mit Blick auf die teils sehr kontrovers geführten öffentlichen Debatten zum Thema konstatieren, dass vor allem polizeiliche Beobachtungspraktiken das Potenzial haben, bei Bürger/innen auch ein Gefühl der Verunsicherung auslösen zu können.

Grundsätzlich sollte daher nach Wegen gesucht werden, um einer in der Bevölkerung ggf. vorhandenen Verunsicherung entgegenzuwirken. Eine Möglichkeit dazu wären vertrauensbildende Maßnahmen, mit denen die Einführung neuer polizeilicher Beobachtungsmaßnahmen flankiert werden. Ziel wäre insbesondere die Informationsvermittlung, um einem aus Wissensdefiziten und falschen Vorstellungen resultierenden Unsicherheitsempfinden vorzubeugen. Eine weitere Möglichkeit wären transparenzfördernde Maßnahmen für bereits bestehende Einsatzformen. Die derzeit von Regierungen und Behörden zumeist verfolgte defensive Informationspolitik scheint nicht zwingend geeignet, Verunsicherungen adäquat zu begegnen. Hier wäre nach Wegen zu suchen, wie durch eine proaktivere Informationspolitik die Transparenz polizeilicher Beobachtungspraktiken erhöht werden könnte, ohne gleichzeitig durch Preisgabe von zu vielen Informationen die operativen Fähigkeiten der Polizeibehörden zu schwächen.

Nicht zuletzt könnten vertrauensbildende und transparenzfördernde Maßnahmen zu einer Demystifizierung staatlicher Beobachtungspraktiken beitragen. Auch wenn sich dadurch wohl niemals Übereinstimmung bei allen gesellschaftlichen Gruppen herstellen lässt, so sind Verständnis und Transparenz über die Funktionsweisen, das Ausmaß sowie die Wirkungen und Folgen technisierter Beobachtung notwendige und bedeutende Voraussetzungen für eine informierte gesellschaftliche Verständigung über einen zielführenden und zugleich gesellschaftlich akzeptablen Einsatz von Beobachtungstechnologien in der zivilen Sicherheit.

1 Einleitung

Die zum Teil rasanten Entwicklungen in den Feldern Sensorik, Informatik und Informationstechnik bilden die Grundlage für ein breites Anwendungsspektrum diverser Technologien bei der Erfassung, Aufzeichnung und Analyse von physikalischen Werten und digitalen Daten verschiedenster Art. Diese Technologien – im Folgenden Beobachtungstechnologien genannt – erlangen sowohl durch ihre bereits erfolgte Verbreitung und Nutzung als auch aufgrund des Entwicklungspotenzials für neue oder erweiterte Anwendungsmöglichkeiten in den unterschiedlichsten Bereichen (Wissenschaft, Medizin, Mobilität, Industrieproduktion, Marketing etc.) immer stärkere Bedeutung.

Ein zentrales Anwendungsfeld von Beobachtungstechnologien ist der Sicherheitsbereich, in dem der Einsatz von Technik mehr denn je integraler Bestandteil ist. Beobachtungstechnologien erweitern das menschliche Wahrnehmungs- und Beurteilungsvermögen für Risiken, Gefahren oder Schäden in vielfältiger Weise, sodass von ihrer Anwendung sämtliche Aufgabenfelder der zivilen Sicherheit profitieren können – angefangen von der Verkehrsüberwachung und dem Umweltmonitoring über den Brand- und Katastrophenschutz, den Rettungsdienst und den Schutz kritischer Infrastrukturen bis hin zur polizeilichen Gefahrenabwehr und Strafverfolgung. Dementsprechend breit ist schon heute das Spektrum der Einsatzformen von Beobachtungstechnologien durch staatliche und nichtstaatliche Sicherheitsakteure und fortwährend kommen neue Entwicklungen und Anwendungen dazu.

Der Einsatz von Beobachtungstechnologien im zivilen Sicherheitsbereich wird in Öffentlichkeit, Wissenschaft und Politik zum Teil allerdings kontrovers diskutiert: Einerseits können Beobachtungstechnologien für den Staat (und seine Behörden) von Nutzen sein, um eine Kernaufgabe – die Gewährleistung von Sicherheit – zu erfüllen. Andererseits werden immer wieder Fragen nach der Verhältnismäßigkeit von technisierten Beobachtungsmaßnahmen gestellt und der erwartete und tatsächliche Nutzen wird kritisch diskutiert. Im Fokus dieser Debatte stehen vor allem polizeiliche Einsatzpraktiken, die unter Umständen mit Eingriffen in individuelle Freiheitsrechte der beobachteten Personen verbunden sein können. In den Blick zu nehmen sind aber auch mögliche Folgen des Technologieeinsatzes für die Einsatzkräfte und die Sicherheitspraxis, da den erwünschten Wirkungen auch unerwartete Effekte gegenüberstehen können, die den intendierten Sicherheitsgewinn wieder schmälern.

Vor dem Hintergrund dieser Entwicklungen und Diskussionen wurde das TAB vom Ausschuss für Bildung, Forschung und Technikfolgenabschätzung mit einem TA-Projekt »Beobachtungstechnologien im Bereich der zivilen Sicherheit – Möglichkeiten und Herausforderungen« beauftragt, um eine umfassende Sachgrundlage für die politische Meinungsbildung bezüglich der erforderlichen

Rahmensetzungen für den Einsatz von Beobachtungstechnologien im zivilen Sicherheitsbereich zu erarbeiten.

Zielsetzung des TA-Projekts

Das Ziel des TAB-Projekts ist es, relevante gesellschaftliche und politische Fragestellungen, die sich mit dem (zunehmenden) Einsatz von Beobachtungstechnologien im zivilen Sicherheitsbereich ergeben, zu identifizieren und kritisch zu reflektieren. Dabei ist es ein besonderes Anliegen, die Vielfalt der (möglichen) Einsatzfelder nicht zuletzt auch hinsichtlich ihrer technischen, rechtlichen und sozialen Komplexität zu verdeutlichen, um Chancen und Herausforderungen vertieft ergründen und herausarbeiten zu können. Dazu notwendig ist ein fundierter Kenntnisstand über

- die wissenschaftlich-technischen Grundlagen der jeweiligen Beobachtungstechnologie in Abhängigkeit von den Einsatzanforderungen und -bedingungen,
- den erwarteten und tatsächlichen Sicherheitsnutzen der jeweiligen konkreten Einsatzformen,
- die rechtlichen Rahmenbedingungen für den Einsatz von Beobachtungstechnologien und die aktuellen Einsatzpraktiken sowie
- mögliche nichtintendierte Wirkungen und Folgen des Technologieeinsatzes auf die beobachteten Personen und die Sicherheitsakteure.

Dieses Wissen bildet die Grundlage zur Ableitung von Gestaltungsoptionen, die zu einem zielführenden und gesellschaftlich tragfähigen Umgang mit Beobachtungstechnologien im Bereich der zivilen Sicherheitsbereich beitragen können.

Der hier verfolgte breite Analyseansatz verweist zugleich auf einige der Herausforderungen, denen sich dieses Projekt zu stellen hatte. So musste angesichts der Fülle an Anwendungen von Beobachtungstechnologien im zivilen Sicherheitsbereich nicht nur eine Auswahl getroffen werden, sondern auch eine Darstellungsform für die komplexe Materie gefunden werden, die sowohl Fachexpert/innen als auch interessierte Laien anzusprechen vermag. Notwendigerweise bedingt dies, dass nicht alle Einsatzformen, Argumente und Erwägungen in ihrer ganzen Tiefe behandelt werden konnten, zugleich aber für das Verständnis wichtige technische und rechtliche Grundlagen dargestellt werden, die Expert/innen hinreichend bekannt sind. Hervorzuheben ist außerdem, dass auf eine Behandlung von nachrichtendienstlichen Beobachtungspraktiken verzichtet wurde, weil dies aufgrund der sehr eingeschränkten Zugriffsmöglichkeit auf spezifische Informationen für das TAB nicht zielführend möglich gewesen wäre.

Als weitere Herausforderung für das Projekt erwies sich eine in Teilen sehr dynamische Rechtslage zum Einsatz von Beobachtungstechnologien. Nicht nur das neue europäische Datenschutzregime, sondern auch eine Reihe von Urteilen

des Bundesverfassungsgerichts hat über die Laufzeit des Projekts von 2016 bis Anfang 2020 dazu geführt, dass sich sowohl der relevante Rechtsrahmen in Teilen erheblich verändert hat als auch die damit verknüpften rechtswissenschaftlichen Diskussionen sich weiterentwickelt haben. Die Entwicklungen bis Anfang 2020 wurden im vorliegenden Bericht soweit erforderlich umfänglich berücksichtigt.

Schließlich bildet die schwierige Frage, wie Sicherheit und Freiheit in Einklang zu bringen sind, seit jeher einen Schwerpunkt der (teils emotional geführten) Debatten um den (vor allem polizeilichen) Einsatz von Beobachtungstechnologien im zivilen Sicherheitsbereich. Diese Frage kann im vorliegenden Bericht selbstverständlich nicht abschließend beantworten werden. Die Intention ist vielmehr, die sachlichen Grundlagen für die hier notwendig zu führenden politischen und gesellschaftlichen Diskussionen über einen gesellschaftlich akzeptablen Einsatz von Beobachtungstechnologien zu liefern.

Hinweis zur Aktualität des Berichts

Der Redaktionsschluss für den vorliegenden Bericht war Anfang 2020. Demzufolge konnten jüngere Entwicklungen, veränderte Rahmenbedingungen und neuere Quellen keine Berücksichtigung finden. Dazu gehören insbesondere die rechtlichen Rahmenbedingungen, die sich seit 2021 teilweise erheblich verändert haben, aber auch seither erzielte Fortschritte in der Forschung und Entwicklung oder Veränderungen in den gesellschaftlichen und politischen Diskursen. Aktualisierungen wurden jedoch in Bezug auf die Anwendungspraxis von Beobachtungstechnologien im Bereich der zivilen Sicherheit vorgenommen. Hierzu wurden Daten für die Jahre bis 2020, die erst nach Redaktionsschluss veröffentlicht wurden, entsprechend ergänzt (Stand März 2022).

Gutachtenvergabe und Aufbau des Berichts

Im Rahmen des TAB-Projekts wurden fünf Gutachten vergeben, deren Ergebnisse neben den vielfältigen und umfangreichen eigenen Recherchen und Analysen in den Bericht eingeflossen sind:

- Beobachtungstechnologien im Bereich der zivilen Sicherheit. Möglichkeiten und Herausforderungen zwischen situational awareness (Lagebewusstsein) und situativem Handeln. Dr. Leon Hempel, Berlin
- Beobachtungstechnologien im Bereich der zivilen Sicherheit – Möglichkeiten und Herausforderungen: Forschungslandschaft. Dr. Silke Römer (mit Beiträgen von Dr. Sabine Müller und Dr. Kay-Uwe Suwelack), INT – Fraunhofer-Institut für Naturwissenschaftlich-Technische Trendanalysen, Euskirchen

- Beobachtungstechnologien im Bereich der zivilen Sicherheit. Möglichkeiten und Herausforderungen von Verfahren informationstechnisch vernetzter Beobachtung. Dr. Leon Hempel, Rainer Rehak, Berlin
- Soziale und psychologische Wirkungen technisierter Beobachtung. Prof. Dr. Regina Ammicht Quinn, PD Dr. Jessica Heesen, Maria Pawelec, Alexander Hauschild (unter Mitarbeit von Andreas Baur-Ahrens, Sophia Booz, Dr. Anne Burkhardt, Sylvia Erben, Friedrich Gabel, Dr. Thomas Grote, Dr. Thilo Hagendorff, Marco Krüger, Sophie Nadolski, Dr. Mone Spindler, Anna Tilling, Judith Zinsmaier). IZEW – Internationales Zentrum für Ethik in den Wissenschaften, Tübingen
- Kommentargutachten zum TAB-Arbeitsbericht »Beobachtungstechnologien im Bereich der zivilen Sicherheit – Möglichkeiten und Herausforderungen«. Prof. Dr. Matthias Bäcker, Mainz

Die Verantwortung für die Auswahl, Strukturierung und Verdichtung des Materials sowie dessen Zusammenführung mit Informationen aus eigenen Recherchen und Analysen liegt bei der Verfasserin und den Verfassern des vorliegenden Berichts, Dr. Claudio Caviezel, Dr. Leon Hempel, Dr. Christoph Revermann und Dr. Saskia Steiger. Den Gutachter/innen sowie allen an der Erstellung der Gutachten beteiligten Expert/innen sei für ihre engagierte Kooperation und ihre Diskussionsbereitschaft sehr herzlich gedankt. Ein herzlicher Dank geht schließlich an Brigitta-Ulrike Goelsdorf und Carmen Dienhardt für die Aufbereitung der Abbildungen und die Erstellung des Endlayouts.

Der Bericht ist wie folgt aufgebaut: Kapitel 2 dient der thematischen und begrifflichen Einführung. Dazu werden die Ziele, Aufgaben und Akteure der zivilen Sicherheit dargestellt. Außerdem erfolgt eine Einteilung der Beobachtungstechnologien in sensor- und datenbasierte Beobachtungstechnologien, wobei sich letztere Kategorie weiter in Verfahren zur Internetbeobachtung und zur informationstechnischen Beobachtung trennen lässt.

Ausgehend von dieser Einteilung werden in den Kapiteln 3 bis 5 die wissenschaftlich-technischen Grundlagen der jeweiligen Beobachtungstechnologien erläutert, aktuelle und mögliche künftige Einsatzfelder sowie damit verbundene technische Herausforderungen beschrieben, die rechtlichen Rahmenbedingungen diskutiert sowie – soweit es die Datenlage erlaubte – aktuelle Einsatzpraktiken und Erkenntnisse zum sicherheitsrelevanten Nutzen des Technologieeinsatzes dargestellt.

Die anschließenden Kapitel nehmen sodann eine technologie- bzw. anwendungsübergreifende Perspektive ein. Kapitel 6 bietet einen Überblick über wichtige regulatorische Fragestellungen, die sich aufgrund der zunehmenden Verbreitung von Beobachtungstechnologien, aber auch infolge der technischen Entwicklung und des Wandels in der Techniknutzung stellen. Der Schwerpunkt liegt hier auf dem Einsatz von Beobachtungstechnologien durch Polizeibehörden.

In Kapitel 7 wird sich mit den gesellschaftlichen Auswirkungen des Einsatzes von Beobachtungstechnologien für zivile Sicherheitsaufgaben befasst. Konkret werden der Kenntnisstand zu möglichen psychischen Wirkungen technisierter Beobachtung dargestellt, mögliche Auswirkungen auf die Technologieanwender behandelt sowie zentrale Fragestellungen und Herausforderungen im Kontext des Spannungsverhältnisses zwischen Sicherheit und Freiheit diskutiert.

Im abschließenden Kapitel 8 werden Gestaltungsoptionen für die Akteure der Forschung, für den Gesetzgeber und für die Sicherheitsakteure behandelt, die bei Überlegungen und Entscheidungen zur Entwicklung, zur Implementierung oder zum Einsatz von Beobachtungstechnologien im Bereich der zivilen Sicherheit Berücksichtigung finden können, um einen zielführenden und zugleich gesellschaftlich tragfähigen Umgang mit technisierten Beobachtungspraktiken zu befördern.

2 Thematische und begriffliche Einführung

2.1 Funktionen der Beobachtung

Der Begriff *Beobachtung* bezeichnet ganz allgemein die zielgerichtete und methodisch kontrollierte Wahrnehmung von Objekten, Ereignissen oder Prozessen mit dem Ziel eines Erkenntnisgewinns (dazu und zum Folgenden IZEW 2017, S. 14 ff.; Hempel 2016, S. 13 ff.). Dabei variieren Gegenstand und Zielrichtung je nach Kontext der Beobachtung: Bildet etwa die exakte Messung von physikalischen Größen die Grundlage naturwissenschaftlicher Beobachtung, so steht im Bereich der Wirtschaft die Beobachtung von Produktionsprozessen, Warenströmen, der Preisentwicklung oder des Kundenverhaltens im Fokus, um Abläufe, Produkte oder Dienstleistungen zu optimieren. In Politik und Verwaltung ist die Erhebung von Informationen über Bürger/innen für die Erfüllung staatlicher Aufgaben und die Planung staatlicher Maßnahmen erforderlich. Im Bereich der Erziehung werden Verhaltensweisen und -bedingungen beobachtet. Eine Gesundheitsversorgung ohne medizintechnische Beobachtung des Patienten ist heute kaum mehr vorstellbar.

Aus gesellschaftlicher und sozialwissenschaftlicher Perspektive von besonderem Interesse sind Formen der Beobachtung, die den Menschen, sein Verhalten oder mit ihm in direkter Beziehung stehende Objekte (z. B. Kfz im Rahmen der Verkehrsbeobachtung) zum Gegenstand haben. Hier umfasst Beobachtung stets auch das Handeln des Beobachters, die Wirkung der Beobachtung auf den Beobachteten und das Verhältnis zwischen beiden. Beispielsweise ist Beobachtung Grundvoraussetzung und Mittel für soziale Kontrolle im Sinne der Selbstkontrolle einer Gesellschaft. Soziale Kontrolle umfasst Prozesse und Strukturen, durch die Mitglieder einer Gesellschaft versuchen, Verhaltenserwartungen und entsprechende Formen des Umgangs miteinander durch sich selbst durchzusetzen. Darunter fallen kleine Gesten der Aufmerksamkeit und der gegenseitigen nachbarschaftlichen Unterstützung genauso wie die Fürsorge oder die Durchsetzung der etablierten staatlichen Rechtsordnung. Soziale Kontrolle verbindet somit stets beide Aspekte: individuelle Anpassung an gesellschaftliche Normen, aber auch Schutz der Individuen durch die Gesellschaft. Ein gewisses Maß an sozialer Kontrolle und damit an Beobachtung ist folglich unerlässlich für den inneren Zusammenhalt und das Funktionieren von Gesellschaften. Erst, wo der Bedarf entsteht, soziale Kontrolle auf externe Instanzen zu verlagern, um das soziale Miteinander zu sichern, entsteht eine neuartige Konstellation institutionalisierter sozialer Beobachtung. Gerade aber, weil in dieser Konstellation die Beobachtungsinstanzen aus der Wechselseitigkeit sozialer Kontrolle herausgenommen sind, verlangt auch deren Beobachtungsverhalten der Kontrolle durch die Politik und die Gesellschaft.

In diesem Kontext wird häufig der Begriff *Überwachung* verwendet, die insofern eine spezifische Form der Beobachtung ist, als es sich um das routinemäßige und systematische Beobachten aus einer Position heraus handelt, in der sich die beobachtend überwachende Instanz der Beobachtung durch die Beobachteten entziehen kann. Ein viel beachtetes Modell für Überwachung stellt das Panoptikon[1] dar. In gesellschaftlichen Debatten wird es oft auf die eine oder andere Weise mit Vorstellungen vom Überwachungsstaat bzw. der Überwachungsgesellschaft oder in Anknüpfung an George Orwells politischer Dystopie »1984« mit Schlagwörtern wie Big Brother in Zusammenhang gebracht. Mit Überwachen ist das Bild eines starken Machtgefälles zwischen den beobachtenden Instanzen und den beobachteten Personen markiert, wobei die Überwachung von oben erfolgt oder auch verteilt, jedoch immer aus der Distanz und häufig im Zusammenhang mit der Ausübung struktureller Gewalt gedacht wird (Hagendorff 2017, S. 195; Nagenborg 2014, S. 214). Beinhaltet aber Überwachung sowohl Kontrolle als auch Schutz, so kann der Begriff ebenfalls positiv konnotiert werden, etwa wenn es um die Überwachung von Erdbebengebieten im Katastrophenschutz, von Pandemien in der Epidemiologie oder von Vitalfunktionen in der Intensivmedizin geht. Aufgrund dieser Ambivalenz soll auf eine Verwendung des Begriffs Überwachung im vorliegenden TAB-Bericht (außer in Eigennamen oder wörtlichen Zitaten) weitgehend verzichtet werden.

Beobachtung ist also ein sehr facettenreicher Begriff. Beobachtung hat in der modernen, funktional differenzierten Gesellschaft einen hohen, in vielen Bereichen essenziellen gesellschaftlichen Nutzen, wenngleich sie in der Form von Überwachung ungleiche Machtverhältnisse befördern bzw. verfestigen kann. Für eine Bewertung von Beobachtungspraktiken entscheidend sind daher immer der Kontext der Beobachtung, ihr Zweck und Umfang, ihre Eingriffstiefe und damit einhergehend die Mittel, also die Technologien, die zur Beobachtung eingesetzt werden.

2.2 Technisierte Beobachtung

Gerade die technische Entwicklung trägt aus zwei wesentlichen Gründen zur Ambivalenz von Beobachtung bei (dazu und zum Folgenden Hempel 2016, S. 13 ff.; IZEW 2017, S. 15 f.). Zum einen verändert die Technisierung des Beobachtungsvorgangs das Konzept der sozialen Kontrolle entscheidend, indem die Beobachtung aus der Distanz möglich wird (z. B. mithilfe einer Videokamera). Soziale Kontrolle ist nicht mehr durch unmittelbare soziale Interaktion gekennzeichnet, sondern kann nun auch in Situationen erfolgen, in denen zwischen

[1] Der Begriff Panoptikon beschreibt ein Konzept zum idealen Gefängnisbau von 1787. Danach werden die isolierten Gefängniszellen kreisförmig um einen zentralen Turm angeordnet. Von diesem Turm aus können alle Zellen beobachtet werden, ohne dass die Zelleninsassen feststellen können, ob sie beobachtet werden oder nicht (IZEW 2017, S. 15).

Beobachter und Beobachteten nur eingeschränkte bzw. keine Möglichkeiten der Kommunikation vorhanden sind und die beobachtete Person außerdem nicht nachvollziehen kann, ob sie tatsächlich (und durch wen) beobachtet wird. Beobachtungstechnologien heben also die Wechselseitigkeit der Wahrnehmung, die zwischenmenschlichen Formen der Beobachtung zugrunde liegt, tendenziell auf, was für die beobachtete Person vielfältige Folgen haben kann, die bis hin zu Einschüchterungseffekten und Verhaltensanpassungen reichen können.

Zum anderen entstehen durch die Technisierung und Digitalisierung sämtlicher Lebensbereiche immer neue Formen der technikvermittelten Beobachtung. Vor allen die Nutzung des Internets mit seinen unzähligen Diensten in Verbindung mit mobilen Endgeräten wie Smartphones bildet die Masse digital verfügbarer Daten, die staatliche Institutionen, aber auch nichtstaatliche Organisationen, Unternehmen oder Privatpersonen in stark wachsendem Umfang sammeln und auswerten können, um Erkenntnisse zu gewinnen, neue Dienstleistungen anzubieten oder auch das Verhalten von Personen zu beeinflussen (z. B. im Marketing). Gerade der Begriff Überwachungsgesellschaft, von der heute oft die Rede ist, bringt zum Ausdruck, dass es die Menschen selbst sind, die durch die Nutzung digitaler Technologien das Material ihrer Beobachtung liefern. Indem Technik in ihrer Funktionsweise immer weniger einsehbar und somit für ihre Nutzer zur Blackbox wird, schafft sie erst die Bedingungen für diese paradoxe Konstellation. Mangelnde Transparenz und unzureichende Möglichkeiten der Kontrolle und Regulierung der beobachtenden Instanzen heben den Einsatz solcher Beobachtungstechnologien schließlich auf ein kritisches Niveau.

2.3 Fokus zivile Sicherheit

Das steigende Ausmaß an Beobachtung, das moderne Gesellschaften zunehmend prägt, kann auch als Ausdruck eines erhöhten Bedürfnisses nach Schutz vor Gefahren gesehen werden, stellt heute doch der Sicherheitsbereich ein zentrales Anwendungsfeld von Beobachtungstechnologien dar. Sozialwissenschaftler sehen denn auch unser Verständnis von Sicherheit einem starken Wandel ausgesetzt, der zu einer Erweiterung des Sicherheitsbegriffs und damit zu einer Ausweitung der staatlichen Sicherheitsaufgaben geführt hat (Kasten 2.1): Stand vor 70 Jahren noch der Schutz der eigenen Bevölkerung vor den Auswirkungen zwischenstaatlicher Kriege im Fokus der Sicherheitspolitik westlicher Staaten, so sind es heute Konzepte eines umfassenden Risiko- und Krisenmanagements, dessen Ziele von der Bekämpfung der Alltagskriminalität über den Schutz kritischer Infrastrukturen (z. B. Telekommunikationsnetze, Flughäfen, Krankenhäuser, Rechenzentren) oder die Minimierung von Risken durch Naturkatastrophen oder Industrieunfälle bis hin zur Steigerung der Reaktionsfähigkeit auf Epidemien oder große Terroranschläge reichen (Bossong/Hegemann 2017, S. 40).

Kasten 2.1 Entwicklung des Sicherheitsverständnisses

Das Thema Sicherheit wurde zu Beginn der 1950er Jahre vor allem als nationale Sicherheit im Kontext der internationalen Politik diskutiert und weitgehend getrennt von Fragen des sozialen Wohlergehens betrachtet. Gesellschaftliche und geopolitische Veränderungsprozesse haben dazu beigetragen, dass sich das Sicherheitsverständnis seitdem stark gewandelt und erweitert hat. Daase und Deitelhoff (2013, S. 16 ff.) beschreiben diese Entwicklung anhand von vier Dimensionen:

- *Individualisierung*: Der Staat als primäres Referenzobjekt der Sicherheitspolitik wird zunehmend durch die Gesellschaft (gemeint als Kollektiv von Bürger/innen, das in Frieden leben und Wohlstand entwickeln kann) und dann durch das Individuum mit seinen elementaren Sicherheitsbedürfnissen nach Freiheit von Angst und Not abgelöst. Mit diesem Perspektivenwechsel geraten neue Gefahren für die Sicherheit in den Blick, z. B. Kriminalität, Drogen- und Waffenhandel, soziale Not, Krankheit oder Migration.
- *Entdifferenzierung*: Neben militärischen werden weitere Gefahren für die Sicherheit festgestellt, z. B. nach der Ölkrise von 1973 wirtschaftliche Gefahren, ab Mitte der 1980er Jahre Umweltgefahren und nach dem Ende des Ost-West-Konflikts vermehrt auch Gefahren aus innergesellschaftlichen Konflikten. Die vormals getrennten Sphären der äußeren, inneren und sozialen Sicherheit gehen immer stärker ineinander über, gleichzeitig werden immer mehr Politikfelder sicherheitsrelevant.
- *Entgrenzung*: Traditionell auf nationale Territorien fokussierte sicherheitspolitische Ansprüche und Praktiken dehnen sich auf globale Zusammenhänge aus.
- *Proaktivierung*: Sicherheitsprobleme werden zunehmend nicht als konkrete Bedrohungen (z. B. Nuklearschlag während des Kalten Krieges), sondern aufgrund der damit verbundenen Ungewissheit als Verwundbarkeiten und Risiken konzeptualisiert (z. B. Naturkatastrophen, Terroranschläge). Dadurch geraten verstärkt Gefahren in den Blick, die noch gar keine sind, aber die Möglichkeit haben, es zu werden. Proaktivierung beschreibt also den Paradigmenwechsel von der Abwehr akuter Bedrohungen zur Reduzierung von Risiken. Eine proaktive Sicherheitspolitik muss Gefahren antizipieren und ist früher zu einem Eingreifen gezwungen als eine traditionell reaktive Sicherheitspolitik.

Das vergleichsweise junge Konzept der *zivilen Sicherheit* kann als eine Antwort auf die Verschiebungen und Erweiterungen im Sicherheitsverständnis betrachtet werden. Der Begriff zivile Sicherheit hat sich – obschon es abgesehen von der Abgrenzung zum Militärischen bislang an einer genauen inhaltlichen Definition

fehlt (Bossong/Hegemann 2017, S. 39) – in den letzten Jahren immer stärker durchgesetzt. Dazu beigetragen hat insbesondere auch das seit 2007 laufende Rahmenprogramm der Bundesregierung »Forschung für die zivile Sicherheit«. Folgt man dem Rahmenprogramm, so ist zivile Sicherheit »grundlegend für das individuelle und soziale Leben aller Bürgerinnen und Bürger« und »nicht zuletzt angesichts der Verwundbarkeiten des modernen Lebens zu einem zentralen Wertbegriff der Gegenwartsgesellschaft geworden«. Explizit wird auf den erweiterten Sicherheitsbegriff Bezug genommen, wonach »der Schutz der inneren Sicherheit Deutschlands immer mehr von globalen Herausforderungen und dem Wandel staatlicher Vorsorgeaufgaben bestimmt« werde (BMBF 2012, S. 12). Ausgangspunkt des Konzepts der zivilen Sicherheit bildet folglich die Annahme einer prinzipiellen Vulnerabilität moderner Gesellschaften, wodurch sich gegenüber dem relativ engen Sicherheitsbegriff nach Ende des Zweiten Weltkrieges das adressierte Gefahrenspektrum stark erweitert hat und Sicherheit als eine gesamtgesellschaftliche Aufgabe aufgefasst wird, an der sich entsprechend sämtliche gesellschaftliche Akteure auch beteiligen (Hempel 2016, S. 97).

2.4 Aufgaben und Akteure der zivilen Sicherheit

Die Basis der gesamtgesellschaftlichen Sicherheitsarchitektur in Deutschland bilden heute die Akteure der nichtpolizeilichen Gefahrenabwehr (Brandschutz, Rettungsdienst, Bevölkerungsschutz), die Polizei, nichtstaatliche Akteure wie beispielsweise private Hilfsorganisationen sowie die (im Folgenden aber nicht weiter behandelten) Streitkräfte (Landesverteidigung) und Nachrichtendienste (Aufklärung im In- und Ausland) (Geier 2017, S. 95 ff.).

2.4.1 Akteure der nichtpolizeilichen Gefahrenabwehr

Zur nichtpolizeilichen Gefahrenabwehr werden der Brandschutz und die Allgemeine Hilfe, der Rettungsdienst und der Bevölkerungsschutz (Katastrophen- und Zivilschutz) gezählt (Geier 2017, S. 94 ff.; Hempel 2016, S. 108):

- Der Brandschutz und die Allgemeine Hilfe als originäre Aufgaben der Feuerwehr umfassen die Gewährleistung vorbeugender und abwehrender Maßnahmen gegen Brände, Brandgefahren und andere alltägliche Gefahren, bei denen technische Hilfen erforderlich sind (z. B. bei Unfällen im Straßenverkehr, der Unterstützung von Suchaktionen, der Beseitigung von Unwetterschäden oder der Rettung von Tieren in Not).
- Rettungsdienste versorgen die Bevölkerung mit Leistungen der Notfallrettung und des Krankentransports.
- Aufgabe des Katastrophenschutzes ist die Abwehr und Beseitigung besonderer Gefahren, bei denen – im Unterschied zur allgemeinen bzw. alltäglichen

Gefahrenabwehr – Leben oder Gesundheit einer Vielzahl von Menschen, die natürlichen Lebensgrundlagen oder bedeutende Sachwerte in ungewöhnlich hohem Ausmaß gefährdet oder geschädigt werden. Den Katastrophenschutzbehörden obliegt es, vorbereitende Maßnahmen für den Eintritt von Katastrophen zu treffen. Im Katastrophenfall arbeiten dann meist alle Akteure der nichtpolizeilichen Gefahrenabwehr unter der Leitung der Katastrophenschutzbehörden an der Bewältigung der Katastrophe mit.

- Als Zivilschutz schließlich wird der (nichtmilitärische) Schutz der Bevölkerung, von Wohnungen, Einrichtungen oder Kulturgütern vor Kriegseinwirkungen im Spannungs- und Verteidigungsfall bezeichnet.

Gemäß der grundgesetzlichen Aufgabenteilung sind die Bundesländer für die allgemeine Gefahrenabwehr und den Katastrophenschutz nach Artikel 30, 70, 83 Grundgesetz[2] (GG) und der Bund für den Zivilschutz nach Artikel 73 Abs. 1 Nr. 1, 87b Abs. 2 GG zuständig. Entsprechend existieren in allen Bundesländern eigene Gesetze für den Brandschutz und die Allgemeine Hilfe, den Rettungsdienst und den Katastrophenschutz (dazu und zum Folgenden Geier 2017, S. 99 ff.). Die Durchführung der Aufgaben haben die Bundesländer größtenteils auf die Kommunen übertragen, im Falle des Brandschutzes und der Allgemeinen Hilfe primär auf die Gemeinden, im Falle des Rettungsdienstes und des Katastrophenschutzes auf die Landkreise bzw. kreisfreien Städte. Die relevanten Akteure der operativen Ebene sind die Berufs- und Freiwilligen Feuerwehren[3] für den Brandschutz und die Allgemeine Hilfe, kommunale Rettungsdienste, die unteren Katastrophenschutzbehörden (in der Regel sind dies die Landräte in den Kreisen bzw. die Oberbürgermeister in den kreisfreien Städten, die für die Durchführung der Aufgaben des Katastrophenschutzes die Verantwortung tragen) sowie private Hilfsorganisationen (z. B. Arbeiter-Samariter-Bund, Deutsches Rotes Kreuz, Johanniter-Unfall-Hilfe) oder privat-kommerzielle Anbieter, die entsprechende Aufgaben im öffentlichen Auftrag ausführen bzw. sich zur Mitwirkung im Katastrophenschutz verpflichtet haben. Die Aufgaben des Bundes im Zivilschutz sind im Zivilschutz- und Katastrophenhilfegesetz[4] (ZSKG) geregelt und umfassen beispielsweise die Förderung der Selbstschutz- und Selbsthilfefähigkeit der Bevölkerung, die Warnung der Bevölkerung, den Schutzbau und grundsätzlich den Bevölkerungsschutz im Verteidigungsfall. Teil des Zivilschutzes des Bundes ist auch die Bundesanstalt Technisches Hilfswerk (THW), deren originäre Aufgabe darin besteht, technische Hilfe im Zivilschutz zu leisten. Dafür hält das THW

2 Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 28. März 2019 (BGBl. I S. 404) geändert worden ist

3 Personell stützt sich der Brandschutz und die Allgemeine Hilfe in Deutschland vorwiegend auf ehrenamtlich tätige Einsatzkräfte: Den rund 30.000 Berufsfeuerwehrleuten stehen ca. 1 Mio. ehrenamtliche Feuerwehrleute gegenüber (Geier 2017, S. 110).

4 Zivilschutz- und Katastrophenhilfegesetz vom 25. März 1997 (BGBl. I S. 726), das zuletzt durch Artikel 2 Nummer 1 des Gesetzes vom 29. Juli 2009 (BGBl. I S. 2350) geändert worden ist

rund 80.000 überwiegend ehrenamtliche Einsatzkräfte und umfangreiche technische Ressourcen für die Rettung, Bergung und Instandsetzung bereit.

Obschon grundsätzlich Aufgabe der Bundesländer, kann der Bund die Länder beim Katastrophenschutz im Wege der Amtshilfe (Artikel 35 Abs. 1 GG) oder im Falle von Naturkatastrophen oder besonders schweren Unglücksfällen (wozu auch terroristische Anschläge gehören können; BVerfG, Urteil vom 15.2.2006, 1 BvR 357/05) unter engen Voraussetzungen im Wege der Katastrophenhilfe (Artikel 35 Abs. 2 u. 3 GG) unterstützen. Die konzeptionellen, organisatorischen und rechtlichen Grundlagen für die Zusammenarbeit zwischen Bund und Ländern im Katastrophenschutz bilden die 2002 beschlossene »Neue Strategie zum Schutz der Bevölkerung in Deutschland« sowie die auf dieser Grundlage 2009 erfolgte Ergänzung des Zivilschutzgesetzes zum Zivilschutz- und Katastrophenhilfegesetz des Bundes[5] (WD 2017c, S. 3). Grundsatz der Neuausrichtung des Bevölkerungsschutzes, die 2002 von der Innenministerkonferenz unter dem Eindruck der Terroranschläge des 11. September 2001 in den USA und des Hochwassers an Donau und Elbe von 2002 verabschiedet wurde, bildet die gemeinsame Verantwortung von Bund und Länder für außergewöhnliche, großflächige oder national bedeutsame Gefahren- und Schadenslagen. Ziele waren u. a. die bessere Verzahnung der Hilfspotenziale des Bundes (insbesondere des THW) und der Länder (Feuerwehren und Hilfsorganisationen) sowie die Schaffung neuer Koordinierungsinstrumente für ein effizientes Zusammenwirken (TAB 2010, S. 40). In der Folge unterstützt bzw. ergänzt beispielsweise der Bund den Katastrophenschutz der Länder u. a. mit Einsatz- oder Spezialfahrzeugen, Ausrüstung (z. B. im Rahmen des CBRN-Schutzes) oder bei der Ausbildung der Einsatzkräfte.

2.4.2 Polizei

Zu den wichtigsten Aufgaben der Polizei gehören die polizeiliche Gefahrenabwehr sowie – als Teil der Strafverfolgungsbehörden unter Leitung der Staatsanwaltschaft – die Strafverfolgung.

Die polizeiliche Gefahrenabwehr dient der Beseitigung und Verhinderung von Gefahren und Störungen der öffentlichen Sicherheit und Ordnung, so insbesondere auch der Verhinderung von Straftaten. Sie umfasst auch Maßnahmen der Gefahrenvorsorge, durch die Gefahren, die zum Zeitpunkt des Handelns noch nicht konkret drohen, die aber später entstehen können, verhindert werden sollen oder durch die eine wirksame Bekämpfung solcher Gefahren ermöglicht werden soll. Hierzu gehört auch die Verhütung von Straftaten. Demgegenüber bezweckt die Strafverfolgung die Aufklärung von Straftaten, die in der Vergangenheit begangen wurden. Diese beinhaltet die Ermittlung und Verfolgung von Straftäter/innen einschließlich der Fahndung nach ihnen. Während also die Gefahren-

5 Gesetz zur Änderung des Zivilschutzgesetzes vom 2. April 2009 (BGBl. I S. 693)

abwehr präventiv-objektiv unmittelbar auf den Schutz der Integrität der Rechtsordnung und der durch sie geschützten Rechtsgüter zielt, ist die Strafverfolgung repressiv-personenbezogen auf die Aufklärung und Aburteilung von Straftaten ausgerichtet.[6]

Wie die nichtpolizeiliche liegt auch die polizeiliche Gefahrenabwehr vorrangig in der Verantwortung der Bundesländer, die durch Landesrecht Organisation, Aufgaben und Befugnisse der jeweiligen Polizeien regeln. Die 16 Landespolizeien weisen eine ähnliche organisatorische Struktur auf, die funktional nach Schutzpolizei (typische Aufgaben: Streifendienst, Verkehrskontrollen, Aufnahme und Bearbeitung von Strafanzeigen, Fahndungen), Kriminalpolizei (Bekämpfung schwerer Formen von Kriminalität) und Bereitschaftspolizei (Bewältigung von [länderübergreifenden] Großeinsätzen wie Demonstrationen oder Fußballspiele) unterscheidet (Groß 2008, S. 22). Teilweise deutliche Unterschiede existieren aber im Hinblick auf die gefahrenabwehrrechtlichen Aufgaben und Befugnisse der verschiedenen Landespolizeien.

Die gefahrenabwehrrechtlichen Gesetzgebungs- und Vollzugskompetenzen des Bundes beschränken sich auf spezifische polizeiliche Aufgabenfelder (Artikel 73, 87 ff. GG). So nimmt die Bundespolizei (BPol) neben dem Grenzschutz die Gefahrenabwehr im Bereich der Bahnanlagen des Bundes sowie des zivilen Luftverkehrs wahr und schützt die Verfassungsorgane des Bundes und die Bundesministerien. Das Bundeskriminalamt (BKA) ist für den Schutz der Mitglieder der Verfassungsorgane verantwortlich, unterstützt die Polizeien des Bundes und der Länder bei der Verhütung von Straftaten mit länderübergreifender oder internationaler Bedeutung und ist außerdem für die Gefahrenabwehr bei Bedrohungen durch den internationalen Terrorismus zuständig. Bestimmte präventive polizeiliche Aufgaben übernehmen schließlich das Zollkriminalamt und die Zollfahndungsämter, so u. a. die Verhütung von Straftaten gegen das Kriegswaffenkontrollgesetz (Geier 2017, S. 113 f.).

Dagegen ist die Gesetzgebung im Bereich der Strafverfolgung nach Artikel 74 Nr. 1 GG dem Bund zugewiesen. Dieser hat von seiner Gesetzgebungskompetenz insbesondere durch die Strafprozessordnung Gebrauch gemacht, die das Handeln der Polizeibehörden anleitet, soweit diese Aufgaben als Strafverfolgungsbehörde wahrnehmen. Auch im Bereich der Strafverfolgung stehen dem Bund nur bereichsspezifische Vollzugskompetenzen zu. So übernimmt beispielsweise das Bundeskriminalamt Aufgaben der Strafverfolgung in bestimmten Bereichen der internationalen und der schweren Kriminalität und unterstützt die Polizeien des Bundes und der Länder bei der Verfolgung von Straftaten mit länderübergreifender oder internationaler Bedeutung. Die Bundespolizei verfolgt

6 Zur teilweisen schwierigen Abgrenzung zwischen Maßnahmen der Gefahrenabwehr und der Strafverfolgung siehe z. B. BVerfG, Beschluss vom 18.12. 2018, 1 BvR 142/15, Rn. 66 ff. (Kfz-Kennzeichenkontrollen 2) und Kapitel 6.2.1

beispielsweise Straftaten, die sich gegen die Sicherheit der Grenze richten oder auf dem Gebiet der Bahnanlagen des Bundes begangen wurden.

2.4.3 Nichtstaatliche Akteure

Die Gewährleistung von Sicherheit ist eine der Kernaufgaben des modernen Staates, der – in den Worten des Bundesverfassungsgerichts – sogar seine »eigentliche und letzte Rechtfertigung« (BVerfG, Beschluss vom 1.8.1978, 2 BvR 1013, 1019, 1034/77, Rn. 115) aus dieser Aufgabe herleitet (Hempel 2016, S. 163). Gleichwohl ging mit den Veränderungen im Sicherheitsverständnis auch ein akteursbezogener Wandel einher, indem neben den traditionellen Behörden und Organisationen mit Sicherheitsaufgaben (BOS) weitere staatliche und zunehmend auch nichtstaatliche Akteure in die Bewältigung der Sicherheitsarbeit einbezogen wurden und immer noch werden (dazu und zum Folgenden Hempel 2016, S. 20, 97 u. 164). Beispielsweise sind innerhalb der letzten 25 Jahren zahlreiche Kooperationsformen zwischen der Polizei und privaten Sicherheitsdienstleistern entstanden, etwa im Bereich des Objektschutzes, der Fluggastkontrolle oder der Sicherheit an Bahnhöfen, in Asylbewerberheimen oder bei Veranstaltungen (Daase/Deitelhoff 2013, S. 63 f.). Heute arbeiten laut Groß (2019, S. 8) mit 250.000 Beschäftigten in etwa gleich viele Personen in der privaten Sicherheitsindustrie, wie es in Deutschland Polizeivollzugsbedienstete gibt. Auch Betreiber von kritischen Infrastrukturen kooperieren auf der Grundlage freiwilliger oder gesetzlicher Verpflichtungen mit den Sicherheitsbehörden, etwa Betreiber von öffentlichen Verkehrsmitteln durch die gemeinsame Nutzung von Videobeobachtungsanlagen oder Telekommunikationsunternehmen im Rahmen der Telekommunikationsüberwachung. Diese Formen der gemeinsamen Sicherheitsgewährleistung haben verschiedene faktische Hintergründe, u. a. gleichlaufende Sicherheitsinteressen, Effektivitätssteigerungen durch Kooperationen, Ressourcenprobleme bei den Sicherheitsbehörden, eine bessere technische Ausstattung privater Betreiber (z. B. im Kontext der Videobeobachtung) oder auch das Hineinwachsen privater Verantwortlichkeiten als Folge der Privatisierung vormals öffentlicher kritischer Infrastrukturen (z. B. im Kontext der Telekommunikationsüberwachung).

Die Umgestaltung betrifft aber insbesondere auch die Frage, wie gesellschaftliche Akteure, die bislang nicht mit Sicherheitsaufgaben assoziiert wurden, in die Sicherheitsvorsorge eingebunden werden (können). Dies bezieht sich etwa auf die Wissenschaft und Technikentwicklung, die u. a. technische Innovationen im Sicherheitsbereich beisteuern, oder die Medien, die sicherheitsbezogene Meldungen verbreiten, aber auch auf Wohnungsbaugesellschaften oder Betreiber von Einkaufzentren, Parkhäusern, Sport- oder Vergnügungsstätten, die mit entsprechenden Sicherheitsstrategien (kriminalpräventive Strategien, Schutzkonzepte, Videobeobachtung etc.) einen Beitrag leisten und damit zugleich für ihre Dienst-

leistungen oder Orte werben können. Nicht zuletzt sind es die Bürger/innen selbst, die zunehmend aktiven Anteil an der Sicherheitsarbeit nehmen oder nehmen sollen. Beispiele hier sind die spontane Hilfe während Katastrophenlagen, ehrenamtliche Polizeidienste (wie die »Sicherheitswacht« in Bayern und Sachsen, der »Freiwillige Polizeidienst« in Hessen und Baden-Württemberg oder die »Sicherheitspartner« in Brandenburg; Groß 2019, S. 7) oder die freiwillige Übersendung von Hinweisen oder privatem Foto- bzw. Videomaterial an Sicherheitsbehörden über Hinweisportale im Internet.

2.5 Gegenstand der Beobachtung in der zivilen Sicherheit

Mit dem Konzept der zivilen Sicherheit hat sich das Gefahrenspektrum und folglich auch die Anwendungsmöglichkeiten für Beobachtungstechnologien im Sicherheitsbereich erheblich erweitert, sodass heute eine enorme Vielfalt an technischen Lösungen und Einsatzformen existiert. Gleichwohl kann in Bezug auf den Gegenstand der Beobachtung zwar nicht generell, aber doch oft ein wesentlicher Unterschied zwischen polizeilichen und nichtpolizeilichen Einsatzformen festgestellt werden: Während sich Beobachtung in der nichtpolizeilichen Gefahrenabwehr häufig auf Unglücksfälle und die daraus resultierenden Personen- und Sachschäden bezieht, richtet sich das Beobachtungsinteresse im polizeilichen Bereich viel stärker auf den Menschen und seinen Aktivitäten.

2.5.1 Nichtpolizeiliche Gefahrenabwehr

Die Gesetze der Bundesländer legen den Handlungsrahmen für die Organisationen und Einrichtungen der nichtpolizeilichen Gefahrenabwehr fest (Kap. 2.4.1). Auch wenn sich diese im Detail teilweise unterscheiden, beziehen sich alle Gesetze auf einen nicht näher definierten Unfall, Notfall, Unglücksfall oder öffentlichen Notstand, bei dem Schäden an Personen, Tieren oder Sachwerten drohen oder bereits eingetreten sind, die bzw. deren Folgen es abzuwenden, abzumildern oder zu beseitigen gilt (dazu und zum Folgenden Hempel 2016, S. 109 ff.). Die zentralen Aufgaben der Beobachtung im Bereich der nichtpolizeilichen Gefahrenabwehr ergeben sich direkt aus dem Umstand, dass Un- oder Notfälle gleich welcher Art meist unvorhersehbar und zufällig geschehen: Erstens sollen Schadensereignisse möglichst zeitnah nach deren Eintritt entdeckt werden können, um Leben zu retten, Schäden möglichst gering zu halten und generell mehr Zeit für die Schadensbewältigung zu haben. Zweitens sind die am Schadensort eintreffenden Einsatzkräfte regelmäßig gezwungen, Gefahren für Personen und Sachen in einer oft diffusen Schadenslage innerhalb kürzester Zeit zu erkennen und zu bewerten, um schnell und effektiv geeignete Maßnahmen zur Rettung von

Menschenleben einzuleiten. Und drittens können sich Schadenslagen auch während des Einsatzes dynamisch entwickeln, was nicht zuletzt zur Gewährleistung der Sicherheit der Einsatzkräfte ein kontinuierliches Monitoring notwendig macht. Wie in den nachfolgenden Kapiteln ausgeführt wird, können Beobachtungstechnologien für die Ereignisfeststellung, die Lageerkundung und das Lagemonitoring von großem Nutzen sein.

2.5.2 Polizeiliche Gefahrenabwehr und Strafverfolgung

Im Fokus der polizeilichen Gefahrenabwehr und Strafverfolgung und folglich auch der polizeilichen Beobachtung stehen in erster Linie der Mensch und seine Aktivitäten, wobei es vor allem darum geht, auffälliges oder abweichendes Verhalten zu erkennen und zu dokumentieren. Es liegt daher auf der Hand, dass Beobachtungstechnologien für die Bewältigung polizeilicher Aufgaben von großer Bedeutung sind, sei dies in Form von Verkehrsradargeräten zur Geschwindigkeitskontrolle, von Metalldetektoren zur Personenkontrolle in sicherheitssensiblen Bereichen oder von Videokameras beispielsweise an kriminalitätsbelasteten öffentlichen Orten. Von einem offenen Einsatz von Beobachtungstechnologien wird außerdem eine kriminalpräventive Wirkung erwartet, indem die Beobachtung auf potenzielle Straftäter/innen einen abschreckenden Effekt hat.

In der polizeilichen Praxis dienen Beobachtungstechnologien heute auch oft der *verdeckten* Informationsbeschaffung. Als solche gehörten sie ursprünglich zum Instrumentarium der Nachrichtendienste, deren traditionelle Aufgabe in der Sammlung und Auswertung von Informationen zur Feststellung äußerer und innerer Gefahren für die Bundesrepublik Deutschland liegt und wofür sie mit weitrechenden Befugnissen zur heimlichen Datenbeschaffung und -analyse ausgestattet wurden. Dass seit den 1970er Jahren auch die Polizeibehörden nach und nach entsprechende Befugnisse erhalten haben, hat verschiedene Ursachen (dazu und zum Folgenden Albrecht 2010; Albers 2015; Bäcker 2015; Bäuerle 2008):

Die polizeiliche Nachfrage nach Maßnahmen zur verdeckten Informationsbeschaffung steht zunächst mit veränderten Formen der Kriminalität im Zusammenhang. Zu nennen sind vor allem der aufkommende Terrorismus seit den 1970er Jahren und andere Formen von organisierter oder aus Netzwerken entstehender Kriminalität (Drogen-, Menschen-, Waffenhandel, Bandenkriminalität etc.). Im Gegensatz zur konventionellen Kriminalität wie etwa Mord oder Totschlag geht es hier nicht nur um die Verfolgung *einzelner* begangener Straftaten (bzw. deren Verhinderung). Damit lässt sich die organisierte Kriminalität kaum effektiv bekämpfen, da sich einzelne Akteure der Organisationen einfach ersetzen lassen (beispielsweise einzelne Drogenhändler). Polizeiliche Maßnahmen müssen vielmehr darauf zielen, die Aktivitäten krimineller Organisationen insgesamt zu unterbinden. Dazu sind nicht nur täter-, sondern auch milieu-, umfeld- und kontaktbezogene Erkenntnisse zur Aufdeckung übergreifender krimineller

Strukturen notwendig, die mithilfe von Maßnahmen für die heimliche Informationsbeschaffung gewonnen werden sollen. Bei der Terrorismusbekämpfung kommt hinzu, dass Anschlagsvorbereitungen sich über einen langen Zeitraum im Verborgenen vollziehen und dann rasch in schwerwiegende Schäden einmünden können. Der hergebrachte Ansatz, dass die Polizei auf konkrete Krisenlagen reagiert, droht hier vielfach zu spät zu kommen und bedarf darum der Ergänzung um ein vorverlagertes Beobachtungsinstrumentarium, mit dessen Hilfe Vorbereitungshandlungen frühzeitig erkannt werden können (Bäcker 2019). Entsprechend wurde etwa die Telekommunikationsüberwachung (TKÜ) im Zuge der Notstandsgesetze von 1968 in die Strafprozessordnung eingeführt, die in weiteren Schüben um zusätzliche verdeckte Ermittlungsmethoden erweitert wurde. Ab 1992 wurde auch damit begonnen, die Polizeibehörden der Länder mit entsprechenden Befugnissen zum Zwecke der Gefahrenabwehr auszustatten.

Die neuen Kriminalitätsformen, aber auch der im Zuge der Erweiterung des Sicherheitsbegriffs einsetzende Wandel zu einer stärker proaktiven Sicherheitspolitik sind auch Gründe für die Einführung des Präventionsprinzips in die polizeiliche Praxis: Während traditionell nur das Vorliegen einer konkreten, unmittelbar bevorstehenden oder gegenwärtigen Gefahr bzw. ein Anfangsverdacht auf eine begangene Straftat polizeiliches Handeln auslösen und legitimieren konnte, wurde die Polizeiarbeit nach und nach auch auf die vorbeugende Verbrechensbekämpfung ausgerichtet. Kennzeichnend hierfür ist die Ausdehnung polizeilicher Eingriffsbefugnisse auf das erweiterte Vorfeld des Verdachts bzw. von Gefahrenlagen oder – alternativ bzw. auch kumulativ – die Schaffung neuer strafrechtlicher Vorfeldtatbestände, die Vorbereitungs-, Unterstützungs- oder Organisationshandlungen vor der eigentlichen Rechtsgutverletzung unter Strafe stellen. Gerade für Vorfeldermittlungen spielen Methoden der heimlichen Informationsbeschaffung eine zentrale Rolle, um kriminelle Strukturen und Potenziale zu erkennen, noch bevor Straftaten oder Gefahren überhaupt sichtbar werden. Ein in diesem Zusammenhang einschneidendes Ereignis waren die Terroranschläge des 11. September 2001 in den USA, die eine ganze Reihe an Gesetzgebungsmaßnahmen in Gang setzten, um die Sicherheitsbehörden mit präventiven und insbesondere auch verdeckten Ermittlungsbefugnissen zur Terrorismusbekämpfung auszustatten. Beispielhaft sei das Terrorismusbekämpfungsgesetz vom 30. November 2001[7] (Sicherheitspaket II) genannt, das vor allem die Nachrichtendienste adressierte, oder das Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt[8], durch welches 2009 das BKA erstmals mit weitreichenden präventivpolizeilichen Befugnissen auch für die verdeckte Informationsbeschaffung ausgestattet wurde.[9]

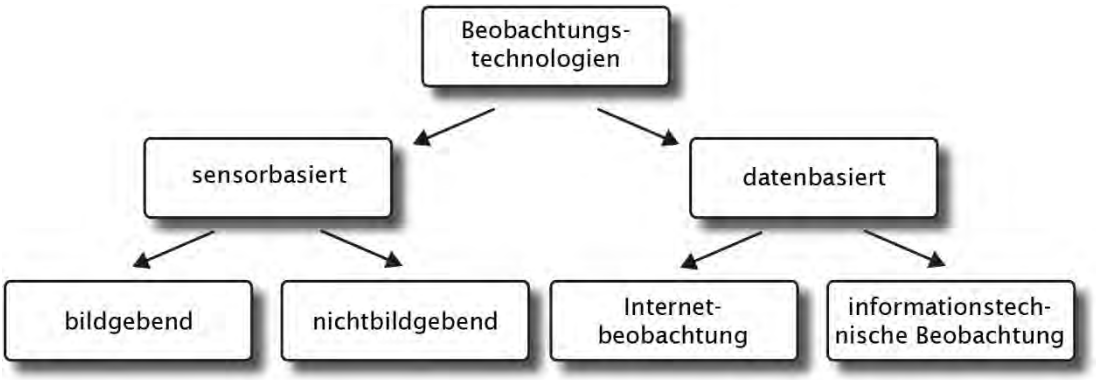
7 BGBl. I 2001, S. 361
8 BGBl. I 2008, S. 3083
9 Eine Darstellung der historischen Entwicklung der Sicherheitsgesetzgebung in Deutschland findet sich beispielsweise in Bäcker et al. (2013, S. 16 ff.).

Prävention kann allerdings auch eine problematische Dynamik bergen: Aufgrund der zahlreichen, oft unbestimmten Gefahrenquellen lässt sie sich immer erweitern, weiter vorverlagern und verbessern und dient so der Legitimierung für die Beobachtung immer breiterer Personenkreise, auch wenn diese dafür keinen Anlass gegeben haben. Eine auf Generalprävention angelegte Sicherheitspolitik müsste letztlich jeden, auch jeden Unschuldigen, als potenziell gefährlich ansehen (Daase/Deitelhoff 2013, S. 23).

2.6 Systematik der Beobachtungstechnologien

Es ist bereits deutlich geworden, dass das Spektrum der heute im zivilen Sicherheitsbereich eingesetzten Beobachtungstechnologien sehr breit ist. Zur Systematisierung (und Gliederung der nachfolgenden Ausführungen) bietet es sich an, zwischen sensor- und datenbasierten Beobachtungstechnologien zu unterscheiden (Abb. 2.1): Sensorbasierte Beobachtungstechnologien erfassen bestimmte physikalische oder chemische Eigenschaften der realen Welt und bereiten die Messgrößen in für den Menschen leicht interpretierbare Informationen auf. Datenbasierte Beobachtungstechnologien hingegen bezwecken die Erhebung und Auswertung von Informationen der digitalen Welt. Zentrale Beobachtungsräume sind hier das Internet und seine Anwendungen, die Dienste und Infrastrukturen der Telekommunikation sowie informationstechnische Endgeräte wie beispielsweise PCs oder Smartphones.

Abb. 2.1 Systematik der Beobachtungstechnologien



Eigene Darstellung nach Hempel (2016, S. 34)

Sensorbasierte Beobachtungstechnologien lassen sich weiter in bildgebende und nichtbildgebende Verfahren einteilen. Die Unterscheidung fußt darauf, dass bildgebende Beobachtungstechnologien durch die Erfassung der von Objekten ausgehenden elektromagnetischen Strahlung ortsaufgelöste Messwerte liefern (so korrespondiert beispielsweise ein Pixel des Sensors einer Videokamera mit einer

Ortskoordinate im Objektraum). Die Interpretation dieser Daten fällt uns Menschen leicht, weil das Auge in Kombination mit dem Gehirn ähnlich funktioniert. Dementsprechend nehmen bildgebende sensorbasierte Beobachtungstechnologien im Bereich der zivilen Sicherheit einen großen Raum ein (Kap. 3.1). Aber auch nichtbildgebende sensorbasierte Beobachtungstechnologien sind im zivilen Sicherheitsbereich von großer Bedeutung. Beispiele sind Metalldetektoren, Mikrofone für die akustische Beobachtung oder Sensoren zum Nachweis toxischer Gase (Kap. 3.2).

Datenbasierte Beobachtungstechnologien gewinnen in der Folge der zunehmenden digitalen Durchdringung aller Lebensbereiche insbesondere als polizeiliche Informationsquelle immer stärker an Bedeutung. Zu unterscheiden ist grundsätzlich danach, ob nur öffentlich zugängliche Inhalte im Internet erhoben und ausgewertet werden (im Folgenden als *Internetbeobachtung* bezeichnet, Kap. 4) oder ob auch persönliche Daten beobachtetet werden, die jemand in der berechtigten Erwartung auf die Vertraulichkeit und Integrität dieser Systeme einem informationstechnischen System anvertraut hat (im Folgenden als *informationstechnische Beobachtung* bezeichnet, Kap. 5).

3 Sensorbasierte Beobachtung

Der Mensch nimmt große Teile der Informationen aus seiner Umwelt über die Augen auf. Insofern kommt der bildgebenden Sensorik im Kontext technisierter Beobachtung auch ein hoher Stellenwert zu. Dies lässt sich sowohl anhand des Einsatzspektrums (Boden, Luft, Weltraum) als auch hinsichtlich der breiten Nutzung des physikalischen Spektralbereichs nachvollziehen (Kap. 3.1). Für Aufgaben im Bereich der zivilen Sicherheit werden aber auch nichtbildgebende Beobachtungsverfahren genutzt. Man denke beispielsweise an Metalldetektoren für Zutrittskontrollen, Geigerzähler zur Messung von Radioaktivität oder Gassensoren zum Nachweis toxischer Gase (Kap. 3.2). Immer stärkere Bedeutung gewinnen schließlich automatisierte Verfahren zur Verarbeitung und Auswertung von Daten, die mit einzelnen oder zu Netzwerken zusammengeschlossenen Sensoren erfasst werden (Kap. 3.3).

Einen umfassenden Überblick über sämtliche Sensortechnologien und Datenauswertungsverfahren zu geben, die potenziell zu Beobachtungszwecken im Bereich der zivilen Sicherheit eingesetzt werden (könnten), würde den Umfang des vorliegenden Berichts sprengen. Deshalb wird sich in diesem Kapitel auf wichtige Beobachtungstechnologien konzentriert, die für zivile Sicherheitsaufgaben bereits heute genutzt werden oder deren Anwendung in naher Zukunft wahrscheinlich ist. Von diesen spielt die Videobeobachtung eine herausragende Rolle. Dies betrifft nicht nur die Verbreitung von Videokameras in zahlreichen Anwendungskontexten und entsprechend auch die Vielfalt der Einsatzpraktiken und involvierten Akteure, sondern auch neue Nutzungsmöglichkeiten durch die Anwendung von komplexen Verfahren der automatisierten Datenauswertung. Die Videobeobachtung wird daher in den Kapiteln 3.4 und 3.5 vertieft behandelt.

Die Ausführungen in den Kapiteln 3.1 bis 3.3 basieren – sofern nicht durch weitere Quellenangaben markiert – auf den Kapiteln 3 bis 5 des Gutachtens von Hempel (2016). Wesentliche Teile der Gutachtenkapitel wurden unter der Leitung von Prof. Dr. Heinz-Wilhelm Hübers am Institut für optische Sensorsysteme des Deutschen Zentrums für Luft- und Raumfahrt (DLR) durch Dr. Anko Börner, Dr. Andreas Eckardt, Eugen Funk, Frank Lehmann sowie Prof. Dr. Ralf Reulke verfasst. Weitere Beiträge steuerten Fredrick Schütte von der antwortING GmbH, Marc Hübner, Dozent am Institut der Feuerwehr Nordrhein-Westfalen, sowie Dr. Stefan Taing von der Munich Innovation Labs GmbH bei. Allen beteiligten Fachexperten sei an dieser Stelle herzlich gedankt.

3.1 Bildgebende Beobachtungstechnologien

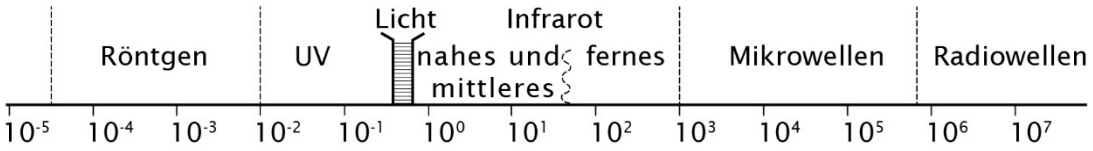
Bildgebende Beobachtungstechnologien nutzen Sensoren zur Messung der von Objekten ausgesandten elektromagnetischen Strahlung und stellen die Messwerte

typischerweise als zweidimensionale Projektion der realen Welt dar. Sie werden in unterschiedlichsten Ausführungen für eine Vielzahl von Anwendungen eingesetzt. Aus praktischer Perspektive orientiert sich eine mögliche Einteilung der Nutzungspraktiken am Einsatzort der Technologie (Boden, Luft, Weltraum). Ein aus technischer Sicht besser geeignetes Kriterium bildet der von den jeweiligen Sensoren erfasste Bereich des elektromagnetischen Spektrums. Im Folgenden soll daher erst die relevante Sensortechnik dargestellt werden, um vom Einsatzort der Beobachtungstechnologie ausgehend sodann wichtige Sicherheitsanwendungen vorzustellen (wobei sich Dopplungen allerdings nicht vollständig vermeiden lassen).

3.1.1 Sensoren für bildgebende Beobachtungstechnologien

Heute sind Sensoren für das gesamte elektromagnetische Spektrum verfügbar (Abb. 3.1). Digitale Foto- oder Videokameras (Abb. 3.2, links) zur Bildgebung im Bereich des *sichtbaren Lichts* (Wellenlängen: 0,4 bis 0,7 Mikrometer) sind üblicherweise mit halbleiterbasierten Sensoren ausgestattet, die aus mehreren Millionen Fotodioden aufgebaut sind. Jede Fotodiode erzeugt bei Strahlungseinfall einen messbaren elektrischen Strom, dessen Stärke proportional zur Lichtintensität ist. Farbige Bilder werden erzeugt, indem vor den einzelnen Detektoren angebrachte Farbfilter nur rotes, grünes oder blaues Licht passieren lassen. Die Farbintensitäten der einzelnen Pixel werden dann durch einfache Datenverarbeitung so aufeinander abgestimmt, dass der Farbeindruck jenem des menschlichen Sehens möglichst nahekommt.

Abb. 3.1 Elektromagnetisches Spektrum



Quelle: TAB 2012, S. 31

An das sichtbare Licht schließt sich in Richtung längerer Wellenlängen der für das menschliche Auge nicht sichtbare Bereich der *nahen bis mittleren Infrarotstrahlung* an (IR-Strahlung; Wellenlängen: 0,7 bis ca. 50 Mikrometer). Objekte emittieren in Abhängigkeit ihrer Temperatur ein charakteristisches Strahlungsspektrum (Planck'sches Strahlungsgesetzes), das bei Temperaturen bis einige 1.000°C sein Emissionsmaximum in Bereich der IR-Strahlung hat. Dies nutzen Wärmebildkameras (auch als Thermalkameras bezeichnet) aus, um Oberflächentemperaturen von Objekten sichtbar zu machen (die Darstellung der Temperatur-

verteilung erfolgt entweder in Schwarz-Weiß oder in Falschfarben). Bei einer Aufnahmedauer von 1 Millisekunde erzielen moderne IR-Kameras Temperaturauflösungen von ungefähr einem hundertstel Grad. Mit kurzen Belichtungszeiten können somit hochempfindliche Messungen durchgeführt werden. Aufbau und Funktionsweise von Wärmebildkameras sind ähnlich wie bei herkömmlichen Kameras (Abb. 3.2, rechts). Als Detektoren kommen entweder Quecksilber-Cadmium-Tellurid-Detektoren (IR-Strahlen erzeugen einen messbaren elektrischen Strom) oder Mikrobolometer (IR-Strahlen führen durch Erwärmung zu messbaren Veränderungen im elektrischen Widerstand) zur Anwendung. Heute erhältliche Sensoren bestehen aus ungefähr einer Million solcher Einzeldetektoren. Die Auflösung ist damit im Vergleich zu herkömmlichen Kameras niedriger, gleichwohl für viele Anwendungen im Sicherheitsbereich ausreichend (Kap. 3.1.2.2).

Abb. 3.2 Kameras für sichtbares Licht und IR-Strahlung im Vergleich

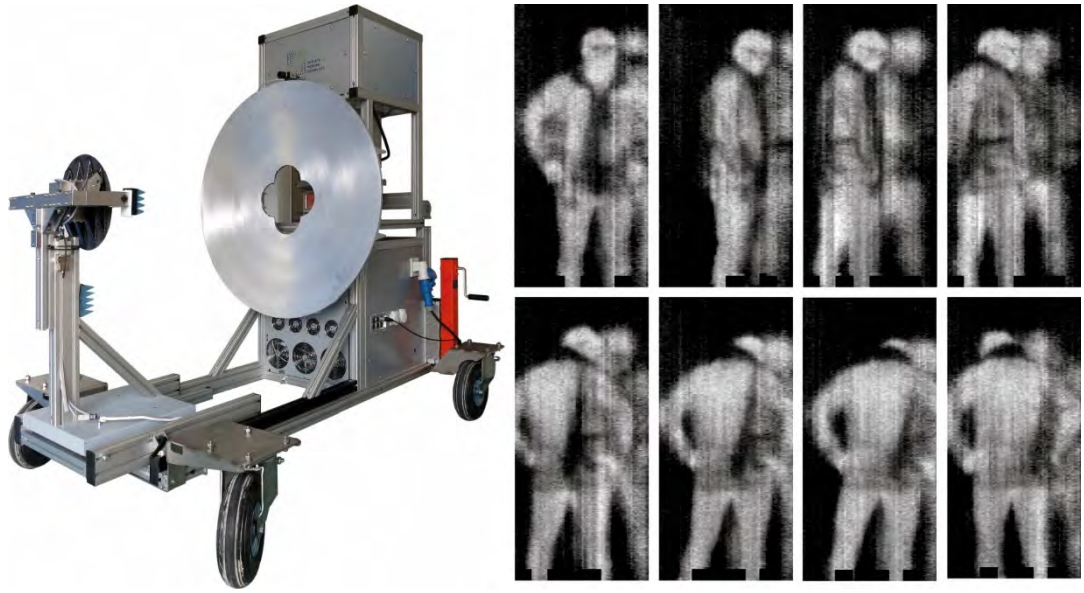
Quellen: links: Bosch Sicherheitssysteme GmbH; rechts: mit freundlicher Genehmigung der InfraTec GmbH

Längere Wellenlängen weist das *ferne Infrarot* auf, das auch als Terahertz (THz)-Strahlung bezeichnet wird (Wellenlängen: ca. 50 Mikrometer bis 1 Millimeter). Dieser Spektralbereich ist technologisch noch vergleichsweise wenig erschlossen, bietet aber für Sicherheitsanwendung ein großes Potenzial (Hoffknecht et al. 2006). Nach demselben Funktionsprinzip wie Wärmebildkameras ermöglichen Kameras auf Basis von THz-Strahlung die Sichtbarmachung von Oberflächentemperaturen. Zugleich durchdringt THz-Strahlung dünne Schichten von unpolaren Materialien[10] wie Textilien, Kunststoffe oder Papier. Dies lässt sich nutzen, um unter der Kleidung verborgene, auch nichtmetallische Gegenstände (z. B.

10 Die Moleküle in unpolaren Stoffen sind elektrisch neutral. Dagegen weisen die Moleküle in polaren Stoffen (z. B. Wasser) aufgrund von Ladungsverschiebungen ein permanentes elektrisches Dipolmoment auf, wodurch polare Stoffe die THz-Strahlung absorbieren.

Handfeuerwaffen, Keramikmesser) selbst aus einer Entfernung von einigen 10 Metern darzustellen (Abb. 3.3, rechts). Dazu wird die von Personen bzw. Objekten natürlich emittierte THz-Strahlung gemessen (*passive* THz-Bildgebung), weshalb – etwa im Gegensatz zur Beobachtung mithilfe von Röntgenstrahlen – der Einsatz von passiven THz-Kameras gesundheitlich unbedenklich ist. Allerdings erfordert die passive THz-Bildgebung große Spiegeloptiken sowie empfindliche supraleitende Mikrobolometer als Detektoren, die auf Temperaturen unterhalb von 5 K (-268 °C) gekühlt werden müssen (Abb. 3.3, links). An der Weiterentwicklung von THz-Kameras wird – auch unterstützt durch die Projektförderung im Rahmen der zivilen Sicherheitsforschung des Bundes[11] – intensiv gearbeitet. Die wesentliche Herausforderung besteht darin, die Geräte einfacher, flexibler und nutzerfreundlicher zu gestalten.

Abb. 3.3 Prototyp einer passiven THz-Videokamera und damit aufgenommene Videosequenz



Videosequenz einer Testperson mit Maschinenpistole, versteckt unter einer Winterjacke (mit Spiegelbild). Die Waffe ist gegenüber dem Hintergrund (menschliche Haut) gut erkennbar. Distanz der Person zur Kamera ca. 20 m.

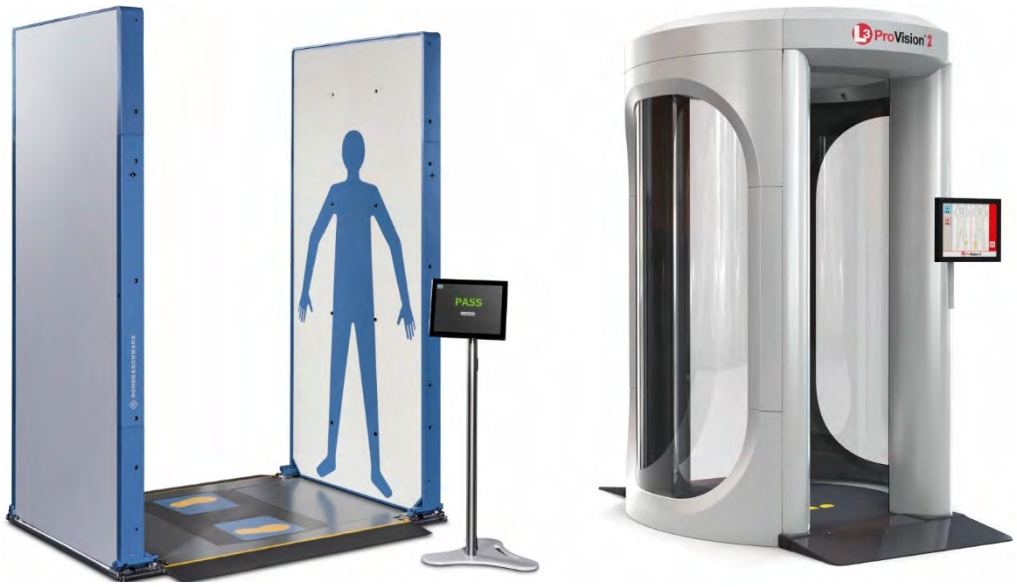
Quelle: ROHDE & SCHWARZ GmbH & Co. KG, Supracon AG

11 Beispielsweise in den Projekten »Passive THz-Videokamera für Sicherheitsanwendungen« (THz-Videocam; Laufzeit 2007 bis 2010); »Demonstration einer Weitwinkel-Terahertz-Wärmebildkamera für die Personenkontrolle« (THz-Videocam-TWO; Laufzeit 2012 bis 2014) oder »Multimodale Fernerkennung verborgener Gefahrenpotenziale in der Personenkontrolle« (HITD; Laufzeit 2018 bis 2021) (https://sifo.bmbfcluster.de/files/CBRNE_Bekanntm._600x800_D_THzVideocam.pdf, https://sifo.bmbfcluster.de/files/Projektumriss_THz-Videocam-TWO.pdf, https://sifo.bmbfcluster.de/files/Projektumriss_HITD.pdf, 31.3.2022).

Alternativ hierzu kann die zu untersuchende Szene oder das zu untersuchende Objekt mit THz-Strahlung angestrahlt werden, um durch diese *aktive* THz-Bildgebung die gestreute und reflektierte Strahlung zu messen. Schwierigkeiten bestehen hier u. a. in ungewollten Reflexionen von unpolaren Materialien (z. B. der Kleider) und bei der Erzeugung geeigneter THz-Strahlung (Heinz et al. 2015, S. 881). Außerdem stellt sich bei der aktiven THz-Bildgebung die Frage nach möglichen Gesundheitsrisiken.

Auf die THz-Strahlung folgen im elektromagnetischen Spektrum die Millimeterwellen (Wellenlängen: 1 bis 10 Millimeter; Teil der Mikrowellen), die ebenfalls Textilien durchdringen. Heute kommerziell verfügbare Sicherheitsscanner zur Personenkontrolle (Körperscanner) beruhen auf Millimeterwellen. Die Systeme werden mit offener oder geschlossener Architektur konzipiert (Abb. 3.4; dazu Kap. 3.1.2.3). Anders als bei der THz-Strahlung reicht jedoch die Leistung der von Personen bzw. Objekten natürlich emittierten Millimeterwellen nicht aus, um detektiert zu werden. Deshalb ist hier eine künstliche Beleuchtung notwendig. Ein weiterer Nachteil gegenüber THz-Strahlung ist die aufgrund der größeren Wellenlängen geringere optische Auflösung von Millimeterwellen. Sie eignen sich daher nur für die Nahfeldabtastung.

Abb. 3.4 Millimeterwellenkörperscanner



R&S QPS 201 von Rohde & Schwarz und ProVision 2 von L3-Communications

Quellen: links: Rohde & Schwarz GmbH & Co. KG;
rechts: EAS Envimet Analytical Systems GmbH

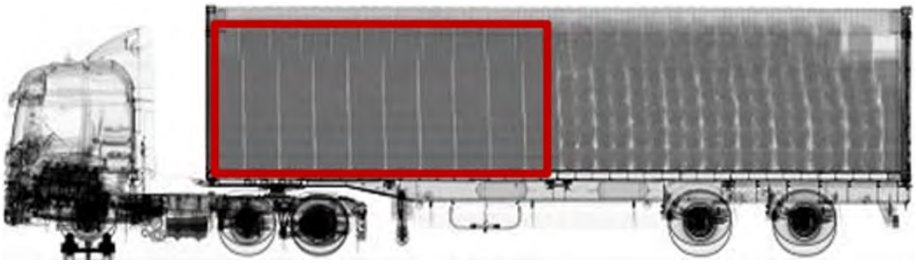
Radar-(Radio-Detection-and-Ranging-)Systeme arbeiten meist mit Wellenlängen zwischen 3 bis 30 Zentimetern (Teil der Mikrowellen). Eine wichtige An-

wendung ist die Beobachtung von bewegten Objekten wie Flugzeugen oder Schiffen. Aber auch beispielsweise Abstandssensoren in Kfz basieren auf Radartechnologie. Es werden keine Bilder im eigentlichen Sinne erzeugt, sondern Entfernungen zu Objekten bestimmt. Dazu sendet ein Impulsradar kurze Strahlungsimpulse aus und misst die Zeit, bis die von einem Objekt reflektierte Strahlung wieder eintrifft. Daraus und aus der Ausrichtung der Radarantenne lassen sich dann Abstand, Richtung und Geschwindigkeit des Objekts bestimmen. Bekannte Einsatzfelder sind die Flugraumüberwachung, Radargeräte zur Geschwindigkeitsmessung im Straßenverkehr oder das Niederschlagsradar. Darüber hinaus gibt es auch bildgebende Radarverfahren, etwa zur Erstellung von dreidimensionalen Modellen der Erdoberfläche mithilfe von Satelliten (dazu Kap. 3.1.4.2).

Radiowellen haben noch größere Wellenlängen im Bereich von Metern bis Kilometern. Sie werden von kleinen Objekten nicht reflektiert, sodass sie in der Satellitenfernerkundung beispielsweise zur Abbildung von Geländeoberflächen unter Baumkronen eingesetzt werden können. Bei entsprechenden Radarsystemen gibt es allerdings noch erheblichen Forschungsbedarf (TAB 2012, S. 33 f.).

Im Spektralbereich mit kürzeren Wellenlängen als sichtbares Licht werden *Röntgenstrahlen* (Wellenlängen: 0,01 bis 10 Nanometer) zur Bildgebung eingesetzt. Vorteile der Röntgenstrahlung sind ihre hohe Durchdringungsfähigkeit und optische Auflösung. Sie werden standardmäßig zur Durchleuchtung von Gepäck und anderen unbelebten Gegenständen bei Zugangskontrollen in öffentlichen Gebäuden, an Flughäfen, auf Firmengeländen oder zur gezielten Überprüfung von Paket- oder Postsendungen eingesetzt. Größere Geräte, sogenannte Portallösungen, können ganze Schiffscontainer oder Lkw durchleuchten (Abb. 3.5), wobei diese Technologie bislang lediglich zur Suche nach Schmuggelware oder gefährlichen Gegenständen an Grenzen oder an Seefrachthäfen zum Containerscreening eingesetzt wird (Kasten 3.1). Von der Röntgendurchstrahlung ist die Röntgenrückstreuung abzugrenzen. Je nach Dichte und Material eines Objekts werden die Röntgenstrahlen unterschiedlich stark reflektiert. Dies kann zur Bildgebung mit einer im Vergleich zur Durchstrahlung viel geringeren Strahlungsintensität eingesetzt werden.

Abb. 3.5 Schmuggelzigaretten im Röntgendurchstrahlungsbild eines Lkw-Anhängers



Quelle: Visser et al. 2016

Kasten 3.1 Personendetektion durch Röntgenstrahlung?

Die Detektion von Personen durch Röntgenstrahlung ist bislang nicht Ziel etablierter Beobachtungsverfahren. Die bei der Durchstrahlungsüberprüfung eingesetzte intensive Röntgenstrahlung stellt ein erhebliches Gesundheitsrisiko dar, weil diese als ionisierende Strahlung lebende Zellen schädigt. Gemäß der Strahlenschutzverordnung (StrlSchV[12]) dürfen daher Röntgenstrahlen aus Strahlenschutzgründen in Deutschland nicht für Sicherheitskontrollen an Personen eingesetzt werden, solange es hierfür keine gesetzliche Grundlage gibt (Anlage 1, Teil B, Punkt 7 StrlSchV). Auch laut der Durchführungsverordnung (EU) 2015/1998[13] (Nr. 4.1.1.2) sind sie für die Personenkontrolle an Flughäfen nicht vorgesehen.

Ob sich die notwendige Strahlendosis durch das Verfahren der Röntgenrückstreuung soweit reduziert lässt, dass ein Einsatz zur Personendetektion als gesundheitlich unbedenklich eingestuft werden kann, ist bislang ungeklärt.

3.1.2 Bodengestützte bildgebende Beobachtungstechnologien

Nach der kurzen Einführung in die Sensortechnik richtet sich das Augenmerk in den nachfolgenden Kapiteln 3.1.2 bis 3.1.4 auf wichtige Anwendungsfelder von bildgebenden Beobachtungstechnologien im Bereich der zivilen Sicherheit.

3.1.2.1 Videokameras

Videokameras gehören zu den am weitesten verbreiteten Beobachtungstechnologien. Zentrales Einsatzfeld im Bereich der zivilen Sicherheit ist die Videobe-

12 Strahlenschutzverordnung vom 29. November 2018 (BGBl. I S. 2034, 2036)
13 Durchführungsverordnung (EU) 2015/1998 zur Festlegung detaillierter Maßnahmen für die Durchführung der gemeinsamen Grundstandards für die Luftsicherheit

obachtung. Grundsätzlich kann zwischen zwei Anwendungsformen unterschieden werden:

- Bei der Videobeobachtung in Echtzeit (Monitoring) werden Videobilder des beobachteten Raums auf einen Monitor übertragen und zeitgleich durch einen menschlichen Betrachter (im Folgenden Videobeobachter) ausgewertet. Das Bildmaterial kann zusätzlich für eine spätere Verwendung (temporär) gespeichert werden.
- Bei reinen Aufzeichnungslösungen (Blackboxlösungen) werden die Videobilder lediglich (temporär) gespeichert. Die Auswertung des Bildmaterials durch Menschen erfolgt nur, wenn sicherheitsrelevante Vorkommnisse dies erforderlich machen.

Die für die Videobeobachtung notwendige Sensor-, Übermittlungs- und Speichertechnik ist im Kern ausgereift, kostengünstig und einfach in der Anwendung. Seit ca. 2013 sind Videokameras mit einer Auflösung von 2 Megapixeln (1.080p Full-HD) erhältlich, mit denen Personengesichter bis auf eine Entfernung von 3 bis 10 Metern (in Abhängigkeit des Blickwinkels) noch erkennbar sind. Zunehmend setzen sich 4-, 8- oder sogar 16-Megapixelkameras durch.[14] Moderne Videobeobachtungssysteme können aus einer Vielzahl an schwenk- und zoomfähigen Kameras aufgebaut sein, die sich durch den Videobeobachter per Fernsteuerung bedienen lassen. Im Gegensatz zu HD- und Megapixelkameras, die über ein einziges Objektiv verfügen, arbeiten Multifocalkameras mit mehreren Objektiven unterschiedlicher Brennweite. Dies erlaubt die Beobachtung großer Areale, wobei gleichzeitig Objekte im Nah- und Fernbereich hochaufgelöst dargestellt werden können. Mit geringem Hardwareeinsatz lassen sich so beispielsweise in Fußballstadien gleichzeitig Überblicksbilder und entfernte Details (z. B. ein Gesicht) beobachten (Hempel 2016, S. 127). Schließlich können heute gängige digitale Bildsensoren Strahlung im nahen IR-Bereich noch erfassen, wodurch sich einfache Nachtsichtfunktionen realisieren lassen. Technische Weiterentwicklungen sind hinsichtlich der Erweiterung des Spektralbereichs, der Vergrößerung der Empfindlichkeit, der Erhöhung der Bildauflösung sowie der Steigerung der Bildqualität (z. B. durch softwaregestützte Bildstabilisierung) zu erwarten.

Die größte technische Herausforderung besteht heute allerdings in der Verwaltung und Handhabung der riesigen Datenmengen durch die stetig wachsende Zahl der eingesetzten Videokameras. Moderne Videobeobachtungssysteme greifen daher zunehmend auf automatisierte Prozesse der Bildanalyse und -interpretation zurück, die den menschlichen Betrachter bei der Bildauswertung unterstützen sollen (dazu Kap. 3.3).

Die Anwendungsfelder der Videobeobachtung im Bereich der zivilen Sicherheit weisen in Bezug auf Einsatzkontext, Zielsetzung und beteiligte Akteure eine

14 https://www.topsicherheit.de/ueberwachungskameras.htm (31.3.2022)

große Bandbreite auf. Die häufigste Anwendungsform ist die offene Videobeobachtung im öffentlich zugänglichen Raum. Sie wird von der Polizei zum Zweck der Gefahrenabwehr beispielsweise an kriminalitätsbelasteten Orten eingesetzt. Der weit überwiegende Teil der im öffentlich zugänglichen Raum installierten Videokameras (z. B. in öffentlichen Verkehrsmitteln, Museen, Einkaufzentren, Sportstadien) wird aber von nichtpolizeilichen öffentlichen oder privaten Akteuren temporär (z. B. im Rahmen von Großveranstaltungen) oder als Dauermaßnahme betrieben. Neben Sicherheitsbelangen der anwesenden Personen stehen hier häufig auch andere (z. B. unternehmerische) Interessen im Vordergrund (z. B. Wahrnehmung des Hausrechts, Schutz vor Vandalismus oder Diebstahl, Kontrolle betrieblicher Abläufe). Grundsätzlich können Videoaufzeichnungen aus der polizeilichen, nichtpolizeilichen öffentlichen oder privaten Videobeobachtung für die Strafverfolgung von Nutzen sein. Der Einsatz von Videobeobachtung im öffentlich zugänglichen Raum wird in Kapitel 3.4 in Bezug auf den rechtlichen Rahmen, aktuelle Praktiken und ihre Wirkungen im Bereich der zivilen Sicherheit vertieft behandelt.

Von der offenen Videobeobachtung im öffentlich zugänglichen Raum in Zielsetzung und Wirkung grundsätzlich verschieden ist der polizeiliche Einsatz von Videotechnik zur heimlichen Beobachtung einzelner Personen. Da dies das aus dem allgemeinen Persönlichkeitsrecht abgeleitete Recht auf informationelle Selbstbestimmung (Kap. 6.1.2.1) in besonderer Weise berührt, dürfen entsprechende Maßnahmen nur unter engen gesetzlichen Voraussetzungen durchgeführt werden. Im Bereich der polizeilichen Gefahrenabwehr ist beispielsweise das BKA zu verdeckten Observationsmaßnahmen mit Videotechnik außerhalb von Wohnungen befugt, um Schäden für bedeutsame Rechtsgüter durch terroristische Straftaten zu verhüten, falls dies auf andere Weise aussichtslos oder wesentlich erschwert wäre (§ 45 Bundeskriminalamtgesetz – BKAG[15]). Vergleichbare gefahrenabwehrrechtliche Befugnisse zur Herstellung heimlicher Videoaufnahmen besitzen in ihren jeweiligen Zuständigkeitsbereichen auch die Bundespolizei (§ 28 Bundespolizeigesetz – BPolG[16]), das Zollkriminalamt und die Zollfahndungsämter (§§ 19, 29 Zollfahndungsdienstgesetz – ZFdG[17]) sowie die Polizeien der Bundesländer (z. B. § 15 Hessisches Gesetz über die öffentliche Sicherheit und Ordnung – HSOG[18]).

Verdeckte Videoaufnahmen in einer Wohnung greifen darüber hinaus in die grundgesetzlich geschützte Unverletzlichkeit der Wohnung (Artikel 13 GG) ein und dürfen beispielsweise durch das BKA nur zur Abwehr von dringenden

15 Bundeskriminalamtgesetz vom 1. Juni 2017 (BGBl. I S. 1354)
16 Bundespolizeigesetz vom 19. Oktober 1994 (BGBl. I S. 2978, 2979), das zuletzt durch Artikel 1 des Gesetzes vom 5. Mai 2017 (BGBl. I S. 1066) geändert worden ist
17 Zollfahndungsdienstgesetz vom 16. August 2002 (BGBl. I S. 3202), das zuletzt durch Artikel 15 des Gesetzes vom 17. August 2017 (BGBl. I S. 3202) geändert worden ist
18 Hessisches Gesetz über die öffentliche Sicherheit und Ordnung in der Fassung der Bekanntmachung vom 14. Januar 2005 (GVBl. I S. 14), zuletzt geändert durch Artikel 2 des Gesetzes vom 23. August 2018 (GVBl. S. 374)

Gefahren auf Grundlage einer richterlichen Anordnung[19] durchgeführt werden (§ 46 BKAG). Ausweislich der jährlich durch das Bundesamt für Justiz veröffentlichten Statistik werden Maßnahmen der optischen (und/oder akustischen, Kap. 3.2.1.1) Wohnraumüberwachung[20] im Bereich der Gefahrenabwehr durch das BKA (und alle anderen Behörden im Zuständigkeitsbereich des Bundes) nur sehr selten eingesetzt – zwischen 2008 und 2020 in insgesamt drei Verfahren.

Im Bereich der Strafverfolgung können Beschuldigte nach § 100h Strafprozessordnung (StPO)[21] auch ohne ihr Wissen außerhalb von Wohnungen mit Videotechnik beobachtet werden, falls ein Anfangsverdacht auf eine Straftat von erheblicher Bedeutung[22] vorliegt. Eine optische Wohnraumüberwachung ist hingegen im strafrechtlichen Ermittlungsverfahren unzulässig.

Die Einsatzmöglichkeiten von Videokameras im Bereich der zivilen Sicherheit beschränken sich aber nicht nur auf die Videobeobachtung im öffentlich zugänglichen Raum oder auf verdeckte polizeiliche Observationsmaßnahmen. Einige Anwendungsbeispiele in der nichtpolizeiliche Gefahrenabwehr sind:

- Das Land Brandenburg beobachtet seine Waldgebiete flächendeckend mit dem Waldbrandfrüherkennungssystem »Fire Watch«. Es besteht aus 108 einzelnen, über das gesamte Waldgebiet verteilten Videokameras. Jede Kamera erfasst den Spektralbereich vom sichtbaren Licht bis ins nahe IR und kann so die typischen Grauwerte einer Rauchwolke in der Brandfrühphase bis in eine Entfernung von 15 Kilometern bei Tag und Nacht automatisiert erkennen. Das System wird mittlerweile auch in anderen Bundesländern und Staaten installiert (Landesbetrieb Forst Brandenburg 2019).[23]
- Das THW setzt tragbare Endoskopkameras für die Suche nach Verschütteten nach Gebäudeeinstürzen ein. Die Drehkugelkamera befindet sich zusammen mit Leuchtdioden am Ende eines flexiblen, bis zu 9 Meter langen Kabels, das

19 Bei Gefahr im Verzug kann die Maßnahme auch durch den Präsidenten des BKA angeordnet werden. Eine richterliche Entscheidung ist unverzüglich nachzuholen.

20 Die Berichterstattung geschieht auf der Grundlage von Artikel 13 Abs. 6 GG. Die Statistiken sind abrufbar unter: www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Wohnraum/Wohnraumueberwachung_node.html (31.3.2022)

21 Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 1 des Gesetzes vom 20. November 2019 (BGBl. I S. 1724) geändert worden ist

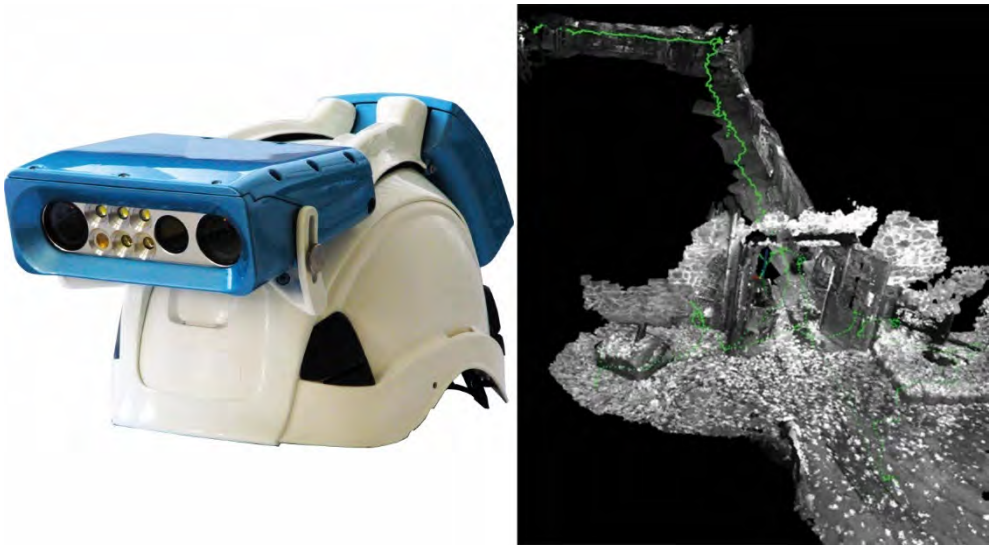
22 Eine eindeutige Definition für »Straftaten von erheblicher Bedeutung« gibt es nicht. Eine solche Straftat liegt vor, wenn sie mindestens der mittleren Kriminalität (i. d. R. Straftaten, die im Höchstmaß mit bis 5 Jahren Freiheitsstrafe bedroht sind) zuzurechnen ist, den Rechtsfrieden empfindlich stört und geeignet ist, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen (BVerfG, Urteil vom 16.6.2009, 2 BvR 902/06, Rn. 73). Es handelt sich beispielsweise um Straftaten auf dem Gebiet des unerlaubten Waffen- oder Betäubungsmittelverkehrs, der Geldfälschung oder um solche Taten, die gewerbs-, gewohnheits-, serien- oder bandenmäßig oder sonst organisiert begangen werden (§ 34 Abs. 3 Polizei- und Ordnungsbehördengesetz Rheinland-Pfalz in der Fassung vom 10.11.1993, zuletzt geändert durch Artikel 1 des Gesetzes vom 23.9.2020).

23 https://www.iq-firewatch.com/technology (31.3.2022)

durch Hohlräume in die Trümmerstrukturen eingeführt werden kann.[24] Ermöglicht wurde diese Anwendung durch die fortschreitende Miniaturisierung der Kameratechnik.

› Eine interessante Anwendung sind mobile Videokamerasysteme zur Eigenverortung und 3-D-Kartierung von unbekannten Umgebungen in Echtzeit. Solche Techniken zur visuellen Navigation können in der zivilen Sicherheit insbesondere dort von Nutzen sein, wo es keine externen Verortungsinfrastrukturen (GPS, WLAN etc.) gibt, also z.B. bei Rettungsaktionen in Gebäuden, Schächten oder Höhlensystemen. Ein tragbares System, das zur Berechnung der Eigenbewegung und 3-D-Kartierung lediglich stereoskopisch aufgenommene Bilder sowie die Daten von eingebauten Beschleunigungssensoren verwendet, wurde am DLR entwickelt und soll in die kommerzielle Anwendung überführt werden (Abb. 3.6) (Funk et al. 2016).

Abb. 3.6 Am DLR entwickeltes integriertes Positionierungssystem



links: tragbares Kamerasystem für die Echtzeiteigenverortung und 3-D-Kartierung in unbekannten Umgebungen; rechts: rekonstruierte Bewegung

Quelle: Deutsches Zentrum für Luft- und Raumfahrt (CC-BY 3.0)

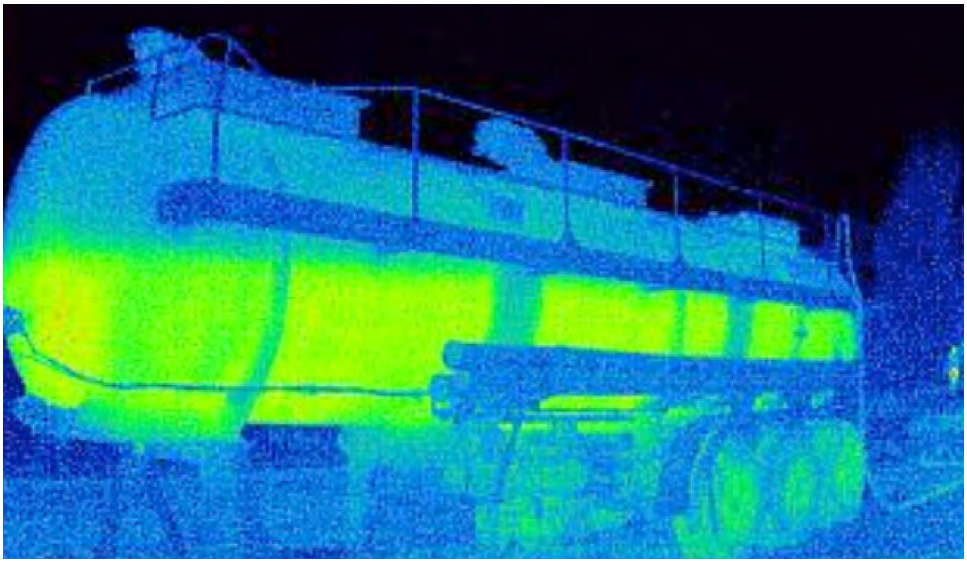
3.1.2.2 Wärmebildkameras

Wärmebildkameras erlauben die Temperaturmessung aus der Ferne, woraus sich auch Anwendungen im Bereich der zivilen Sicherheit ergeben. Einige Beispiele sind:

24 www.thw.de/SharedDocs/Ausstattungen/DE/Geraete/Endoskopkamera.html (31.3.2022)

› Bei Feuerwehren gehören mobile Wärmebildkameras zur Standardausrüstung. Das Einsatzspektrum umfasst u. a. die Lokalisierung bzw. Ortung von Brandherden oder Glutnestern, die Orientierung in verrauchten Gebäuden, die Kontrolle der Wärmeentwicklung in Geräteinstallationen, Heustöcken etc. oder die Suche nach vermissten Personen. Auch können Flüssigkeitsbehälter (z. B. Gefahrenguttanks) aus der Ferne in Bezug auf den Füllstand oder undichte Stellen kontrolliert werden, sofern Flüssigkeit und Umgebung unterschiedliche Temperaturen aufweisen (Abb. 3.7) (Wienecke 2013, S. 1 u. 12 f.). Auch das THW nutzt Wärmebildkameras für die Vermisstensuche.[25]

Abb. 3.7 Füllstandsmessung mithilfe einer Wärmebildkamera



Quelle: Wärmebildkameras im Einsatz; WBK-Ausbilderhandbuch Feuerwehr

› Mit Wärmebildkameras lassen sich Personen oder Objekte, deren Oberflächentemperaturen sich von der Umgebungstemperatur unterscheiden, auch bei völliger Dunkelheit beobachten. Darauf basieren mobile oder in Videobeobachtungssysteme integrierte Nachtsichtgeräte, die etwa im Rahmen von Grenzkontrollen eingesetzt werden. Außerdem können aus der Analyse der Verteilung der Oberflächentemperaturen von Objekten Informationen zur inneren Struktur sowie zu möglicherweise darin (verborgenen) Gegenständen oder Personen gewonnen werden. So wird beispielsweise die Eignung von Wärmebildkameras, im fließenden Straßenverkehr Fahrzeuge auf versteckte Personen zu detektieren, derzeit im Projekt »Analyse über rechtliche, gesellschaftliche und technische Aspekte und Maßnahmen zur Aufdeckung illegaler Migration und Bekämpfung der Schleusungskriminalität« (STRATUM;

25 www.thw.de/SharedDocs/Ausstattungen/DE/Geraete/waermebildkamera.html (31.3.2022)

Laufzeit 2019 bis 2022) im Rahmen der zivilen Sicherheitsforschung des Bundes untersucht.26

- Während der Ebolavirusepidemie in Westafrika von 2014 bis 2016 und aktuell während der Covid-19-Pandemie seit Anfang 2020 wurden und werden Wärmebildkameras verstärkt an internationalen Flughäfen eingesetzt, um Passagiere aus betroffenen Gebieten auf Fieber und damit auf eine potenzielle Erkrankung zu kontrollieren.

3.1.2.3 Scanner für die Personenkontrolle

Auf deutschen Flughäfen sind bereits über 200 Sicherheitsscanner zur Kontrolle von Fluggästen im Einsatz, die zur Bildgebung Millimeterwellen verwenden (Körperscanner). Sie sollen sukzessive die derzeit vorhandenen Metalldetektorschleusen ersetzen (Bundesregierung 2017a, S. 3), die sicherheitsrelevante nichtmetallische Gegenstände (z. B. Keramikmesser) nicht erkennen können.

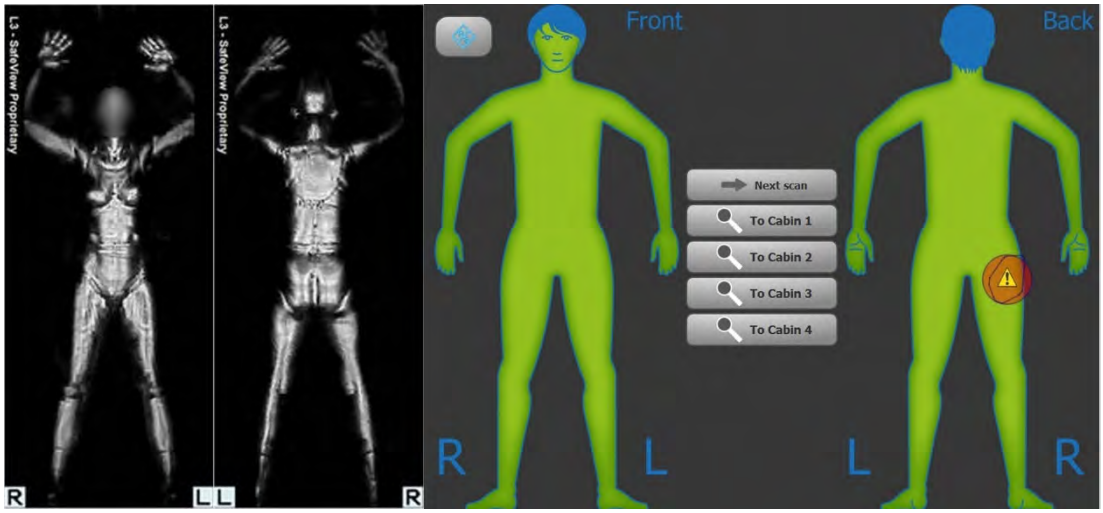
Millimeterwellen durchdringen Textilien, sodass die erzeugen Rohbilder gescannte Personen nackt darstellen (Abb. 3.8, links). Außer den Konturen des Körpers können zudem etwa Prothesen, die auf Behinderungen weisen, sichtbar werden. Dies stellt eine neue Qualität technisierter Beobachtung dar, weil hierdurch die Privat- bzw. Intimsphäre einer Person verletzt wird. Entsprechend wurde die Einführung dieser Systeme von kontroversen Diskussionen in der Öffentlichkeit begleitet (Körperscanner wurden auch als Nacktscanner bezeichnet). Um die Privat- und Intimsphäre der gescannten Personen zu schützen, arbeiten heute eingesetzte Systeme mit einer automatisierten Erkennung und Klassifizierung potenziell gefährlicher Gegenstände, deren Lage in einer schematischen Darstellung des menschlichen Körpers markiert wird (Abb. 3.8, rechts). Werden die Rohbilder direkt von Menschen ausgewertet, so gelten strenge Datenschutzanforderungen. Im Falle von Fluggastkontrollen beispielweise muss die Auswertung räumlich getrennt von der gescannten Person erfolgen, es dürfen sich keine Smartphonekameras etc. am Ort der Bildauswertung befinden und sämtliche Bilder sind zu löschen, sobald der Fluggast die Kontrolle ohne Beanstandung passiert hat (Durchführungsverordnung [EU] 2015/1998, Nr. 4.1.1.10 in Verbindung mit Nr. 12.11.1).

Sicherheitsscanner mit Millimeterwellen setzen eine künstliche Beleuchtung der zu kontrollierenden Person voraus, sodass sich die Frage nach möglichen gesundheitlichen Wirkungen stellt. Zwar handelt es sich bei Millimeterwellen um nichtionisierende Strahlung, allerdings könnte diese im Körper absorbiert und durch thermische Wirkungen zur Schädigung von Zellen der Haut oder des peripheren Blutkreislaufes und Nervensystems führen. Aktuelle Systeme verursachen deutlich niedrigere Strahlenbelastungen als die empfohlenen Grenzwerte vom Europäischen Rat und von der Internationalen Kommission zum Schutz vor

26 https://sifo.bmbfcluster.de/files/Projektumriss_STRATUM.pdf (31.3.2022)

nichtionisierender Strahlung (ICNIRP). Allerdings verweist das Bundesamt für Strahlenschutz BfS (2019) auf eine unbefriedigende Studienlage, die noch keine abschließende Bewertung zulässt.

Abb. 3.8 Rohbilder und schematische Ergebnisdarstellung durch einen Millimeterwellensicherheitsscanner



Quellen: links: https://en.wikipedia.org/wiki/Full_body_scanner (31.10.2019);
rechts: Rohde & Schwarz GmbH & Co. KG

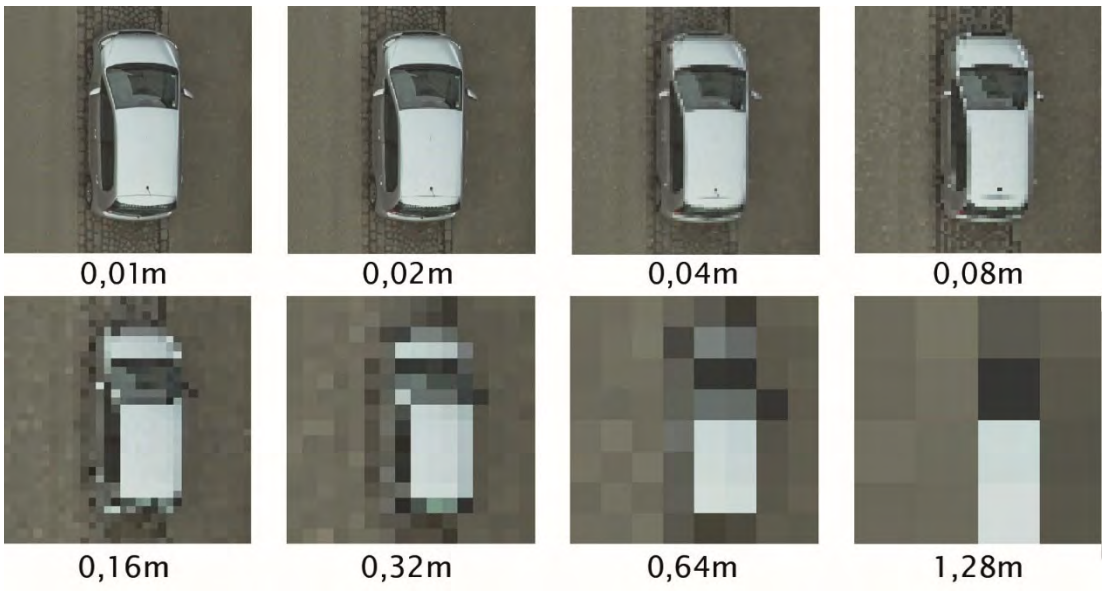
Sicherheitsscanner, die mit passiver THz-Bildgebung arbeiten, sind gesundheitlich unbedenklich, weil hier die vom Körper natürlich abgestrahlte Strahlung für die Detektion ausreicht. Für den Praxiseinsatz steht die Technik aber noch nicht zur Verfügung (Kap. 3.1.1). Ein weiterer Vorteil der THz-Bildgebung könnte darin bestehen, dass die Beobachtung durch kameraartige Systeme aus einigen Metern Entfernung erfolgen könnte. Denkbar wäre somit auch eine Personenkontrolle quasi im Vorbeigehen (prinzipiell auch ohne Wissen der gescannten Personen). Inwiefern dies im Interesse beispielsweise von Flugpassagieren wäre, bleibt allerdings zu hinterfragen.

3.1.3 Luftgestützte bildgebende Beobachtungstechnologien

Die Informationsgewinnung mit luftgestützten bildgebenden Beobachtungstechnologien gewinnt für zivile Sicherheitsaufgaben kontinuierlich an Bedeutung. Das Spektrum der möglichen Einsatzfelder ist breit und erstreckt sich von der Umweltbeobachtung im Bereich des Katastrophenschutzes über die Bereitstellung von Lagebildern bis hin zur Observation einzelner Personen oder Objekte zu Zwecken der polizeilichen Gefahrenabwehr oder Strafverfolgung.

Eine entscheidende Größe ist die erzielbare Bodenauflösung (Seitenlänge eines Quadrats am Erdboden, das als einzelner Pixel dargestellt wird), da zwischen der Aufgabenstellung der Beobachtung und der Bodenauflösung ein enger Zusammenhang besteht (Abb. 3.9): So reicht beispielsweise eine Bodenauflösung von ca. 30 Zentimetern aus, um ein Auto noch grob als solches erkennen zu können, während für eine eindeutige Identifizierung 10 bis 20 Zentimeter erforderlich sind und für eine technische Analyse (z. B. Modell des Fahrzeuges) eine noch höhere Bodenauflösung nötig ist. Die technisch maximal mögliche Bodenauflösung bestimmt sich aus der Flughöhe des Trägersystems und den Eigenschaften des Sensorsystems (z. B. Auflösung des Sensors, Brennweite der Optik). In der Praxis wird sie aufgrund von störenden Umwelteinflüssen (Wolken, Nebel, Staubpartikel in der Luft, atmosphärische Turbulenzen oder Dichteschwankungen etc.) allerdings häufig nicht erreicht. Bei allen Anwendungen gilt grundsätzlich, dass zwischen den Parametern Bodenauflösung, Größe des zu beobachtenden Gebiets und erzeugte Datenmenge ein Kompromiss gefunden werden muss.

Abb. 3.9 Objekterkennung in Abhängigkeit der Bodenauflösung



Quelle: Dr. Michael Cramer, Institut für Photogrammetrie (ifp), Universität Stuttgart

Die Wahl des Trägersystems und der eingesetzten Sensoren richtet sich nach den Anforderungen der jeweiligen Beobachtungsaufgabe. Wichtige Kriterien bei den Trägersystemen sind Flughöhe, -geschwindigkeit und -dauer, Reichweite, Kosten, Zulassung und nicht zuletzt die Erfordernisse seitens der Sensorik. In Bezug auf die bildgebenden Sensoren ist grundsätzlich zwischen Video- und Fotokamerasystemen zu unterschieden: Videokameras erlauben die Beobachtung bewegter Szenen, aufgrund der geringeren Pixelzahl der eingesetzten Sensoren sind damit

allerdings nur grobaufgelöste Übersichtsaufnahmen möglich. Hochaufgelöste Übersichtsbilder erfordern den Einsatz (spezieller) Fotokameras, die jedoch nur Momentaufnahmen liefern.

3.1.3.1 Trägersysteme

Fliegende Trägersysteme für bildgebenden Sensoren werden zumeist nach Antriebsart (Hubschrauber, Tragflächenflugzeug), Gewicht, Einsatzhöhe sowie nach bemannten oder unbenannten Systemen in Klassen eingeteilt.

Hubschrauber sind sehr wendig und haben die Fähigkeit zur stationären Beobachtung von Punktzielen. Der Aktionsradius und die Missionsdauer (2 bis 3 Stunden) sind allerdings begrenzt, zudem verursachen Hubschrauber hohe Einsatzkosten (2.000 bis 10.000 Euro/Flugstunde). Zweimotorige Propellerflugzeuge können zwischen 4 bis 8 Stunden in der Luft bleiben und haben aufgrund höherer Fluggeschwindigkeiten einen größeren Aktionsradius als Hubschrauber. Die Einsatzkosten liegen etwa bei 2.000 bis 3.000 Euro/Flugstunde. Durch die Miniaturisierung der Sensorsysteme können zunehmend auch einmotorige Flugzeuge und Ultraleichtflugzeuge für Beobachtungsaufgaben eingesetzt werden. Sie haben geringe Einsatzkosten (Ultraleichtflugzeug: 200 Euro/Flugstunde, Cessna 185: 800 Euro/Flugstunde) und lange Einsatzzeiten (bis zu 11 Stunden). Mit noch geringeren Kosten können in der Regel unbemannte Trägersysteme (Unmanned Aerial System – UAS oder Drohne) betrieben werden, die sich gegenüber bemannten Systemen vor allem durch ihr geringes Startgewicht auszeichnen. Hier reicht das Spektrum von relativ einfachen, manuell gesteuerten Fluggeräten mit geringer Nutzlast und eingeschränktem Aktionsradius (z. B. Multicopter der Gewichtsklasse bis 5 Kilogramm) bis zu größeren Systemen mit hoher Reichweite, beispielsweise unbemannte Tragflächenflugzeuge, die vorher festgelegte Gebiete autonom abfliegen.

Je nach Anwendung ist eine räumlich und geografisch genaue Verortung der Bilddaten für die Bildverarbeitung und -auswertung unerlässlich. Hierzu sind die Träger- bzw. Sensorsysteme zusätzlich mit hochwertigen Navigations-, Positions- und Lagemessgeräten ausgestattet. Falls erforderlich ermöglicht es eine Datenübertragung per Satellitenlink, Funk oder WLAN zu einer Bodenstation, dass die Bilddaten nach einer automatisierten Vorverarbeitung auf dem Trägersystem (beispielsweise zur Korrektur geometrischer Verzerrungen) nahezu in Echtzeit am Einsatzort oder in einem Lagezentrum bereitstehen.

3.1.3.2 Luftgestützte Videokamerasysteme

Luftgestützte Videokamerasysteme werden im zivilen Sicherheitsbereich beispielsweise zur Lageaufklärung und -beobachtung oder Vermisstensuche eingesetzt. Als Trägersysteme kommen in erster Linie Hubschrauber, zunehmend aber

auch rotorbetriebene unbemannte Fluggeräte (Multicopter) zum Einsatz, die für diese Aufgabe die notwendige Bewegungsflexibilität in der Luft aufweisen. Die Systeme sind meist mit Tageslicht- und Wärmebildkameras ausgestattet. Aktuell eingesetzte Videokameras arbeiten in der Regel im HD-Format (1.920 x 1.080 Pixel). Übersichtsbilder können daher insbesondere bei größerer Flughöhe nur sehr grob aufgelöst dargestellt werden. Für eine hohe Bodenauflösung sind große Zoomfaktoren erforderlich, wodurch allerdings das Blickfeld stark eingeengt wird (Strohhalmperspektive). Auch reicht die räumliche Lagegenauigkeit der aktuellen Technik noch nicht aus, um beispielsweise Zeitreihen eines bestimmten Gebietsausschnitts durch räumliche Überlagerung automatisiert auszuwerten.

Videokamerasysteme auf Hubschraubern

Auf Hubschraubern werden Videokameras als Außenladung in Messköpfen mitgeführt, die in alle Richtungen beweglich sind und so eine Rundumsicht erlauben. Typischerweise sind die Messköpfe mit mehreren Optiken unterschiedlicher Zoomeinstellungen und spektraler Eigenschaft ausgerüstet. Oft werden Tageslicht- und Wärmebildkameras mit aktiver Beleuchtung und Laserentfernungsmessgeräte kombiniert. Die Abbildung 3.10 zeigt exemplarisch ein solches System, das auch von Polizeibehörden in Deutschland eingesetzt wird.[27]

Abb. 3.10 Luftgestütztes Videokamerasystem

Quelle: Hochschule der Polizei des Landes Brandenburg

27 Typische polizeiliche Einsatzformen können in einem Video der Polizei Brandenburg betrachtet werden: www.youtube.com/watch?v=9eDb_n1gZQU (31.3.2022)

Die hubschraubergestützte Videobeobachtung durch die Polizei wird anlassbezogen u. a. zur Lageaufklärung und -beobachtung (bei Staatsbesuchen, öffentlichen Veranstaltungen bzw. Versammlungen unter freien Himmel, aber auch z. B. bei Waldbränden), zur Vermisstensuche oder zur Verfolgung von Punktzielen (fliehende Personen, gestohlene Fahrzeuge etc.) eingesetzt. Rechtliche Grundlage dafür sind die im Polizei- bzw. Strafverfahrensrecht geregelten Befugnisse für den Einsatz mobiler polizeilicher Videobeobachtung (Kap. 3.4.2.1).

Videokamerasysteme auf unbemannten Fluggeräten

Ferngesteuerte unbemannte Multicopter eignen sich als Trägersysteme für kleinere Videokamerasysteme. Auf dem Markt ist eine Vielzahl von Geräten erhältlich, angefangen von einfachen und kostengünstigen Kameradrohnen für den Hobbybereich bis hin zu professionellen Systemen, die sich durch robustere Fluggeräte, höherwertigere Sensoren und bessere Flug- und Bildstabilisierungstechniken auszeichnen (Rüffer 2016). Die Videodaten können per WLAN oder Funk direkt auf einen Monitor am Boden übertragen werden.

Polizeibehörden in Deutschland nutzen professionelle unbemannte Fluggeräte seit rund 10 Jahren beispielsweise für die Tatort- und Beweissicherung, um Fluchtwege von Tätern nachzuvollziehen, zur Verkehrsraumbeobachtung oder Vermisstensuche (dazu und zum Folgenden Benöhr-Laqueur 2018, S. 14 ff.). Auf den Einsatz über Menschenansammlungen zu Zwecken der Gefahrenabwehr (z. B. bei Demonstrationen oder Fußballspielen) wurde bisher weitgehend verzichtet.[28] 2018 hat Bayern als erstes Bundesland eine spezielle Ermächtigungsgrundlage für den polizeilichen Einsatz von unbemannten Luftfahrtsystemen geschaffen, die ausdrücklich auch deren Verwendung zur Herstellung von offenen Bildaufnahmen bei oder im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen bzw. zur Gefahrenabwehr vorsieht (Artikel 47 Abs. 1 Nr. 1 i.V.m. Artikel 33 Abs. 1 bis 3 BayPAG[29]). Dass hierbei dieselben eingriffsrechtlichen Voraussetzungen wie für herkömmliche Formen der offenen polizeilichen Videobeobachtung (Kap. 3.4.2.1) gelten, wird von verschiedenen Seiten kritisch gesehen. Begründet werden die Bedenken damit, dass durch den Einsatz von unbemannten Fluggeräten, die im Vergleich etwa zu Hubschraubern typischerweise viel unauffälliger und so für die Betroffenen möglicherweise kaum wahrnehmbar sind, der Einschüchterungseffekt und in der Folge auch die Eingriffsqualität der Videobeobachtung intensiviert werden (z. B. Kingreen 2018, S. 75). Zu klären wären insofern die Bedingungen, unter welchen der Kameraeinsatz auf unbe-

28 2010 wurde ein solches Gerät bei einer Demonstration gegen einen Castor-Transport eingesetzt. Der nichtgenehmigte polizeiliche Einsatz und die anschließende öffentliche Debatte darüber führten im Folgenden zu einem Verzicht weiterer Nutzungen über Menschenansammlungen (Benöhr-Laqueur 2018, S. 14 f.).

29 Polizeiaufgabengesetz (PAG) in der Fassung der Bekanntmachung vom 14. September 1990 (GVBl. S. 397, BayRS 2012-1-1-I), das zuletzt durch § 1 des Gesetzes vom 18. Mai 2018 (GVBl. S. 301, 434) geändert worden ist

mannten Fluggeräten noch als offene bzw. bereits als verdeckte polizeiliche Maßnahme einzuordnen ist.

In der nichtpolizeilichen Gefahrenabwehr können professionelle Systeme vor allem im Brand- und Katastrophenschutz für die schnelle Lageaufklärung bei großen und/oder komplizierten Einsatzlagen von erheblichem Nutzen sein. Nicht nur lassen sich damit schnell für die Einsatzplanung wichtige Überblicksaufnahmen erstellen, auch erlaubt die hohe Manövrierfähigkeit von Multicoptern ggf. sogar Erkundungsflüge im Inneren von brennenden, verrauchten oder einsturzgefährdeten Gebäuden, ohne dass sich Einsatzkräfte dafür in Gefahr begeben müssten (Buchenau/Rüffer 2019). Weitere Einsatzmöglichkeiten sind u. a. die Personensuche, die Erkundung von Aufstellungsräumen oder die Dokumentation von Schadenslagen. Generell von Nachteil für die meisten Einsatzfelder im zivilen Sicherheitsbereich sind allerdings die aktuell noch kurzen Einsatzzeiten der batterieangetriebenen Geräte (weniger als 1 Stunde).

Unbemannte Fluggeräte dürfen von BOS erst seit Inkrafttreten der Verordnung zur Regelung des Betriebs von unbemannten Fluggeräten[30] im April 2017 ohne Sondergenehmigung genutzt werden. Zuvor musste für jeden Einsatz und jede Übung eine Einzelfallerlaubnis beantragt werden, was die praktische Anwendung stark einschränkte (THW 2017). Auch sind BOS seitdem von den allgemeinen Betriebsverboten für unbemannte Fluggeräte nach § 21b Abs. 1 Luftverkehrs-Ordnung[31] (z. B. maximale Flughöhe von 100 m, Flugverbot außerhalb der Sichtweite, Überflugverbot bei Menschenansammlungen, Industrieanlagen) ausgenommen. Erst die neue Rechtslage ermöglicht die Ausschöpfung der vielfältigen Einsatzpotenziale im Bereich der zivilen Sicherheit. So plant etwa das THW (2017), unbemannte Luftgeräte in die bundesweite und bundeseinheitliche Ausstattung zu integrieren. Erste Anwendungserfahrungen sammelt beispielsweise auch die Johanniter-Unfall-Hilfe, die seit 2016 mehrere Schnelleinsatzgruppen mit entsprechenden luftgestützten Systemen ausgestattet hat (Die Johanniter 2018).

Mit den neuen Einsatzmöglichkeiten im Bevölkerungsschutz verbindet sich ein erheblicher Forschungs- und Entwicklungsbedarf, um entsprechende Systeme speziell für die hier bestehenden Bedürfnisse bereitzustellen. Hierzu gehören u. a. längere Flugzeiten, eine höhere Wetterstabilität, höhere Tragkraft, Automatisierung (im Hinblick auf Flugsteuerung und Datenauswertung) und nicht zuletzt auch Sicherheitsaspekte (BMI 2017). Erste Forschungs- und Entwicklungsprojekte in diesem Feld wurden und werden im Rahmen des zivilen Sicherheitsforschungsprogramms des Bundes gefördert, u. a.

30 Verordnung zur Regelung des Betriebs von unbemannten Fluggeräten vom 30. März 2017, BGBl. I, S. 683

31 Luftverkehrs-Ordnung vom 29. Oktober 2015 (BGBl. I S. 1894), die zuletzt durch Artikel 2 der Verordnung vom 11. Juni 2017 (BGBl. I S. 1617) geändert worden ist

- »Effizienter Einsatz von Unbemannten Flugsystemen für Werkfeuerwehren« (EffFeu; Laufzeit 2016 bis 2019): Es soll ein unbemanntes Fluggerät entwickelt werden, das Gefahrenpotenziale in großflächigen Arealen lokalisieren und relevante Informationen an die Einsatzkräfte weiterleiten kann. Dies soll durch eine situationsabhängige Steuerung des Fluggeräts und eine automatisierte Objekterkennung der Kameras erreicht werden.[32]
- »Luftbasierte Einsatzumgebungsaufklärung in 3D« (EINS3D, Laufzeit 2016 bis 2019): Es soll ein unbemanntes Fluggerät zur 3-D-Kartierung eines Einsatzgebiets in Echtzeit entwickelt werden. Dazu soll das System eigenständig Flugrouten planen und Suchmuster berücksichtigen, um Gefahrenquellen zu lokalisieren.[33]
- »Lageunterstützung bei Seenoteinsätzen durch unbemannte Luftfahrtsysteme« (LARUS, Laufzeit 2016 bis 2019): Es soll ein unbemanntes, mit Videokameras und weiteren Sensoren ausgestattetes Tragflächenflugzeug für die automatisierte Suche und Ortung von Menschen in Seenot entwickelt werden.[34]
- »Flugsystem-Assistierte Leitung komplexer Einsatzlagen« (FALKE; Laufzeit 2018 bis 2021): Zur besseren Bewältigung eines Massenunfalls mit vielen Verletzten soll ein System für die teilautomatisierte Suche und Sichtung von Verletzten am Einsatzort entwickelt werden. Dazu soll eine kontaktlose Vitalparameterdetektion durch Kombination von Video- und Wärmebildkameras sowie Radarsensoren für den Einsatz auf einem unbemannten Fluggerät realisiert werden.[35]

Neben technischen Weiterentwicklungen besteht zur Erschließung der Einsatzpotenziale angesichts der nunmehr nahezu erlaubnis- und verbotsfreien Nutzung unbemannter Fluggeräte durch BOS schließlich der Bedarf nach einheitlichen Standards und Regelungen für den Betrieb und Einsatz der Geräte sowie die Ausbildung der Piloten, um einen sachgerechten und sicheren Umgang damit zu gewährleisten. Zu diesem Zweck wurden unter der Federführung des BBK zwischen 2017 und 2019 die »Empfehlungen für Gemeinsame Regelungen zum Einsatz von Drohnen im Bevölkerungsschutz« (BBK 2019b) erarbeitet. Die Regelungen sollen im Zeitraum von 2 Jahren erprobt werden, um sie daraufhin zu evaluieren und ggf. zu überarbeiten.

3.1.3.3 Luftgestützte Fotokamerasysteme

Für Beobachtungsaufgaben, die Luftbilder mit hoher Bodenauflösung voraussetzen, sind Fotokamerasysteme aufgrund der höheren Pixelzahl der Sensoren

32 https://sifo.bmbfcluster.de/files/Projektumriss_EffFeu.pdf (31.3.2022)
33 https://sifo.bmbfcluster.de/files/Projektumriss_EINS3D.pdf (31.3.2022)
34 https://sifo.bmbfcluster.de/files/Projektumriss_LARUS_LZV.pdf (31.3.2022)
35 https://sifo.bmbfcluster.de/files/Projektumriss_FALKE.pdf (31.3.2022)

besser geeignet. Je nach Einsatzzweck kommen unterschiedliche Lösungen zur Anwendung. Sollen etwa Luftaufnahmen eines räumlich überschaubaren Areals ohne großen Anspruch an die Lagegenauigkeit hergestellt werden, so reichen dazu kommerziell erhältliche Fotokameras als Sensoren und fernsteuerbare Multicopter als Trägersysteme aus. Solche Systeme werden beispielsweise durch die Polizei zur Aufnahme und Vermessung von Unfallstellen oder Tatorten eingesetzt.

Von solchen relativ einfachen Lösungen abzugrenzen sind fotogrammetrische Luftbildkamerasysteme, die für den Einsatz auf Flugzeugen entwickelt wurden. Sie liefern hochaufgelöste Luftbilder mit hoher Lagegenauigkeit, die in Ergänzung zu Satellitenbilddaten zur Vermessung und Kartierung der Erdoberfläche genutzt werden. In Verbindung mit komplexen Verarbeitungsmethoden sind daraus neue digitale Kartenprodukte entstanden wie beispielsweise digitale Oberflächenmodelle, die nicht nur die Topografie, sondern auch zum Zeitpunkt der Aufnahme vorhandene größere Objekte (Gebäude, Bäume etc.) dreidimensional und maßstabsgetreu in interaktiven Karten darstellen.[36] Solche Kartenprodukte, die von gemeinnützigen wie auch von kommerziellen Anbietern zur Verfügung gestellt werden (GDACS, OpenStreetMap, DLR, Google Maps, Garmin etc.), können auch für Aufgaben der zivilen Sicherheit von hohem Nutzen sein. So greifen Disponenten in Leitstellen darauf zurück, um laufende Einsätze mit Lageinformationen zu unterstützen (z. B. in Bezug auf mögliche Aufstell- und Parkflächen für die Rettungsfahrzeuge oder Wasserentnahmestellen). Auch sind sie für die ersten in einer Katastrophenregion eintreffenden Rettungskräfte oft von entscheidender Bedeutung, um eine schnelle und effiziente Rettungskette zu ermöglichen (Kraft et al. 2018, S. 124). Von Nachteil ist allerdings, dass die Luftbilddaten teilweise mehrere Jahre alt sind und insbesondere keine Bewertung von aktuellen Schadenslagen zulassen.

Von großem Interesse sind daher luftgestützte Fotokamerasysteme, die die Beobachtung und Kartierung eines Interessengebiets in (nahezu) Echtzeit ermöglichen. Exemplarisch für eine solche Lösung steht das am DLR entwickelte »Modular Airborne Camera System« (MACS). Dabei handelt es sich um eine Reihe von verschiedenen prototypischen Fotokamera- und Bildauswertungssystemen, die jeweils an die Anforderungen der Beobachtungsaufgabe und der vorgesehenen Trägersysteme angepasst sind. Das MACS-RT (Real Time) ist für die Echtzeitbeobachtung ausgelegt. Kamerasystem und Datenfunkübertragung sind in einem Außenlastbehälter unter der Tragfläche eines Flugzeugs untergebracht. Bei einer angenommenen Flughöhe von 1.000 Metern und Fluggeschwindigkeit von 180 Kilometern pro Stunde kann jede Minute ein Gebietsstreifen der Breite von 500 Metern und Länge von 3 Kilometern bei einer Bodenauflösung von 13 Zen-

36 Ein bekanntes Beispiel hierfür sind die 3-D-Ansichten (Globusansicht) von Google Maps, die für zahlreiche Städte weltweit frei zur Verfügung stehen, z. B. www.google.de/maps/@52.5169068,13.3701301,194a,35y,57.42h,59.97t/data=!3m1!1e3 (31.3.2022)

timetern aufgenommen werden. Die Luftbilder werden noch an Bord zu einer digitalen Lagebildkarte verarbeitet und können mit einer Zeitverzögerung von nur ca. 4 Sekunden an eine Einsatzzentrale übertragen werden.[37] Speziell für die Katastrophenhilfe wurde das MACS-SaR (Search and Rescue) entwickelt. Das sehr leichte und kompakte Kamerasystem wird in ein unbemanntes Tragflächenflugzeug integriert, das mithilfe drehbarer Propeller senkrecht starten und landen kann (Abfluggewicht inklusive Kamerasystem: 10 Kilogramm). Eine aktuelle, geografisch korrekte Lagebildkarte eines Gebiets von 700 x 450 Metern mit einer Bodenauflösung von 3 Zentimetern kann nach nur 10 Minuten Flugzeit direkt nach der Landung erstellt werden (Abb. 3.11) (Kraft et al. 2018, S. 125 ff.).

Abb. 3.11 Hochauflösendes MACS-SaR Kamerasystem

Quelle: Deutsches Zentrum für Luft- und Raumfahrt, Germandrones GmbH

Luftgestützte Fotokamerasysteme zur Echtzeitbeobachtung und -kartierung werden zurzeit als Prototypen entwickelt und unter realen Einsatzbedingungen getestet. Im Bereich der nichtpolizeilichen Gefahrenabwehr könnten sie insbesondere für die Bewältigung großer Schadenslagen (Großfeuer, Industrieunfälle, Naturkatastrophen) von erheblicher praktischer Bedeutung sein, da sie eine schnelle Analyse von Zufahrtswegen, Gebäudeschäden, Trümmerstrukturen oder Umweltschäden (z. B. optisch sichtbare Gewässerverunreinigungen nach Unfällen in der chemischen Produktion) über größere Areale ermöglichen und dadurch die Einsatzplanung und Orientierung im Schadensgebiet unterstützen (Kraft et al. 2018, S. 133 f.). Ebenso eignen sie sich zur Überprüfung von Linienbauwerken (Straßen, Stromleitungen, Gleisanlagen, Pipelines), was auch Anwendungspotenziale in der polizeilichen Gefahrenabwehr eröffnet. So wurde beispielsweise im Auftrag der Bundespolizei der gesamte Streckenverlauf der neuen ICE-Hochgeschwindigkeitsstrecke zwischen München und Berlin (insgesamt über 600 Kilo-

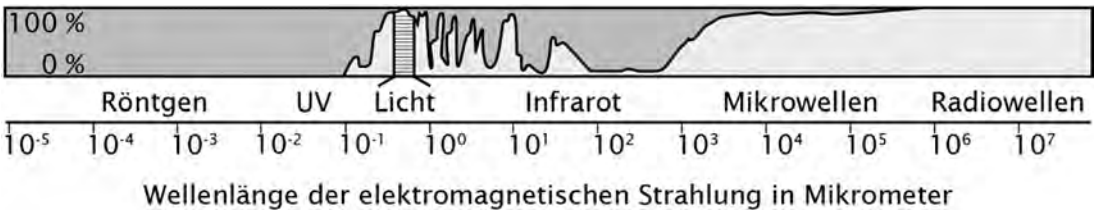
37 Ein Video des Systems kann unter www.dlr.de/os/de/Portaldata/48/Resources/videos/os-ak/MACS-RT_OHB_promo_v6_720p_web.mp4 (31.3.2022) betrachtet werden.

meter) kurz vor Streckeneröffnung mithilfe des MACS aus der Luft aufgenommen (Bodenauflösung: 5 Zentimeter), um die Beschaffenheit der Bahntrasse entlang der kompletten Strecke zu überprüfen. Dies diente der Sicherung der Eröffnungsfeierlichkeiten, die mit der Fahrt zweier Sonderzüge begangen wurde (DLR 2018, S. 9).

3.1.4 Weltraumgestützte bildgebende Beobachtungstechnologien

Weltweit gibt es eine Vielzahl von Satelliten[38], die für Beobachtungsaufgaben in unterschiedlichen zivilen Anwendungsfeldern (z. B. Natur- und Umweltmonitoring, Wetter und Klima, Land- und Forstwirtschaft, Ressourcenmanagement, Katastrophen- und Krisenmanagement) eingesetzt werden. Gegenüber luftgestützten Systemen sind die Beschaffungskosten für weltraumbasierte Beobachtungstechnologien zwar viel höher, allerdings liefern sie nach der Inbetriebnahme während ihrer gesamten Lebensdauer (bis ca. 10 Jahre) kontinuierlich Bilder und ermöglichen zudem eine globale Abdeckung, ohne dass Ländergrenzen oder nationale Lufträume eine Rolle spielen. Die zur Bildgebung nutzbaren Spektralbereiche hängen entscheidend von der Durchlässigkeit der Atmosphäre ab. Unterscheiden lassen sich mehrere atmosphärische Fenster, die zumindest teilweise elektromagnetische Welle passieren lassen. Die wichtigsten liegen im Bereich des sichtbaren Lichts, im Infrarotbereich sowie im Radiofenster im Mikrowellenbereich, in dem die Atmosphäre nahezu vollständig durchlässig ist (Abb. 3.12) (TAB 2012, S. 32).

Abb. 3.12 Atmosphärische Durchlässigkeit für elektromagnetische Wellen



Quelle: TAB 2012, S. 31

3.1.4.1 Passive Beobachtungssysteme

Passive Systeme kommen ohne künstliche Beleuchtung der Erdoberfläche aus. Für Aufnahmen im Wellenbereich des sichtbaren Lichts und des nahen Infrarots dient die Sonne als natürliche Beleuchtungsquelle, Sensoren für mittlere und/oder

38 Eine Übersicht der Erdbeobachtungssatelliten mit einer Bodenauflösung von 0,3 bis 2 Metern gibt es unter www.satimagingcorp.com/satellite-sensors (31.3.2022)

ferne IR-Strahlung nutzen die thermische Eigenemission von Objekten zur Bildgebung.

In der Regel werden quer zur Flugrichtung ausgerichtete Zeilensensoren mit bis zu 100.000 Pixeln verwendet, da die nahezu ruhige Flugbewegung der Satelliten ein ungestörtes Abscannen der Erdoberfläche in Streifen von einer Breite bis einige Kilometer erlaubt. Typischerweise werden die Bilder gleichzeitig in mehreren Spektralkanälen erfasst: Zum einen im panchromatischen Kanal, der meist über den gesamten Bereich des sichtbaren Lichts aufzeichnet, zum anderen in mehreren separaten und nur für bestimmte Bereiche des sichtbaren bzw. des IR-Wellenspektrums empfindliche Kanäle (multi- oder hyperspektral abbildende Systeme).[39] Letztere sind im Sicherheitskontext beispielsweise zum Auffinden von militärischen Tarnungen von Interesse, spielen für zivile Sicherheitsanwendungen aber noch eine untergeordnete Rolle.

Abb. 3.13 WorldView-1-Aufnahme (Bodenauflösung 50 Zentimeter)

Quelle: Satellite imagery (c) Maxar Technologies

Die meisten Beobachtungssatelliten fliegen in erdnahmen Umlaufbahnen (ca. 200 bis 2.000 Kilometer Höhe). Aufgrund der relativen Nähe zur Erdoberfläche können solche Systeme im Bereich des sichtbaren Lichts Bodenauflösungen von bis zu 20 Zentimetern erzielen (militärische Satelliten erreichen durch größere

39 Eine ausführliche Darstellung der Funktionsprinzipien und Anwendungsbereiche der Erdfernerkundung mithilfe von Satelliten findet sich im TAB-Arbeitsbericht Nr. 154 (TAB 2012, S. 29 ff.).

Spiegeldurchmesser sogar 10 Zentimeter Bodenauflösung). Im Vergleich dazu liegt die Bodenauflösung bei Beobachtungssatelliten in geostationären Umlaufbahnen (ca. 36.000 Kilometer) bei 250 Metern und darüber. Sie dienen vorrangig der Wetterbeobachtung (TAB 2012, S. 56). Der Nutzen von Satellitenbildern für Aufgaben der zivilen Sicherheit hängt allerdings nicht nur von einer hohen Bodenauflösung ab. Die Abbildung 3.13 zeigt eine Aufnahme des Erdbeobachtungssatelliten »WorldView-1« (Flughöhe: 496 Kilometer) mit Flüchtlingen, die den Tschad verlassen. Trotz der vergleichsweise schlechten Bodenauflösung von 50 Zentimetern (Abb. 3.9) lässt sich die Zahl der fliehenden Personen mithilfe von mathematischen Modellen, die typische Dichten bei Menschenansammlungen, Fortbewegungsgeschwindigkeiten u. Ä. Wissen berücksichtigen, auf ein Prozent genau bestimmen.

3.1.4.2 Aktive Beobachtungssysteme

Aktive satellitengestützte Beobachtungssysteme senden elektromagnetische Wellen aus und analysieren das von der Erdoberfläche reflektierte Signal. Das Synthetic Aperture Radar (SAR) erlaubt die Erzeugung von dreidimensionalen Geländemodellen der Erdoberfläche mit einer Genauigkeit von bis zu 10 Zentimetern. Dazu wird das reflektierte Radarsignal von zwei Antennen in einem Abstand von mehreren Metern detektiert (zur Vergrößerung des Antennenabstands wird auch die Flugbewegung des Satelliten ausgenutzt). Aus den unterschiedlichen Beobachtungswinkeln lässt sich die dreidimensionale Geländeoberfläche rekonstruieren. Radarwellen haben gegenüber sichtbarem Licht oder IR-Wellen den Vorteil, dass sie Wolken und teilweise auch die Vegetation durchdringen, sodass die Topografie davon ungestört abgebildet wird.

LIDAR (Light Detection and Ranging) oder auch LaDAR (Laser Detection and Ranging) ist eine dem Radar sehr verwandte Methode, bei der Laserstrahlen verwendet werden. Diese Systeme werden sowohl für die Gasanalyse (atmosphärische Spurengase) als auch für die Erstellung topografischer Geländeoberflächenmodelle verwendet.

3.1.4.3 Einsatz in der nichtpolizeilichen Gefahrenabwehr

Satellitendaten können insbesondere im Kontext von großräumigen Notfällen, Krisen oder Katastrophen (Hochwasser, Waldbrände, Hangrutschungen, Erdbeben, Vulkanausbrüche, humanitäre Krisen etc.) von hohem praktischem Nutzen für die Vorbereitung (Risikoanalysen, Gefährdungskartierung), Lagebewältigung (Lagebeurteilung, Schadensaufnahme, Planung und Durchführung von Rettungsaktionen) und Wiederherstellung (Wiederaufbaukartierung) sein. Die Auswertung von Satellitendaten setzt allerdings spezifische Fachkenntnisse, Zeit und Ressourcen voraus, die laut Löw et al. (2018, S. 24) bei den Behörden oft nicht

vorhanden sind. Daher wurden in den letzten 20 Jahren verschiedene nationale und internationale Dienste entwickelt, mit deren Hilfe Akteure der nichtpolizeilichen Gefahrenabwehr (sowie andere Endnutzer von Satellitendaten) mit bedarfsgerechten Informationsprodukten versorgt werden können. Das Verfahren wird im Folgenden exemplarisch am Beispiel des Dienstes für Katastrophen- und Krisenmanagement des Europäischen Erdbeobachtungsprogrammes Copernicus kurz erläutert (dazu und zum Folgenden TAB 2012, S. 182 ff.; Löw et al. 2018; EK o.J.).

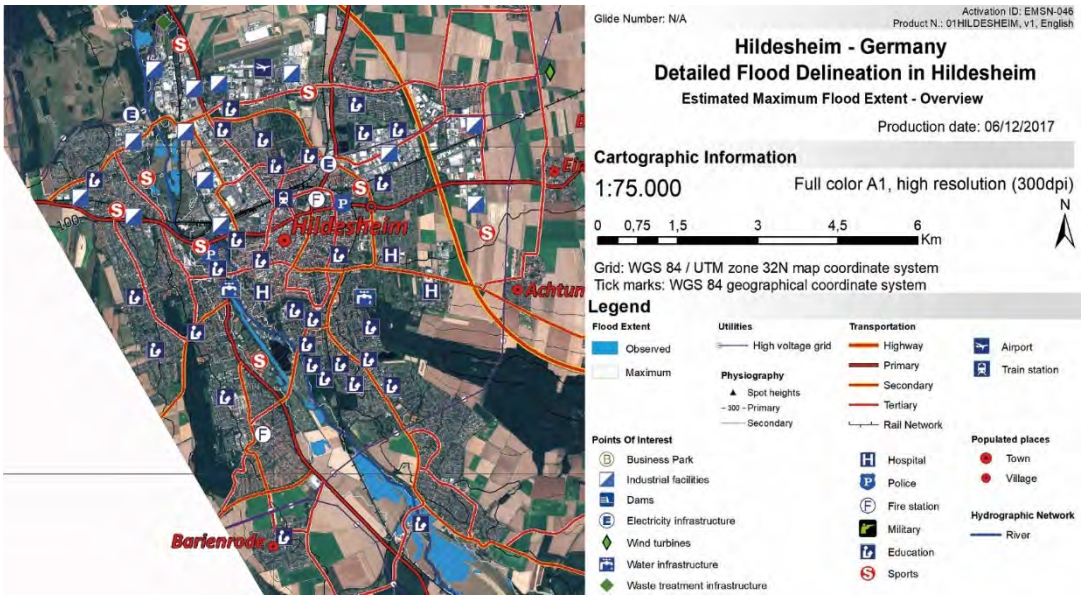
Der Copernicus-Dienst für Katastrophen- und Krisenmanagement besteht aus zwei wesentlichen Komponenten: Frühwarnung und Kartierung. Für die Frühwarnung stehen aktuell drei Module zur Hochwasservorhersage, Waldbrandinformation und Dürreüberwachung zur Verfügung. Mithilfe der Satellitendaten (sowie je nach Anwendung zusätzlicher Daten aus nichtweltraumgestützten Messsystemen) werden Risiken für das Auftreten entsprechender Ereignisse mit teilweise mehreren Tagen Vorlaufzeit berechnet. Die Waldbrand- und Dürrevorhersagen sind frei im Internet verfügbar, auf Hochwasserprognosen haben nur die zuständigen nationalen Behörden kostenfrei Zugriff.[40]

Die Komponente Kartierung besteht aus zwei Modulen: Notfallkartierung sowie Risikoanalysen und Wiederaufbau. Der Dienst zur Notfallkartierung kann im Falle von Katastrophen durch berechtigte Nutzerorganisationen aktiviert werden (in Deutschland ist dies das Gemeinsame Melde- und Lagezentrum von Bund und Länder – GMLZ im BBK). Es werden dann möglichst zeitnah zum Ereignis aktuelle Lagekarten der betroffenen Gebiete erstellt. Der gesamte Prozess von der Aufnahme der Satellitenbilder, Analyse und Bereitstellung der Lagekarten dauert erfahrungsgemäß zwei bis drei Tage (vor allem die Programmierung der Satelliten für die Aufnahme und Lieferung der Bilddaten nimmt viel Zeit in Anspruch). Solche Informationen sind für Akteure im Katastrophenschutz daher vor allem in großen und langanhaltenden Lagen hilfreich. Der Dienst existiert seit 2012 und wurde seitdem 571-mal aktiviert (Stand März 2022), in Deutschland zuletzt aus Anlass der Hochwasserkatastrophe Mitte Juli 2021.[41]

Das Modul Risikoanalysen und Wiederaufbau dient der Vorbereitung auf mögliche Krisenlagen bzw. als Unterstützung von Aufräumarbeiten. Auf Anfrage der berechtigten Nutzerorganisationen wird Kartenmaterial bereitgestellt, das beispielsweise Vorher-Nachher-Vergleiche ermöglicht oder mit ereignisspezifischen bzw. sozioökonomischen Daten aufbereitet wurde. Die Abbildung 3.14 zeigt beispielhaft eine mithilfe von Satellitenradardaten erstellte Karte der hochwasserbetroffenen Flächen in der Region Hildesheim während des Hochwassers im Juli 2017.

40 https://emergency.copernicus.eu (31.3.2022)
41 https://emergency.copernicus.eu/mapping/list-of-activations-rapid (31.3.2022)

Abb. 3.14 Hochwasserkarte des für Hildesheim und Umgebung (Ausschnitt)



Quelle: Copernicus Emergency Management Service, European Union, EMSN046

Die Neu- bzw. Weiterentwicklung von Copernicus-Diensten für den öffentlichen Bedarf wird vonseiten der Bundesregierung durch eine Reihe von Förder- und Entwicklungsmaßnahmen aus unterschiedlichen Ressorts (u. a. BMVI, BMWi, BMBF) unterstützt (Bundesregierung 2017b, S. 12).

3.1.4.4 Einsatz in der polizeilichen Gefahrenabwehr und Strafverfolgung

Laut Auskunft der Bundesregierung (2018m) nutzen das BKA und weitere Polizeibehörden aktuelle Satellitenbilder anlassbezogen u. a. zur Objektaufklärung, zur Vorbereitung von Exekutivmaßnahmen, zur Planung von Großereignissen oder zur Aufklärung von Tatorten. So wurde etwa für das LKA Hamburg die Hamburger Innenstadt am Tag vor dem G20-Gipfel 2017 mit dem kommerziellen Satellitensystem »WorldView-4« aufgenommen. Das Satellitenbild mit einer Bodenauflösung von 30 Zentimetern sollte der aktuellen Lagebeurteilung des Veranstaltungsortes dienen. Darüber hinaus werden Satellitenbilder auch zur Gefährdungs- und Lagebeurteilung im Ausland herangezogen.

Die Satellitenbilder werden vom Zentrum für Satellitengestützte Kriseninformation (ZKI) am DLR bereitgestellt. Der ZKI-DE-Fernerkundungsservice für Bundesbehörden funktioniert ähnlich wie der Copernicus-Dienst zur Notfallkartierung und kann von berechtigten Nutzern aktiviert werden (dazu gehören seit 2017 alle Ressorts der Bundesverwaltung). Die Zusammenarbeit basiert auf Verträgen zwischen dem DLR und dem Bundesministerium des Innern, für Bau und

Heimat (BMI) (Vertragslaufzeit 2013 bis 2020). 2021 wurde dieser Dienst an das Bundesamt für Kartografie und Geodäsie (BKG) übergeben. Zwischen 2013 und 2017 wurde der Dienst, der neben weltweiten Satellitenbildern auch hochaufgelöste Luftbilder zur Verfügung stellt, insgesamt 62-mal aktiviert. Zu den häufigsten Nutzern gehörte mit knapp der Hälfte der Aktivierungen in diesem Zeitraum das BKA (11 Aktivierungen mit Interessengebieten im Inland, 18 Aktivierungen mit Interessengebieten im Ausland), gefolgt vom BBK mit rund 15 % der Aktivierungen (DLR 2017, 2018; Bundesregierung 2018m, S. 6).

3.2 Nichtbildgebende Beobachtungstechnologien

Neben den bildgebenden gibt es eine große Vielfalt an nichtbildgebenden Beobachtungstechnologien. Für den Bereich der zivilen Sicherheit spielt die akustische Beobachtung mit Mikrofonen eine wichtige Rolle. Darüber hinaus existieren zahlreiche weitere Sensoren zum Nachweis bestimmter physikalischer oder chemischer Eigenschaften, die speziell für den jeweiligen Anwendungszweck entwickelt wurden bzw. werden. Es würde allerdings den Umfang des vorliegenden Berichts sprengen, alle diese Sensoren im Einzelnen hinsichtlich ihrer verschiedenen Funktionsprinzipien und (potenziellen) Einsatzfelder vorzustellen. Im folgenden Kapitel wird sich deshalb auf einige wichtige Anwendungen im Bereich der zivilen Sicherheit beschränkt.

3.2.1 Akustische Beobachtungstechnologien

Das Funktionsprinzip von Mikrofonen basiert auf einer Membran, die sich im Schallfeld bewegt. Die Bewegungen werden in elektrische Signale umgewandelt, die verarbeitet (z. B. verstärkt, digitalisiert, gespeichert, übertragen) und schließlich über einen Lautsprecher als Ton wieder ausgegeben werden. Aufzeichnungsgeräte bestehend aus Mikrofon und Verarbeitungs-, Speicher-, oder Übertragungskomponenten gibt es je nach Anwendungszweck in ganz verschiedenen Varianten.

3.2.1.1 Polizeiliche Anwendungsfelder

In polizeilichen Anwendungskontexten steht die Herstellung von Tonaufzeichnungen von Personen im Vordergrund. Sehr kleine Geräte (Miniwanzen) eignen sich für verdeckte Ermittlungsmaßnahmen in geschlossenen Räumen (dazu und zum Folgenden Hempel 2016, S. 70 f.). Sie sind entweder mit einem internen Speichermedium, das für die Auswertung entnommen werden muss, oder mit einem Hochfrequenzsender ausgestattet, der ein Mithören in Echtzeit innerhalb der Sendereichweite zulässt. Mittlerweile gibt es auch Geräte mit Mobilfunkanbin-

dung, die das Abhören aus der Ferne erlauben. Während Miniwanzen in die Nähe der Zielperson gebracht werden müssen, ist es mit Richtmikrofonen möglich, Gespräche aus einer Distanz von mehreren 100 Metern mitzuhören. Dazu ist eine exakte Ausrichtung des Mikrofons auf die Geräuschquelle nötig. Um störende Schallquellen aus anderen Richtungen auszublenden, sind Richtmikrofone häufig mit einem Hohlspiegel ausgestattet, der den Schall aus einer Richtung auf das Mikrofon fokussiert. Eine Besonderheit sind Lasermikrofone. Hier wird ein Laserstrahl beispielsweise auf eine Fensterscheibe gerichtet. Geräusche im Innenraum versetzen die Fensterscheibe in Schwingungen, die im reflektierten Lasersignal gemessen und vom Lasermikrofon wieder in Töne umgewandelt werden.

Die Herstellung von Tonaufzeichnungen in offener oder verdeckter Form stellt einen Eingriff in das aus dem allgemeinen Persönlichkeitsrecht (Artikel 2 Abs. 1 i.V.m. Artikel 1 Abs. 1 GG) abgeleiteten Recht auf die Vertraulichkeit des nichtöffentlich gesprochenen Wortes (Kap. 6.1.2.1) der betroffenen Personen dar und bedürfen daher immer einer speziellen gesetzlichen Ermächtigungsgrundlage. Im Bereich der Strafverfolgung ist die Polizei nach § 100f StPO in Fällen schwerer Straftaten (Katalogstraftaten nach § 100a Abs. 2 StPO[42]) und auf richterliche Anordnung[43] hin dazu befugt, heimlich Gespräche von Beschuldigten oder deren Kontaktpersonen außerhalb von Wohnungen abzuhören, falls die Ermittlungen auf andere Weise aussichtslos oder wesentlich erschwert wären. Abhörmaßnahmen in einer Wohnung greifen zusätzlich in die Unverletzlichkeit der Wohnung (Artikel 13 GG) ein und sind daher nach § 100c StPO an noch engere Voraussetzungen geknüpft (u. a. Verdacht auf eine besonders schwere Straftat nach § 100b Abs. 2 StPO, gezielte Beobachtung nur des Beschuldigten, Beachtung besonderer Vorschriften zum Schutz des Kernbereichs privater Lebensgestaltung nach § 100d StPO). Gemäß der durch das Bundesamt für Justiz veröffentlichten Statistik zur akustischen Wohnraumüberwachung[44] führen die Strafverfolgungsbehörden des Bundes und der Länder entsprechende Maßnahmen vergleichsweise selten durch (zwischen 2008 und 2020 in durchschnittlich 8 Verfahren pro Jahr).

Gefahrenabwehrrechtliche Befugnisse zur Herstellung von Tonaufzeichnungen von Personen in offener bzw. verdeckter Form gibt es unter engen Voraussetzungen z. B. für das BKA im Rahmen der Verhütung terroristischer Straftaten (§§ 45, 46 BKAG), für die Bundespolizei im Bereich der Grenzsicherung und des

42 Dazu zählen z. B. Staatsschutzdelikte, Straftaten gegen die sexuelle Selbstbestimmung, Mord und Totschlag, Raub oder räuberische Erpressung, organisierte Kriminalität wie Bandendiebstahl, gewerbsmäßige Hehlerei oder bandenmäßiger Schmuggel, gemeingefährliche Straftaten wie Brandstiftung oder schwere Betäubungsmittelkriminalität.

43 Bei Gefahr in Verzug kann die Maßnahme durch die Staatsanwaltschaft angeordnet werden. Die Anordnung muss binnen 3 Werktagen durch ein Gericht bestätigt werden (§ 100e Abs. 1 StPO).

44 Die Berichterstattung geschieht auf der Grundlage von Artikel 13 Abs. 6 GG. Die Statistiken sind abrufbar unter www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Wohnraum/Wohnraumueberwachung_node.html (31.3.2022)

Objektschutzes (§ 26 BPolG) oder beim Einsatz von Bodycams (§ 27a BPolG; Kap. 3.4.3.3) oder für die Polizeien der Bundesländer zum Schutz besonders bedeutsamer Rechtsgüter (z. B. §§ 21 bis 23 Polizeigesetz Baden-Württemberg[45]).

3.2.1.2 Nichtpolizeiliche Anwendungsfelder

Die akustische Beobachtung hat auch Anwendungen im Bereich der nichtpolizeilichen Gefahrenabwehr. Rettungskräfte etwa nutzen akustische Ortungsgeräte zur Suche nach verschütteten Personen. Dazu werden mehrere Bodenmikrofone (Geophone) in einigem Abstand auf den Trümmern beispielsweise eines eingestürzten Gebäudes ausgelegt (Abb. 3.15). Empfangene Geräusche wie Hilferufe, Klopfen oder von Bewegungen werden durch einen Verstärker millionenfach hervorgehoben und über einen Kopfhörer ausgegeben. Zur Lokalisierung des Verschütteten verbleibt das Geophon mit dem stärksten Signal an der Stelle, während die anderen kreisförmig darum herum neu ausgerichtet werden. Dieser Vorgang wird dann mehrfach wiederholt.[46]

Abb. 3.15 Akustische Ortungsgeräte im Einsatz beim THW

Quelle: Bundesanstalt Technisches Hilfswerk

45 Polizeigesetz (PolG) Baden-Württemberg in der Fassung vom 13. Januar 1992. Letzte berücksichtigte Änderung: §§ 13 und 14 geändert, § 10 a neu eingefügt durch Artikel 1 des Gesetzes vom 28. November 2017 (GBl. S. 631)

46 www.thw.de/SharedDocs/Ausstattungen/DE/Geraete/akustisches_Ortungsgerät.html (31.3.2022)

Auch hierbei werden Tonaufnahmen einer Person hergestellt, sodass grundsätzlich das Recht auf informationelle Selbstbestimmung der verschütteten Person betroffen ist. Trotzdem bedarf der Einsatz von Beobachtungstechnologien zur Rettung von Opfern eines Unglücksfalls – jedenfalls nach einer pragmatisch ansetzenden Rechtsauffassung[47] – keiner speziellen gesetzlichen Ermächtigungsgrundlage. Insoweit kann hier laut Faßnacht (2012, S. 73 ff.) nämlich von einer *mutmaßlichen Einwilligung* der verunglückten Person in die staatliche Einwirkung auf ihre grundrechtlich geschützten Güter ausgegangen werden, da die Einholung einer ausdrücklichen Einwilligung im Falle des zu rettenden Opfers nicht möglich ist. So ist anzunehmen, dass eine verunglückte Person gerettet werden will und dafür geringe Eingriffe in ihre grundrechtlich geschützten Güter hinnimmt. Liegt eine (mutmaßliche) Einwilligung vor, handelt es sich nicht um einen Eingriff in das betreffende Grundrecht, weshalb es auch keiner Eingriffsrechtfertigung bedarf.

3.2.2 Sensoren zur Detektion und Analyse von gefährlichen Substanzen und Explosivstoffen

Die Detektion, Identifikation und das kontinuierliche Monitoring von gefährlichen chemischen, biologischen, radiologischen, nuklearen und explosiven Stoffen (CBRNE-Gefahrenstoffe) sind aus offensichtlichen Gründen von herausragender Bedeutung im Bereich der zivilen Sicherheit. Hierfür wurde eine Fülle von Mess- und Analyseverfahren entwickelt. Ein aus Anwendersicht erheblicher Nachteil vieler dieser Verfahren ist allerdings, dass entsprechende Messgeräte in unmittelbare Nähe der verdächtigen Substanzen eingesetzt werden müssen oder Stoffproben erforderlich sind, die später in speziellen Analysegeräten am Einsatzort oder im Labor untersucht werden. Dies kann Einsatzkräfte insbesondere in schwierigen Lagen (z. B. bei Explosionsgefahr, an kontaminierten oder schwer zugänglichen Orten) gefährden. Von besonderem Interesse sind daher sensorbasierte Nachweisverfahren, die gefährliche Substanzen am Einsatzort aus einer sicheren Entfernung (mindestens mehrere Meter) quasi in Echtzeit detektieren und identifizieren können. Dies kann auf zwei Wegen erreicht werden: Zum einen besteht die Möglichkeit, geeignete Sensoren mithilfe von ferngesteuerten unbenannten Trägersystemen (Roboter, Drohnen) in die Nähe der verdächtigen Substanzen zu transportieren. Zum anderen erlauben optische Verfahren die Ferndetektion verschiedener chemischer Stoffe (Hempel 2016, S. 72).

47 Soweit bekannt gibt es hierzu noch keine klärende Rechtsprechung.

3.2.2.1 CBRNE-Sensoren auf Trägersystemen

Zur schnellen (innerhalb von Sekunden) Detektion sowie ggf. Identifikation und Analytik[48] von chemischen einschließlich explosiven, radiologischen oder nuklearen Gefahrenstoffen am Einsatzort gibt es eine Vielzahl an Sensoren mit unterschiedlichen Messprinzipien (z. B. elektrochemische, katalytische, chromatografische oder spektrografische Nachweisverfahren für chemische Stoffe; Halbleiterdetektoren, Szintillationszähler oder Zählrohre zum Nachweis ionisierender Strahlung).

Feuerwehren beispielsweise setzen bei Löscheinsätzen Mehrgasmessgeräte zum Monitoring der Umgebungsluft auf Atemgifte oder explosionsfähige Atmosphären ein. Die tragbaren Geräte lassen sich mit austauschbaren Einzelgassensoren bestücken (z. B. mit Sensoren zur Detektion von Kohlenmonoxid, Chlor, Blausäure, Schwefelwasserstoff, Methan, flüchtigen organischen Kohlenstoffverbindungen). Die Auswahl der verwendeten Sensoren richtet sich nach dem jeweiligen Anwendungskontext. Ziel ist es, die Sicherheit von Einsatzkräften und Anwohnern zu gewährleisten (Hempel 2016, S. 111). Durch die Miniaturisierung lassen sich Mehrgasmessgeräte mittlerweile so leicht und kompakt bauen, dass sie mit handelsüblichen Drohnen transportiert werden können.

Die Abbildung 3.16 (links) zeigt exemplarisch ein aktuell auf dem Markt verfügbares System, das Messwerte in Echtzeit per Funk an die Einsatzkräfte übertragen und zusätzlich mit einem Szintillationszähler zur Messung von Gammastrahlung ausgestattet werden kann (Honeywell International Inc. 2018).

Abb. 3.16 Unbemannte Trägersysteme für Sensoren

Quelle: links: Aerialtronics DV B.V., rechts: AIRSENSE Analytics GmbH

48 Durch Verfahren der Detektion ist die Anwesenheit bestimmter Kategorien von Gefahrenstoffen, z. B. von flüchtigen organischen Verbindungen, ggf. auch ohne genaue Spezifizierung festzustellen (Ja/Nein-Aussage). Verfahren der Identifikation und Analytik dienen dem qualitativen (zweifelsfreie Identifikation) und quantitativen Nachweis von Gefahrenstoffen (BBK 2016, S. 26 f.).

Aus dem im Rahmen der zivilen Sicherheitsforschung des Bundes geförderten Projekt »Detektoren-Array mit Gaschromatograf zur Identifikation toxischer Substanzen« (DACHS; Laufzeit 2007 bis 2010) ist ein tragbares Messgerät hervorgegangen, das die Messsignale mehrerer festinstallierter Sensoren verschiedenen Typs gemeinsam auswertet. Die unterschiedlichen Signalmuster ermöglichen die parallele Detektion und teilweise Identifikation zahlreicher chemischer Gefahrenstoffe einschließlich gängiger Kampfstoffe mit einem einzigen Gerät und ohne einsatzspezifische Sensorbestückung (Matz et al. 2012, S. 7). Das Gefahrenstoffdetektorarray (GDA) gehört inzwischen zur Ausrüstung der Analytischen Task Force (ATF) des Bundes[49] und kann auch auf ferngesteuerten Fahrsystemen eingesetzt werden (Abb. 3.16 rechts).

An der Optimierung von Sensorsystemen im Hinblick auf ihre Sensitivität für die unterschiedlichsten chemischen und radiologischen Gefahren und ihre Anwendung auf unbemannten Trägersystemen am Boden, im Wasser und in der Luft wird zurzeit intensiv geforscht, u. a. auch im Rahmen der zivilen Sicherheitsforschung des Bundes. Einige exemplarische Forschungs- und Entwicklungsprojekte sind:

- »UAV-Assisted Ad Hoc Networks for Crisis Management and Hostile Environment Sensing« (ANCHORS; Laufzeit 2012 bis 2015): Es wurden hochsensible Sensoren für radiologische und nukleare Gefahren entwickelt und Testflüge mit einem Schwarm an miteinander vernetzen Drohnen durchgeführt, um effektiver nach radiologischen Quellen zu suchen (Schulcz et al. 2015);
- »Mobiles Sensornetz zur autonomen und großflächigen Unterwasserortung und Identifikation von Gefahrenstoffen in Häfen und Binnengewässern« (MoSAIk; Laufzeit 2016 bis 2018): Ziel des Projekts war die Entwicklung eines Unterwasserüberwachungssystems mit autonomen Unterwasserfahrzeugen und flexibler Sensorik, das zur flächendeckenden Detektion von beispielsweise Schweröl oder giftigen Chemikalien eingesetzt werden kann.[50]
- »Baukleines Hochdruck-Massenspektrometer zur schnellen und sicheren Spreng- und Gefahrenstoffdetektion« (HiP-MS; Laufzeit 2017 bis 2020): Es soll eine Massenspektrometer für den mobilen Einsatz entwickelt werden.[51]

Im Vergleich zur Situation bei chemischen oder radiologischen Gefahren ist die Entwicklung von mobilen Sensorsystemen für biologische Gefahrenstoffe ungleich schwieriger, da die Detektion und Identifikation von Bakterien, Viren, Pilzen oder biologischen Toxinen besondere Anforderungen an die Diagnostik

49 Die ATF besteht aus besonders für die Bewältigung von CBRN-Lagen ausgebildeten Einsatzkräften und spezieller Messtechnik. Das Personal stellen die Kommunen bzw. die Länder, der Bund steuert Messtechnik und Einsatzfahrzeuge bei, koordiniert die Spezialausbildung und beteiligt sich an den Unterhaltskosten. Aktuell ist die AFT an insgesamt acht Standorten in Deutschland stationiert (BBK o. J.a).

50 https://sifo.bmbfcluster.de/files/Projektumriss_MOSAIK.pdf (31.3.2022)

51 https://sifo.bmbfcluster.de/files/Projektumriss_HiP-MS.pdf (31.3.2022)

stellen. Entsprechende Nachweisverfahren beruhen oft auf einer speziellen Abfolge von Stoffwechselreaktionen, sodass sie komplex und zeitintensiv sind und daher in der Regel nur in dafür spezialisierten Laboren durchgeführt werden können (BBK o.J.b). Derzeit wird daran gearbeitet, solche Verfahren in handliche, robuste und auch von Rettungskräften ohne spezifische Laborkenntnisse einfach zu bedienende Messgeräte für einen Vor-Ort-Einsatz zu implementieren. Eine noch größere technische Herausforderung stellt die Realisierung von automatisierten Systemen dar, die selbständig Proben nehmen und auf unbemannten Trägersystemen zum Einsatz kommen können. Die Entwicklungen in diesem Gebiet werden auch durch die zivile Sicherheitsforschung des Bundes vorangetrieben. Beispielhaft lassen sich folgende Forschungs- und Entwicklungsprojekte aufzählen:

- »Sichereres Erkennen biologischer Gefahrenstoffe vor Ort« (GEFREASE; Laufzeit 2012 bis 2015). Im Rahmen des deutsch-französischen Forschungsprojekts wurde ein schnelles Vor-Ort-Nachweisverfahren für eine Reihe von bioterroristisch relevanten Toxinen auf der Basis neuartiger Antikörper und elektrochemischer Sensoren entwickelt. Alle Verfahrenskomponenten (Fluidik- und Elektronikmodul, Reagenzienzuführung, Batterie) sind in einem feldfähigen Koffer untergebracht. Zur Probennahme und -vorbereitung (Verdünnung, Filtration) stehen für die Einsatzkräften Probenvorbereitungskits zur Verfügung (Pöhlmann/Elßner 2015, S. 29).
- »Sensor-basierte und automatisierte Detektion von hoch- und niedermolekularen biologischen Toxinen« (SensTox; Laufzeit 2015 bis 2019). Es soll ein transportables, automatisiertes Biosensorsystem entwickelt werden, mit dem gleichzeitig hochmolekulare sowie niedermolekulare Toxine detektiert werden können.[52]

3.2.2.2 Optische Nachweisverfahren

Optische Verfahren auf der Basis von elektromagnetischen Wellen erlauben prinzipiell die Detektion und Identifikation von chemischen Gefahrenstoffen auch aus größerer Entfernung. Eine Möglichkeit ist die IR-Spektroskopie, die darauf beruht, dass viele Moleküle im IR-Spektralbereich ein charakteristisches Emissions- bzw. Absorptionsspektrum aufweisen. Diese Spektren können entweder aktiv oder passiv gemessen werden (in ersterem Fall wird das Absorptionsspektrum einer mit IR-Strahlung beleuchteten Probe, in letzterem Fall die von einer Probe natürlich emittierte IR-Strahlung gemessen). Durch den Vergleich mit einer Referenzdatenbank kann das Molekül schließlich identifiziert werden. Mit IR-Fernerkundungsgeräten lassen sich allerdings keine durch Gegenstände verdeckte oder unter der Kleidung versteckte Substanzen (z. B. Sprengstoffe)

52 https://sifo.bmbfcluster.de/files/Projektumriss_SensTox.pdf (31.3.2022)

detektieren. Zumindest für letztere Aufgabe befinden sich zurzeit Spektrometer mit THz-Strahlung in der Entwicklung (Kap. 3.1.1).

Die Analytische Task Force des Bundes ist mit mobilen IR-Fernerkundungsgeräten ausgestattet, die ein passives IR-Spektrometer für gasförmige Substanzen mit einer Videokamera kombinieren. Die im Einsatzfahrzeug installierten Geräte lassen sich aus dem Fahrzeugdach motorisiert ausfahren und ermöglichen so eine 360°-Bilderfassung (Abb. 3.17, links). Damit können Gefahrenstoffwolken aus toxischen Industriegasen oder chemischen Kampfstoffen aus einer Entfernung von bis zu 5 Kilometern gemessen und als farbige Gebiete in einem Videobild der Umgebung angezeigt werden (Abb. 3.17, rechts). In der internen Gerätedatenbank hinterlegte Referenzstoffe werden identifiziert, andere als Abweichung von der Umgebungsluft erkannt und ebenfalls angezeigt (BBK 2019a, S. 10; Bruker Optik GmbH 2017). Allerdings liefern diese Systeme keine Entfernungsinformationen, außerdem kann das Sichtfeld und damit die Anwendbarkeit durch dichte Bebauung in Städten eingeschränkt werden. Um diese Limitierungen zu beseitigen, soll deshalb im Forschungsprojekt »Atmosphärische Detektion von Gefahrstoffen durch mobile Infrarotspektroskopie« (ATHMOS; Laufzeit 2018 bis 2021) ein IR-Spektrometer für den Einsatz auf unbemannten Fluggeräten entwickelt werden. Das System soll es ermöglichen, weitgehend automatisiert dreidimensionale Abbildungen von Gefahrenstoffwolken zu erzeugen und deren Ausbreitung nahezu in Echtzeit zu visualisieren.[53]

Die Anwendbarkeit optischer Nachweisverfahren zur Ferndetektion von biologischen Gefahrenstoffen wurde bislang noch nicht demonstriert.

Abb. 3.17 IR-Fernerkundungsgerät SIGIS 2

Quellen: links: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, rechts: Donato et al. 2018, S. 9

53 https://sifo.bmbfcluster.de/files/Projektumriss_ATHMOS.pdf (31.3.2022)

3.2.3 Ortungstechnologien

Zur Ortung von Personen mithilfe technischer Mittel gibt es eine Reihe von Möglichkeiten. Im Folgenden werden sensorbasierte Ansätze vorgestellt, während informationstechnische Ortungsverfahren in Kapitel 5 behandelt werden.

3.2.3.1 Ortung von Personen mithilfe von globalen Navigationssatellitensystemen

Globale Satellitennavigationssysteme (GNSS) wie GPS, Galileo oder GLONASS bestimmen die Position eines GNSS-Empfängers durch Distanzmessungen zu mindestens vier Satelliten. Schon einfachere GNSS-Sensoren, wie sie bei modernen Smartphones mittlerweile zum Standard gehören, ermöglichen unter optimalen Bedingungen (Messung auf freier Fläche) die Positionsbestimmung mit einer Genauigkeit von 5 bis 10 m. Störungen im Satellitenempfang (z. B. durch Bäume, Gebäude oder die Topografie) können die Positionsangaben allerdings verfälschen (GeoSN 2017).

Polizeiliche Anwendungsfelder

Im polizeilichen Bereich kommen GNSS-Empfänger zur Lokalisierung von Personen oder Fahrzeugen zum Einsatz (auch als GPS-Tracker oder – nicht ganz korrekt – als Peilsender bezeichnet). Die bei Zielperson oder -objekt angebrachten GNSS-Empfänger zeichnen ihren Standort kontinuierlich auf oder übermitteln diesen in regelmäßigen Zeitabständen z. B. über eine Mobilfunkverbindung an die Polizei. Im Bereich der Strafverfolgung dürfen GNSS-Empfänger zur heimlichen Ortung von Personen eingesetzt werden, da sie zu den in § 100h Abs. 1 Nr. 2 StPO genannten technischen Mitteln zur Ermittlung des Aufenthaltsortes eines Beschuldigten gehören (WD 2018a, S. 7). Zulässig ist dies allerdings nur bei Straftaten von erheblicher Bedeutung und nur falls die Ermittlung des Aufenthaltsortes auf andere Weise weniger erfolgversprechend oder erschwert wäre. Ähnliche, an enge Voraussetzungen geknüpfte Befugnisnormen finden sich auch im Bereich der polizeilichen Gefahrenabwehr (für das BKA z. B. in § 45 Abs. 2 Nr. 3 BKAG).

Die elektronische Aufenthaltsüberwachung (EAÜ) mittels Fußfesseln im Rahmen der Führungsaufsicht nach der Haftzeit gemäß § 68b Abs. 1 Nr. 12 Strafgesetzbuch basiert ebenfalls auf GNSS-Empfängern. Die Träger der Fußfesseln können damit im Alarmfall (z. B. beim Verlassen eines festgelegten Bereichs, bei der Beschädigung der Fußfessel) jederzeit von der Gemeinsamen elektronischen Überwachungsstelle der Länder (GÜL) in Bad Vilbel (Hessen) geortet werden (eine kontinuierliche Ortung findet aus Datenschutzgründen nicht statt). Eine gerichtliche Anordnung zur EAÜ war bis 2017 nur unter engen Voraussetzungen

bei schweren Sexual- und Gewaltstraftaten möglich, wenn die Gefahr bestand, dass die Täter weitere Straftaten begingen. Auf dieser Grundlage wurde die Maßnahme beispielsweise im Jahr 2016 bundesweit bei 88 Personen durchgeführt (Hessisches Ministerium für Justiz 2017). 2017 wurden die Einsatzmöglichkeiten der EAÜ im Rahmen der Führungsaufsicht auf extremistische Straftäter/innen, die wegen schwerer Staatsschutzdelikte verurteilt wurden, ausgeweitet.[54] Im Rahmen seiner Aufgabe zur Abwehr von Gefahren des internationalen Terrorismus hat etwa das BKA 2017 die Befugnis erhalten, auf richterliche Anordnung hin den Aufenthaltsort von Personen, von denen eine terroristische Straftat erwartet wird (sogenannte Gefährder), mittels elektronischer Fußfessel jederzeit feststellen zu können (§ 56 BKAG). Laut Auskunft der Bundesregierung (2019a, S. 12) wird durch das BKA derzeit (Stand März 2019) keiner der rund 440 islamistischen Gefährder, die sich in Deutschland aufhalten, mit einer elektronischen Fußfessel beobachtet. Vergleichbare gefahrenabwehrrechtliche Befugnisse zum Einsatz der EAÜ gibt es für die Polizeibehörden einiger Bundesländer (z. B. § 34c PolG NRW[55], Artikel 34 BayPAG).

Polizeiliche und nichtpolizeiliche Anwendungsfelder

Standortangaben aus GNSS-Empfänger werden im zivilen Sicherheitsbereich außerdem im Falle von Notrufen, bei denen der Anrufende sich nicht mehr verständlich machen kann oder seinen genauen Aufenthaltsort nicht kennt, genutzt. Bis vor Kurzem hatten die Leitstellen in Deutschland allerdings keine Möglichkeit, *direkt* auf GNSS-Koordinaten des Mobilfunkgeräts des Notrufenden zuzugreifen (eine Standortbestimmung erfolgte lediglich über die in der Regel wesentlich ungenauere Funkzellenabfrage, Kap. 5.2.2.2).[56] Personen in Notlagen bzw. Ersthelfer mussten die Koordinaten manuell abrufen und an die Leitstelle durchgeben, was Zeit kostete und in Stresssituationen und ggf. für ältere Personen regelmäßig schwierig war. Seit Oktober 2019 wird deutschlandweit für 3 Jahre das Advanced-Mobile-Location-(AML-)Notfallsystem getestet, dass ohne Interaktion des Notrufenden auskommt (Kiss 2019). Erkennt das Betriebssystem des Smartphones, dass eine Notrufnummer gewählt wird, werden automatisch die Ortungsfunktionen aktiviert und die Standortkoordinaten an einen zentralen Server in der Integrierten Leitstelle Freiburg geschickt. Die Standortdaten stehen dann der Leitstelle, die den Notruf entgegengenommen hat, für 60 Minuten zum

54 Dreiundfünfzigstes Gesetz zur Änderung des Strafgesetzbuches – Ausweitung des Maßregelrechts bei extremistischen Straftätern (BGBl. 2017, S. 1612)

55 Polizeigesetz des Landes Nordrhein-Westfalen (PolG NRW) in der Fassung der Bekanntmachung vom 25. Juli 2003, die zuletzt durch Artikel 1 des Gesetzes vom 18. Dezember 2018 (GV. NRW. S. 741) geändert worden ist

56 Gemäß § 4 der Verordnung über Notrufverbindungen sind Telefondiensteanbieter bei Notrufen dazu verpflichtet, den Leitstellen Angaben zum Standort des Endgeräts zu übermitteln. Im Falle des Mobilfunks ist das Gebiet der Funkzelle anzugeben, in die das Gerät eingebucht ist (Bundesnetzagentur 2018, S. 17).

Abruf zur Verfügung und werden danach gelöscht (Integrierte Leitstelle Freiburg 2018). Andere europäische Länder wie Belgien, Estland, Großbritannien, Litauen oder Österreich nutzen das AML-Notrufsystem bereits seit einigen Jahren.[57]

Einen Schritt weiter noch geht das seit April 2018 in sämtlichem Neufahrzeugen (Typzulassung) in der EU per Verordnung (EU) 2015/758[58] vorgeschriebene eCall-Notrufsystem: Sobald Crashsensoren einen schweren Aufprall des Fahrzeugs feststellen (z. B. durch Aktivierung der Airbags), wird automatisch eine Notrufverbindung zu einer Leitstelle hergestellt, über welche zusätzlich die durch einen GNSS-Empfänger ermittelten Koordinaten des Unfallorts sowie weitere unfallrelevante Informationen (z. B. Unfallzeitpunkt, Fahrtrichtung) an die Leitstelle übertragen werden. Datenschutzrechtlichen Bedenken in Bezug auf die automatisierte Ortung wurde durch strenge Regelungen hinsichtlich der Nutzung des Systems (nur in Notfallsituationen), der Art der übertragenen Daten sowie Speicherdauern und Löschfristen Rechnung getragen.

3.2.3.2 Ortung von verschütteten Personen mit Radar

Eine interessante Sicherheitsanwendung der Radartechnik (Kap. 3.1.1) ist das Bioradar, das zur Ortung von Verschütteten z. B. beim THW zum Einsatz kommt.[59] Die tragbare Radarantenne wird auf den Trümmerkegel positioniert. Treffen die Radarwellen auf Bewegungen innerhalb des Trümmerhaufens, ändert sich die Frequenz der reflektierten Wellen. Dadurch lassen sich auch minimale Bewegungen wie die eines Brustkorbs bei der Atmung oder eines schlagenden Herzens feststellen. So kann mit hoher Wahrscheinlichkeit auf das Vorhandensein einer lebenden Person innerhalb des Strahlungskegels der Radarantenne geschlossen werden (nicht jedoch auf ihre genaue räumliche Lage). Die Radarwellen dringen je nach Material und Schüttung bis zu 10 Meter tief in die Trümmer ein. Die abgegebene Leistung der Radarantenne beträgt nur rund 1 % der abgestrahlten Leistung eines Mobilfunkgeräts, weshalb eine gesundheitliche Gefährdung der Opfer oder Rettungskräfte auszuschließen ist (Faßnacht 2012, S. 20 f. u. 75). Auch bedarf der Einsatz des Bildradars keiner gesetzlichen Ermächtigungsgrundlage, da von einer mutmaßlichen Einwilligung des Verschütteten ausgegangen werden kann (Kap. 3.2.1.2).

57 https://ec.europa.eu/digital-single-market/en/news/112-112-day-locating-emergency-calls-aml-technology-rise (31.3.2022)
58 Verordnung (EU) 2015/758 über Anforderungen für die Typgenehmigung zur Einführung des auf dem 112-Notruf basierenden bordeigenen eCall-Systems in Fahrzeugen und zur Änderung der Richtlinie 2007/46/EG
59 www.thw.de/SharedDocs/Ausstattungen/DE/Geraete/bioradar.html (31.3.2022)

3.2.4 Beobachtung von Rettungskräften oder Einsatzstellen

Ein Nutzungsschwerpunkt von Beobachtungstechnologien bei Einsätzen der nichtpolizeilichen Gefahrenabwehr liegt in der Gewährleistung der Sicherheit von Einsatzkräften. Neben bildgebenden Beobachtungstechnologien auf Hubschraubern oder unbemannten Fluggeräten (Kap. 3.1.3) zur schnellen Lagebewertung oder tragbaren Messgeräten zum Schutz vor Gefahrenstoffen (Kap. 3.2.2) kommen hier weitere sensorbasierte Beobachtungstechnologien zur Anwendung.

3.2.4.1 Atemschutzüberwachung

Die Beobachtung von Einsatzkräften, die mit Atemschutz arbeiten (z. B. der Angriffstrupp der Feuerwehr), erfolgt bislang meist dadurch, dass regelmäßig der verbleibende Luftvorrat und die Position der Trupps über Funk abgefragt und dokumentiert werden. Mittlerweile verwenden einige Feuerwehren[60] Sensorsysteme, die den verbleibenden Atemluftvorrat und die Bewegungen der Einsatzkräfte kontinuierlich messen und die Daten per Funk an die Einsatzleitung übertragen (letzteres, um etwa Bewusstlosigkeit festzustellen) (Hempel 2016, S. 118).

3.2.4.2 Schutzanzüge mit integrierter Sensorik

Für die Einsatzkräfte der Feuerwehr kann eine zu große Hitzeentwicklung bei Bränden sehr schnell zu lebensbedrohlichen Situationen führen. Die Folgen reichen von Hitzeerschöpfung über Kreislaufprobleme bis hin zu Bewusstlosigkeit oder Schock, die sich durch einen gleichzeitigen Anstieg der Hauttemperatur, der Körperkerntemperatur und der Herzfrequenz ankündigen. Im Stadium der Forschung und Entwicklung befinden sich daher Schutzanzüge mit integrierten Sensoren, die neben verschiedenen Umgebungsparametern (Temperatur, Luftfeuchtigkeit) auch eine Reihe von Vitalparametern der Einsatzkräfte kontinuierlich messen. Die Daten lassen sich per Funk an die Einsatzleitung übertragen, die so anhand von Grenzwerten kritische Situation für die Einsatzkräfte frühzeitig erkennen kann (Roßnagel et al. 2012, S. 9 ff.). Zwar sind Sensorsysteme zur Messung diverser Vitalparametern am Markt verfügbar, beispielsweise in Form von Handgelenksbändern (zur Messung der Herzfrequenz), Dehnungsmessstreifen (Atemfrequenz) oder von IR-Thermometern im Ohr (Körperkerntemperatur). Da solche Sensoren jedoch direkten Körperkontakt benötigen, besteht die Herausforderung darin, sie in die Schutzbekleidung der Einsatzkräfte zu integrieren, ohne gleichzeitig die Einsatzkräfte in ihrer Handlungs- und Bewegungsfreiheit

60 Beispielsweise der Löschzug Seppenrade der Freiwilligen Feuerwehr Lüdinghausen in Nordrhein-Westfalen (www.feuerwehr-seppenrade.de/index.php/technik/technik-mehr/fuer-atemschutz/305-msa-alpha-personal-network, 31.3.2022)

wesentlich zu behindern (Gödde/Wessels 2012, S. 17 ff.). Aus Forschungsprojekten sind zwar erste Prototypen für sensorische Schutzbekleidung hervorgegangen,[61] anwendungsreife Lösungen existieren bislang allerdings noch nicht. Ihr Einsatz wäre ebenfalls unter datenschutzrechtlichen Aspekten zu diskutieren: Nicht nur erlaubt die Auswertung der Daten vielfältige Rückschlüsse auf das Verhalten und die Arbeitsweise der Einsatzkräfte, auch handelt es sich bei den erhobenen Vitalparametern um Gesundheitsdaten, die einen besonders hohen Schutzbedarf aufweisen (Roßnagel et al. 2012, S. 24 f.).

3.2.4.3 Monitoring von Einsatzstellen mit Laser oder Radar

Auf dem Prinzip der Abstandmessung basieren lasergestützte Einsatzstellensicherungssysteme zum permanenten Monitoring von einsturzgefährdeten Gebäuden bzw. Trümmerstrukturen sowie von Deichen, Dämmen, Hängen oder Felsen, bei denen Brüche bzw. Abbrüche drohen. Durch Messen der Zeit bis zum Eintreffen des reflektierten Laserstrahls können kleinste Bewegungen aus sicherer Entfernung sofort erkannt werden. Beim THW werden solche Geräte eingesetzt, um Rettungskräften bei drohenden Gefahren ein rechtzeitiges Verlassen der Einsatzstelle zu ermöglichen.[62] Bisher setzen solche Systeme allerdings die Anbringung von Reflektoren als Messpunkte an instabilen Strukturen voraus, was nicht ohne Risiko ist. In dem durch die zivile Sicherheitsforschung des Bundes geförderten Projekt »Radar-Warn- und Informationssystem für Anwendungen im Katastrophenschutz« (RAWIS, Laufzeit 2014 bis 2018)[63] wurde daher ein Demonstrator für ein radarbasiertes System entwickelt, das eine Einsatzstelle ohne vorheriges Anbringen von Messpunkten lückenlos überwachen kann (Fraunhofer FHR 2018).

3.3 Automatisierte Datenauswertung

Die automatisierte Verarbeitung von Sensordaten ist ein integraler Bestandteil vieler sensorbasierter Beobachtungstechnologien. Typische Aufgaben sind einfache Korrekturfunktionen (z. B. Rauschunterdrückung und Kontrastkorrekturen in Foto- oder Videodaten), die Datenaufbereitung zur besseren Visualisierung (z. B. Falschfarbendarstellung bei Wärmebildkameras) oder die Zusammenführung

61 Beispielsweise aus den Projekten »Systemintegrierte Schutzbekleidung für Feuerwehr und Katastrophenschutz« (SensProCloth, Laufzeit 2008 bis 2011) oder »Intelligente Einsatzbekleidung für Polizei- und Sicherheitskräfte« (iBePol, Laufzeit 2011 bis 2014) im Rahmen der Sicherheitsforschung des Bundes (www.sifo.de/de/sensprocloth-systemintegrierte-sensorische-schutzbekleidung-fuer-feuerwehr-und-1813.html, www.sifo.de/sifo/de/projekte/querschnittsthemen-und-aktivitaeten/praxistransfer-und-kompetenzaufbau/kmu-innovativ/ibepol/ibepol-intelligente-einsatzbek-polizei-und-sicherheitskraefte.html; 31.3.2022).

62 www.thw.de/SharedDocs/Ausstattungen/DE/Geraete/ESS.html (31.3.2022)

63 https://sifo.bmbfcluster.de/files/Projektumriss_RAWIS.pdf (31.3.2022)

und Verarbeitung von Daten aus unterschiedlichen Sensoren (z. B. im Kontext der Gefahrenstoffdetektion). Ziel ist es, die Qualität der Sensordaten derart aufzubereiten, dass ein menschlicher Beobachter sie möglichst intuitiv bewerten und daraus die benötigten Informationen schnell und sicher ableiten kann.

An Bedeutung gewinnen in den vergangenen Jahren aber zunehmend auch Verfahren der automatisierten Datenverarbeitung, die weit über die qualitative und visuelle Aufbereitung von Sensordaten hinausgehen. Hier besteht das Ziel vielmehr darin, den menschlichen Beobachter bei der Analyse und Interpretation der Daten zu unterstützen bzw. solche Aufgaben ganz auf die Beobachtungstechnologie zu übertragen (Kees 2015, S. 19). Anwendung finden solche Verfahren aktuell vor allem auf Foto- oder Videodaten aus bildgebenden Beobachtungstechnologien. Nicht zuletzt konnten bei Algorithmen zur Bildanalyse in den vergangenen Jahren substanzielle Fortschritte erzielt werden. So gehören einfachere Analysefunktionen, die keiner komplexen semantischen Interpretation der beobachteten Ereignisse bedürfen, bereits heute zum Standardumfang von auf dem Markt unter der Bezeichnung »intelligente Videoüberwachung« angebotenen Systemen. Dazu zählen etwa die automatisierte Raumüberwachung (Alarm bei Anwesenheit von Personen in zuvor festgelegten Bereichen) oder Funktionen zur Personenzählung oder Verweildauermessung.[64] Das Einsatzspektrum im unternehmerischen bzw. privaten Bereich ist sehr vielfältig, angefangen von der effektiven Beobachtung großer Flächen (private Grundstücke, Industrieanlagen) über die Anlagensteuerung (z. B. Steuerung von Lüftungssystemen in Abhängigkeit der Anzahl anwesender Personen) bis hin zur Analyse von Kunden- oder Besucherbewegungen im Einzelhandel oder in Museen (Besucherzahlen, Verweildauer vor Produkten bzw. Exponaten, Bildung von Warteschlangen etc.) (Hempel 2016, S. 27).

Die Innovationen im Bereich der automatisierten Bildauswertung eröffnen auch Spielräume für neue Anwendungskonzepte im Bereich der zivilen Sicherheit. Im Folgenden werden entlang von typischen Aufgabenstellungen wichtige Verfahren sowie aktuelle und künftig mögliche Einsatzfelder von Beobachtungstechnologien mit automatisierter Datenauswertung (Kurzform: automatisierte Beobachtungstechnologien) im zivilen Sicherheitsbereich vorgestellt. Polizeiliche Nutzungspotenziale solcher Verfahren werden vertieft in Kapitel 3.5 am Beispiel der automatisierten Gesichtserkennung behandelt.

3.3.1 Erkennung bewegter Objekte in Videodaten

Für die Erkennung bewegter Objekte (Personen, Kfz etc.) vor einem statischen Hintergrund wurden zahlreiche Verfahren entwickelt. Ein sehr einfacher Ansatz ist es, ein Bild pixelweise mit einem oder mehreren vorangegangenen Bildern zu

64 Beispielsweise www.intenta.de/de/sensorsysteme/security.html; www.intelli-vision.com/intelligent-video-analytics (31.3.2022).

vergleichen (Temporal Differencing). Überschreitet der Unterschied einen bestimmten Grenzwert, gilt der Pixel als bewegt und wird zusammen mit anderen Pixeln zu bewegten Bildbereichen zusammengefasst. Andere Verfahren wie beispielsweise das Background Modeling schätzen den statischen Anteil einer Szene (Hintergrund) und vergleichen dies mit dem aktuellen Bild. Anwendung finden solche Verfahren beispielsweise in der Verkehrsbeobachtung (Hintergrund: Straße ohne Autos) oder für den Perimeterschutz (Hintergrund: überwachtes Areal ohne Personen bzw. bewegliche Objekte) (Hempel 2016, S. 74 ff.).

3.3.2 Verfolgung bewegter Objekte in Videodaten

Sind bewegte Objekte erst einmal erkannt, können diese von Bild zu Bild verfolgt werden. Auch hierfür wurde eine Vielzahl an Algorithmen entwickelt. Beim Active Contour-based Tracking beispielsweise werden die Objektumrisse als einhüllende Kontur repräsentiert und in den nachfolgenden Bildern immer wieder aktualisiert. Beim Model-based Tracking werden Objekte durch Modelle angenähert (ein menschlicher Körper beispielsweise durch bewegliche Strichmännchen). Position und Pose des Objekts im nächsten Bild werden dann anhand des bisherigen Verlaufs und eines Bewegungsmodells geschätzt, mit dem tatsächlichen Bild verglichen und ggf. angepasst (Kees 2015, S. 49). Durch Berechnung von Trajektorien für die bewegten Objekte können diese auch verfolgt werden, wenn sie in einer Szene zeitweise hinter anderen Objekten verschwinden (Hempel 2016, S. 78). Darüber hinaus wird derzeit an der Verbesserung von Verfahren gearbeitet, die Personen oder Objekte über mehrere verschiedene Kamerapositionen hinweg verfolgen können (z. B. Cho/Yoon 2016). Eine flächendeckende vernetzte Videobeobachtung vorausgesetzt, wäre es damit prinzipiell möglich, z. B. fliehende Personen oder Autos über ganze Stadtgebiete zu verfolgen.

3.3.3 Objektklassifizierung in Foto- oder Videodaten

Grundlage vieler Anwendungen der automatisierten Bildanalyse ist die Einteilung der abgebildeten Objekte in verschiedene Klassen. Ein einfacher Ansatz ist, verschiedene Formen mit Punktwolken, umrahmenden Boxen oder Silhouetten anzunähern. Anhand von Verteilung, Positionen und Seitenverhältnissen dieser Strukturen können die Formen verschiedenen Objektklassen (z. B. Person, Kfz, bestimmter Buchstabe) zugeordnet werden (Kees 2015, S. 48).

Eine Anwendung im zivilen Sicherheitsbereich sind Systeme zum automatisierten Kfz-Kennzeichenabgleich: Per Videokamera werden die Kennzeichen von den vorbeifahrenden Fahrzeugen erfasst und mittels Objektklassifizierung in maschinenlesbare Buchstaben und Ziffern umgewandelt, um sie dann in Echtzeit mit dem Bestand einer Datenbank (z. B. eine Fahndungsdatenbank) abzugleichen und in Trefferfällen einen Alarm auszulösen. Solche Systeme werden seit Mitte

der 2000er Jahre von den Polizeibehörden in einigen Bundesländern[65] eingesetzt (Hempel 2016, S. 123). Die Bundespolizei kann seit 2017 solche Systeme anlassbezogen zur Gefahrenabwehr oder Straftatenverhütung im Rahmen der Kontrolle des grenzüberschreitenden Verkehrs einsetzen (§ 27b BPolG). Im März 2019 sprach sich der Deutsche Bundestag für eine Änderung des Straßenverkehrsgesetzes aus,[66] die es den zuständigen Verkehrsüberwachungsbehörden ermöglicht, Systeme zum automatisierten Kfz-Kennzeichenabgleich für die stichprobenartige Überprüfung des Vollzugs von immissionsbedingten Verkehrsbeschränkungen oder -verboten einzusetzen.[67]

Große Fortschritte bei komplexeren Aufgaben der Objektklassifizierung konnten in den letzten 15 Jahren durch die Nutzung von Modellen aus dem maschinellen Lernen (ML) erzielt werden (siehe Exkurs in Kap. 3.3.8). Für das Training der Modelle sind große Bilddatenbanken notwendig, wobei jedem Bild die Bezeichnung des darauf abgebildeten Objekts manuell zugeordnet werden muss. Um gute Ergebnisse zu erzielen, sind typischerweise für jede Objektklasse mehrere Hundert Beispielbilder erforderlich (LeCun et al. 2015, S. 440). Solch umfangreiche Bilddatenbanken stehen erst seit wenigen Jahren zur Verfügung (Krizhevsky et al. 2012), wobei hier insbesondere der Umstand von Nutzen ist, dass Privatpersonen immer mehr Fotos ins Internet stellen. Ein fertig trainiertes ML-Modell kann Objekte so schnell klassifizieren, dass es auch für die Echtzeitauswertung von Videodaten eingesetzt werden kann. Als Ergebnis werden Bildregionen mit klassifizierten Objekten identifiziert und durch eine Box zusammen mit einem Wahrscheinlichkeitswert, dass es dabei um das jeweilige Objekt handelt, markiert (Abb. 3.18).

Eine Anwendung von ML-Modellen zur Objektklassifizierung im Bereich der zivilen Sicherheit sind Sicherheitsscanner für die Personenkontrolle (Kap. 3.1.2.3). Hier geht es darum, potenziell gefährliche Gegenstände (z. B. Handfeuerwaffen, Messer, Sprengstoffe) von harmlosen Objekten (z. B. Knöpfe, Reisverschlüsse) und menschlichen Körperteilen (z. B. Genitalien) zu unterscheiden. Dazu werden die Modelle mit einer Vielzahl von Bildern von Testpersonen mit und ohne verdächtige Gegenstände trainiert (Karamalis/Evers 2015).

65 Systeme zum automatisierten Kfz-Kennzeichenabgleich werden (Stand April 2019) in Brandenburg, Berlin, Bayern, Hessen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen, Rheinland-Pfalz, Sachsen und Thüringen eingesetzt (Bundesregierung 2019d, S. 4 f.).

66 Neuntes Gesetz zur Änderung des Straßenverkehrsgesetzes vom 8.4.2019 (BGBl. I, S. 430)

67 Im Juni 2021 wurde mit § 163g StPO auch im Strafprozessrecht eine Grundlage für einen örtlich begrenzten und vorübergehenden Einsatz solcher Systeme zu Fahndungszwecken bei Straftaten von erheblicher Bedeutung geschaffen (Artikel 1 Nr. 29 Gesetz zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften vom 25.6.2021; BGBl. I, S. 2099).

Abb. 3.18 Objektklassifizierung in Videodaten mit ML-Modellen

Quelle: Ren et al. 2017

3.3.4 Situations- und Verhaltensanalysen in Videodaten

Nach der Erkennung, Verfolgung und Klassifizierung von Objekten können Analysen höherer Ebenen durchgeführt werden. Einfachere Situations- bzw. Verhaltensanalysen, die keine komplexe semantische Interpretation der beobachteten Ereignisse erfordern, gehören bereits heute zum Funktionsumfang kommerzieller Videobeobachtungssysteme (Kees 2015, S. 19). Dazu zählen etwa die automatisierte Raumüberwachung (befinden sich Personen oder Kfz in einem festgelegten Bereich?), die Personenzählung bzw. -dichtemessung (z. B. im Kontext von Veranstaltungen), das Erkennen von stehengelassenen Gegenständen oder die Messung der Aufenthaltsdauer einer Person an einem Ort (z. B. um herumlungerndes Verhalten zu detektieren). Ob solche einfacheren Formen der Situations- und Verhaltensanalysen auch für polizeiliche Zwecke von Nutzen sein können, wird mithilfe von Darstellern seit Juni 2019 im Rahmen des Teilprojekts 2 im Pilotprojekt »Sicherheitsbahnhof Berlin Südkreuz« durch das Bundesministerium des Innern, für Bau und Heimat, die Bundespolizei, das Bundeskriminalamt und die Deutsche Bahn (DB) AG getestet. Zu den hier erprobten Funktionalitäten gehören folgende Szenarien (Bundesregierung 2018n, S. 21 ff.; DB AG 2019):

- abgestellte Gegenstände;
- Betreten festgelegter Bereiche;
- liegende (hilfsbedürftige) Personen;
- Bewegung von Personengruppen;
- Ansammlungen von Personen (z. B. vor Rolltreppen);
- Personenzählung für bestimmte Flächen (insbesondere Bahnsteigüberfüllung).

Schwieriger und oft noch in einem frühen Forschungsstadium sind komplexere Verhaltensanalysen. Vergleichsweise einfach ist die Herangehensweise, in Videobildern nach bestimmten statischen Körperhaltungen zu suchen, die auf gewisse Verhaltensweisen schließen lassen, etwa erhobene Arme auf aggressives Verhalten oder eine gebückte Körperhaltung auf Angst (Menevidis/Ajami 2013,

S. 38 ff.). Weitergehende Ansätze modellieren ganze Bewegungsabläufe wie Schlagen, Treten, Rennen oder Stürze anhand von Gelenkstellungen und Winkelgeschwindigkeiten der Gliedmaßen, um etwa Gewaltausbrüche erkennen zu können (Hempel 2016, S. 79). Die Eignung solcher Systeme für die Bekämpfung von Straßenkriminalität wird seit Ende 2018 durch das Polizeipräsidium Mannheim an ausgewählten Kriminalitätsschwerpunkten erprobt (Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg 2018). Zur Anwendung gelangt hier eine unter Laborbedingungen entwickelte Software des Fraunhofer Instituts für Optronik, Systemtechnik und Bildauswertung, die nun schrittweise an den Einsatz unter realen Bedingungen angepasst werden soll (Fraunhofer IOSB o. J.).

Grundlage für die Detektion auffälligen Verhaltens sind stets Verhaltensmodelle, anhand derer die beobachteten Bewegungsinformationen in normales bzw. atypisches Verhalten eingeteilt werden (dazu und zum Folgenden Kees 2015, S. 54 f.). Solche Modelle können manuell erstellt werden, was für komplexe Bewegungsabläufe allerdings sehr aufwendig und fehleranfällig ist. Eine andere Möglichkeit ist, die Modelle anhand einer Vielzahl an Trainingsszenen mit der Methode des überwachten Lernens aus dem maschinellen Lernen (Exkurs in Kap. 3.3.8) zu trainieren. Beide Herangehensweisen setzen jedoch die Festlegung von wohldefinierten normalen bzw. atypischen Verhaltenskategorien voraus. Dies ist in der Praxis häufig nur schwer realisierbar, da menschliches Verhalten enorm vielfältig und meist nicht vorhersehbar ist. Von Nutzen könnte hier ggf. die Methode des unüberwachten Lernens aus dem maschinellen Lernen sein (Kap. 3.3.8.1). Ein Merkmal zur Unterscheidung zwischen normalen und anomalen Verhaltensweisen könnte dann beispielsweise die beobachtete Häufigkeit von Ereignissen sein (insofern also selten vorkommende Verhaltensweisen als anomal klassifiziert würden). Dies könnte allerdings dazu führen, dass etwa gehbehinderte Personen grundlos als potenziell gefährlich eingestuft werden, was eine Diskriminierung darstellen würde (Ammicht Quinn et al. 2015, S. 26). Weitere mögliche Risiken des Einsatzes von ML-gestützten Verfahren werden in Kapitel 3.3.8.2 beschrieben.

3.3.5 Gesichtserkennung in Foto- oder Videodaten

Mit Methoden der Objekterkennung und -klassifizierung können auch Personen bzw. deren Gesichter in Foto- oder Videodaten aufgefunden werden. Handelt es sich hierbei um eine unbekannte Person, kann als nächster Schritt versucht werden, deren Identität durch einen Abgleich mit zuvor in einer Datenbank gespeicherten Gesichtsbildern bekannter Personen festzustellen. Methoden, Einsatzfelder und Leistungsfähigkeit der automatisierten Gesichtserkennung für Aufgaben im Bereich der zivilen Sicherheit werden vertieft in Kapitel 3.5 behandelt.

3.3.6 Altersbestimmung, Gefühlsanalyse, Ermittlung der sexuellen Orientierung

Mithilfe der automatisierten Datenverarbeitung können aus Foto- oder Videoaufnahmen von Menschen weitere Informationen über Personen gewonnen werden. Bei solchen Algorithmen handelt es sich meist um Forschungsbeiträge aus dem Bereich des maschinellen Lernens, die – soweit bekannt – für Sicherheitsanwendungen derzeit nicht zum Einsatz kommen. Trotzdem werden hier einige Beispiele aufgeführt, um das prinzipielle Potenzial solcher Ansätze zu illustrieren.

- *Altersbestimmung*: Mit Methoden des maschinellen Lernens wurden Modelle entwickelt, die auf der Grundlage eines Gesichtsbilds das Alter der abgebildeten Person mit einem durchschnittlichen Fehler von nur rund 4 Jahren bestimmen können (Huerta et al. 2015).
- *Emotionsanalyse*: Aus den Bewegungen der Gesichtsmuskeln bzw. dem Gesichtsausdruck können ML-Modelle auf die Emotionen (z. B. Freude, Angst, Wut) einer Person schließen. Die derzeit besten Modelle sollen in über 75 % der Fälle richtige Ergebnisse liefern können (Ko 2018).
- *Ermittlung der sexuellen Orientierung*: Vor einiger Zeit schlug die Forschungsarbeit von Wang und Kosinski (2018) hohe Wellen. Die Autoren trainierten ein ML-Modell an Gesichtsbilder von Personen, deren sexuelle Orientierung bekannt war (es wurden Bilder aus einer Datingplattform verwendet). Das fertig trainierte Modell konnte anschließend unbekannte Männer (also solche, deren Gesichtsbilder nicht für das Training verwendet wurden) in 81 % der Fälle richtig in homo- bzw. heterosexuell einteilen. Bei Frauen lag die Erkennungsrate bei 71 %.

3.3.7 Erkennung und Analyse von Geräuschen

Im Sicherheitsbereich bisher weniger im Fokus standen automatisierte Analyseverfahren für Sensordaten von nichtbildgebenden Beobachtungstechnologien. Gleichwohl gibt es auch hierzu diverse Forschungsanstrengungen, u. a. im Kontext der akustischen Beobachtung. Neben der Spracherkennung geht es hier vor allem um die automatisierte Erkennung und Analyse von definierten Geräuschen in Audioaufnahmen. Die Vorgehensweise ähnelt jener der automatisierten Bildanalyse, indem zunächst relevante Ereignisse von den Hintergrundgeräuschen getrennt werden, um sie dann in vordefinierte Klassen einzuteilen. In den vergangenen Jahren wurden etwa Algorithmen entwickelt, die menschliche Schreie, Weinen, Schüsse aus Feuerwaffen, brechendes Glas oder Explosionen in Umgebungsgeräuschen zuverlässig erkennen können (Sharan/Moir 2015, S. 91). Die Geräuschquellen können nach Bedarf lokalisiert und ggf. verfolgt werden. Aus den so gewonnen Informationen lassen sich schließlich Situationsanalysen erstellen (Crocco et al. 2016).

Obschon die automatisierte Geräuscherkennung und -analyse ein noch junges Forschungsfeld ist (Sharan/Moir 2015, S. 90), gibt es in anderen Ländern bereits erste konkrete Sicherheitsanwendungen. Ein US-amerikanisches Unternehmen beispielsweise bietet ein System zur akustischen Beobachtung des öffentlichen Raums an, welches durch ein engmaschiges Netz an Mikrofonen das Geräusch von abgefeuerten Schusswaffen erkennen und lokalisieren können soll. Verdachtsfälle werden von einem Operator überprüft, der dann ggf. die Polizei verständigt. Dadurch sollen Tatorte nicht nur schneller erreicht, sondern auch dann lokalisiert werden können, wenn (noch) gar kein Notruf eingegangen ist. Nach Unternehmensangaben wurde das System 2018 bereits in über 85 Städten der USA eingesetzt (ShotSpotter 2018).

Ein weiteres Beispiel sind Systeme zur Warnung vor und Lokalisierung von Tornados, die derzeit entwickelt werden. Sturmsysteme emittieren bis zu 2 Stunden vor der Bildung eines Tornados für Menschen kaum wahrnehmbare Schallwellen sehr tiefer Frequenzen (Infraschallwellen), die sich mit empfindlichen Mikrofonen in einer Entfernung von bis zu 500 Kilometern detektieren und analysieren lassen (Elbing et al. 2018).

3.3.8 Exkurs: maschinelles Lernen

Für viele mathematische Problemstellungen können Informatiker Algorithmen entwickeln, indem sie einen konkreten Lösungsweg durch eine Abfolge von Programmanweisungen fest vorgeben. Für komplexe Aufgaben erweist sich diese Herangehensweise allerdings oft als extrem aufwendig und wenig erfolgreich. Ein anderer Ansatz ist daher, einem Algorithmus die Möglichkeit zu geben, selbst einen Lösungsweg für ein Problem zu finden (Hempel 2016, S. 74). Die Idee entstammt dem Forschungsgebiet des maschinellen Lernens, das wiederum seine Ursprünge im Forschungsgebiet der künstlichen Intelligenz hat.

3.3.8.1 Methoden des maschinellen Lernens

Überwachtes Lernen

Eine mögliche Methode ist das überwachte Lernen: Ausgangspunkt ist ein Modell, das Eingabedaten in zunächst beliebiger Weise auf Ausgabedaten (z. B. ein Set von vorgegebenen Outputkategorien) abbilden kann. Für die Aufgabe der Objekterkennung beispielsweise soll das Modell Bilder von Objekten vorgegebenen Objektklassen zuordnen (z. B. »Person«, »Motorrad«, »Bus«, »Flugzeug«; Abb. 3.18). Damit das Modell ein Bild von einem Objekt mit einer bestimmten Wahrscheinlichkeit der richtigen Kategorie zuordnen kann, muss es zunächst mit einem ausreichend großen Satz an Eingabedaten und dazugehörigen *korrekten* Lösungen trainiert werden (dazu und zum Folgenden Angerer 2018). Dazu ist

eine Fehlerfunktion erforderlich, die für jedes Input-Output-Datenpaar einen Wert für die Abweichung zwischen dem Modelloutput und der korrekten Lösung berechnet. Dieser Wert hängt von den Eingabedaten und den internen Parametern des Modells ab. Das eigentliche Training erfolgt nun durch einen speziellen Algorithmus, der für jedes Input-Output-Datenpaar den Wert der Fehlerfunktion berechnet und danach die internen Modellparameter derart anpasst, dass der Fehlerwert geringfügig kleiner wird. Wird dies mit einer Vielzahl von Trainingsdatensätzen wiederholt, lernt das Modell, immer bessere Ergebnisse zu erzielen. Sobald das Modell mit der gewünschten Wahrscheinlichkeit korrekte Ergebnisse liefert, werden alle internen Modellparameter abgespeichert und der Lernerfolg des fertigen Modells anhand von Eingabedaten, die nicht für das Training verwendet wurden, überprüft. Besteht das Modell diesen Test, ist es bereit für den Praxiseinsatz. Zu betonen ist, dass bei dieser Methode nur fertig trainierte und damit statische Modelle in entsprechende Softwareprodukte eingebunden werden, nicht aber die für das Training verantwortlichen Algorithmen (Zweig 2018, S. 13).

Die verwendeten Modelle sind in ihrem Aufbau sehr komplex und verfügen oft über eine sehr große Zahl an einstellbaren internen Parametern (bis zu mehreren Millionen). Entsprechend müssen sie – je nach Anwendungskontext und Qualität der Trainingsdaten – auch mit einer riesigen Menge an Datensätzen trainiert werden, um gute Vorhersagen erzielen zu können (Schroff et al. 2015). Den Weg dazu haben erst zwei Entwicklungen der jüngeren Vergangenheit geebnet (TAB 2016b, S. 106): Zum einen ist dies die rasante Entwicklung der Computer- und Speicherleistung, zum anderen die immer größeren, insbesondere über das Internet zugänglichen Datenmengen, die für das Training der Modelle benötigt werden.

Unüberwachtes Lernen

Neben dem überwachten Lernen gibt es weitere Lernmethoden. Beim unüberwachten Lernen beispielsweise sollen die Modelle ohne Vorgaben vom Menschen lernen, Muster in den Eingabedaten zu erkennen. Dazu werden anhand der statistischen Eigenschaften der Inputdaten die Outputkategorien durch den Algorithmus selbst entwickelt. Diese Kategorien sind für den Menschen in der Regel intuitiv nicht verständlich, hierfür ist eine Interpretationsleistung erforderlich. Da hier der Lernprozess im Gegensatz zum überwachten Lernen keine (i. d. R. durch Menschen) korrekt klassifizierte Input-Output-Datenpaare voraussetzt, kann die Trainingsphase auch während des realen Einsatzes fortgesetzt werden, um so die Menge an Trainingsdaten zu vergrößern. Der Nachteil dieser selbstlernenden Systeme ist aber, dass sie einer ständigen Anpassung und Veränderung in Abhängigkeit der jeweiligen Eingabedaten unterliegen, sodass sie

unter Umständen auch nichterwünschte Verhaltensweisen lernen können (TAB 2020, S. 52 f.).

3.3.8.2 Begrenzungen und Risiken

Konnten in den letzten Jahren durch die Anwendung von Methoden des maschinellen Lernens enorme Fortschritte bei der automatisierten Datenauswertung erzielt werden, so gilt es auch, damit verbundene Begrenzungen und Risiken nicht aus dem Blickfeld zu verlieren. Nachfolgend werden einige problematische Aspekte des Einsatzes von ML-basierten Verfahren in sicherheitsrelevanten Anwendungskontexten kurz beschrieben (dazu auch TAB 2020, S. 57 ff.).

Bias

Ein Bias liegt vor, wenn die Ergebnisse eines algorithmischen Verfahrens systematisch von einem gesetzten Standard abweichen. Da Algorithmen bzw. ML-Modelle eine komplexe Wirklichkeit niemals objektiv, neutral und präzise abbilden können, sondern immer nur Auswahlentscheidungen reflektieren, die in ihrem Design getroffen werden müssen (TAB 2020, S. 58), sind Bias bei der algorithmischen Datenverarbeitung in gesellschaftlichen Anwendungskontexten oft ein inhärentes Problem. So haben beispielsweise Lischka und Klingel (2017) für eine Reihe von Anwendungsfeldern von ML-gestützten Verfahren zur Verarbeitung von Sozialdaten Fallbeispiele dokumentiert, in denen Bias zu Fehlern und Schäden für die betroffenen Personen geführt haben. Dazu gehören etwa Verfahren, die für die Zuordnung von Studienplätzen für angehende Studierende oder für die Berechnung der Kreditwürdigkeit von Privatkunden eingesetzt werden, aber auch Methoden zur Erstellung von Kriminalitätsprognosen, die im Rahmen der vorhersehenden Polizeiarbeit Anwendung finden (dazu Kap. 4.3).

Eine wesentliche Quelle für einen Bias in ML-Modellen sind Trainingsdaten, die für den intendierten Einsatzzweck nicht repräsentativ sind. Werden beispielsweise Systeme zur Gesichtserkennung mit einem Set von Bildern von Personen trainiert, das in Bezug auf Geschlecht, Alter, Hautfarbe oder Ethnizität nicht ausgewogen ist, sinkt die Erkennungsleistung der resultierenden ML-Modelle für die unterrepräsentierten Personengruppen. Für diese Personen erhöht sich dadurch die Erkennungsfehler- und die Fehlalarmrate[68] (McDuff et al. 2018, S. 1). Systembedingte Diskriminierungen durch ML-gestützte Verfahren für die Erkennung oder Analyse von Gesichtern wurden für verschiedene kommerzielle Softwareprodukte bereits nachgewiesen, wobei die Fehlerraten typischerweise für Frauen, dunkelhäutige oder jüngere Personen höher ausfielen (Raji/Buolamwini 2019; Buolamwini/Gebru 2018; Klare et al. 2012). Mögliche Konsequenzen für die Betroffenen hängen vom jeweiligen Anwendungskontext ab: Sollen etwa Gesichts-

68 Siehe Definitionen in Kap. 3.5.2.2.

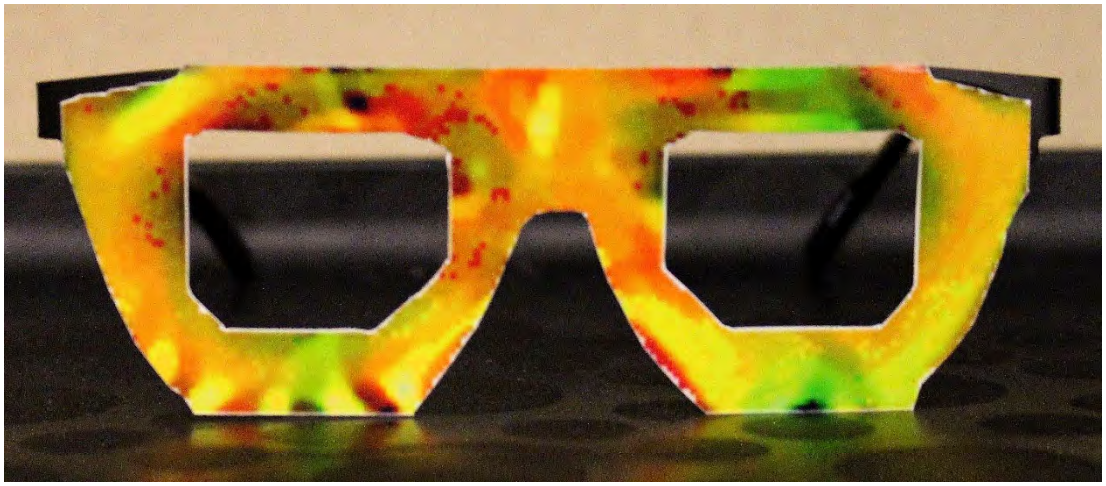
erkennungssysteme in Verbindung mit der Videobeobachtung zur Personenfahndung in Echtzeit eingesetzt werden (Kap. 3.5), würden gesuchte Personen seltener erkannt und unbeteiligte Personen häufiger als verdächtig markiert werden, wenn sie einer der unterrepräsentierten Gruppen angehörten.

Vorhersagbarkeit und Verlässlichkeit des Verhaltens

Im Fall von selbstlernenden Systemen, die auch während des realen Einsatzes lernen und ihr Verhalten entsprechend anpassen können, ist offensichtlich, dass die Vorhersagbarkeit im Lauf der Zeit abnimmt und ab einem bestimmten Zeitpunkt nicht mehr gewährleistet werden kann (TAB 2020, S. 59).

Aber auch die mit der Methode des überwachten Lernens bereits fertig trainierten ML-Modelle können unter Umständen ein schwer vorhersagbares Verhalten produzieren. Für ML-Modelle zur Objektklassifizierung beispielsweise ist bekannt, dass sie durch minimale, durch das menschliche Auge praktisch nicht erkennbare Abweichungen in den Ausgangsbildern dazu gebracht werden können, ein zuvor korrekt klassifiziertes Bild völlig falsch einzuordnen (TAB 2020, S. 59 ff.). Ein anderes Beispiel ist eine von Sharif et al. (2016) entwickelte Technik zur Täuschung von Gesichtserkennungssystemen durch Brillen, deren Ränder mit einem speziellen Muster bedruckt sind (Abb. 3.19). Personen, die die präparierten Brillen trugen, wurden von kommerziellen Gesichtserkennungssystemen entweder gar nicht mehr (Verschleierung) oder als eine beliebig wählbare andere Person erkannt (Identitätsdiebstahl). Es liegt auf der Hand, dass Verfahren der automatisierten Datenauswertung, deren Verhaltensweisen nicht verlässlich vorhersagbar oder gar manipulierbar sind, in sicherheitskritischen Einsatzkontexten äußerst problematisch sind.

Abb. 3.19 Brille zur Täuschung von Gesichtserkennungssystemen



Quelle: Sharif et al. 2016, S. 9

ML-Modelle als Blackbox

Ein generelles Problem ist daher auch, dass ML-Modelle häufig vom Typ Blackbox sind. So basiert die Entwicklung von konventionellen Algorithmen in der Regel auf kausalitätsbasierten Modellen bzw. Theorien zur Lösung des jeweiligen Problems. Die kausalen Zusammenhänge werden in eine Abfolge von festen Programmanweisungen übersetzt und als Algorithmus implementiert. Wie der Algorithmus zu seinem Ergebnis gelangt, kann an den einzelnen Schritten genau nachvollzogen werden. Beim Ansatz des maschinellen Lernens ist es für den Softwareentwickler hingegen nicht mehr erforderlich, kausale Zusammenhänge zu kennen. Stattdessen werden während des Trainings der Modelle statistische Verbindungen zwischen beliebigen Merkmalen der Eingabe- und Ausgabedaten hergestellt, ohne dass es zwischen diesen eine kausale Beziehung geben muss (Hempel/Rehak 2017, S. 105). Für die Entwickler/innen (geschweige denn für die Anwender/innen) der Modelle ist es daher nicht mehr möglich, sowohl die für die Bewertung relevanten Merkmale als auch die innere Logik eines ML-Modells nachzuvollziehen.

Wie vor diesem Hintergrund behördliche Anwendungen von ML-gestützten Verfahren zur Personenbewertung mit dem Grundsatz der Nachvollziehbarkeit staatlichen Handelns in Einklang gebracht werden kann, ist eine offene Frage. Zwar werden derzeit verschiedene Ansätze erforscht, wie die Arbeitsweise von ML-Modellen für den Menschen besser nachvollziehbar gemacht werden könnte, der Weg dahin scheint allerdings noch weit (TAB 2020, S. 61 f.).

Mensch-Maschine-Interaktion

Die Implementierung von ML-gestützten Verfahren in gesellschaftlichen Einsatzkontexten kann nicht nur unerwünschte Folgen für die von der Datenverarbeitung betroffenen Personen haben. Darüber hinaus sind auch die Wirkungen auf die Anwender/innen der Technologien zu betrachten. Hier zu nennen sind etwa Probleme, die bei der Mensch-Maschine-Schnittstelle entstehen können. Ein übersteigertes Vertrauen in die Leistungsfähigkeit solcher Verfahren beispielsweise könnte bei den Anwender/innen zu einer Abnahme des Situationsbewusstseins führen, was sich unter Umständen negativ auf den damit eigentlich intendierten Sicherheitsgewinn auswirken könnte. Mögliche Risiken der Mensch-Maschine-Interaktion beim Einsatz von Beobachtungstechnologien mit automatisierter Datenauswertung im Bereich der zivilen Sicherheit sind Thema in Kapitel 7.2.

3.4 Vertiefung: offene Videobeobachtung im öffentlich zugänglichen Raum

Die Polizei setzt die offene Videobeobachtung im öffentlich zugänglichen Raum, zu dem öffentliche (Straßen, Plätze etc.) und halböffentliche Räume (Bahnhöfe, Flughäfen, Sportstadien etc.) gehören, vorrangig als Instrument der präventiven und repressiven Kriminalitätsbekämpfung ein: Zum einen soll der offene Einsatz von Videobeobachtung eine kriminalpräventive Wirkung entfalten, indem potenzielle Straftäter/innen dadurch eher damit rechnen müssen, entdeckt und für ihre Taten zur Rechenschaft gezogen zu werden. Zum anderen soll gespeichertes Videomaterial die Aufklärung begangener Straftaten unterstützen und damit von Nutzen für die Strafverfolgung sein. Dabei bedarf jede Form der polizeilichen (und generell der staatlichen) Videobeobachtung einer gesetzlichen Grundlage, die Anlass, Zweck und Grenzen des Einsatzes festlegt, da sie einen Eingriff in das Recht auf informationelle Selbstbestimmung (Kap. 6.1.2.1) darstellt, das laut Bundesverfassungsgericht (BVerfG, Beschluss vom 23.2.2007, 1 BvR 2368/06, Rn. 39) auch den informationellen Schutzinteressen des Einzelnen in der Öffentlichkeit Rechnung trägt.

Der weit überwiegende Teil der im öffentlich zugänglichen Raum installierten Videokameras wird allerdings von anderen Akteuren als der Polizei betrieben. Diese Formen stützen sich in der Regel auf das Datenschutzrecht, das den offenen Einsatz von Videobeobachtung im öffentlich zugänglichen Raum durch öffentliche Stellen zur Erfüllung ihrer Aufgaben und durch private Akteure zur Wahrnehmung berechtigter Interessen erlaubt. Entsprechend vielfältig sind die Einsatzzwecke, bei denen Sicherheitsbelange oft (z. B. Erkennung von Gefahrensituationen, Schutz vor Vandalismus, Diebstahl und andere Eigentumsdelikte, Wahrnehmung des Hausrechts durch Zugangskontrolle), aber nicht immer im Fokus stehen (z. B. Kontrolle betrieblicher Abläufe, Parkraumbewirtschaftung, Analyse des Kundenverhaltens im Einzelhandel).

Für die Kriminalitätsbekämpfung können gleichwohl alle Formen der offenen Videobeobachtung im öffentlich zugänglichen Raum von Bedeutung sein, denn der damit assoziierte Nutzen für die Kriminalprävention und Strafverfolgung hängt – in Abhängigkeit der Einzelheiten des konkreten Einzelfalls – in der Regel nicht vom jeweiligen Betreiber und primären Einsatzzweck ab. Voraussetzung hierfür ist allerdings, dass nichtpolizeiliche öffentliche und private Betreiber mit den Polizei- und Strafverfolgungsbehörden kooperieren, indem sie ihnen Zugriff auf Livebilder oder gespeichertes Videomaterial gewähren, wenn dies im Rahmen der Aufgabenwahrnehmung zur Gefahrenabwehr oder Strafverfolgung notwendig erscheint.

Bevor in Kapitel 3.4.4 der tatsächliche Nutzen der offenen Videobeobachtung im öffentlich zugänglichen Raum als Instrument der Kriminalitätsbekämpfung diskutiert wird, soll es angesichts der vielfältigen Einsatzformen im

Folgenden zunächst um die relevanten Akteure und rechtlichen Grundlagen (Kap. 3.4.2) sowie um die aktuellen Einsatzpraktiken (Kap. 3.4.3) gehen. Als Auftakt wird kurz die Geschichte der Videobeobachtung im öffentlich zugänglichen Raum skizziert.

3.4.1 Anfänge der Videobeobachtung im Sicherheitsbereich

Der Einsatz der Videobeobachtung für Sicherheitsaufgaben hat seit Mitte des 20. Jahrhunderts weltweit und auch in Deutschland kontinuierlich zugenommen (dazu und zum Folgenden Lin 2006, S. 15 ff.; Kammerer 2010; Hempel 2016, S. 21 ff.). Wurde Videotechnik ursprünglich nur zur Überwachung militärischer Anlagen benutzt, betraf das erste polizeiliche Anwendungsfeld die Verkehrslenkung. In Deutschland war Hamburg 1956 die erste Stadt, die das Verkehrsgeschehen mit stationären Kameras beobachtete, um bei stockenden Verkehrsflüssen Ampelanlagen manuell ansteuern zu können. In den Folgejahren schafften sich weitere Städte wie München, Hannover oder Kassel Kameras zur Verkehrsbeobachtung an. Ab 1960 wurden die installierten Videobeobachtungssysteme nicht mehr nur als Instrument der Verkehrslenkung angesehen, sondern zunehmend auch als eine Technik, mit deren Hilfe Verstöße gegen die Straßenverkehrsordnung effizient verfolgt werden konnten.

Neben verkehrspolizeilichen Funktionen trat in den 1960er Jahren zunehmend die Beobachtung von Versammlung und Großveranstaltungen in den Fokus polizeilicher Videobeobachtung. 1964 nahm die Münchner Polizei ein mobiles Videobeobachtungssystem auf einem Lkw in Betrieb, das mit Teleobjektiven, Aufzeichnungsgeräten und zur Datenübermittlung mit einer über 7 Meter hohen Antenne ausgestattet war. Davon versprach sich die Polizei schon damals einen Mehrfachnutzen: Die Präsenz der Videokameras sollte eine präventive Wirkung entfalten, die Liveübertragung zur Einsatzzentrale eine effiziente Lenkung der Polizeikräfte vor Ort ermöglichen und die gespeicherten Aufnahmen schließlich der Beweissicherung und ggf. Identifizierung von Störern dienen. Ähnliche Fernsehübertragungswagen wurden ab Ende der 1960 beispielsweise von der Polizei Nürnberg oder West-Berlin eingesetzt.

In den 1970er Jahren traten die kriminalpräventive Wirkung und der Nutzen für die Strafverfolgung in den Vordergrund. 1976 richtete Hannover die mit mehr als 20 stationären Kameras damals modernste und umfangreichste Videobeobachtungsanlage Deutschlands ein mit dem Ziel, die Straßenkriminalität, Prostitution etc. in der Innenstadt einzudämmen. 1996 begann die Polizeidirektion Leipzig das Pilotprojekt »Videoüberwachung von Kriminalitätsschwerpunkten« gegen Autoeinbrüche, Taschendiebstähle und Drogenhandel am Bahnhofvorplatz. Diesem Beispiel folgend starteten weitere Polizeibehörden ähnliche Modellversuche, z. B. in Magdeburg, Halle, Frankfurt am Main, Regenburg und

Stuttgart. 2005 wurden Kriminalitätsschwerpunkte bereits in 26 deutschen Städten mit insgesamt 94 Videokameras durch die Polizei beobachtet.

Zur raschen Ausbreitung der Videobeobachtung im öffentlich zugänglichen Raum in Deutschland trugen aber weniger polizeiliche Aktivitäten als vielmehr der Kameraeinsatz durch andere öffentliche Stellen und insbesondere durch private Akteure bei. Kommunen statteten zunehmend Rathäuser, Krankenhäuser, Schulhöfe, Schwimmbäder, Museen, Wertstoffsammelplätzen oder öffentliche Verkehrsmittel mit Videobeobachtungssystemen aus, um als Eigentümer solche Einrichtungen vor Schäden zu bewahren und den störungsfreien Betrieb zu ermöglichen (Lin 2006, S. 117). Durch die Privatwirtschaft wurden sehr schnell Kaufhäuser, Tankstellen, Hotelfoyers oder Publikumsbereiche von Banken mit Kameras ausgerüstet, um Einbrüchen, Diebstählen oder Schäden durch Vandalismus vorzubeugen bzw. solche Vergehen vor Gericht nachweisen zu können. Im Jahr 2000 wurde alleine die Zahl der in Deutschland im öffentlich zugänglichen Raum privat betriebenen Videokameras – je nach Angaben – auf zwischen 300.000 bis 500.000 Stück geschätzt (Lin 2006, S. 16).

Es waren vor allem soziale Ereignisse und deren mediale Verbreitung, die maßgeblich zur gesellschaftlichen Wahrnehmung und Akzeptanz der Videobeobachtung im öffentlichen Raum beitrugen und damit die Grundlage für deren rasche Verbreitung legten. Ein Beispiel hierfür ist der Mord an dem 3-jährigen James Bulger durch zwei Heranwachsende im Jahr 1993 in Liverpool, der durch die Videobeobachtung zwar nicht verhindert, jedoch aufgeklärt werden konnte (Kasten 3.2).

Die hohen Erwartungen bezüglich der kriminalpräventiven Wirkung der Videobeobachtung im öffentlichen Raum konnten durch erste Evaluationen ab dem Jahr 2000 allerdings nicht bestätigt werden (z. B. Welsh/Farrington 2002). Zeitgleich steigerte die einsetzende Digitalisierung der Videotechnik die Erwartungen. Lieferten analoge Systeme meist verschwommene, grobkörnige und Bilder schlechter Qualität, die auf Magnetbändern abgespeichert wurden, boten moderne digitale Systeme fortan hohe Bildqualitäten und Farbübertragung. Zudem erweiterten ferngesteuerte bewegliche Kameras mit Zoomfunktionen das Sichtfeld, ermöglichten IR-Sensoren Nachtaufnahmen und erlaubten effiziente und preiswerte Speichermöglichkeiten sowie die Vernetzung und Datenübertragung über das Internet die zunehmende Miniaturisierung und flexible Anwendung von Video- und Speichertechnik. Auf dieser Basis weiteten sich auch die Einsatzmöglichkeiten der Videobeobachtung immer mehr aus sowohl in Bezug auf die beobachteten Räume (z. B. Fahrzeuge des öffentlichen Personenverkehrs) als auch auf die Situationen der Beobachtung (z. B. mobile Videobeobachtung durch hand- oder am Körper getragene Kameras).

Kasten 3.2 Der James-Bulger-Fall

Am 12. Februar 1993 lockten zwei 10-jährige Jungen den 3-jährigen James Bulger aus einem Einkaufszentrum in Liverpool heraus, führten ihn über mehrere Kilometer hinweg zu einer Bahnstrecke und erschlugen ihn dort. Auf dem Weg zum Tatort wurden die 3 Kinder von 38 Passanten beobachtet, die allerdings nicht einschritten, obwohl James immer wieder nach seiner Mutter schrie. Die vom Ereignis getätigten Videoaufnahmen – eine zeigt die Entführung des Jungen durch einen seiner Mörder im Einkaufzentrum – trugen schließlich zur Identifizierung der Mörder bei. Die Grausamkeit des Ereignisses bestand in einem gefühlten Versagen allgemeiner sozialer Kontrollmechanismen. Der Schutz des öffentlichen Raums wurde als unzureichend bewertet, zugleich empfahl sich die Videobeobachtung als Maßnahme, an die sich jene fehlende soziale Verantwortung delegieren ließe. Fortan wurde die Videobeobachtung als ein kriminalpräventives Instrument angepriesen, das Straftaten verhindern und die Kriminalität reduziert könne. Dies führt in Großbritannien zu einer im Verhältnis zu anderen Ländern überdurchschnittlich rasanten und hohen Verbreitung von Videobeobachtungssystemen (Hempel/Töpfer 2009).

3.4.2 Aktueller Stand: Akteure und rechtliche Grundlagen in Deutschland

Heute wird Videobeobachtung im öffentlich zugänglichen Raum von unterschiedlichen Akteuren in verschiedenen Formen eingesetzt. Ein einheitliches Gesetz, das alle Einsatzformen regeln würde, gibt es in Deutschland allerdings nicht. Vielmehr existiert ein komplexes Regelungsgefüge aus zahlreichen spezialgesetzlichen und/oder datenschutzrechtlichen Regelungen zur Videobeobachtung sowohl auf Bundes- als auch Länderebene (WD 2016c, S. 3). Seit dem 25. Mai 2018 sind zusätzlich die Vorschriften der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung)[69] zu beachten, die gegenüber nationalen Gesetzen einen Anwendungsvorrang genießen. Zwar enthält die Datenschutz-Grundverordnung im Gegensatz etwa zum Bundesdatenschutzgesetz (BDSG)[70] keine spezifischen Vorschriften zur Videobeobachtung. Allerdings gilt sie für alle Arten der Verarbeitung personenbezogener Daten, wozu auch die Videobeobachtung zählt, falls die Aufnahmen von einer Qualität sind, die prinzipiell eine Identifizierung einzelner Personen ermöglicht.

69 Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

70 Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097)

Vor diesem Hintergrund bietet es sich für die nachfolgenden Ausführungen an, die im vorliegenden Kontext relevanten Akteure nach öffentlichen und nichtöffentlichen Stellen zu differenzieren, wobei sich erstere Gruppe weiter in Polizei- und Strafverfolgungsbehörden und andere öffentliche Stellen einteilen lässt. So unterscheidet beispielsweise das BDSG zwischen öffentlichen und nichtöffentlichen Stellen. Die Datenschutz-Grundverordnung hingegen behandelt öffentliche und nichtöffentliche Stellen zwar im Ansatz gleichberechtigt, stellt für sie jedoch unterschiedliche Erlaubnistatbestände für Datenverarbeitungen bereit und enthält insbesondere für hoheitliche Datenverarbeiter eine Reihe von bereichsspezifischen Ausnahmeregelungen und Öffnungsklauseln (Bäcker 2019). So gelten für die Datenverarbeitung zu Zwecken der Gefahrenabwehr und Strafverfolgung, die zur Hauptsache durch Polizei- und Strafverfolgungsbehörden erfolgt, die Regelungen der Datenschutz-Grundverordnung nicht.[71] Hinsichtlich dieser Datenverarbeitungen legt lediglich die Richtlinie (EU) 2016/680[72] einen Mindeststandard datenschutzrechtlicher Anforderungen fest, die von den Mitgliedstaaten umzusetzen sind.

3.4.2.1 Polizeiliche Videobeobachtung

Gemäß Artikel 2, Abs. 2 lit. d findet die Datenschutz-Grundverordnung keine Anwendung auf Behörden, die personenbezogene Daten »zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit« verarbeiten. Die Videobeobachtung durch Polizeibehörden zu Zwecken der Gefahrenabwehr oder Strafverfolgung richtet sich daher nach nationalen Gesetzen, die allerdings der Richtlinie (EU) 2016/680 genügen müssen.

Bei der Videobeobachtung im öffentlich zugänglichen Raum zu Zwecken der Gefahrenabwehr unterscheiden die Polizeigesetze des Bundes und der Länder zwischen vier Einsatzformen (dazu und zum Folgenden WD 2017a u. 2018b):

- die Videobeobachtung bei öffentlichen Veranstaltungen,
- an gefährdeten Orten,
- in oder im Umfeld von gefährdeten Objekten oder
- durch Bodycams.

71 Für polizeiliche Datenverarbeitungen, die nicht im Zusammenhang mit Aufgaben der Gefahrenabwehr oder Strafverfolgung stehen (z. B. die Verarbeitung personenbezogener Daten im Kontext des Internetauftritts einer Polizeibehörde), gelten allerdings die Regelungen der Datenschutz-Grundverordnung.

72 Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates

Nahezu alle Polizeigesetze der Länder ermächtigen bei Gefährdungslagen zur *offenen Videobeobachtung von öffentlichen Veranstaltungen und Ansammlungen*, wozu etwa Sportveranstaltungen oder Volksfeste zählen. Entsprechende Befugnisse für die Bundespolizei sind auf ihre Aufgabenbereiche bezogen (u. a. Grenzschutz, Bahnpolizei, Luftsicherheit, Schutz der Bundesorgane) und erstrecken sich beispielsweise auf die Videobeobachtung von Ansammlungen an der Bundesgrenze (§ 26 BPolG). Wann eine die Videobeobachtung erlaubende Gefährdungslage vorliegt, wird teilweise unterschiedlich festgelegt. Laut baden-württembergischem Polizeigesetz beispielsweise besteht sie, wenn terroristische Anschläge drohen oder erfahrungsgemäß erhebliche Gefahren für die öffentliche Sicherheit entstehen können (§ 21 Abs. 1 PolG BW[73]). Gemäß dem bayerischen Polizeigesetz müssen Tatsachen die Annahme rechtfertigen, dass Ordnungswidrigkeiten von erheblicher Bedeutung oder Straftaten begangen werden. Hier sind überdies Übersichtsaufnahmen erlaubt, sobald dies wegen der »Größe oder Unübersichtlichkeit der Örtlichkeit erforderlich ist« (Artikel 33 Abs. 1 BayPAG[74]). Die Aufzeichnungen sind in der Regel spätestens zwei Monate nach der Erhebung zu löschen, soweit sie nicht zur Verfolgung von Straftaten oder Gefahrenabwehr weiter benötigt werden. Handelt es sich allerdings um öffentliche Versammlungen im Anwendungsbereich des Versammlungsrechts, gehen die Vorschriften der Versammlungsgesetze des Bundes oder – soweit vorhanden – der Länder dem allgemeinen Polizeirecht vor. Nach bundesrechtlichem Versammlungsgesetz etwa sind Videoaufnahmen von Teilnehmern nur dann zulässig, wenn anzunehmen ist, dass von ihnen erhebliche Gefahren für die öffentliche Sicherheit ausgehen. Zudem sind die Aufzeichnungen nach Beendigung der Versammlung unverzüglich zu löschen, soweit sie nicht zur Verfolgung von Straftaten oder Gefahrenabwehr weiter benötigt werden (§§ 12a, 19a Versammlungsgesetz[75]).

Bis auf das Land Berlin enthalten alle Polizeigesetze der Länder Befugnisse zur *offenen Videobeobachtung an gefährdeten Orten*. Darunter werden zumeist Kriminalitätsschwerpunkte verstanden, also kriminalitätsbelastete öffentlich zugängliche Orte, an denen Tatsachen die Annahme rechtfertigen, dass weitere Straftaten begangen werden.

Ebenfalls fast alle Landespolizeigesetze enthalten Befugnisse zur offenen *Videobeobachtung in oder bei gefährdeten Objekten*. Gemeint sind hier in der Regel Versorgungs- und Verkehrseinrichtungen, öffentliche Verkehrsmittel, Amts-

73 Polizeigesetz Baden-Württemberg in der Fassung vom 13. Januar 1992 (GBl. S. 1, ber. S. 596, 1993 S. 155) zuletzt geändert durch Gesetz vom 28. November 2017 (GBl. S. 631) m.W.v. 8.12.2017

74 Polizeiaufgabengesetz (PAG) in der Fassung der Bekanntmachung vom 14. September 1990 (GVBl. S. 397, BayRS 2012-1-1-I), das zuletzt durch § 1 des Gesetzes vom 18. Mai 2018 (GVBl. S. 301 u. 434) geändert worden ist

75 Versammlungsgesetz in der Fassung der Bekanntmachung vom 15. November 1978 (BGBl. I S. 1789), das zuletzt durch Artikel 2 des Gesetzes vom 8. Dezember 2008 (BGBl. I S. 2366) geändert worden ist

gebäude, Religionsstätten oder Denkmäler. Entsprechend ihren Aufgabenbereichen darf die Bundespolizei die Videobeobachtung zur Gefahrenabwehr an Grenzübergängen oder in bzw. im Umfeld von Bahnhöfen, Flughäfen, Gebäuden der Verfassungsorgane etc. einsetzen (§ 27 BPolG).

Schließlich dürfen Bundespolizisten nach § 27a BPolG sowie Landespolizisten in einigen Bundesländern zum Eigenschutz mobile *Videokameras offen am Körper* (Bodycams) tragen.

Im Gegensatz zum polizeilichen Gefahrenabwehrrecht enthält das Strafverfahrensrecht keine Ermächtigungsgrundlagen zur Beobachtung des öffentlich zugänglichen Raums mit Videokameras. Hier beschränken sich die Befugnisse auf die Herstellung von gezielten Aufnahmen bestimmter Personen (auch ohne deren Wissen) außerhalb von Wohnungen aus Anlass einer Verdachtslage auf eine Straftat von erheblicher Bedeutung (§ 100h StPO). Obschon auch diese Form der polizeilichen Videobeobachtung im öffentlich zugänglichen Raum stattfinden kann, so bezieht sie sich immer auf einzelne Personen, wodurch sie sich von den zuvor genannten gefahrenabwehrrechtlichen Einsatzformen unterscheidet.

Soweit keine bereichsspezifischen Normen anwendbar sind, kommt ggf. ein Einsatz auf Grundlage der Datenschutzgesetze des Bundes bzw. der Länder in Betracht, die auch Vorschriften zur Videobeobachtung im öffentlich zugänglichen Raum durch öffentliche Stellen des Bundes bzw. der Länder enthalten (Kap. 3.4.2.2). Diese Vorschriften finden etwa für die Videobeobachtung zur Ausübung des Hausrechts in Polizeidienststellen Anwendung.

3.4.2.2 Videobeobachtung durch nichtpolizeiliche öffentliche Stellen

Für öffentliche Stellen, die Daten zu anderen Zwecken als zur Gefahrenabwehr und Strafverfolgung verarbeiten (im Folgenden: nichtpolizeiliche öffentliche Stellen), findet die Datenschutz-Grundverordnung Anwendung. Allerdings kann für diese Akteursgruppe in bestimmten Fällen die Öffnungsklausel in Artikel 6 Abs. 1 S. 1 lit. e, Abs. 2, Abs. 3 Datenschutz-Grundverordnung in Betracht kommen, welche die Datenverarbeitung für Aufgaben erlaubt, die im öffentlichen Interesse liegen oder in Ausübung öffentlicher Gewalt erfolgen, sofern hierfür nationale Gesetze als Rechtsgrundlage existieren. Dabei erlaubt die Öffnungsklausel laut Kühling et al. (2016, S. 31 ff.) den Mitgliedstaaten auch, die Aufgaben, die im öffentlichen Interesse liegen, selbst festzulegen. In Deutschland zählen dazu etwa die gesamte Ordnungsverwaltung (z. B. Gewerbe- oder Bauaufsicht), die Leistungsverwaltung (z. B. öffentliche Verkehrsmittel, Bildung, Energie- und Wasserversorgung) oder die Lenkungsverwaltung (z. B. Förderung kultureller Angebote).

In Bezug auf die Videobeobachtung wird die Öffnungsklausel u. a. durch § 4 Abs. 1 Nr. 1 BDSG für öffentliche Stellen des Bundes und durch entsprechende

landesdatenschutzrechtliche Normen für öffentliche Stellen der Länder einschließlich Kommunen ausgefüllt. Die Normen erlauben unter bestimmten Voraussetzungen die offene Videobeobachtung im öffentlich zugänglichen Raum, soweit sie zur Aufgabenerfüllung öffentlicher Stellen erforderlich ist.[76] Dass zu diesen Aufgaben auch der Schutz von Personen oder Objekten im Bereich von öffentlichen Einrichtungen zählt, wird in den Normen oft (z. B. § 14 Abs. 1 NDSG[77], Artikel 24 BayDSG[78]), aber nicht immer explizit erwähnt (z. B. § 4 HDSIG[79]). Auch bezüglich der konkreten Zulässigkeitsvoraussetzungen sind die verschiedenen bundes- bzw. landesrechtlichen Regelungen uneinheitlich ausformuliert, sehen aber zumeist ausdrücklich eine Abwägung mit den schutzwürdigen Interessen der Betroffenen vor (WD 2018b, S. 4). Falls die Videodaten auch gespeichert werden, so sind diese zu löschen, wenn sie zur Erreichung des Zwecks der Videobeobachtung nicht mehr benötigt werden. Für andere Zwecke dürfen sie nur verwendet werden, wenn dies zur Gefahrenabwehr oder Strafverfolgung erforderlich ist.

3.4.2.3 Videobeobachtung durch nichtöffentliche Stellen (private Unternehmen oder Personen)

Bis zum Inkrafttreten der Datenschutz-Grundverordnung wurde die Videobeobachtung im öffentlich zugänglichen Raum durch private Personen oder Unternehmen durch § 6b BDSG (a.F.) geregelt, der im Zuge der Anpassung des nationalen Datenschutzrechts an die Datenschutz-Grundverordnung im Wesentlichen unverändert in § 4 BDSG überführt wurde. Demnach ist private Videobeobachtung im öffentlich zugänglichen Raum nur zulässig, falls sie zur Wahrnehmung des Hausrechts (§ 4 Abs. 1 S. 1 Nr. 2 BDSG) oder berechtigter Interessen (§ 4 Abs. 1 S. 1 Nr. 3 BDSG) erforderlich ist, offen erfolgt und keine schutzwürdigen Interessen der betroffenen Personen überwiegen. Die erhobenen Daten dürfen nur für den festgelegten Zweck verwendet und ggf. gespeichert werden, für einen anderen Zweck nur, soweit dies zur Gefahrenabwehr oder Strafverfolgung erforderlich ist. Schließlich sind ggf. gespeicherte Videodaten unverzüglich zu löschen, sobald sie zur Zweckerreichung nicht mehr erforderlich sind.

Durch den Anwendungsvorrang der Datenschutz-Grundverordnung gibt es laut einem aktuellen Urteil des Bundesverwaltungsgerichts (BVerwG, Urteil vom 27. März 2019, BVerwG 6 C 2.18, Rn. 44 ff.) seit dem 25. Mai 2018 allerdings keinen Raum für eine Anwendung des § 4 Abs. 1 S. 1 BDSG auf die Videobeobachtung durch Private mehr. Denn während die Datenschutz-Grundver-

76 Als erforderlich gilt eine Videobeobachtung dann, wenn das festgelegte Ziel damit erreicht werden kann und dafür auch keine weniger eingriffsintensiven Mittel zur Verfügung stehen (LDI NRW 2016).
77 Niedersächsisches Datenschutzgesetz (NDSG) vom 16. Mai 2018
78 Bayerisches Datenschutzgesetz (BayDSG) vom 15. Mai 2018
79 Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG) vom 3. Mai 2018

ordnung für Aufgaben, die im öffentlichen Interesse liegen, Öffnungsklauseln vorsieht (Kap. 3.4.2.2), gilt dies nicht für die Datenverarbeitung zu privaten Zwecken. Entsprechend ist die Zulässigkeit der privaten Videobeobachtung im öffentlich zugänglichen Raum alleine nach den Regelungen der Datenschutz-Grundverordnung zu beurteilen.

Maßgeblich ist hier zunächst die Generalklausel für die Datenverarbeitung in Artikel 6 Abs. 1 lit. f Datenschutz-Grundverordnung, die aber im Wesentlichen die bereits aus dem BDSG bekannten Zulässigkeitskriterien für die private Videobeobachtung ansetzt (Wahrung berechtigter Interessen, Erforderlichkeit, Interessenabwägung). Auch müssen wie bisher der Umstand der Videobeobachtung gemäß Artikel 12 ff. Datenschutz-Grundverordnung erkennbar gemacht und die Daten nach Artikel 17 Datenschutz-Grundverordnung unverzüglich gelöscht werden, sobald sie nicht mehr notwendig sind (DSK 2018b). Neu hingegen ist die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung für die »systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche« (Artikel 35 Abs. 3 lit. c Datenschutz-Grundverordnung). Von Letzterem abgesehen aber dürfen private Akteure somit auch unter der Datenschutz-Grundverordnung an den in Deutschland eingespielten datenschutzrechtlichen Vorgaben zur Videobeobachtung nach § 4 Abs. 1 S. 1 BDSG (bzw. § 6b Abs. 1 S. 1 BDSG a.F.) im Wesentlichen festhalten (Kühling 2017, S. 1987).

Anders ist dies aber ggf. für die 2017 durch das Videoüberwachungsverbesserungsgesetz[80] in das BDSG aufgenommene Regelung nach § 4 Abs. 1 S. 2 BDSG zu bewerten, nach welcher bei der privaten Videobeobachtung in öffentlich zugänglichen großflächigen Anlagen (z. B. Sportstätten, Einkaufszentren) oder Einrichtungen und Fahrzeugen des öffentlichen Personenverkehrs bei der Abwägungsentscheidung zwischen den Betreiberinteressen und den Rechten Betroffener der Sicherheit und dem Schutz der Bevölkerung ein besonderes Gewicht beizumessen ist. Durch diese gesetzliche Wertung zugunsten eines Einsatzes sollte laut dem Gesetzesentwurf der Bundesregierung (2017f, S. 10) die private Videobeobachtung in hochfrequentierten öffentlichen Räumen in einem höheren Maße als zuvor ermöglicht und so die Sicherheit der Bevölkerung insgesamt erhöht werden.[81] Ob bzw. inwieweit Artikel 6 Abs. 1 lit. f. Datenschutz-Grundverordnung, der die Datenverarbeitung ausdrücklich auch zur Wahrung der Interessen Dritter vorsieht, es nunmehr ermöglicht, eine Berücksichtigung besonderer Bedrohungslagen solcher Einrichtungen in der Abwägungsentscheidung zuzu-

80 Gesetz zur Änderung des Bundesdatenschutzgesetzes – Erhöhung der Sicherheit in öffentlichen zugänglichen großflächigen Anlagen und im öffentlichen Personenverkehr durch optisch-elektronische Einrichtungen vom 28.4.2017 (BGBl. I S. 968)

81 Die Gesetzesänderung war teils starker Kritik ausgesetzt, z. B. durch die Datenschutzbehörden des Bundes und der Länder (DSK 2016): Zum einen wurde eine Verlagerung der Verantwortung für die Sicherheit der Bevölkerung auf private Stellen abgelehnt, zum anderen wurde die Eignung privater Videobeobachtung für Aufgaben der Gefahrenabwehr infrage gestellt, da private Betreiber meistens nicht in der Lage seien, Videobilder in Echtzeit auszuwerten, um bei Gefahren eingreifen zu können.

lassen, bleibt fraglich. Wohl eher dagegen spricht die Maßgabe des Bundesverwaltungsgerichts (BVerwG, Urteil vom 27.3.2019, BVerwG 6 C 2.18, Rn. 46) im zuvor genannten Urteil, nach welcher eine Privatperson sich nicht selbst zum Sachwalter des öffentlichen Interesses erklären kann und insbesondere nicht zum Schutz der öffentlichen Sicherheit neben oder gar anstelle der Behörden berufen ist.

3.4.2.4 Zugriffsmöglichkeiten für Polizei- und Strafverfolgungsbehörden auf Videomaterial aus nichtpolizeilichen Quellen

Der bestehende Rechtsrahmen steht Kooperationen zwischen polizeilichen und nichtpolizeilichen Akteuren der Videobeobachtung nicht im Wege. So erlauben die datenschutzrechtlichen Vorgaben zur Videobeobachtung im öffentlich zugänglichen Raum explizit die Übermittlung von sicherheitsrelevantem Videomaterial an Polizei- oder Strafverfolgungsbehörden, falls dies zum Zwecke der Gefahrenabwehr oder Strafverfolgung erforderlich ist (§ 4 Abs. 3 S. 3 BDSG für öffentliche Stellen des Bundes sowie entsprechende landesdatenschutzrechtliche Normen für öffentliche Stellen der Länder). Die Übermittlung steht auch im Einklang mit der Datenschutz-Grundverordnung, die solche Zweckänderungen durch die Öffnungsklausel in Artikel 6 Abs. 4 Datenschutz-Grundverordnung erlaubt, wenn dies sich als notwendige und verhältnismäßige Maßnahme zum Schutz der öffentlichen Sicherheit und zur Verfolgung von Straftaten erweist (Kühling et al. 2016, S. 346).

Die Kooperation kann – falls erforderlich – durch die gesetzlichen Befugnisse für Polizei- und Strafverfolgungsbehörden zur Erhebung, Sicherstellung bzw. Beschlagnahme auch eingefordert bzw. erzwungen werden. Zum Beispiel dürfen Videoaufnahmen aus privaten Quellen, die als Beweismittel für Ermittlungen von Bedeutung sein könnten, zum Zweck der Strafverfolgung sichergestellt bzw. im Falle der Weigerung auf richterliche Anordnung hin beschlagnahmt werden (§§ 94 ff. StPO). Nach dem Verhältnismäßigkeitsgrundsatz muss sich die Beschlagnahme allerdings auf die Daten beschränken, die für die Verfolgung einer Straftat notwendig sind, und hat in angemessenem Verhältnis zur Schwere der Tat und Stärke des Tatverdachts zu stehen (TLfDI 2016, S. 111 f.). Entsprechende bereichsspezifische Sicherstellungsbefugnisse existieren für die polizeiliche Gefahrenabwehr, etwa für das BKA im Rahmen der Befugnisse zur Abwehr terroristischer Gefahren nach § 60 Abs. 1 Nr. 1 BKAG oder für die Bundespolizei im Rahmen ihrer Aufgabenbereiche (u. a. Grenzschutz, Bahnpolizei, Schutz der Bundesorgane) nach § 47 Nr. 1 BPolG.

3.4.3 Beispiele aus der aktuellen Einsatzpraxis

Über das aktuelle Ausmaß des Einsatzes offener Videobeobachtung im öffentlich zugänglichen Raum in Deutschland sind keine belastbaren Zahlen verfügbar, da es für den Betrieb solcher Anlagen weder für öffentliche noch für nichtöffentliche Stellen eine Meldepflicht gibt. Auch ist eine eindeutige Zuordnung aktueller Einsatzpraktiken nach den aus rechtlicher Perspektive relevanten Akteursgruppen (Polizeibehörden, nichtpolizeiliche öffentliche Stellen, private Akteure) aufgrund vielfältiger Kooperationsformen oft nicht möglich. So bestehen insbesondere zwischen den Betreibern von kritischen Infrastrukturen und der Polizei teilweise Partnerschaften im Bereich der Videobeobachtung, die beispielweise die gemeinsame Nutzung der Videotechnik oder die Übermittlung von Videodaten in Echtzeit an Polizeibehörden beinhalten. Nachfolgend werden aktuelle Einsatzpraktiken der Videobeobachtung im öffentlich zugänglichen Raum exemplarisch entlang einiger für die zivile Sicherheit wichtiger Anwendungsfelder dargestellt – eine vollständige Übersicht kann an dieser Stelle aber nicht geleistet werden.

3.4.3.1 Stationäre polizeiliche Videobeobachtung an gefährdeten Orten

Die offene polizeiliche Videobeobachtung durch stationäre Kameras an Kriminalitätsschwerpunkten hat – gemessen an der Anzahl der eingesetzten Videokameras – nur einen geringen Anteil an der Videobeobachtung im öffentlich zugänglichen Raum. Beispiele aus einigen Bundesländern sind:

- In *Nordrhein-Westfalen* wurden seit Inkrafttreten der rechtlichen Grundlage im Jahr 2003 bis 2016 lediglich Teile der Altstadt von Düsseldorf und Mönchengladbach polizeilich videobeobachtet. Seit 2016 sind einzelne Standorte in Aachen, Essen, Dortmund, Duisburg und Köln hinzugekommen (Glaubitz et al. 2018, S. 3 ff.). Insgesamt handelt es sich um rd. 100 Videokameras (zum Vergleich: Alleine die Kölner Verkehrs-Betriebe AG setzte 2015 rund 2.500 Kameras ein; Kap. 3.4.3.5).
- In *Hessen* setzte die Polizei 2016 zu diesem Zweck insgesamt 143 Videokameras an 20 Standorten in 16 Städten ein (LKA Hessen 2017, S. 3).
- In *Sachsen* wurden laut des Sächsischen Staatsministeriums des Innern (2018, Anlage 1) mit Stand Januar 2018 4 Standorte in Leipzig polizeilich videoüberwacht.
- In *Bayern* wurden im Jahr 2016 ausweislich der Angaben der Bayerischen Staatsregierung (2017) insgesamt 11 Standorte in 7 Städten polizeilich videobeobachtet. Darüber hinaus fand eine temporäre Videobeobachtung mit stationären Anlagen während sieben Großanlässen statt (z. B. während des Oktoberfestes in München oder des ECHELON-Festivals in Bad Aibling).

Einige Einblicke in die konkrete Einsatzpraxis gewährt beispielsweise der Evaluationsbericht zur polizeilichen Videobeobachtung in Nordrhein-Westfalen von Glaubitz et al. (2018, S. 3 ff. u. 26 ff.): Hier werden die Videobilder in Echtzeit in die örtlich zuständige Polizeidienststelle auf Monitore übertragen und durch Beamte der Leitstelle ausgewertet. Zusätzlich werden die Aufnahmen gespeichert. Auswertung und Speicherung finden nicht permanent, sondern abhängig von den lokalräumlichen Bedingungen nur während festgelegten Betriebszeiten statt (z. B. täglich zwischen 10 und 1 Uhr). Bei besonderen Einsatzlagen (z. B. Weihnachtsmarkt) werden die Betriebszeiten teilweise ausgeweitet. Versammlungen, die unter das Versammlungsrecht fallen, werden nur videobeobachtet, sofern dies im Einzelfall durch den Polizeiführer angeordnet wird. Gespeicherte Aufnahmen werden spätestens nach Ablauf der gesetzlich festgestellten Speicherungsfrist automatisiert gelöscht. Eine längerfristige Archivierung zwecks Bekämpfung und Verfolgung von Straftaten erfolgt nur auf Antrag durch die Staatsanwaltschaft oder ein Gericht. Zum Einsatz kommen statische wie auch bewegliche Videokameras mit Zoomfunktion und hoher Bildqualität (so soll etwa ein Autokennzeichen auf eine Entfernung von 300 Metern noch erkennbar sein), wobei die Bildqualität aber laut Aussagen von involvierten Beamten bei Regen, Blaulicht oder Dämmerung stark abnehme. Private Bereiche (z. B. Fenster von angrenzenden Wohnhäusern) werden verpixelt dargestellt. Die Videobeobachter/innen am Monitor konzentrieren sich vorrangig auf die Feststellung von Raub-, Taschendiebstahl-, Betäubungsmittel- und Gewaltdelikten sowie besonderer Deliktformen wie Antanzen. Im Ereignisfall werden Sofortmaßnahmen durch Einsatzkräfte vor Ort eingeleitet. In einigen Dienststellen werden Videobeobachter nicht länger als ein paar Stunden am Bildschirm eingesetzt, anderenorts wird in 8-Stunden-Schichten gearbeitet. Involvierte Beamte bemängelten teilweise, dass zu wenig Personal für eine effiziente Nutzung der polizeilichen Videobeobachtung vorhanden sei. Dabei beschränkte sich der Wunsch nach mehr Personal nicht nur auf die Videobeobachter, sondern auch auf die Einsatzkräfte vor Ort, die mit den Videobeobachter/innen zusammenarbeiten.

3.4.3.2 Temporäre mobile polizeiliche Videobeobachtung

Ein wichtiges Anwendungsfeld der Videobeobachtung bei der Bundespolizei und bei den Landespolizeien bildet der offene temporäre Einsatz von mobilen Videokameras im Kontext von öffentlichen Veranstaltungen oder Versammlungen auf Grundlage der in Kapitel 3.4.2.1 aufgeführten Befugnisse (dazu und zum Folgenden Hempel 2016, S. 102 ff.). Zur Anwendung kommen u. a. Hubschrauber mit zoomfähiger HD-Kameratechnik (Kap. 3.1.3.2), Übertragungswagen, temporäre Kameras auf Hausdächern oder von Polizeibeamten getragene Stabkameras. Je nach Technik und Einsatzweck werden die Videodaten zur Auswertung live an die Einsatzleitung übertragen oder zur Beweissicherung lediglich auf dem Gerät

gespeichert. Über Einsatz und Form der Videobeobachtung entscheidet in der Regel die Einsatzleitung in Abhängigkeit der jeweiligen Lage.

Nachfolgend wird exemplarisch auf die Situation im Land Berlin eingegangen (dazu und zum Folgenden Hempel 2016, S. 102 ff.). Da hier keine gesetzliche Grundlage für die stationäre Videobeobachtung an gefährdeten Orten existiert, hat sich ein eigenständiges Nutzungskonzept anlassbezogener mobiler Videobeobachtung aus der Einsatzpraxis herausgebildet. Die im Rahmen der gesetzlichen Befugnisse getätigten Videoaufzeichnungen werden von Polizeibeamten nach dem Einsatz in Bezug auf mögliche Straftaten hin ausgewertet und in einem zentralen Archiv hinterlegt. Archiviert werden ausschließlich Medien, auf denen sich während eines Einsatzes aufgezeichnete Straftaten befinden. Die Archivierung soll es Sachbearbeiter/innen, aber auch Staats- und Rechtsanwält/innen ermöglichen, Tathandlungen anhand des Materials situationsorientiert nach Ort und Zeit zu analysieren. Zwischen 2010 und 2015 wurden pro Jahr durchschnittlich 610 Medien (Bänder, SD-Karten etc.) mit Einsatzaufnahmen zur beweissicheren Dokumentation archiviert, die jeweils mehrere Straftaten enthalten können. Die meisten Aufzeichnungen entstanden an Samstagen, vor allem aber am 1. Mai, auf der Grundlage des Versammlungsrechts. Hierbei stehen vor allem Straftaten wie Flaschen- oder Steinwürfe im Vordergrund.

3.4.3.3 Polizeilicher Einsatz von Bodycams

Eine spezielle Form der temporären mobilen polizeilichen Videobeobachtung ist der Einsatz von Bodycams (auch als Körperkameras bezeichnet). Dabei handelt es sich um kleine Videokameras, die von Polizeibeamten im Einsatz sichtbar am Körper getragen werden (zumeist an der Schulter). Die Videodaten werden zum Zweck der Strafverfolgung lokal gespeichert, eine Auswertung in Echtzeit findet nicht statt. Primäres Ziel des Einsatzes von Bodycams ist aber eine präventiv abschreckende Wirkung potenzieller Gewalttäter/innen zur Eigensicherung der Polizeibeamten: Durch den offenen Kameraeinsatz soll insbesondere in Einsatzsituationen, in denen mit einem problematischen Verlauf zu rechnen ist, ein deeskalierenden Effekt erzeugt werden, der zur Verminderung von Gewalt- oder Widerstandshandlungen gegen Polizeibeamte beitragen soll (Hempel 2016, S. 104).[82]

Der polizeiliche Nutzen von Bodycams wird seit 2013 in diversen Pilotprojekten durch verschiedene Landespolizeien (z. B. in Hessen, Bayern, Rheinland-Pfalz, Bremen) und auch durch die Bundespolizei erprobt (Ergebnisse der Pilotprojekte werden in Kapitel 3.4.4.1 diskutiert). Mittlerweile verfügen die Polizeien mehrerer Bundesländer und seit 2017 auch die Bundespolizei über gefah-

82 Interessanterweise wird mit dem Einsatz von Bodycams in den USA die umkehrte Zielsetzung verfolgt: Dort steht die Verminderung polizeilicher Gewaltanwendung gegenüber Bürger/innen im Vordergrund, um das Vertrauen der Bevölkerung in die Polizei (wieder) zu stärken (Kersting et al. 2017, S. 3).

renabwehrrechtliche Befugnisse zum Einsatz von Bodycams (§ 27a BPolG).[83] Nach Angaben der Bundesregierung (2019i, S. 2) sollen die Beamten der Bundespolizei bis Ende 2020 mit insgesamt ca. 2.300 Bodycams ausgestattet werden.

Aufgrund uneinheitlicher Regelungen sind unterschiedliche Einsatzpraktiken zu erwarten. So dürfen Bodycams in einigen Bundesländern erst in Gefahrensituationen eingeschaltet werden. In anderen Bundesländern und bei der Bundespolizei darf die Kamera im Bereitschaftsbetrieb kontinuierlich aufzeichnen (Prerecording). Dabei werden die Aufnahmen nach einer festgelegten Zeit (z. B. 30 Sekunden) automatisch überschrieben, es sei denn, der Beamte betätigt den Aufnahmeknopf, wodurch vorangegangene sowie aktuelle Aufnahmen gespeichert werden (WD 2017a, S. 4).

3.4.3.4 Videobeobachtung im öffentlich zugänglichen Raum durch nichtpolizeiliche öffentliche Stellen

Das aktuelle Ausmaß der Videobeobachtung im öffentlich zugänglichen Raum durch öffentliche Stellen, die nicht den Polizei- und Strafverfolgungsbehörden zuzuordnen sind, ist nicht bekannt, da für öffentliche wie auch für private Akteure keine Verpflichtungen zur zentralen oder dezentralen Erfassung von Videobeobachtungsanlagen bestehen.

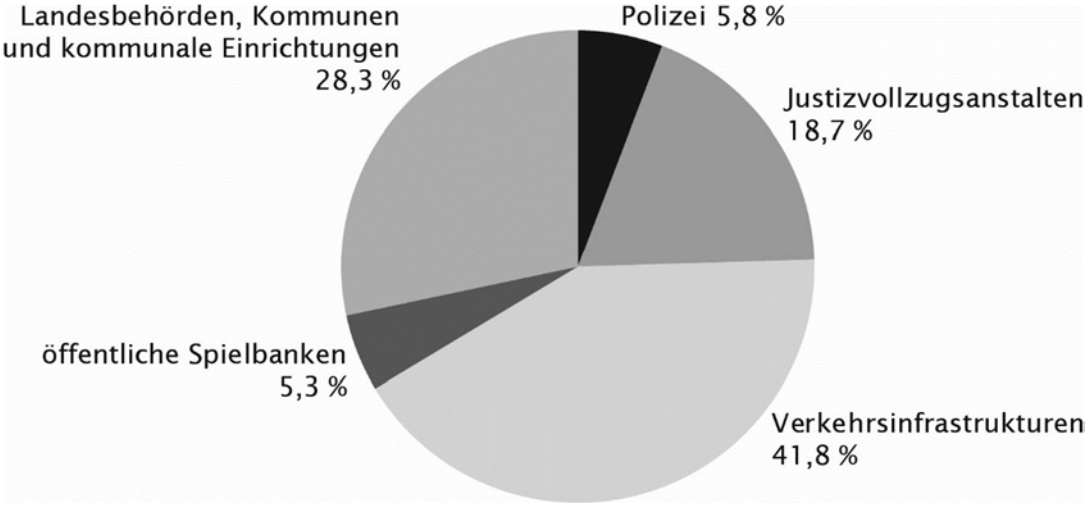
Vereinzelt erlauben Antworten von Landesregierungen auf entsprechende parlamentarische Anfragen einige Aufschlüsse über die Einsatzpraxis. Beispielsweise hat die Bayerische Staatsregierung (2013) unter Beteiligung aller Ressorts und Kommunen das Ausmaß der Videobeobachtung durch öffentliche Stellen in Bayern für die Jahre 2008 bis 2012 erhoben.[84] Demnach wuchs die Zahl der im öffentlich zugänglichen Raum durch öffentliche Stellen installierten Videokameras von 2008 bis 2012 um 50 % auf über 17.000. Die detaillierte Übersicht erlaubt auch einige Rückschlüsse auf die jeweiligen Betreiber und die damit verfolgten Zwecke (Abb. 3.20): Gemessen an der Gesamtzahl der in Bayern durch öffentliche Stellen installierten Kameras hatte die polizeiliche Videobeobachtung mit rd. 6 % einen relativ geringen Anteil, wobei hiervon 80 % der Kameras zum Objektschutz oder zur Ausübung des Hausrechts in Dienststellen und nicht vorrangig zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung eingesetzt wurden. Einschließlich des Kameraeinsatzes in Justizvollzugsanstalten waren Polizei-, Strafverfolgungs- und Strafvollzugsbehörden für rd. ein Viertel der Videobeobachtung durch öffentliche Stellen verantwortlich. Mit einem Anteil von rd. 42 % wurden Videokameras weitaus häufiger im Kontext von Verkehrsinfrastrukturen eingesetzt (Autobahnen, Tunnels, Flughäfen, öffentlicher Perso-

83 Die entsprechenden landesrechtlichen Befugnisse sind in der Ausarbeitung des Wissenschaftlichen Dienstes (2017a, S. 4 f.) aufgelistet.

84 Auf eine Erhebung aktueller Einsatzzahlen anlässlich einer gleichlautenden parlamentarischen Anfrage von 2016 verzichtete die Bayerische Staatsregierung (2017) unter Verweis auf den hohen Aufwand.

nennah- und -fernverkehr), wobei hier allerdings teilweise auch privat betriebene Kameras einbezogen wurden (u. a. 446 Videokameras der Flughafen München GmbH). Typische Einsatzzwecke in diesem Bereich sind Verkehrslenkung, Kontrolle betrieblicher Abläufe, Zugangskontrollen, Objektschutz und nicht zuletzt auch Sicherheitsbelange der hier anwendenden Personen (dazu Kap. 3.4.3.5). In Spielbanken der staatlichen Lotterieverwaltung wurden rd. 900 Videokameras eingesetzt. Schließlich wurden weitere 4.800 Videokameras (rd. 28 %) durch Landesbehörden, Kommunen oder kommunale Einrichtungen in bzw. im Umfeld von öffentlichen Gebäuden oder Anlagen (Ministerien, Rathäuser, Krankenhäuser, Schulen und andere Bildungseinrichtungen, Wertstoffhöfen, Schwimmbädern etc.) oder Kulturgütern (Museen, Denkmäler, Schlösser etc.) betrieben, hauptsächlich zu Zwecken der Zugangskontrolle und des Objektschutzes (Schutz vor Sachbeschädigungen, Diebstahl, Vandalismus).

Abb. 3.20 Videobeobachtung durch öffentliche Stellen in Bayern 2012



Eigene Darstellung auf Basis von Daten der Bayerischen Staatsregierung (2013)

Durch die Bayerische Staatsregierung (2017) wurde außerdem der Bestand an Videokameras erhoben, die 2016 durch nichtpolizeiliche öffentliche Stellen zur Beobachtung von Straßen, Wegen und Plätzen wie Parkanlagen, Marktplätze oder Busbahnhöfe mit der originären Zielrichtung der Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung im Einsatz waren. Eine kommunale Videobeobachtung vorrangig zum Zweck der Gefahrenabwehr fand demnach an insgesamt 48 Standorten in 37 bayerischen Gemeinden bzw. Städten mit rd. 200 Videokameras statt. Gemessen an der Gesamtzahl von rd. 16.000 Kameras, die bereits 2012 durch nichtpolizeiliche öffentliche Stellen in Bayern eingesetzt wurden, lässt dies den Schluss zu, dass die Gefahrenabwehr nur selten der

Einsatzschwerpunkt der Videobeobachtung durch nichtpolizeiliche öffentliche Stellen ist.

3.4.3.5 Videobeobachtung im öffentlichen Verkehr

Ein traditionell wichtiges Anwendungsfeld der Videobeobachtung im öffentlich zugänglichen Bereich ist der öffentliche Personenverkehr mit Bahnen oder Bussen, der in Deutschland durch eine Vielzahl von Verkehrsunternehmen betrieben wird. Die rechtlichen Grundlagen für den Kameraeinsatz sind bei öffentlich-rechtlichen Unternehmen der Länder oder Gemeinden (z. B. Berliner Verkehrsbetriebe AöR, Verkehrsverbund Rhein-Ruhr AöR) die jeweiligen landesdatenschutzrechtlichen Bestimmungen zur Videobeobachtung im öffentlich zugänglichen Raum (Kap. 3.4.2.2) und bei privatrechtlich organisierten Unternehmen (z. B. Münchner Verkehrsgesellschaft mbH, Deutsche Bahn AG) die Regelungen der Datenschutz-Grundverordnung (Kap. 3.4.2.3).

Videobeobachtung im öffentlichen Personennahverkehr (ÖPNV)

Gestützt auf die (bisherigen) datenschutzrechtlichen Grundlagen hat sich die Zahl der Videokameras im ÖPNV in den letzten Jahren stark erhöht. Mittlerweile wurde eine flächendeckende Kameraausstattung in Bahnhöfen oder Fahrzeugen des ÖPNV vielfach bereits erreicht bzw. sind für die nahe Zukunft geplant. Die Berliner Verkehrsbetriebe (BVG) beispielsweise statteten bereits sämtliche U-Bahnhöfe und U-Bahnen, 88 % der Straßenbahnen und 96 % der Busse mit Videobeobachtung aus (Stand Ende 2017). Dafür wurden alleine in Bahnhöfen und Anlagen der U-Bahn über 3.100 Videokameras installiert, wobei aktuell die teilweise noch vorhandene analoge Kameratechnik mit digitaler Videotechnik viel besserer Bildqualität ersetzt wird (BVG 2018, S. 24 f.). Die Gesamtzahl der in Berlin im ÖPNV eingesetzten Kameras wurde 2016 mit 13.643 Stück angegebenen (Der Senat von Berlin 2016, S. 2). Ähnliche Zahlen zum Einsatz der Videobeobachtung im ÖPNV können auch für andere deutsche Städte berichtet werden (Tab. 3.1).

Weitere 28.000 Videokameras nutzt die DB AG (2017) in Zügen des Nah- und S-Bahnverkehrs. Die Videobeobachtung wird von den Verkehrsbetrieben für unterschiedliche Zwecke eingesetzt, angefangen von der Kontrolle betrieblicher Vorgänge (z. B. Fahrgastwechsel) über den Objektschutz bis hin zur Verhinderung und Aufklärung von Straftaten gegen Fahrgäste oder Mitarbeiter.

In Fahrzeugen kommen meist Blackboxlösungen zum Einsatz, bei welchen die Videodaten lediglich lokal aufgezeichnet und – sofern keine sicherheitsrelevanten Vorkommnisse bekannt wurden – nach einem festgelegten Zeitraum (z. B. 48 Stunden) automatisch wieder gelöscht werden. Sie dienen vorrangig der Beweissicherung und damit potenziell der Abschreckung von Täter/innen und der

Aufklärung von Straftaten (Düsseldorfer Kreis 2015, S. 3). Teilweise (beispielsweise in Bussen) können sich die Fahrer die Bilder der im Fahrzeug installierten Kameras auf einem Monitor live anzeigen lassen.

Tab. 3.1 Anzahl Videokameras in Anlagen des ÖPNV (Auswahl)

Verkehrsbetrieb	Anzahl Kameras
ÖPNV Berlin:	
U-Bahnhöfe und U-Bahnanlagen der BVG AöR	ca. 3.100
insgesamt	ca. 13.600
Hamburger Hochbahn AG:	
U-Bahnhöfe und -Bahnen	ca. 2.600
Busse	ca. 3.400
Münchner Verkehrsgesellschaft mbH (MVG):	
U-Bahnhöfe und Betriebsanlagen	ca. 1.750
U-Bahnen, Busse, Trams	ca. 3.850
Kölner Verkehrs-Betriebe AG (KVB):	
Stadtbahnen, Stadtbahnhaltestellen und Busse	ca. 2.500

Quelle: BVG 2018, S. 24; Der Senat von Berlin 2016, S. 2; Hamburger Hochbahnen AG 2018; Stadt Köln 2015; WD 2017d, S. 3

Davon abzugrenzen ist die Videobeobachtung in Echtzeit, bei der die Bilder in eine Leitstelle übertragen werden und von Sicherheitsdisponenten anlassbezogen (z. B. im Falle von Notrufen oder besonderen Lagen) oder anlasslos live betrachtet und ausgewertet werden. Dies ermöglicht im Ereignisfall eine schnelle Vor-Ort-Intervention (Düsseldorfer Kreis 2015, S. 3), etwa durch Lautsprecherdurchsagen oder die Alarmierung von Sicherheits- oder Rettungskräften. Die Videobeobachtung in Echtzeit ist technisch aufwendiger und mit einem hohen Personaleinsatz verbunden, weshalb sie aktuell hauptsächlich in Bahnhöfen zur Anwendung kommt. Beispielsweise setzen die Berliner Verkehrsbetriebe rund um die Uhr drei Videobeobachter für die anlasslose Livebeobachtung des Geschehens in den U-Bahnhöfen ein, wobei allerdings auch sie jeweils nur einen kleinen Ausschnitt des gesamten U-Bahnnetzes gleichzeitig im Auge behalten können (Die rbb Reporter 2018, ab Minute 6:30). Am Beispiel der Berliner Verkehrsbetriebe lässt sich auch die in der Regel enge Zusammenarbeit zwischen Verkehrsunternehmen und Polizeibehörden im Bereich der Videobeobachtung im ÖPNV illustrieren. So können auf Antrag der Berliner Landespolizei die Videoaufnahmen aus den U-Bahnhöfen in Echtzeit in die Einsatzzentrale der Landespolizei übertragen werden, zudem steht der Polizei ein Arbeitsplatz in der Leitstelle der BVG zur Verfügung, der eine dauerhafte Einsichtnahme der Livebilder von derzeit sechs U-Bahnhöfen ermöglicht (BVG 2018, S. 18 u. 22). Außerdem werden

die bei der BVG gespeicherten Videoaufnahmen immer häufiger von den Strafverfolgungsbehörden angefragt (Kap. 3.4.4.2).

Videobeobachtung im öffentlichen Schienenpersonenfernverkehr

Im Fernverkehr setzt die Deutsche Bahn AG die offene Videobeobachtung in wachsendem Umfang an Personenbahnhöfen ein und betreibt mittlerweile rund 7.000 Videokameras an mehr als 1.000 Bahnhöfen[85] (DB AG 2017) (zum Vergleich: 2010 waren es 3.000 Videokameras an 300 Bahnhöfen; Bundesregierung 2010, S. 3 f.). Die Bilder werden in Echtzeit in die 3-S-Zentralen (Service, Sicherheit und Sauberkeit) übertragen und durch Mitarbeiter der DB AG live betrachtet und ausgewertet. Zwecke sind u. a. die Kontrolle von Betriebsabläufen, die Präzisierung von Zugansagen und nicht zuletzt auch Sicherheitsbelange. Der Ausbau und die Modernisierung der teilweise noch analogen Videotechnik an deutschen Bahnhöfen werden gemeinsam von der DB AG und dem Bund finanziert (DB AG 2017).

Die Bundespolizei nutzt im Rahmen ihrer bahnpolizeilichen Aufgaben und Befugnisse zum Einsatz von Videobeobachtung (§ 27 BPolG) die Videotechnik der DB AG. Die Modalitäten der Nutzung (u. a. Zweckbindung, Aufzeichnung der Videodaten, Löschungsfristen, Wartung, Instandhaltung) sind in vertraglichen Vereinbarungen geregelt (Bundespolizeipräsidium 2018, S. 11). Die Videodaten werden an großen Bahnhöfen live in die Einsatzzentralen der Bundespolizei übertragen. Zudem sind die 3-S-Zentralen mit gesonderten Arbeitsplätzen für BOS ausgestattet, die lageabhängig durch Beamte der Bundespolizei besetzt werden. Von hier aus lassen sich auch schwenkbare oder zoomfähige Kameras ansteuern. Schließlich findet in einigen Bahnhöfen auch eine Speicherung der Videoaufnahmen statt, wobei aber nur die Bundespolizei und die Strafverfolgungsbehörden Zugriff auf die Aufzeichnungen haben (Hempel 2016, S. 125). Diese sind spätestens nach 30 Tagen zu löschen, sofern sie nicht mehr zur Gefahrenabwehr oder für die Strafverfolgung benötigt werden (§ 27 BPolG).

3.4.3.6 Videobeobachtung im öffentlich zugänglichen Raum durch private Unternehmen und Personen

Der weitaus größte Teil der Videokameras, die im öffentlich zugänglichen Raum installiert sind, wird durch private Unternehmen oder Personen betrieben. Die Anwendungsformen sind sehr vielfältig sowohl in Bezug auf den Einsatzort (Verkehrsinfrastrukturen, Einkaufszentren, Tankstellen, Banken, Hotels, Parkhäuser, Sport-, Veranstaltungs- oder Vergnügungsstätten etc.) als auch auf den Einsatzzweck (Zugangskontrolle, Schutz von Personen vor Übergriffen, Schutz vor und

85 Dies entspricht bei einer Gesamtzahl an Personenbahnhöfen der Deutschen Bahn AG von ca. 5.700 (Statista 2020) rund jedem sechsten Bahnhof.

Beweissicherung im Falle von Vandalismus, Diebstahl oder Einbruch, Kontrolle betrieblicher oder logistischer Abläufe, Analyse des Kundenverhaltens etc.).

Zum Ausmaß der privaten Videobeobachtung in Deutschland gibt es soweit bekannt keine aktuellen Schätzungen. Ausgehend allerdings von den 300.000 bis 500.000 privaten Videokameras im öffentlich zugänglichen Raum, die bereits vor 20 Jahren im Einsatz gewesen sein sollen (Kap. 3.4.1), dürfte sich deren Zahl heute im Millionenbereich bewegen. In welchem Umfang Polizei- und Strafverfolgungsbehörden im Rahmen ihrer Befugnisse (Kap. 3.4.2.4) auf Videomaterial aus privaten Quellen zu Zwecken der Gefahrenabwehr und Strafverfolgung zurückgreifen, ist nicht bekannt.

3.4.4 Stand der Forschung zur Wirksamkeit der offenen Videobeobachtung im öffentlich zugänglichen Raum

Als Instrument der Kriminalitätsbekämpfung werden mit der offenen Videobeobachtung im öffentlich zugänglichen Raum drei wesentliche Zielsetzungen verfolgt:

- Senkung der Kriminalitätsbelastung durch Prävention;
- Verbesserung der Strafverfolgung durch Beweissicherung;
- Steigerung der subjektiven Sicherheit durch Erhöhung des Sicherheitsgefühls.

3.4.4.1 Kriminalpräventive Wirkung der Videobeobachtung

Die kriminalpräventive Wirkung der offenen Videobeobachtung fußt zum einen auf dem Effekt der Abschreckung: Durch die Aufzeichnung der Videobilder erhöht sich für den/die potenzielle/n Täter/in die subjektive Wahrscheinlichkeit, durch die Strafverfolgungsbehörden ermittelt und für seine/ihre Tat zur Rechenschaft gezogen zu werden. Weil der/die Täter/in nicht wissen kann, ob eine Aufzeichnung tatsächlich auch stattfindet, entfalten demnach selbst Kameraattrappen eine abschreckende Wirkung (Glaubitz et al. 2018, S. 8). Zum anderen besteht, falls die Aufnahmen nicht nur aufgezeichnet, sondern auch in Echtzeit durch Videobeobachter/innen ausgewertet werden, die Möglichkeit, Straftaten durch intervenierendes Handeln ggf. noch verhindern zu können (Glaubitz et al. 2018, S. 8). Die Voraussetzungen hierfür sind allerdings hoch: Nicht nur müssen Videobeobachter/innen frühe Gefährdungsanzeichen richtig erkennen können, auch sind schnelle Interventionszeiten beispielsweise durch Einsatzkräfte vor Ort erforderlich (Hempel 2016, S. 23). Die dafür notwendigen Kompetenzen und Ressourcen sind am ehesten bei Polizeibehörden und ggf. bei professionellen privaten Sicherheitsdienstleistern zu vermuten. So gehen beispielsweise die unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK 2016) davon aus, dass private Betreiber meistens nicht in der Lage sind, Videobilder in Echtzeit so auszuwerten, dass bei Gefahren direkt und schnell eingegriffen werden kann.

Zur kriminalpräventiven Wirkung der Videobeobachtung gibt es mittlerweile eine Vielzahl an Evaluationen, allerdings mit teils widersprüchlichen und oft hinter den Erwartungen liegenden Ergebnissen (dazu und zum Folgenden auch Glaubitz et al. 2018, S. 9 ff.). In einer vielzitierten Metaanalyse haben etwa Welsh und Farrington (2009) insgesamt 41 Evaluationen vorrangig aus Großbritannien ausgewertet. Bezogen auf den Beobachtungsraum bewirkte die Videobeobachtung nur in Parkhäusern einen Kriminalitätsrückgang (Reduktion um 51 % in videobeobachteten Bereichen gegenüber Kontrollbereichen ohne Videobeobachtung). In anderen Räumen (Innenstadtbereich, öffentliche Verkehrsmittel, gemeinnützige Einrichtungen) zeigte die Videobeobachtung dagegen heterogene Effekte und – über alle Evaluationen betrachtet – keine statistisch signifikante kriminalpräventive Wirkung. Da die Evaluationen häufig keine genauen Angaben zu den jeweiligen Einsatzmodalitäten (z. B. polizeiliche oder private Videobeobachtung, Echtzeitauswertung oder lediglich Aufzeichnung) machten, bleibt beispielsweise unklar, inwieweit ein gemessener Kriminalitätsrückgang auf dem Effekt der Abschreckung oder auf der Verhinderung durch Interventionen beruhte. Konträr zu Welsh und Farrington (2009) hat beispielsweise Alexandrie (2017) in einer Metaanalyse mit 7 Evaluationen[86] jüngeren Datums für Parkplatzumgebungen keine kriminalitätssenkende Wirkung der Videobeobachtung festgestellt, dafür aber für öffentliche Straßen und innerstädtische U-Bahnhöfe (Rückgang um 24 bis 28 % im Vergleich zu unbeobachteten Kontrollbereichen). Hinsichtlich der Frage, ob die Videobeobachtung zu einer Verdrängung von Kriminalität in unbeobachtete Räume führt, zeigten die in den beiden Metaanalysen erfassten Evaluationen ebenfalls kein eindeutiges Bild.

Bezogen auf einzelne Deliktarten zeigten beide Metaanalysen dagegen übereinstimmend, dass sich die kriminalitätsreduzierende Wirkung der Videobeobachtung – wenn überhaupt – vorrangig auf Eigentumsdelikte (Sachbeschädigung, Diebstahl, Raub, Einbruch) bezieht, während Gewalt-, Sexual- oder Tötungsdelikte nicht verhindert werden können. Dies scheint insofern plausibel, als dass es sich bei Eigentumsdelikten um geplante Straftaten handelt, bei denen rational handelnde Täter/innen das Entdeckungsrisiko ggf. einkalkulieren und sich infolgedessen durch die Videobeobachtung von ihrem Vorhaben abhalten lassen, während Gewaltdelikte oftmals im Affekt oder unter Alkohol- bzw. Drogeneinfluss begangen werden (Glaubitz et al. 2018, S. 9 ff.). In Bezug auf geplante Straftaten gilt allerdings auch, dass insbesondere professionelle Täter/innen entsprechende Vorkehrungen treffen können (z. B. Maskierung), um trotz Videobeobachtung nicht identifiziert und überführt zu werden (Häcker 2018, S. 2). Beispielsweise lassen Aussagen von Personen aus der Graffitiszene eine abschreckende Wirkung zwar erkennen, allerdings wird diese durch Verhaltensanpassungen auch wieder gemindert (Hempel 2016, S. 182):

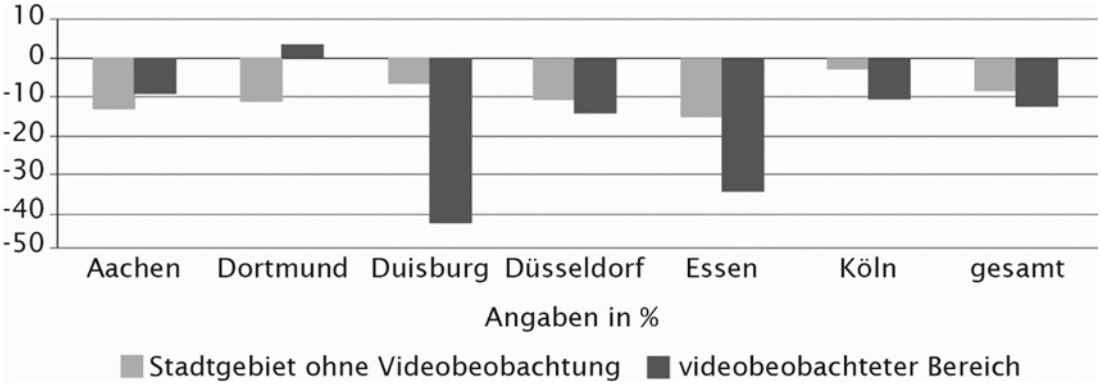
86 Die Evaluationen wurden in den USA, Schweden, Kolumbien und Uruguay durchgeführt.

- »Die Sache ist die, also Kameras, natürlich achtet man schon darauf, dass man vermummt ist, wenn eine Kamera da ist, aber im Endeffekt ist es ja eh so, dass wirklich nicht alles angeguckt wird. … Es ist natürlich schon ein Hindernis, mit den Kameras, zum Beispiel wird in den neuen U-Bahnen kaum gemalt, weil da überall Kameras sind.«
- »Jeder, der sich ein wenig auskennt, weiß, die sitzen vor einem Hauptmonitor, meistens, und haben dann drei, vier Bahnhöfe vielleicht, jeder Bahnhof hat vielleicht zehn, fünfzehn Kameras mit den Ausgängen, das ja immer unterschiedlich, und die wechseln dann immer auf dem Monitor, das heißt, es wird nur … stichprobenartig kontrolliert. Und wenn man weiß, wie man diese Kameras umgehen kann, dann können die auch nichts aufzeichnen.«

Schließlich darf auch die Möglichkeit nicht außer Acht gelassen werden, dass Täter bewusst videobeobachtete Bereiche zur Durchführung ihrer Handlungen auswählen könnten, um eine Öffentlichkeit dafür herzustellen (z. B. terroristische Attentäter/innen).

Die heterogenen und teils ernüchternden Ergebnisse werden auch in einer Evaluation aus Deutschland aus dem Jahr 2018 bestätigt. Das Kriminologische Forschungsinstitut Niedersachsen hat die Wirkung der stationären polizeilichen Videobeobachtung an gefährdeten Orten (Kap. 3.4.3.1) in Nordrhein-Westfalen mit folgenden Ergebnissen evaluiert (Abb. 3.21) (Glaubitz et al. 2018, S. 36 ff.).

Abb. 3.21 Veränderung der Delikthäufigkeit im 1-Jahreszeitraum vor und nach Einführung der Videobeobachtung im Vergleich zum Stadtgebiet ohne Videobeobachtung



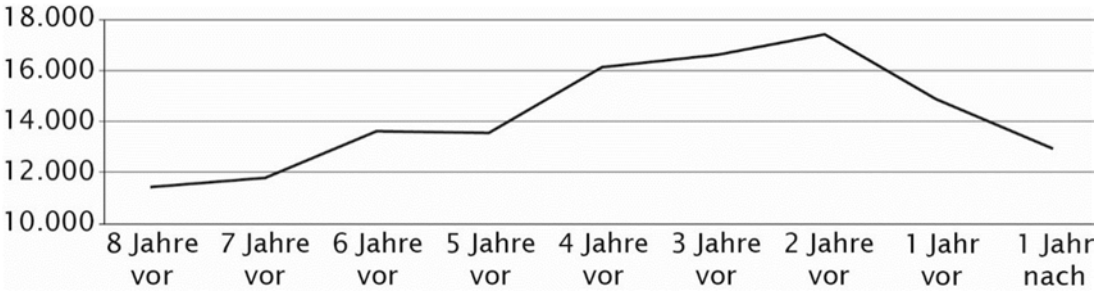
Quelle: Glaubitz et al. 2018, S. 38

Zu einem statistisch signifikanten Rückgang des Kriminalitätsaufkommens im videobeobachteten Bereich im Vergleich zum übrigen Stadtgebiet ohne Videobeobachtung kam es in Duisburg (Rückgang um 38 %) und mit wesentlich geringerer Effektstärke in Essen (Rückgang um 23 %) und in Köln (Rückgang um 8 %). In Aachen fällt der Rückgang der Straßenkriminalität im videobeob-

achteten Bereich dagegen geringer aus als im restlichen, nicht videobeobachteten Stadtgebiet. In Dortmund kam es im beobachteten Gebiet sogar zu einem Anstieg der Deliktzahlen, während im restlichen Stadtgebiet eine Reduktion zu verzeichnen war. In Bezug auf die Deliktbereiche zeigte sich einzig bei Straftaten gegen die sexuelle Selbstbestimmung ein statistisch signifikanter und auch in der Höhe nennenswerter Rückgang in videobeobachteten Gebieten relativ zu unbeobachteten Stadtteilen (Rückgang um 39 %). Demgegenüber fiel der Effekt bei einfachem Diebstahl oder sonstigen Straftaten aus dem Strafgesetzbuch schwach (Reduktion um jeweils 8 %) bzw. bei schwerem Diebstahl, Rohheitsdelikten oder Verstößen gegen das Betäubungsmittelgesetz als statistisch nicht signifikant aus.

Gegen einen kriminalpräventiven Effekt der polizeilichen Videobeobachtung in Nordrhein-Westfalen spricht überdies die Tatsache, dass bei der Analyse der Delikthäufigkeit im zeitlichen Verlauf über alle betrachteten videobeobachteten Bereiche (wie auch im übrigen Stadtgebiet) die Trendwende bereits 2 Jahre vor der Einführung der Videobeobachtung eingesetzt hat. Die Videobeobachtung hat also nicht zu einem Knick in der Verlaufskurve geführt (Abb. 3.22) (Glaubitz et al. 2018, S. 40 f.).

Abb. 3.22 Delikthäufigkeit über alle betrachteten videobeobachteten Bereiche im Zeitverlauf (relativ zur Einführung der Videobeobachtung)



Quelle: Glaubitz et al. 2018, S. 41

Als Ursache für die gemessenen heterogenen kriminalpräventiven Effekte vermuten die Autoren unterschiedliche Implementierungen der polizeilichen Videobeobachtung an den Standorten. Die Videobeobachtung wurde jeweils in ein Maßnahmenbündel integriert, sodass letztlich unklar bleibt, welchen Beitrag die Videobeobachtung selbst neben begleitenden Maßnahmen geleistet hat, die seitens der Polizei im Zusammenhang mit der Einführung der Videobeobachtung ergriffen wurden (Glaubitz et al. 2018, S. 42 f.). Ruch (2017, S. 3) mutmaßt sogar, dass ein ggf. gemessener positiver Effekt weniger auf die Videobeobachtung als vielmehr auf die Tatsache zurückzuführen sei, dass die Einführung der Maßnahme deutlich mache, dass man sich um das betroffene Gebiet kümmere: Dies verstärke den sozialen Zusammenhalt und die informelle soziale Kontrolle, was nachweislich ein kriminalpräventiver Faktor sei.

Dies verweist auf weitere generelle Schwierigkeiten bei der Wirkungsevaluation von Videobeobachtung: Zum einen sind die verwendeten Daten zur Kriminalitätsbelastung (z. B. aus Kriminalitätsstatistiken oder polizeilichen Vorgangsbearbeitungssystemen) oft nicht differenziert genug, um Veränderungen in der Kriminalitätsrate belastbar auf die Einführung von Videobeobachtung zurückführen zu können (Matzner 2016, S. 66). Zum anderen spiegeln polizeiliche Daten nicht das tatsächliche Deliktaufkommen (Dunkelfeld) wider, sondern lediglich die Anzahl der polizeilich registrierten Straftaten (Hellfeld). Im Zuge der Einführung von Videobeobachtung ist daher zu erwarten, dass Straftaten polizeilich registriert werden, von denen die Polizei vorher keine Kenntnis erlangt hatte (Glaubitz et al. 2018, S. 23). Es könnte allerdings auch der Effekt auftreten, dass die Anzahl an festgestellten Delikten sinkt, weil die Polizei es nicht mehr für nötig hält, videobeobachtete Orte durch Polizeistreifen häufig zu kontrollieren. In beiden Fällen würde die Gesamtzahl der tatsächlich begangenen Delikte gleichbleiben, unabhängig davon, ob mehr oder weniger Delikte Eingang in polizeiliche Statistiken finden (IZEW 2017, S. 44).

Kasten 3.3 Spezialfall Bodycams

In Falle von Bodycams (Kap. 3.4.3.3) soll die präventive Wirkung durch eine Deeskalation in polizeilichen Einsatzsituation und in der weiteren Folge durch eine Verminderung von Gewalt- und Widerstandshandlungen gegen Polizeibeamte erzielt werden. Die Wirksamkeit von Bodycams wurde bisher aber noch nicht hinreichend wissenschaftlich belegt.

Durchgeführte Pilotprojekte zum Einsatz von Bodycams deuten auf ein generelles Potenzial von Bodycams zur Deeskalation hin. Dies gilt zumindest in der subjektiven Wahrnehmung der mit Bodycams ausgerüsteten Polizeibeamten. Ein entsprechender Evaluationsbericht der Polizei Bremen (2017) beispielsweise bezieht sich auf Aussagen der betroffenen Polizeibeamten im Anschluss an jeden Einsatz. Demnach führten Bodycams in rund einem Drittel der Einsatzsituationen zu einer wahrnehmbaren, aus der Sicht der Beamten positiven Verhaltensänderung bei den Adressaten der polizeilichen Maßnahmen (teilweise reichte bereits die Ankündigung, die Bodycam einzuschalten). Übereinstimmend wurde aber auch berichtet, dass die deeskalierende Wirkung mit zunehmenden Grad der Beeinflussung der betroffenen Personen durch Alkohol oder Betäubungsmittel nachließ.[87] Ebenso zeigte sich bei gruppendynamischen Prozessen (z. B. bei latent aggressiven Personengruppen) eine nur geringe bzw. keine Wirkung.

87 Im Pilotprojekt wurden Bodycams im Bereich der Bremer Discomeile meist zur Nachtzeit eingesetzt. Daher stand der weit überwiegende Teil der betroffenen Personen unter Alkohol- oder Drogeneinfluss (Polizei Bremen 2017, S. 8).

Ob die subjektiv wahrgenommene deeskalierende Wirkung von Bodycams zumindest in bestimmten Einsatzsituationen auch zur Verminderung der Zahl an Gewalt- oder Widerstandshandlungen gegen Polizeibeamte führt, konnte bislang allerdings noch nicht wissenschaftlich belastbar belegt werden. So gelangte etwa die Metaanalyse von 10 Feldversuchen in sechs verschiedenen Ländern von Ariel et al. (2016) sogar zu dem konträren Ergebnis, nämlich dass Angriffe auf Beamte nicht abnehmen, sondern moderat zunehmen, wenn diese Bodycams tragen. Zu einem ähnlichen Ergebnis führte auch die wissenschaftliche Begleitung des Einsatzes von Bodycams in sechs Polizeiwachen der Polizei Nordrhein-Westfalen im Zeitraum von Mai 2017 bis Januar 2018 durch das Institut für Polizei- und Kriminalwissenschaft der Fachhochschule für öffentliche Verwaltung NRW (Kersting et al. 2019, S. 5 ff.): Hier zeigte sich, dass der Anteil der registrierten geschädigten Polizeibeamten in den Schichten mit Bodycam über dem Anteil in den Schichten ohne Bodycam lag. Zur Erklärung der erwartungswidrigen Befunde ergab sich aus den Daten und den Ergebnissen von quantitativen Befragungen, Gruppendiskussionen und Videoanalysen, dass Bodycams das Verhalten von Polizeibeamten in Richtung eines unangemessen zurückhaltenden Einschreitens und einer formaleren Sprache beeinflussen und dadurch tätliche Angriffe begünstigen. Auch die Akzeptanz seitens der Polizeibeamten ergab ein differenziertes Bild: Bodycams wurden zu jeweils gleichen Anteilen als positiv, neutral bzw. negativ bewertet. Die Studienautoren empfehlen daher, dass in den Dienststellen ein kulturelles Klima der Akzeptanz und Offenheit zu schaffen sei, damit die Einsatzkräfte keine Hemmungen vor der Dokumentation ihrer Verhaltensweisen durch Bodycams haben, sondern sie darin ermutigt, ihr Verhalten ausschließlich an den Erfordernissen des polizeilichen Einsatzes auszurichten.

3.4.4.2 Nutzen der Videobeobachtung für die Strafverfolgung

Die regelmäßig hinter den Erwartungen liegenden Befunde zur kriminalpräventiven Wirkung der offenen Videobeobachtung im öffentlich zugänglichen Raum rücken verstärkt andere Zielsetzungen in den Fokus. So können Videoaufzeichnungen bei der Rekonstruktion eines Tathergangs oder der Überführung eines Tatverdächtigen zweifellos von Nutzen sein und so zur Aufklärung von Straftaten beitragen. Bilder aus Videoaufzeichnungen werden zudem regelmäßig für Öffentlichkeitsfahndungen eingesetzt, um namentlich unbekannte Tatverdächtige mithilfe von Hinweisen aus der Bevölkerung zu identifizieren oder sie dazu zu bewegen, sich selbst der Polizei zu stellen. Bekannte Beispiele hierfür sind der James-Bulger-Fall (Kasten 3.2 in Kap. 3.4.1), die Aufklärung des Anschlags auf den Boston Marathon im Jahr 2013 (Feltes/Ruch 2017, S. 5) oder in Deutschland etwa der Fall des »U-Bahn-Treters« in Berlin, der 2016 in einem U-Bahnhof eine

junge Frau unvermittelt eine Treppe herunter getreten hatte und durch Videoaufzeichnungen ermittelt werden konnte (Welt 2017).

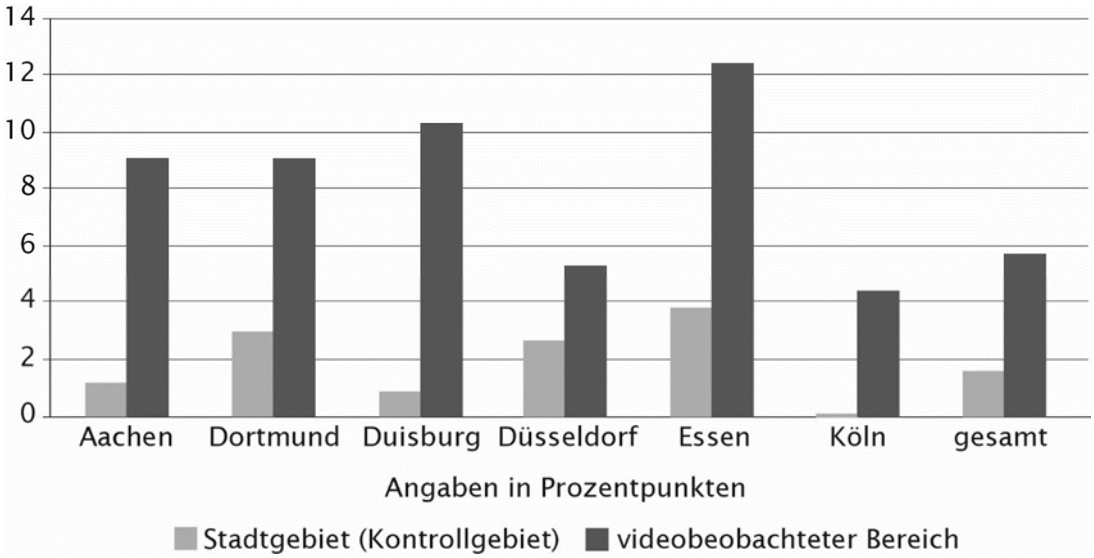
Ob es sich bei solchen – oft medien- bzw. öffentlichkeitswirksamen – Ermittlungserfolgen allerdings um die Regel oder eher um Ausnahmefälle handelt, ist schwierig zu bewerten. Inwieweit Videoaufzeichnungen relevante Hinweise für die Aufklärung einer Straftat liefern können, hängt von vielen Faktoren ab, angefangen von der Qualität der Bilder, der Menge des vorhandenen bzw. ausgewerteten Videomaterials (bezogen auf den Zeitraum vor und nach der Tat und das Gebiet um den Tatort) über die Erfahrungen der auswertenden Ermittlungsbeamten bis hin zu den jeweiligen Einsatzformen und -kontexten der Videobeobachtung vor Ort. So dürfte sich der Nutzen der Videoaufzeichnungen in Abhängigkeit davon, ob etwa Kriminalitätsschwerpunkte, öffentliche Verkehrsinfrastrukturen, Kulturveranstaltungen oder Einkaufszentren beobachtet werden, unterschiedlich darstellen, weil sich Art und Aufkommen von Kriminalität an diesen Orten und damit auch die Aufklärungsquoten ganz wesentlich unterscheiden.

Entsprechend zeigen (vorrangig im angelsächsischen Raum) durchgeführte Studien ein uneinheitliches Bild (dazu und zum Folgenden IZEW 2017, S. 46 f.): Während beispielsweise die Videobeobachtung in San Francisco einen (allerdings begrenzten) Nutzen für die Strafaufklärung zeigte (King et al. 2008, S. 157), hatte sie in Los Angeles überhaupt keinen Effekt auf die Verhaftungsraten (Cameron et al. 2008, S. 4). In Glasgow entwickelte sich die Aufklärungsrate infolge des Einsatzes von Videobeobachtung sogar rückläufig, während die Zahl der registrierten Verbrechen anstieg (Kammerer 2008, S. 74). Eine Studie in den Städten Baltimore, Chicago und Washington von La Vigne et al. (2011, S. 87 f.) kam zu dem Ergebnis, dass Videobeobachtung vor allem dann bei der Aufklärung von Straftaten helfe, wenn hochauflösende Kameras mit in Echtzeit bedienbaren Schwenk- und Zoomfunktionen und speziell dafür geschulte Videobeobachter eingesetzt würden.

Für die Situation in Deutschland deutet im Falle der polizeilichen Videobeobachtung an gefährdeten Orten die Entwicklung der Aufklärungsquoten in den nordrhein-westfälischen Städten, in denen sie eingesetzt wird, auf einen generell positiven quantitativen Effekt hin: So stieg hier im Jahr nach Einführung der Maßnahme die Aufklärungsquote im Vergleich zum Vorjahr in allen videobeobachteten Bereichen um mehrere Prozentpunkte und lag auch deutlich über der Steigerung, die im restlichen Stadtgebiet ohne Videobeobachtung gemessen wurde (Abb. 3.23). In Köln beispielsweise erhöhte sich die Zahl der Fälle, in denen ein Tatverdächtiger ermittelt werden konnte, im videobeobachteten Gebiet von 44,7 auf 49,1 %, während sie im übrigen Stadtgebiet mit ca. 39 % nahezu konstant blieb. Nach einzelnen Deliktarten aufgeschlüsselt lässt sich dieses Ergebnis vor allem auf eine Steigerung der Aufklärungsquote bei Straftaten gegen die sexuelle Selbstbestimmung von 33 % vor auf 66 % nach der Einführung der Videobeobachtung zurückführen, während die Steigerung bei anderen

Deliktarten mit 2 bis 5 Prozentpunkten moderater ausfiel (Glaubitz et al. 2018, S. 48 ff. u. 87). Zu beachten ist hier allerdings, dass die Videobeobachtung an ausgewählten Orten stattfand, an denen generell überdurchschnittlich viele Delikte erwartet wurden. Außerdem kam leistungsfähige Videotechnik zum Einsatz, die durch geschulte Polizeibeamte bedient wurde (Kap. 3.4.3.1), insofern sich dieses Ergebnis auch mit zuvor erwähntem von La Vigne et al. (2011) deckt.

Abb. 3.23 Veränderung der Aufklärungsquote im 1-Jahreszeitraum vor und nach Einführung der Videobeobachtung im Vergleich zum Stadtgebiet ohne Videobeobachtung



Quelle: Glaubitz et al. 2018, S. 49

Ob sich dieser positive Befund daher auch auf andere Formen und Räume der Videobeobachtung und insbesondere auch auf nichtpolizeiliche Anwendungskontexte übertragen lässt, ist ungewiss und kann an dieser Stelle mangels aussagekräftiger wissenschaftlicher Studien nicht beantwortet werden.

Zumindest als Indiz dafür, dass auch nichtpolizeiliche Formen der Videobeobachtung für die Strafaufklärung zunehmende Bedeutung erlangen, kann der Umstand gewertet werden, dass die Zahl der Anfragen von Polizei- und Strafverfolgungsbehörden nach Videoaufzeichnungen aus nichtpolizeilichen oder privaten Quellen stetig zunimmt. Gingen beispielsweise bei den Berliner Verkehrsbetrieben im Jahr 2008 noch rund 2.000 diesbezügliche Anfragen ein, waren es 2016 bereits mehr als 7.600. Dies entspricht einer Steigerung um 380 %, während die Zahl der Straftaten (ohne Taschen- und einfachen Diebstahl) im gleichen Zeitraum um 36 % zurückging (BVG 2017, S. 15 u. 48). Es liegen allerdings keine belastbaren Zahlen vor, in wie vielen Fällen die Videoaufzeichnungen tatsächlich zur Überführung von Straftäter/innen beitragen konnten (Hempel 2016, S. 101).

Insofern besteht hier noch ein großer empirischer Forschungsbedarf, wobei entscheidend ist, dass zur Ermittlung des Nutzens für die Strafverfolgung stets die räumlichen und sozialen Kontexte der Videobeobachtung detailliert zu untersuchen sind (IZEW 2017, S. 47)

3.4.4.3 Erhöhung des Sicherheitsempfindens durch Videobeobachtung

Schließlich ist der Einsatz der Videobeobachtung im öffentlich zugänglichen Raum mit der Erwartung verbunden, dass sich Personen in videobeobachteten Räumen sicherer fühlen als in unbeobachteten Bereichen. Die Steigerung des subjektiven Sicherheitsempfindens durch die offene Videobeobachtung gilt oft als zentrales Argument für ihre Einführung bzw. Ausweitung beispielsweise in Bahnhöfen oder Fahrzeugen des ÖPNV (Hempel 2016, S. 23).

Die Befunde wissenschaftlicher Untersuchungen sprechen allerdings eher dafür, diesen positiven psychologischen Effekt der Videobeobachtung nicht zu überschätzen (dazu und zum Folgenden IZEW 2017, S. 42 f.). In der Studie von Williams und Ahmed (2009) beispielsweise wurden den 120 Teilnehmer/innen sechs Bilder derselben Straßenecke präsentiert. Auf den Bildern waren entweder eine junge Frau, ein männlicher Skinhead oder gar keine Person anwesend und jede dieser drei Szenen wurde einmal mit und einmal ohne eine vor Ort fest installierte Videokamera gezeigt. Die Probanden wurden dann u. a. dazu befragt, wie sie sich fühlten, wenn sie alleine in der jeweiligen Szenerie spazieren gehen würden. Außerdem sollten sie beschreiben, wie sie die abgebildeten Personen wahrnahmen.[88] Ein Ergebnis der Studie war, dass die Probanden sich in der Szene mit dem männlichen Skinhead am unsichersten fühlten und negativer über den Skinhead urteilten als über die junge Frau, dies aber nur, wenn gleichzeitig eine Videokamera auf den Bildern zu sehen war. Die Autoren werteten dies als Beleg dafür, dass negative Stereotype durch Videokameras verstärkt werden. Dies würde der Annahme widersprechen, dass Videokameras in öffentlich zugänglichen Räumen notwendigerweise zu einem erhöhten Sicherheitsgefühl beitragen (Williams/Ahmed 2009, S. 753).

Ditton (2000, S. 702) gelangte nach einer Befragung von über 3.000 Personen in Glasgow zu dem Schluss, dass Videobeobachtung nicht dazu führe, dass sich Menschen sicherer fühlen, die sich zuvor unsicher fühlten, sondern lediglich das Sicherheitsgefühl von Menschen verstärke, die sich ohnehin bereits sicher fühlen.[89] Kudlacek (2015, S. 44 ff.) führte einige Studien aus Deutschland aus den

88 Dazu wurden die Probanden gebeten, einen Tag im Leben der abgebildeten Personen anhand typischer Aktivitäten zu beschreiben. Die Antworten wurden dann bestimmten Verhaltenskategorien (antisoziales Verhalten, Freizeitverhalten, Arbeitskontext oder sonstiges) zugeordnet.

89 So gaben 56 % der Befragten an, sich durch Videobeobachtung sicherer zu fühlen. Von diesen Befragten gaben gleichzeitig die meisten (81 %) an, sich auch ohne Kameras bereits sicher zu fühlen (Ditton 2000).

frühen 2000er Jahren auf, die Belege für eine Erhöhung des subjektiven Sicherheitsgefühls durch Videobeobachtung fanden. Demgegenüber ergab eine Befragung von Rothmann (2010) in Wien, dass es für das subjektive Sicherheitsempfinden von Passant/innen auf videobeobachteten Plätzen keinen Unterschied machte, ob sie von der Beobachtung wussten oder nicht. Bornewasser und Schulz (2008) stellten in einer Untersuchung in Brandenburg zwar ein geringfügig höheres Sicherheitsgefühl bei Passant/innen auf videobeobachteten Plätzen im Vergleich zu solchen auf unbeobachteten Plätzen fest, die Unterschiede waren jedoch nicht signifikant. Signifikant sicherer fühlten sich lediglich die im beobachteten Raum tätigen Gewerbetreibenden (nach Glaubitz et al. 2018, S. 12). Eine Befragung von Hempel et al. (2014) von Fahrgästen des ÖPNV ergab, dass sich in einer mehr oder minder alltäglichen Situation (z. B. abends den Zug verpasst zu haben) gerade einmal 6 %, in bereits angespannten Situationen nur 5 % der Befragten bewusst unter eine Kamera stellten. Kudlacek (2015, S. 92) mutmaßt überdies, dass Videobeobachtung auch mit einem verringerten Sicherheitsgefühl korrelieren könne, da der Kameraeinsatz die Vermutung nahelegt, dass ein Kriminalitätsproblem vorliege, welches die Beobachtung notwendig mache.

Die Frage, ob Videobeobachtung sich positiv auf das Sicherheitsgefühl auswirkt, ist auch Gegenstand regelmäßiger Bevölkerungsumfragen. In Erhebungen wird dies von ungefähr der Hälfte der Befragten bejaht (Tab. 3.2).

Tab. 3.2 Repräsentative Bevölkerungsumfragen zur Videobeobachtung im öffentlichen Raum (Auswahl)

Umfrage	Sicherheitsempfinden	Zustimmungswerte
Sicherheit in der Stadt; bundesweite Umfrage von Forsa (2018)	53 % halten Videoüberwachung für (sehr) wichtig, um sich in der Öffentlichkeit sicher zu fühlen	Videoüberwachung im öffentlichen Raum ist richtig? ja: 87 %, nein: 10 %
Videoüberwachung in Berlin; Forsa-Umfrage im Auftrag der Berliner Zeitung (Thomsen 2018)	41 % fühlen sich an videoüberwachten Orten sicherer, bei 57 % hat die Videoüberwachung keinen Einfluss auf das Sicherheitsgefühl	Videoüberwachung an öffentlichen Plätzen sollte ausgeweitet werden? ja: 75 %, nein: 23 %
Fahrgastbefragung Videoaufzeichnung in Niedersachsen; (Forsa 2016)	ohne Videokameras würden sich 56 % unsicherer fühlen; 44 % würden sich ähnlich sicher bzw. sicherer fühlen	Videoaufzeichnung in Zügen ist richtig? ja: 93 %, nein: 7 %

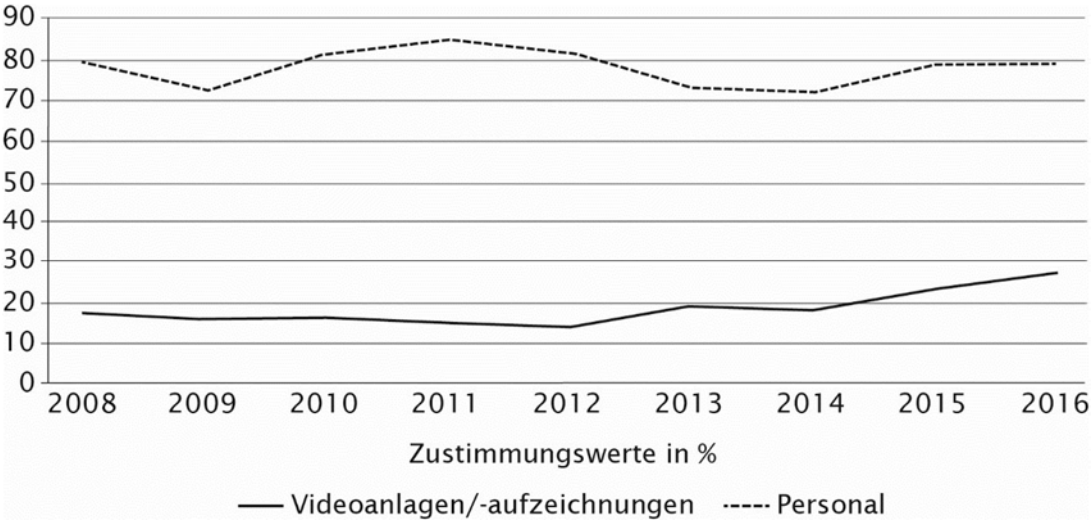
Eigene Zusammenstellung

Allerdings fällt auf, dass die Zustimmungswerte für den Einsatz der Videobeobachtung unter denselben befragten Personen über 30 Prozentpunkte höher

ausfallen. Das heißt im Umkehrschluss, dass ca. zwei von fünf Personen, die den Einsatz der Videobeobachtung prinzipiell befürworten, sich dadurch nicht unbedingt sicherer fühlen. Die vorhandene hohe Akzeptanz für die Videobeobachtung im öffentlich zugänglichen Raum darf demnach nicht ohne Weiteres mit der Annahme gleichgesetzt werden, diese habe positive Auswirkungen auf das Sicherheitsempfinden (Feltes/Ruch 2017, S. 2).

Der gemäß Umfragen vorhandene hohe Einfluss der Videobeobachtung auf das subjektive Sicherheitsgefühl relativiert sich allerdings, wenn die Maßnahme anderen Instrumenten zur Erhöhung des subjektiven Sicherheitsempfindens gegenübergestellt wird. In der bundesweiten Umfrage von Forsa (2018, S. 12) »Sicherheit in der Stadt« beispielsweise sind für die Befragten eine ausreichende Beleuchtung (96 % Zustimmung), ein sauberes und gepflegtes Stadt- und Straßenbild (91 % Zustimmung) oder Polizeibeamte in der Nähe (91 % Zustimmung) deutlich häufiger wichtige Faktoren zur Steigerung ihres Sicherheitsempfindens als die Videobeobachtung (Zustimmung 53 %). Auch im Kontext des ÖPNV messen Fahrgäste laut den jährlich durchgeführten Erhebungen der Berliner Verkehrsbetriebe der Anwesenheit von Personal eine deutlich höhere Bedeutung für ihr Sicherheitsempfinden zu als der Videobeobachtung (Abb. 3.24).

Abb. 3.24 Kundenbefragung der BVG zu Faktoren, die das Sicherheitsgefühl verbessern



Quellen: BVG 2017, S. 25; Hempel 2016, S. 24

Demnach bleibt die Kamera nur ein stummer Beobachter, der in sicherheitsrelevanten Situationen im Gegensatz zu anderen Fahrgästen oder Sicherheitspersonal weder eine wechselseitige Kommunikation erlaubt noch in das Handlungsgeschehen deeskalierend bzw. schützend eingreifen kann (Hempel 2016, S. 24). Falls keine Echtzeitauswertung der Bilder durch Videobeobachter stattfindet und

folglich auch eine schnelle Intervention ausgeschlossen ist, wird mithin eine Sicherheitserwartung erzeugt, die gar nicht eingehalten werden kann. In der Regel ist den Videokameras nicht anzusehen, ob bzw. wie die Bilder ausgewertet werden. Ob in Notsituationen schnelle Hilfe erwartet werden kann, bleibt also ungewiss (Hempel 2016, S. 124).

3.5 Vertiefung: automatisierte Videobeobachtung am Beispiel der Gesichtserkennung

Die unmittelbare Folge der Ausweitung der Videobeobachtung im öffentlich zugänglichen Raum ist eine stetig steigende Masse an Videodaten, deren Bewältigung durch menschliche Beobachter zunehmend an Grenzen stößt. Zwar kann der Aufwuchs an Bildern im Bereich der Strafverfolgung ggf. die Aufklärungsarbeit unterstützen (Kap. 3.4.4.2), gleichzeitig aber bindet die Auswertung des Materials immer mehr personelle und zeitliche Ressourcen, die dann ggf. an anderer Stelle in der Ermittlungsarbeit fehlen. Auch die Videobeobachtung in Echtzeit zu Zwecken der Gefahrenabwehr ist sinnvoll nur mit einem hohen Personaleinsatz realisierbar, da ein Videobeobachter gleichzeitig nur eine beschränkte Anzahl an Monitoren überblicken kann und nur über eine begrenzte Konzentrationsfähigkeit verfügt. So geht etwa das Bundespolizeipräsidium (2018, S. 36) davon aus, dass der Mehrwert der Videobeobachtung infolge der sinkenden Aufmerksamkeit des Videobeobachters bereits nach 20 Minuten in signifikanter Weise beeinträchtigt wird. Sicherheitsakteure treten daher nicht nur für eine Ausweitung, sondern auch für eine Automatisierung der Videobeobachtung ein, indem zur Entlastung des menschlichen Beobachters bestimmte Aufgaben der Bildanalyse und -interpretation auf die Beobachtungstechnologie übertragen werden.

Einfache Formen der Videobeobachtung mit automatisierter Datenauswertung (im Folgenden: automatisierte Videobeobachtung) haben bereits anwendungsreife erreicht (Kap. 3.3): Verfahren der Bewegungserkennung beispielsweise können den Videobeobachter unterstützen, indem Ereignisse, die sich durch einfache Regeln charakterisieren lassen (Person betritt gesperrten Bereich, zu viele Personen in einem festgelegten Bereich, liegengebliebener Gegenstand etc.) erkannt und Alarm ausgelöst wird. Fortschritte wurden in den letzten Jahren auch im Bereich der Detektion und Identifikation von Gesichtern erzielt. Dagegen befinden sich Verfahren zur Analyse komplexer Situationen oft noch in einer frühen Forschungsphase, allerdings handelt es sich hierbei derzeit um ein sehr dynamisches Forschungsfeld.

In der polizeilichen Praxis beschränkt sich der Einsatz von automatisierter Videobeobachtung derzeit noch auf einige wenige Anwendungsfelder, beispielsweise auf den automatisierten Kfz-Kennzeichenabgleich (Kap. 3.3.3) oder den Einsatz von Gesichtserkennungssystemen als Hilfsmittel zur retrospektiven Auswertung von Foto- oder Videomaterial im Bereich der Strafverfolgung. Ein

Einsatz zur automatisierten Personenidentifikation oder Erkennung von potenziellen Gefahrensituationen *in Echtzeit* findet – soweit bekannt – im polizeilichen Realbetrieb bislang noch nicht statt. So handelt es sich beispielsweise bei der von der Bundespolizei mitgenutzten Videotechnik der DB AG an deutschen Bahnhöfen (Kap. 3.4.3.5) ausschließlich um konventionelle Videobeobachtung (Bundesregierung 2018a, S. 2). Gleichwohl ist seitens der Behörden das Interesse erkennbar, künftig in stärkerem Maße Formen der automatisierten Videobeobachtung für polizeiliche Zwecke einzusetzen. Kennzeichnend hierfür sind entsprechende Forschungs- und Entwicklungsprojekte im Rahmen der nationalen[90] und EU-weiten[91] Forschungsförderung, aber auch erste Pilotprojekte zur Erprobung solcher Lösungen in der polizeilichen Praxis. Aktuelle Beispiele sind das seit August 2017 laufende Pilotprojekt »Sicherheitsbahnhof Berlin Südkreuz«, das durch das Bundesministerium des Innern, für Bau und Heimat (BMI), die Bundespolizei, das Bundeskriminalamt und die Deutsche Bahn AG durchgeführt wird, oder das Ende 2018 begonnene Pilotprojekt des Polizeipräsidiums Mannheim, in dem der Nutzen solcher Systeme für die Bekämpfung von Straßenkriminalität getestet wird (Kap. 3.3.4).

Leistungsfähige Verfahren der automatisierten Bildauswertung können aber weit mehr als nur unterstützende Instrumente für den menschlichen Beobachter sein. Durch die Automatisierung verändert sich auch der Charakter der (konventionellen) Videobeobachtung grundlegend (Kees 2015, S. 3). Dies kann vielfältige Auswirkungen sowohl auf die beobachteten Personen als auch auf die Anwender/innen der Beobachtungstechnologien selbst haben. Auf die gesellschaftlichen Folgen von automatisierten Beobachtungstechnologien wird in Kapitel 7 eingegangen. Zunächst aber sollen im Folgenden die Technologie und der mögliche Nutzen einer automatisierten Videobeobachtung für polizeiliche Einsatzzwecke am Beispiel der automatisierten Gesichtserkennung vertieft diskutiert werden.

90 Beispielsweise die Projekte »Automatisierte Detektion interventionsbedürftiger Situationen durch Klassifizierung visueller Muster« (ADIS; Laufzeit 2010 bis 2013) oder »Analyse von Personenbewegungen an Flughäfen mittels zeitlich rückwärts- und vorwärtsgerichteter Videodatenströme« (APFel; Laufzeit 2010 bis 2014) im Rahmen der Sicherheitsforschung des Bundes (https://sifo.bmbfcluster.de/files/Mustererkennung_D_ADIS.pdf, https://sifo.bmbfcluster.de/files/Projektumriss_APFel.pdf, 31.3.2022).

91 Beispielsweise die Projekte »Intelligent information system supporting observation, searching and detection for security of citizens in urban environment« (INDECT; Laufzeit 2009 bis 2014) oder »Smart video-surveillance system to detect and prevent local crimes in urban areas« (SMARTPREVENT; Laufzeit 2014 bis 2016) im Rahmen des 7. EU-Forschungsrahmenprogramms.

3.5.1 Anwendungsfelder der automatisierten Gesichtserkennung

Bei einem Gesichtserkennungssystem (GES) lassen sich grundsätzlich zwei Betriebsarten unterscheiden (TAB 2002, 19 f.):

- *Verifikation*: Bestätigung der behaupteten Identität einer Person. Das Gesichtsbild der Person wird mit dem Gesichtsbild derjenigen Person abgeglichen, die sie zu sein behauptet;
- *Identifikation*: Erkennung einer Person aus einer Menge registrierter Personen. Das Gesichtsbild der Person wird mit allen in einer Datenbank hinterlegten Gesichtsbildern der registrieren Personen auf Übereinstimmung geprüft.

Typisches Einsatzgebiet von Verifikationsverfahren sind biometrische Zugangskontrollsysteme. Dazu hinterlegen alle zutrittsberechtigten Personen ein Gesichtsbild in der Datenbank des GES. Biometrische Zugangskontrollsysteme werden vorrangig im privaten bzw. unternehmerischen Umfeld eingesetzt. Die Bundespolizei nutzt Verifikationsverfahren im Rahmen der teilautomatisierten Grenzkontrolle (EasyPASS, Kap. 3.5.4.1).

Für polizeiliche Aufgaben von Interesse sind aber vor allem Identifikationsverfahren. Es kann grob zwischen folgenden Einsatzfeldern unterschieden werden (Hornung/Schindler 2017, S. 206 f.):

Retrospektive Sichtung von Foto- oder Videomaterial

Gesichtserkennungssysteme können als Hilfsmittel für die retrospektive Auswertung von gespeichertem Foto- oder Videomaterial verwendet werden. In der einfachsten Variante lassen sich solche Systeme zum schnellen Auffinden von Personen anhand ihrer Gesichter in Foto- oder Videomaterial einsetzen. Dies reduziert den zeitlichen und personellen Aufwand für die Auswertung großer Datenbestände, da Material, auf dem keine Personen (bzw. Gesichter) erkennbar sind, aussortiert werden kann.

Weitere Funktionen stehen zur Verfügung, wenn das GES alle auf dem Material gefundenen Gesichter für einen späteren Gesichtsabgleich erfasst und in eine Referenzdatenbank aufnimmt (die Vorgehensweise wird im nächsten Kapitel erörtert). Wurde beispielsweise eine Person während der Begehung einer Straftat gefilmt, kann sich der Betrachter alle Sequenzen im vorhandenen Videomaterial anzeigen lassen, in denen dieselbe Person ebenfalls auftaucht. So kann der Tathergang aus unterschiedlichen Blickwinkeln betrachtet oder das Verhalten der Person in der Vor- und Nachtatphase ermittelt werden, außerdem können der Person ggf. noch weitere, bislang unbekannte Straftaten zugeordnet, aber auch sie entlastende Informationen gewonnen werden (HmbBfDI 2018, S. 6 f.).

Retrospektive Identitätsfeststellung und Rückwärtssuche

Ist auf den auszuwertenden Aufnahmen das Gesicht eines unbekannten Tatverdächtigen zu erkennen, so kann er möglicherweise namentlich identifiziert werden, indem sein Gesichtsbild mit polizeilichen Lichtbilddatenbanken abgeglichen wird (retrospektive Identitätsfeststellung). Eine Variante davon ist die Rückwärtssuche, bei der das vorhandene Material gezielt nach bestimmten Personen durchsucht wird, für die Gesichtsbilder z. B. aus einer polizeilichen Datenbank vorliegen. Im Unterschied zur bloßen Sichtung findet hier eine Verknüpfung mit Informationen aus anderen, mit dem auszuwertenden Material nicht im Zusammenhang stehenden Quellen statt.

Personenfahndung in Echtzeit

Hierzu wird ein Videobeobachtungssystem über ein GES mit einer Fahndungsdatenbank verknüpft. Die Gesichter aller videobeobachteten Personen werden kontinuierlich in Echtzeit mit den in einer Datenbank hinterlegten Gesichtsbildern abgeglichen. Im Falle einer Übereinstimmung alarmiert das System die verantwortlichen Stellen, wo über weitere Maßnahmen entscheiden wird.

3.5.2 Verfahren und Leistungsfähigkeit aktueller Gesichtserkennungssysteme

3.5.2.1 Allgemeine Vorgehensweise

Voraussetzung ist zunächst ein Algorithmus, der menschliche Gesichter auf Fotos oder in Videosequenzen auffinden kann (Gesichtsdetektion). Die eigentliche Gesichtserkennung läuft sodann in drei Teilschritten ab (BSI o.J.):

- *Template erzeugen*: Um den Vergleich zweier Gesichtsbilder möglichst schnell durchzuführen, wird für jedes Gesichtsbild ein biometrischer Datensatz aus charakteristischen Gesichtsmerkmalen angefertigt.
- *Referenzdatenbank erstellen*: Für alle Personen, die vom GES erkannt werden sollen, wird aus einem oder mehreren Gesichtsbildern ein Referenztemplate erzeugt und zusammen mit der Identität der jeweiligen Person in einer Datenbank gespeichert.
- *Gesichtsvergleich*: Für die unbekannte Person wird aus einem Gesichtsbild mit derselben Berechnungsmethode ein Testtemplate erstellt. Das Testtemplate wird dann mit einem (Verifikation) bzw. mit allen (Identifikation) in der Datenbank vorhandenen Referenztemplates auf Übereinstimmung geprüft.

In den letzten 20 Jahren wurde eine Vielzahl von Algorithmen sowohl für die Gesichtsdetektion als auch für die Gesichtserkennung entwickelt. Ältere Verfahren beruhen auf klassischen Bildanalyseverfahren, um in Bildern von Gesichtern markante Stellen (Mitte der Pupillen, Nasenspitze, Kinnspitze, Haaransatz etc.) zu finden und aus den relativen Abständen, Flächen und Winkeln zwischen diesen Stellen ein Template zu berechnen. Schwierigkeiten bereiten hier insbesondere Bilder, auf denen Gesichter nur im Profil zu sehen sind. Neuere Ansätze basieren auf Modellen aus dem maschinellen Lernen, die mit Millionen von Gesichtsbildern trainiert wurden. Der große Vorteil ist, dass die Modelle durch geschickte Wahl der Trainingsbilder auch lernen, Gesichter in unterschiedlichen Posen zuverlässig in Foto- oder Videodaten aufzufinden bzw. miteinander zu vergleichen (z. B. Schroff et al. 2015).

3.5.2.2 Leistungskennzahlen aktueller Gesichtserkennungssysteme

Idealerweise wäre ein biometrischer Datensatz einzigartig für ein menschliches Individuum, sodass Test- und Referenztemplate stets übereinstimmen würden. In der Praxis ist dies aus unterschiedlichen Gründen nicht möglich (TAB 2002, S. 21 f.):

- Der Messvorgang (hier: Foto- bzw. Videoaufnahme) und die Erzeugung von Templates aus biometrischen Merkmalen bedeuten immer eine starke Informationsreduktion. Dies mindert die Genauigkeit des Systems.
- Biometrische Merkmale können sich durch Alterungsprozesse, Krankheiten oder Verletzungen verändern. Bei der Gesichtserkennung tritt hinzu, dass Menschen ihr Aussehen durch Haarwuchs oder das Tragen von Brillen, Kopfbedeckungen, Kosmetik etc. häufig verändern.
- Weitere Schwierigkeiten bereiten störende Umwelteinwirkungen während der Messung, beispielsweise unterschiedliche Lichtverhältnisse.

Als Ergebnis liefert ein GES daher einen Wert für den Grad der Übereinstimmung zwischen dem Test- und einem bzw. allen Referenztemplates in der Datenbank (z. B. 95 %). Dem System ist folglich ein Schwellenwert vorzugeben, ab welchem die Identifikation einer Person als erfolgreich betrachtet wird. Die Wahl dieses Schwellenwerts hat einen großen Einfluss auf die Erkennungsleistung eines GES, wobei generell zwischen zwei Arten von Fehlern zu unterscheiden ist (NIST 2014, S. 16 f.):

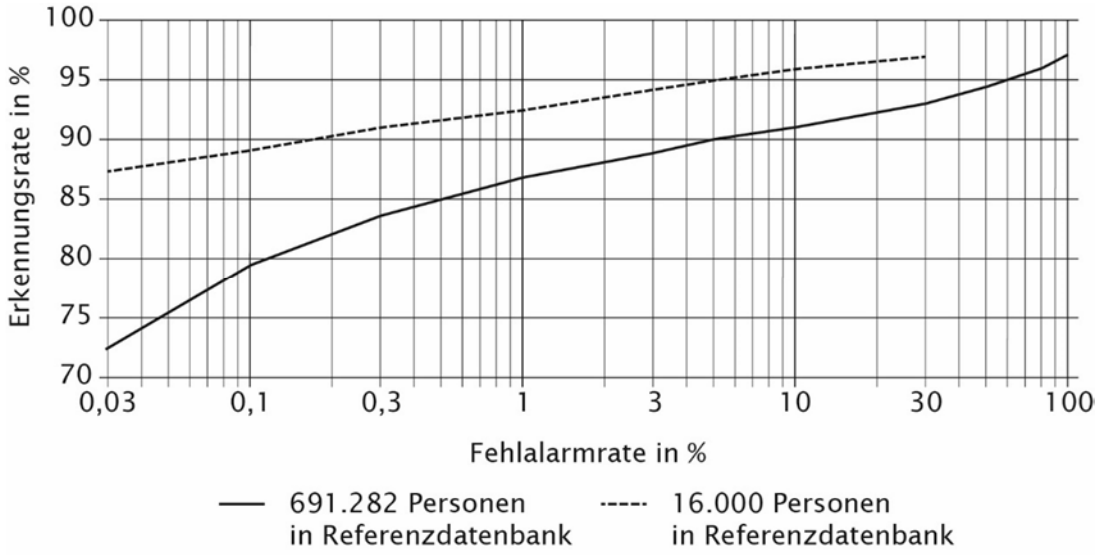
- *Erkennungsfehler (Falsch-negativ-Identifikation)*: Für eine Person, die in der Datenbank vorhanden ist, liefert das System einen Übereinstimmungswert zwischen Test- und Referenztemplate unterhalb des Schwellenwerts. Die Person wird vom System *nicht* erkannt.
- *Fehlalarm (Falsch-positiv-Identifikation)*: Für eine Person, die nicht in der Datenbank vorhanden ist, liefert das System einen Übereinstimmungswert

zwischen Test- und einem Referenztemplate in der Datenbank, der über dem Schwellenwert liegt. Die Person wird vom System *fälschlicherweise* erkannt.

Mit einem niedrig eingestellten Schwellenwert lässt sich die Zahl der Erkennungsfehler reduzieren (und somit die Zahl der richtigen Erkennungen steigern), gleichzeitig aber erhöht dies die Zahl der Fehlalarme. Umgekehrt lassen sich häufige Fehlalarme durch einen hohen Schwellenwert vermeiden, allerdings reduziert sich dadurch auch die Zahl der richtigen Erkennungen.

Dieser Zusammenhang veranschaulicht Abbildung 3.25 anhand der Erkennungsrate (Anzahl richtige Erkennungen im Verhältnis zur Anzahl der Suchläufe mit Personen in der Datenbank) und der Fehlalarmrate (Anzahl der Fehlalarme im Verhältnis zur Anzahl der Suchläufe mit Personen, die nicht in der Datenbank erfasst sind).

Abb. 3.25 Leistung aktueller Gesichtserkennungssysteme



Man beachte die logarithmische Skala bei der Fehlalarmrate.

Quelle: angepasst nach NIST 2017b, S. 15

Dargestellt sind die Leistungskennzahlen für den Algorithmus, der im Testbericht des US-amerikanischen National Institute of Standards and Technology (NIST 2017b) von 2017 am besten abgeschnitten hat.[92] Demnach werden bei einer Fehlalarmrate von 10 % über 90 % der Personen in der Datenbank richtig identifiziert, während für niedrigere Fehlalarmraten die Erkennungsleistung rasch abfällt (auf rd. 72 % bei einer Fehlalarmrate von 0,03 %). Diese Werte erreichte der

92 Das NIST führt in regelmäßigen Zeitabständen standardisierte Leistungstests aktueller Gesichtserkennungssysteme aus Forschungseinrichtungen oder von kommerziellen Anbietern durch.

Algorithmus für eine Referenzdatenbank mit rund 700.000 Personen (Abb. 3.25, durchgezogene Linie). Bei weniger umfangreichen Referenzdatenbanken erhöht sich die Erkennungsleistung deutlich, da sich dadurch die Aufgabe für den Algorithmus vereinfacht (Abb. 3.25, gestrichelte Linie).

Welches Verhältnis zwischen Erkennungs- und Fehlalarmrate für ein GES durch die Wahl des Schwellenwertes idealerweise eingestellt wird, hängt von der konkreten Anwendung ab. Bei der retrospektiven Auswertung von Foto- oder Videomaterial zur Identifizierung einer mutmaßlich straffälligen Person ist eine hohe Erkennungsrate wichtiger als eine geringe Zahl an falschen Zuordnungen, die – mit beträchtlichem Arbeits- und Zeitaufwand zwar – durch den menschlichen Betrachter aussortiert werden können. Soll hingegen Videobeobachtung in Verbindung mit einem GES zur Personenfahndung in Echtzeit an einem stark frequentierten öffentlich zugänglichen Raum eingesetzt werden, so ist eine sehr niedrige Zahl an Fehlalarmen ausschlaggebend für eine handhabbare Anwendung des Systems, da anderenfalls der Aufwand für die Validierung der Treffer beträchtlich wäre.

3.5.3 Anwendungsbeispiel: Personenfahndung in Echtzeit

Die im Testbericht des NIST (2017b) gemessenen Leistungskennzahlen für den besten Algorithmus (Kap. 3.5.2.2) können als Ausgangspunkt für eine grobe Wirkungsabschätzung der automatisierten Videobeobachtung zur Personenfahndung in Echtzeit herangezogen werden. Dies soll anhand von zwei prinzipiell denkbaren Einsatzszenarien geschehen, wobei aber zu betonen ist, dass die Abschätzungen in beiden Fällen auf hypothetischen und stark vereinfachten Annahmen beruhen.

3.5.3.1 Anwendungsszenario I: Fahndung nach Personen, die zur Festnahme ausgeschrieben sind

Das Videobeobachtungssystem eines Bahnhofs mit täglich 100.000 Passant/innen wird durch ein GES mit dem elektronischen Informationssystem der Polizei (INPOL-Z) verknüpft. Die Gesamtzahl der hier verzeichneten Fahndungsnotierungen mit dem Zweck der Festnahme beläuft sich aktuell auf rund 175.000 (Stand März 2018; Bundesregierung 2018h, S. 3). Folgende Annahmen werden getroffen:

- Die Hälfte der Fahndungsnotierungen enthält Lichtbilder in ausreichender Qualität, um sie als Referenzbilder in die Datenbank des GES aufzunehmen (insgesamt 87.500 gesuchte Personen in der Referenzdatenbank);
- Von diesen gesuchten Personen hält sich die Hälfte aktuell in Deutschland auf (insgesamt 43.750 Personen);

- Das Verhältnis zwischen diesen gesuchten Personen und unbeteiligten Bürger/innen ist unter den Bahnhofspassanten gleich wie in der Gesamtbevölkerung (43.750:82,5 Mio.).
- Im Videostrom des Videobeobachtungssystems sind Gesichtsbilder aller Bahnhofspassanten in ausreichender Qualität für einen Gesichtsabgleich durch das GES enthalten. Für alle Bahnhofspassanten wird ein Gesichtsabgleich durchgeführt.

Unter diesen Annahmen befinden sich unter den Bahnhofspassanten 53 gesuchte und in der Referenzdatenbank des GES aufgenommene Personen sowie 99.947 unbeteiligte Bürger/innen. Bei einer Erkennungsrate von ca. 90 % und einer Fehlalarmrate von 10 % (Leistungskennzahlen nach Abb. 3.25 für eher umfangreiche Referenzdatenbanken) könnte das System die meisten der hier anwesenden gesuchten Personen (insgesamt 50) korrekt identifizieren, gleichzeitig würden täglich ca. 10.000 Fehlalarme (rd. 400 pro Stunde) auftreten. Soll die Zahl der Fehlalarme auf einen noch handhabbaren Wert von ca. 30 pro Tag reduziert werden (entspricht einer Fehlalarmrate von 0,03 %), würden bei einer Erkennungsrate von ca. 72 % noch täglich ca. 38 gesuchte Personen vom System korrekt erkannt werden.

3.5.3.2 Anwendungsszenario II: Fahndung nach Tatverdächtigen während polizeilichen Sonderlagen

Als Maßnahme der Fahndungsunterstützung im Falle von islamistischen Terroranschlägen wird die Videobeobachtung der fünf größten deutschen Bahnhöfe (insgesamt täglich rd. 2 Mio. Besucher)[93] mit Gesichtserkennungssystemen ausgerüstet. Die Referenzdatenbanken bestehen aus Gesichtsbildern von Personen, die als islamistische Gefährder oder Relevante Personen eingestuft wurden.[94] Laut Bundesregierung (2018i, S. 3) gibt es derzeit (Stand November 2018) 654 Gefährder und Relevante Personen, die sich in Deutschland aufhalten und nicht in Haft sind. Es soll angenommen werden, dass für diese Personen Gesichtsbilder in ausreichender Qualität vorhanden sind.

Unmittelbar vor einem bevorstehenden bzw. nach einem erfolgten terroristischen Anschlag werden die Gesichtserkennungssysteme hochgefahren und – um die Wahrscheinlichkeit für einen Fahndungserfolg zu erhöhen – mit einer hohen Erkennungsrate von mindestens 90 % betrieben. In diesem Fall würde eine Fehlalarmrate von ca. 0,15 % (Leistungskennzahlen nach Abb. 3.25 für eher kleine Referenzdatenbanken) zu täglich rund 3.000 falschen Treffermeldungen führen (durchschnittlich 25 Fehlalarme pro Bahnhof und Stunde).

93 Dabei handelt es sich um die Hauptbahnhöfe Hamburg, Frankfurt am Main, München, Köln und Berlin (Statista 2018).

94 Ein Gefährder ist eine Person, zu der bestimmte Tatsachen die Annahme rechtfertigen, dass sie politisch motivierte Straftaten begehen wird. Als relevant gilt eine Person, die entsprechende Aktivitäten unterstützt oder sich daran beteiligt (BKA o. J.a).

3.5.3.3 Technische und praktische Herausforderungen im Realbetrieb

Die Messung der in Abbildung 3.25 dargestellten Leistungskennzahlen erfolgte unter Laborbedingungen: Als Referenzbilder dienten qualitativ hochwertige Gesichtsbilder (ein Bild pro Person). Die Testbilder wurden aus Videoaufnahmen (hier: von einer Flughafenhalle) extrahiert. Die so präparierten Bilder zeigten Gesichter von Personen, die entweder in der Referenzdatenbank vorkamen (Messung der Erkennungsrate) oder nicht (Messung der Fehlalarmrate).

Unter realen Einsatzbedingungen gehört es dagegen zur Aufgabe des GES, Gesichter in Videoströmen zu detektieren und für einen Vergleich geeignete Bildausschnitte zu extrahieren. Die Schwierigkeit dieser Aufgabe steigt mit abnehmender Qualität der Videoaufnahmen (in Bezug auf Auflösung, Schärfe, Ausleuchtung, Kompression etc.), mit zunehmender Abweichung der Blickrichtung weg von der Kamera und mit dem Grad der Verdeckung von Gesichtern durch andere Personen, Gegenstände oder bauliche Strukturen. Daher können – trotz der in den letzten Jahren mit Methoden des maschinellen Lernens erzielten Fortschritte – Gesichtserkennungssysteme bereits daran scheitern, die in den Videoströmen tatsächlich vorhandenen Gesichter überhaupt als solche zu detektieren. Entsprechend sinkt gemessen an der Zahl der im videobeobachteten Bereich anwesenden Personen sowohl die Erkennungs- als auch die Fehlalarmrate.

In der Praxis lässt sich die Erkennungsleistung entsprechender Systeme durch bessere Algorithmen, Videotechnik, Beleuchtung oder die Herstellung geeigneter Beobachtungsbedingungen durch Nutzung bzw. Anpassung der räumlichen Strukturen (Kasten 3.4) zwar verbessern, aber nicht beliebig steigern. Denn das Verhalten der zu beobachtenden Personen kann grundsätzlich nicht beeinflusst werden. So ist zu berücksichtigen, dass Personen, nach denen gefahndet wird, versucht sein werden, sich der Beobachtung aktiv zu entziehen, beispielsweise durch das Vermeiden direkter Blicke in Kameras, das Tragen von Sonnenbrillen, Hüten etc. oder durch das Umgehen videobeobachteter Bereiche (NIST 2017a, S. 6). Dadurch verringert sich die Erkennungsrate, nicht aber die Fehlalarmrate.

Für den Nutzen entsprechender Systeme letztlich entscheidend ist aber die Frage, ob die bzw. wie viele der gesuchten Personen die videobeobachteten Bereiche überhaupt betreten. Dies ist naturgemäß eine unbekannte Größe. Allerdings ist wohl davon auszugehen, dass die Zahl der Fahndungserfolge im Zeitverlauf generell abnehmen dürfte (bei unveränderter Fehlalarmrate), weil die gesuchten Personen im Wissen um die automatisierte Fahndung verstärkt andere Reiserouten wählen dürften. Auch deshalb erscheint es kaum möglich, alleine auf der Basis von Leistungskennzahlen eines GES, die in einer experimentellen Testumgebung gemessenen wurden, Vorhersagen zum polizeilichen Nutzen der automatisierten Videobeobachtung zur Personenfahndung in Echtzeit unter realen Einsatzbedingungen zu machen.

Kasten 3.4 Die Gesichtsfalle (»facetrap«)

Die meisten der mit aktuell an Bahnhöfen, Flughäfen etc. installierten Videobeobachtungssystemen getätigten Aufnahmen dürften den Qualitätsanforderungen von Gesichtserkennungssystemen nicht genügen, da die Bildqualität zu gering oder das betreffende Gesicht nicht ausreichend erkennbar ist. Vor allem in Räumen mit großem Publikumsverkehr ist es schwierig, ein Gesicht innerhalb einer Menge von Gesichtern so aufzunehmen, dass die identifizierenden Merkmale extrahiert werden können. Um für den Gesichtsabgleich geeignetes Bildmaterial zu erhalten, müssen also möglichst sämtliche Quellen im Raum, die die Bildqualität beeinträchtigen, ausgeschaltet bzw. unter Kontrolle gehalten werden.

Eine Möglichkeit bzw. Voraussetzung dazu bildet die Nutzung bzw. Anpassung der räumlichen Strukturen im beobachteten Raum. Um kontrollierte Bedingungen für die Bildaufnahme zu realisieren, können beispielsweise Rolltreppen, über denen die Kameras angebracht werden, genutzt werden. Ihre Konstruktion vereinzelt die Passanten und ordnet sie über- bzw. untereinander an. Außerdem tendieren Rolltreppennutzer/innen dazu, geradeaus und nach vorne zu blicken, was ggf. durch ein Blinklicht in Kameranähe noch verstärkt werden kann. Die räumliche Anordnung fungiert also als eine Art Gesichtsfalle (»facetrap«; Woodward et al. 2003, S. 14), welche die für einen erfolgreichen Gesichtsabgleich erforderliche Pose bei den Zielpersonen bewirkt. Wo immer Gesichtserkennungssysteme eingesetzt werden sollen, sind somit auch entsprechende Raumbedingungen zu schaffen.

Quelle: Woodward et al. 2003

3.5.4 Aktuelle Einsatzpraktiken

3.5.4.1 Verifikationsverfahren

Verifikationsverfahren kommen etwa bei der teilautomatisierten Grenzkontrolle (EasyPASS) zum Einsatz, die die Bundespolizei derzeit an acht deutschen Flughäfen einsetzt:[95] Der Reisende liest seinen elektronischen Reisepass ein und betritt eine Schleuse. Hier werden mit einer Kamera Gesichtsbilder erstellt, die dann mit dem auf dem Chip im Pass gespeicherten Gesichtsbild des Reisenden abgeglichen werden. Wird dadurch die Identität des Reisenden bestätigt, kann er die Schleuse passieren (Hempel 2016, 90 ff.).

95 www.easypass.de/EasyPass/DE/Wo_gibt_es_EasyPass/wo_gibt_es_easypass_node.html (31.3.2022)

3.5.4.2 Identitätsfeststellung, Sichtung von Foto- oder Videomaterial

Zur Identitätsfeststellung werden Gesichtserkennungssysteme von Polizeibehörden bereits standardmäßig eingesetzt. Beispielsweise nutzen Bundeskriminalamt, Bundespolizei und die meisten Landeskriminalämter seit 2007 ein entsprechendes System, um Fotos von unbekannten Personen mit dem Lichtbildbestand von INPOL abzugleichen, in dem zurzeit über 5,8 Mio. Bilder von ca. 3,6 Mio. erkennungsdienstlich behandelten Personen gespeichert sind (Stand März 2022[96]) (Bundesregierung 2013b, S. 10). Die Zahl der durchgeführten Abfragen stieg von 1.297 im Jahr 2009 auf 53.971 im Jahr 2019. Dadurch konnten 2009 insgesamt 72 Personen und 2019 insgesamt 2.123 Personen identifiziert werden (Bundesregierung 2018q, S. 9 ff., u. 2020a, S. 6 f.).

Zur retrospektiven Auswertung von gespeichertem Foto- oder Videomaterial hat das BKA 2017 die Software »Videmo 360 Search« eines deutschen Herstellers[97] beschafft (Bundesregierung 2018d, S. 9). Dieselbe Software wird beispielsweise auch von der Polizei Hamburg zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel eingesetzt (HmbBfDI 2018, S. 2).

3.5.4.3 Personenfahndung in Echtzeit

Die Personenfahndung in Echtzeit mithilfe der Videobeobachtung in Verbindung mit einem GES fand bzw. findet in Deutschland bislang nur im Rahmen von Versuchsprojekten statt. Das BKA testete entsprechende kommerziell verfügbare Systeme erstmals von Oktober 2006 bis Januar 2007 am Hauptbahnhof Mainz mit 200 freiwilligen Probanden. Bei einer Fehlalarmrate von 0,1 % konnten nur niedrige Erkennungsraten von 60 % (mit Tageslicht) bzw. 10 bis 20 % (ohne Tageslicht) erzielt werden (BKA 2007, S. 5).

Eine erneute Erprobung von aktuell auf dem Markt verfügbaren Gesichtserkennungssysteme fand im Zeitraum von August 2017 bis Juli 2018 durch das Bundesministerium des Innern, für Bau und Heimat, die Bundespolizei und das Bundeskriminalamt mit insgesamt 513 freiwilligen Probanden im Teilprojekt 1 »Biometrische Gesichtserkennung« im Rahmen des Pilotprojekts »Sicherheitsbahnhof Berlin Südkreuz« statt (Bundesregierung 2018e, S. 4).[98] Im Vergleich zum Versuch von 2006/2007 konnten hier deutlich höhere Erkennungsraten (insbesondere auch nachts) gemessen werden (Kasten 3.5).

96 https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Erkennungsdienst/erkennungsdienst_node.html (31.3.2022)
97 https://videmo.de/de (31.3.2022)
98 Im Anschluss an Teilprojekt 1 werden im derzeit laufenden Teilprojekt 2 die polizeilichen Einsatzmöglichkeiten automatisierter Videobeobachtung zur Erkennung potenzieller Gefahrensituationen getestet (Kap. 3.3.4).

Kasten 3.5 Pilotprojekt »Sicherheitsbahnhof Berlin Südkreuz«: Vorgehen im Teilprojekt 1 »Biometrische Gesichtserkennung« und zentrale Ergebnisse

Für den Versuch wurden drei Gesichtserkennungssysteme unterschiedlicher Hersteller mit Echtzeitdaten von drei (der insgesamt 77) im Bahnhof installierten Videokameras versorgt. Die Referenzdatenbanken bestanden aus Gesichtsbildern der Probanden. Die Probanden trugen Transponder auf sich, um ihre Anwesenheitszeiten in videobeobachteten Bereichen zu dokumentieren. Dadurch konnte jede Erkennung eindeutig als richtig oder falsch (Fehlalarm) klassifiziert und die Zahl der Erkennungsfehler bestimmt werden.

Die Leistung der Gesichtserkennungssysteme wurde in zwei Testphasen gemessen: Wurde für die erste Testphase jeweils ein qualitativ hochwertiges Referenzbild von jedem Probanden benutzt, waren es in der zweiten Testphase jeweils mehrere (bis zu fünf) Gesichtsbilder, die aus dem Videoströmen der im Versuch benutzten Kameras extrahiert wurden. Dadurch sollten die Systeme für Referenzbilder mit der Qualität von Fotos aus erkennungsdienstlicher Behandlung als auch von typischen Fahndungsfotos erprobt werden.

In Testphase 1 (hochqualitative Referenzbilder) erzielte das in Bezug auf die Erkennungsleistung beste System eine durchschnittliche Erkennungsrate von 68,5 % bei einer Fehlalarmrate von 0,19 %. In Testphase 2 (Fahndungsfotos) zeigte das beste Einzelsystem eine durchschnittlich Erkennungsrate von 82,8 % bei einer Fehlalarmrate von 0,07 %. Die Systemleistung wurde vor allem durch die in Abhängigkeit von Kameraposition und Tageszeit vorherrschenden Lichtverhältnisse beeinflusst. Beispielsweise wiesen die Erkennungsraten des besten Systems in Testphase 2 eine Spannbreite von 60 % (Gegenlicht bei Tag) bis 91 % (künstliches Licht bei Dämmerung) auf.

Von der Möglichkeit, das Verhältnis zwischen Erkennungs- und Fehlalarmrate durch die Wahl der Schwellenwerte für die einzelnen Gesichtserkennungssysteme zu beeinflussen (Kap. 3.5.2.2), wurde kein Gebrauch gemacht. Stattdessen wurde der Ansatz verfolgt, die einzelnen Systeme durch logische Verknüpfungen zu einem Gesamtsystem zu kombinieren. Durch logische ODER-Verknüpfung (als Treffer des Gesamtsystems gelten alle Treffer von mindestens einem der Einzelsysteme) kann die Erkennungsrate gesteigert werden, allerdings nur unter Inkaufnahme einer höheren Fehlalarmrate (z. B. Gesamtsystem in Testphase 2: Erkennungsrate 91,2 %, Fehlalarmrate: 0,34 %). Durch logische UND-Verknüpfung (Ergebnisse der Einzelsysteme müssen übereinstimmen, um als Treffer des Gesamtsystems zu gelten) verringert sich die Fehlalarmrate, allerdings auch die Erkennungsrate (z. B. Gesamtsystem in Testphase 2: Erkennungsrate: 68,1 %, Fehlalarmrate: 0,00018 %).

Quelle: Bundespolizeipräsidium 2018

Auf Grundlage der Testergebnisse wurde im Abschlussbericht des Bundespolizeipräsidiums (2018, S. 39) empfohlen, entsprechende Systeme an ausgewählten Bahnhöfen als Unterstützungsinstrument der polizeilichen Fahndung einzusetzen. Auch das BMI (2018) bewertete den Versuch als erfolgreich: Demnach zeigten die Ergebnisse, dass »Gesichtserkennungssysteme in Zukunft einen wesentlichen Mehrwert für die polizeiliche Arbeit, insbesondere der Bundespolizei, darstellen können«.

Aufgrund der deutlichen Leistungsunterschiede in Abhängigkeit der logischen Verknüpfung schlägt das Bundespolizeipräsidium (2018, S. 24) unterschiedliche Betriebsmodi vor: Bei besonderen polizeilichen Lagen (z. B. Terroranschläge) könnte ein Betrieb mit hohen Erkennungsraten (ODER-Verknüpfung) die Wahrscheinlichkeit für Fahndungserfolge vergrößern (allerdings unter Inkaufnahme einer höheren Fehlalarmrate). Im polizeilichen Alltag wäre dagegen eine geringe Fehlalarmrate (UND-Verknüpfung) von Vorteil (allerdings unter Inkaufnahme einer niedrigeren Erkennungsrate), um den Aufwand für die Validierung falscher Erkennungen zu reduzieren. In diesem Zusammenhang fällt die sehr geringe Fehlalarmrate von 0,00018 % in Testphase 2 ins Auge.

Die Aussagekraft der im Versuch erzielten Ergebnisse wird jedoch teilweise angezweifelt. So kritisierte etwa der Chaos Computer Club (CCC 2018) insbesondere das Vorgehen in der zweiten Testphase, als Referenzbilder vom getesteten System selbst aufgezeichnete Gesichtsbilder zu benutzen. Vermutet wird, dass die guten Testergebnisse nur deshalb erzielt wurden, weil Referenz- und Testbilder am gleichen Ort entstanden waren. Dadurch ließen sich die gemessenen Leistungskennzahlen nicht auf reale Einsatzszenarien in anderen Umgebungen (bzw. mit Referenzbildern aus anderen Quellen) übertragen. Bemängelt wurde außerdem, dass im Abschlussbericht rechtliche Probleme, Kostenfragen oder mögliche Risiken eines realen Einsatzes für unbeteiligte Passanten nicht angesprochen wurden. Beispielsweise fehle es an einem repräsentativen Abbild der Bevölkerung (Alter, Geschlecht, Ethnie) unter den Probanden, welches nötig gewesen wäre, um durch eine Aufschlüsselung der Erkennungs- bzw. Fehlerraten nach unterschiedlichen Personengruppen Hinweise auf ggf. vorhandene Diskriminierungspotenziale zu erhalten (Kap. 3.3.8.2). Insgesamt würden die Ergebnisse des Versuchs daher nicht als Begründung für einen künftigen Einsatz ausreichen.

Aktivitäten im Ausland

Aufgrund der wenigen Erfahrungen in Deutschland sollen im Folgenden diesbezügliche Aktivitäten im Ausland kurz vorgestellt werden.

In Großbritannien testet die Polizei von Südwales die Personenfahndung in Echtzeit unter realen Einsatzbedingungen. Seit 2017 werden bei größeren Veranstaltungen (z. B. Sportveranstaltungen, Rockkonzerte) die Videoströme von

stationären und mobilen Videokameras nach polizeilich gesuchten Personen durchsucht. Eine Evaluation der ersten Einsätze zwischen Juni 2017 und März 2018 durch unabhängig Experten von der Cardiff University ergab u. a. folgende Kernbefunde (Davies et al. 2018, S. 6 ff.):

- Bei den insgesamt 11 Einsätzen wurden in der Summe 2.900 Treffermeldungen generiert. Davon erwiesen sich 144 als korrekte und 2.755 als inkorrekte Identifizierungen (Fehlalarme).
- Die Verwendung eines besseren Algorithmus und die gewonnenen Einsatzerfahrungen trugen in der zweiten Hälfte des Versuchszeitraums zu einer deutlichen Reduktion der Zahl der Fehlalarme bei. Hier kam es bei insgesamt 8 Einsätzen zu 146 Treffermeldungen, wovon sich 38 als korrekt herausstellten.
- Das eingesetzte GES zeigte bei größeren Menschenansammlungen Probleme, da die Software bei Aufnahmen mit vielen Personen hängen blieb oder abstürzte. Zudem erwies sich die Bildqualität als wichtiger Erfolgsfaktor für die Detektion und den Abgleich von Gesichtern. Bei abnehmendem Tageslicht wurden Gesichter durch das GES zunehmend nicht mehr als solche erkannt.

Zwar können aus den Ergebnissen keine Aussagen zu den Erkennungs- bzw. Fehlalarmraten abgeleitet werden, da die Zahl der durch das GES abgeglichenen Gesichtsbilder gesuchter bzw. unbeteiligter Personen nicht mitgeteilt wurde. Somit lassen sich die Befunde auch nicht auf andere Einsatzszenarien übertragen. Gleichwohl verdeutlicht der Versuch die technischen und praktischen Herausforderungen im Realbetrieb (Kap. 3.5.3.3).

In Bezug auf die Anwendung der Videobeobachtung in Verbindung mit automatisierter Gesichtserkennung nimmt die Volksrepublik China eine hervorgehobene Rolle ein (Kasten 3.6). Zwar ist die Quellenlage unzureichend, um eine Bewertung der hier eingesetzten Systeme hinsichtlich ihrer Leistung und ihres polizeilichen Nutzens vorzunehmen, gleichwohl aber lässt sich aus den Aktivitäten das Ausmaß erahnen, mit welchem die chinesische Regierung diese Beobachtungstechnologien für zivile Sicherheitsaufgaben einzusetzen plant.

Kasten 3.6 Automatisierte Videobeobachtung in der Volksrepublik China

Laut diversen chinesischen Medienberichten und Behördenmitteilungen führen staatliche Stellen gegenwärtig landesweit Pilotprojekte zu unterschiedlichen Einsatzszenarien durch. Die Polizei der Stadt Zhengzhou beispielsweise erprobt aktuell den Einsatz von Brillen mit integrierter Videokamera, die es damit ausgerüsteten Streifenpolizisten ermöglichen sollen, Personen in einer Distanz bis 5 Meter innerhalb von wenigen Minuten per Gesichtserkennung

zu identifizieren (Jing 2018). In anderen Städten setzten Polizeibehörden die Videobeobachtung mit Gesichtserkennung bereits zur Personenfahndung in Echtzeit während Konzerten, Festivals oder in U-Bahnhöfen ein (Mo 2018). Die Polizeibehörden von Shanghai nutzen Gesichtserkennung zur Identifikation von Fahrradfahren, die gegen Verkehrsregeln verstoßen (Chen 2017). Außerdem werden hier automatisierte Videobeobachtungssysteme zur Aufdeckung weiterer Regelverstöße im Straßenverkehr (z. B. Fahren ohne Gurt, Telefonieren am Steuer, Missachtung von Vortrittsregeln) getestet (Shanghai Municipal People's Government 2017).

Diese Aktivitäten sind eingebettet in weitergehende Bestrebungen der chinesischen Regierung, landesweit ein gesellschaftliches Bonitätsprogramm (»Social Credit System«) zu etablieren (dazu und zum Folgenden Ohlberg et al. 2018, S. 4 ff.). Der Kern bildet eine individuelle Bonitätsstatistik für alle Bürger und Unternehmen, um Fehlverhalten strafrechtlich oder durch reputationsschädigende Maßnahmen zu sanktionieren. In die Bonitätsstatistik einfließen soll neben finanziellen Kennzahlen (z. B. zur Kreditwürdigkeit) auch eine Bewertung des sozialen Verhaltens der Bürger sowohl in positiver (z. B. Pflege von Erwachsenen) als auch in negativer Hinsicht, wofür Informationen aus herkömmlichen Quellen (Strafregister, Finanzdaten etc.) auch mit Daten aus der digitalen Beobachtung verknüpft werden sollen. Die Umsetzung des Bonitätssystems befindet sich derzeit in der Anfangsphase. Erhebung, Austausch (z. B. zwischen lokalen und zentralen Regierungsbehörden, zwischen privatwirtschaftlichen und staatlichen Akteuren) und Einbindung der Daten in das Bonitätssystem ist längst nicht ausgereift.

3.5.5 Rechtliche Einordnung

Die Frage, ob ein Einsatz der Videobeobachtung in Verbindung mit Gesichtserkennungssystemen nach derzeitiger Rechtlage zulässig ist, wird in der Literatur unterschiedlich beantwortet.

3.5.5.1 Sichtung von Foto- oder Videomaterial und Identitätsfeststellung

So erachten beispielsweise Hornung und Schindler (2017, S. 207) den Einsatz von Gesichtserkennungssystemen als bloßes *Hilfsmittel zur Sichtung* von rechtmäßig hergestelltem Foto- oder Videomaterial nach geltendem Recht als zulässig, da die jeweiligen Befugnisse zur Anfertigung der Aufnahmen (Kap. 3.4.2) auch das Recht umfassen, das Material zur gesetzlichen Aufgabenerfüllung zu sichten auch mithilfe von computergestützten Hilfsmitteln. Dies gelte zumindest, solange keine Verknüpfungen mit Informationen aus anderen, mit den auszuwertenden Aufnahmen nicht im Zusammenhang stehenden Quellen stattfinde.

Letzteres ist bei der *Identitätsfeststellung* der Fall, weshalb ein Abgleich der aufgezeichneten Gesichter z. B. mit polizeilichen Lichtbilddatenbanken laut Hornung und Schindler (2017, S. 207) nicht mehr auf die Ermächtigung zur Anfertigung der Aufnahmen gestützt werden könne. Möglich sei hier aber ein Rückgriff auf Regelungen zum Datenabgleich: Laut § 98c StPO beispielsweise dürfen zur Aufklärung einer Straftat personenbezogene Daten aus einem Strafverfahren mit anderen zur Strafverfolgung oder Gefahrenabwehr gespeicherten Daten maschinell abgeglichen werden. Voraussetzung wäre somit ein Tatverdacht gegen die zu identifizierende Person, was dann allerdings eine *Rückwärtssuche* ausschließen würde.

Zu einer gänzlich anderen Rechtsauffassung gelangt etwa der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI 2018). Dieser erachtet bereits den Einsatz von Gesichtserkennungssystemen als bloßes *Hilfsmittel zur Sichtung* als rechtswidrig, wenn dafür von allen auf den auszuwertenden Aufnahmen erkennbaren Gesichtern Templates erstellt und zum Zwecke eines späteren Abgleichs in Referenzdatenbanken gespeichert würden. Hierbei handle es sich nicht um eine vom Wortlaut bestehender Eingriffsnormen gedeckte technische Erneuerung oder Weiterentwicklung, sondern um »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 Betroffenen anlasslos Gesichtsmerkmale ausliest und maschinenlesbar abspeichert« (HmbBfDI 2018, S. 9). Notwendig sei daher eine eigenständige gesetzliche Grundlage, die nicht nur die Anlassstraftaten für einen derartigen Einsatz von Gesichtserkennungssystemen regle, sondern auch Art und Umfang des herangezogenen Videomaterials sowie den Zeitraum, für den die Videosequenzen ausgewertet und Templates daraus erstellt werden dürften (HmbBfDI 2018, S. 21).

3.5.5.2 Personenfahndung in Echtzeit

Auch zur Frage, ob ein Einsatz von Gesichtserkennungssystemen zur Personenfahndung in Echtzeit nach geltendem Recht zulässig wäre, finden sich in der Literatur unterschiedliche Meinungen (WD 2016a). Einerseits wird die Ansicht vertreten, dass sich bestehende Befugnisse auch auf eine intelligente Selektion mittels eines Abgleichs mit zuvor gespeicherten personenbezogenen Daten erstrekken. Andererseits und überwiegend wird jedoch argumentiert, dass eine automatisierte gegenüber der manuellen Sichtung von Videodaten in Echtzeit ein ganz anderes Auswertungsinstrument darstelle, das in seiner Eingriffsintensität weit über die konventionelle Videobeobachtung hinausgehen könne (so etwa Hornung/Schindler 2017, S. 207 f.): Dadurch würden nämlich grundsätzlich alle im videobeobachteten Bereich anwesenden Personen nicht nur erfasst, sondern mittels Abgleich mit einer Datenbank beständig überprüft werden, ohne dass diese

in den allermeisten Fällen hierfür einen Anlass gegeben haben bzw. auch nur konkrete Erkenntnisse dafür vorliegen, dass sich die gesuchten Personen unter ihnen befinden könnten. Problematisiert wird ferner, dass einmal installierte Systeme nicht für Fahndungszwecke, sondern prinzipiell auch zur automatisierten und heimlichen Erstellung von Bewegungs- und Verhaltensprofilen gesuchter Personen herangezogen werden könnten. Anlass, Zweck und Grenzen des polizeilichen Einsatzes solcher Systeme müssten daher durch eine eigenständige Rechtsgrundlage klar geregelt werden.

In diesem Zusammenhang von Bedeutung könnte eine aktuelle Entscheidung des Bundesverfassungsgerichts zum präventivpolizeilichen Einsatz von Systemen zum automatisierten Kfz-Kennzeichenabgleich (Kap. 3.3.3) in drei Bundesländern (Bayern, Hessen und Baden-Württemberg) sein. Zum Beispiel war die Polizei in Bayern dazu ermächtigt, automatisierte Kennzeichenkontrollen zur Abwehr einer Gefahr einzusetzen (Artikel 39 Abs. 1 i.V.m Artikel 13 Abs. 1 Nr. 1 PAG in der Fassung vom 18.5.2018). Laut Bundesverfassungsgericht sind automatisierte Kennzeichenkontrollen zur Abwehr jeder Gefahr mit dem Übermaßverbot jedoch nicht vereinbar, vielmehr muss der Einsatz auf einen der Verhältnismäßigkeit genügenden Rechtsgüterschutz beschränkt werden. Außerdem stellt das Gericht (BVerfG, Beschluss vom 18. Dezember 2018, 1 BvR 142/15, Leitsatz 4 u. Rn. 102 ff.) klar, dass die Reichweite der für den Datenabgleich herangezogenen Fahndungsbestände anlassbezogen zu begrenzen ist. So stellt der automatisierte Kennzeichenabgleich einen Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Personen *von erheblichem Gewicht* dar, auch dann, wenn der Abgleich ergebnislos bleibt (Nichttreffer) und die erhobenen Daten unmittelbar wieder gelöscht werden (sodass den Betroffenen weder Unannehmlichkeiten noch Konsequenzen erwachsen).[99] Begründet wird dies damit, dass, wenn gezielt mittels Datenabgleich Personen im öffentlichen Raum daraufhin überprüft werden, ob sie polizeilich gesucht werden, auch dann ein behördliches Interesse an ihren Daten vorliegt, wenn der Abgleich letztlich zu einem Nichttreffer führt. Denn die Einbeziehung der Daten aller Personen ist notwendiger Teil der Kontrolle und gibt der Fahndungsmaßnahme erst ihren Sinn. Zudem wird für alle betroffenen Personen eine ungehinderte Weiterfahrt unter den Vorbehalt gestellt, dass keine Erkenntnisse gegen sie vorliegen. Für das Gericht (BVerfG, Beschluss vom 18. Dezember 2018, 1 BvR 142/15, Rn. 47 ff.) ist der automatisierte Kfz-Kennzeichenabgleich daher nicht erst hinsichtlich seiner Folgen, sondern als solcher freiheitsbeeinträchtigend. Als Grundrechtseingriff von erheblichem Gewicht – so das Gericht weiter (BVerfG, Beschluss vom 18. Dezember 2018, 1 BvR 142/15, Rn. 89 ff.) – genügen automatisierte Kennzeichenabgleiche verfassungsrechtlichen Anforderungen nur, wenn sie grundsätzlich

99 Das Bundesverfassungsgericht (BVerfG, Urteil vom 11. März 2008, 1 BvR 2074/05, Rn. 68) korrigierte damit seine bisherige Rechtsprechung, nach welcher der automatisierte Kennzeichenabgleich in Nichttrefferfällen keinen Grundrechtseingriff begründete.

durch hinreichend konkrete, objektiv bestimmte Gründe veranlasst sind, dem Schutz von Rechtsgütern von zumindest erheblichen Gewicht oder sonst einem vergleichbar gewichtigen öffentlichen Interesse[100] dienen sowie übergreifende Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle beachtet werden. In der Folge hat der Bayerische Gesetzgeber den Einsatz entsprechender Systeme auf die Abwehr von Gefahren für Rechtsgüter von zumindest erheblichen Gewicht beschränkt.[101]

Die durch das Bundesverfassungsgericht angelegten verfassungsrechtlichen Maßstäbe zum automatisierten Kfz-Kennzeichenabgleich lassen sich ggf. auf die Personenfahndung in Echtzeit mittels Gesichtserkennung übertragen, da beide Verfahren deutliche Ähnlichkeiten aufweisen. Demnach wäre diese Praxis an enge Voraussetzungen zu knüpfen. Als mögliche Elemente für eine grundrechtsschonende gesetzliche Regelung zur Personenfahndung in Echtzeit mittels GES schlagen etwa Hornung und Schindler (2017, S. 208) u. a. vor:

- Beschränkung des verwendeten Fahndungsbestands (z. B. auf Personen, die schwerer oder schwerster Straftaten verdächtig bzw. überführt sind);
- Begrenzung des räumlichen Anwendungsbereichs auf Orte mit hoher Wahrscheinlichkeit für das Auffinden der gesuchten Personen (z. B. Flughäfen, Bahnhöfe);
- Beschränkung der Möglichkeiten zur Erstellung von Bewegungsprofilen;
- Technisch-organisatorische und verfahrensrechtliche Vorkehrungen zum Schutz des Persönlichkeitsrechts unbeteiligter Personen (z. B. unmittelbare Löschpflicht für Fehlalarme oder Logdateien, Dokumentation- und Berichtspflichten).

100 Hierzu zählt das Bundesverfassungsgericht (BVerfG, Beschluss vom 18. Dezember 2018, 1 BvR 142/15, Rn. 99) z. B. besonders schutzwürdige Rechtsgüter wie Leib, Leben und Freiheit der Person und der Bestand und die Sicherheit des Bundes und der Länder oder den Schutz von nicht unerheblichen Sachwerten.

101 Gesetz zur Änderung der Bestimmungen zu automatisierten Kennzeichenerkennungssystemen (AKE-Änderungsgesetz) vom 10. Dezember 2019 (BVBl. 2019, S. 691)

4 Internetbeobachtung und Ansätze der vorhersehenden Polizeiarbeit

Sicherheitsbehörden und Rettungsorganisationen sind darauf angewiesen, mit veränderten Kommunikationsmustern Schritt zu halten und insofern auch verlässlich über Aktivitäten und Trends im Internet und in den sozialen Medien informiert zu sein. Grundsätzlich können von Nutzer/innen ins Internet gestellte Informationen für Sicherheitsakteure eine wichtige Informationsquelle sein. Die dort nachvollziehbare Kommunikation ermöglicht es nicht nur, mit Bürger/innen einsatzbezogen zu interagieren (z. B. im Rahmen der Suche nach Zeugen oder von vermissten Personen), sondern erlaubt auch Beobachtungen von bestimmten Phänomenen, Szenen oder Themen mit dem Ziel, potenzielle Gefahren und Straftaten im Vorfeld ihrer Entstehung und Planung nachzuvollziehen und ihre Ausführung durch geeignete präventive Interventionen zu verhindern. Für die Strafverfolgung liefern Internetrecherchen ggf. Anhaltspunkte für den Zeitpunkt, den Ort und auch den Modus Operandi von Straftaten (z. B. wenn Täter Bilder von gestohlenen Waren oder Tatorten, etwa bei unerlaubten Graffiti, im Internet veröffentlichen) oder erlauben Rückschlüsse auf das soziale Umfeld, die Interessen, Meinungen oder Aufenthaltsorte von Verdächtigen (Bayerl/Rüdiger 2017, S. 927 f.).

Entsprechend findet die Beobachtung des Internets durch Sicherheitsakteure heute verstärkt statt. Insbesondere im Rahmen polizeilicher Tätigkeiten basiert sie auf einer langjährigen Anwendung von proaktiven Strategien, die darauf ausgerichtet sind, Kriminalität zu erkennen und zu begegnen, bevor Taten ausgeübt werden. Dabei kommen zunehmend auch algorithmenbasierte Techniken zur Erkennung von Kriminalitätsmustern zum Einsatz. In Anlehnung an Perry et al. (2013) lassen sich vier allgemeine Kategorien von prädiktiven Beobachtungsmethoden benennen, die das Feld der Internetbeobachtung einschließlich der vorhersehenden Polizeiarbeit (Predictive Policing) umreißen:

- einfache Methoden wie die Verwendung von Checklisten und Indizes;
- klassische statistische Verfahren wie Regressions- oder Trendanalysen;
- komplexe Anwendungen, die anspruchsvolle Algorithmen und große Datenmengen verlangen;
- maßgeschneiderte Methoden, die bestehende Techniken nutzen, um Daten beispielsweise in Form von Kartendiagrammen zu visualisieren.

Dementsprechend finden sich bei BOS unterschiedliche Formen und Praktiken der Internetbeobachtung. Deren Übergänge sind fließend, denn in der Regel bauen die Entwicklungen aufeinander auf. Das Spektrum reicht von der manuellen Beobachtung von Webseiten über die teilautomatisierte Erfassung und Auswertung von Inhalten aus sozialen Medien (Social Media Intelligence) bis hin zu

aktuellen Implementierungen von Vorhersagesoftware im Rahmen des Predictive Policing bei einzelnen Länderpolizeien, deren Ziel es ist, auf Basis unterschiedlicher Daten mögliche künftige Tatorträume zu markieren, um durch Interventionsmaßnahmen wie die Erhöhung der Polizeipräsenz potenziellen Straftaten vorzubeugen.

Im Fokus der polizeilichen Internetbeobachtung und des Predictive Policing in Deutschland stehen heute einzelne Phänomenbereiche bzw. Kriminalitätsfelder wie organisierte Kriminalität, politisch motivierte Kriminalität, Terrorismus oder Wohnungseinbruchsdiebstahl. Das Beobachtungsinteresse kann aber auch auf weitere Kriminalitätsbereiche ausgedehnt werden. Ermöglicht wird dies nicht zuletzt durch die Einbeziehung und Verknüpfung von immer mehr Daten aus dem Internet und anderen öffentlichen Quellen (z. B. Kartenmaterial, Veranstaltungskalender, sozioökonomische Daten) sowie aus polizeilichen Datenbanken unter Verwendung von zunehmend leistungsfähigen Algorithmen. Vor allem indem Personen in wachsendem Umfang Informationen über sich und ihr Leben – Identitäten, Beziehungen, Aktivitäten, persönliche Vorlieben und Ansichten – im Internet veröffentlichen, können prinzipiell ganz unterschiedliche gesellschaftliche Ereignisse zum Gegenstand sicherheitsbezogener Beobachtung werden, sofern diese nur eine Präsenz im Internet oder den sozialen Medien erhalten. Mögliche Konsequenzen davon für das individuelle Nutzerverhalten und die Gesellschaft sind Thema in Kapitel 7.1.

Klar ist aber auch, dass ein verstärkter Einsatz solcher Instrumente ebenfalls grundlegende Auswirkungen auf die Sicherheitspraxis insgesamt haben wird. Beispielsweise reihen sich – trotz aller Unterschiede – sämtliche Formen der Internetbeobachtung einschließlich des Predictive Policing in die allgemeine Entwicklungstendenz gezielter, zukunftsorientierter Polizeiarbeit ein, »die sich auf die Identifizierung, Analyse und das ›Management‹ von fortbestehenden und sich entwickelnden ›Problemen‹ oder ›Risiken‹ konzentriert … und nicht auf die reaktive Untersuchung und Aufdeckung einzelner Verbrechen« (TAB-Übersetzung; nach Maguire 2000, S. 315). Für die Bewertung solcher Instrumente entscheidend ist daher nicht zuletzt, inwiefern sich durch deren Anwendung auch die Risikowahrnehmung der Sicherheitsakteure und damit die Polizeiarbeit insgesamt ändert. Solche Fragen, die sich generell im Kontext des Einsatzes von Beobachtungstechnologien im zivilen Sicherheitsbereich stellen, werden in Kapitel 7.2 angesprochen.

4.1 Manuelle Internetbeobachtung

Im Rahmen der manuellen Internetbeobachtung wird händisch nach sicherheits- bzw. lagerelevantem Text-, Bild- oder Videomaterial in frei verfügbaren Internetquellen – Webseiten, Foren, Blogs wie Twitter, soziale Netzwerke wie Face-

book, Multimediaplattformen wie YouTube – gesucht, um aus der Analyse und Bewertung der gewonnenen Informationen verwertbares Wissen zu generieren.

4.1.1 Einsatzformen und Ziele manueller Internetbeobachtung

Zwischen den verschiedenen BOS lassen sich nicht nur bestimmte Nutzungsentwicklungen, sondern auch gewisse Nutzungsunterschiede feststellen.

Aufgabenbedingt steht bei Landeskriminalämtern sowie dem Bundeskriminalamt die strafrechtlich relevante Beobachtung von einschlägigen Internetseiten und sozialen Medien im Vordergrund. Gilt generell, dass das Internet und Onlineplattformen von Straftäter/innenn genutzt werden, um Straftaten zu planen, anzukündigen oder zu kommunizieren, zielt die Beobachtung darauf ab, Hinweise auf bevorstehende bzw. bereits begangene Straftaten zu generieren. So hat sich die Internetbeobachtung vor allem in den Bereichen der organisierten Kriminalität, Cyberkriminalität oder des Terrorismus bereits als standardisiertes Ermittlungsinstrument etabliert (Epple/Ludewig 2019, S. 20). In Anlehnung an Omand (2012, S. 805 f.) lassen sich hierbei drei prinzipielle Zielsetzungen unterscheiden, wobei diese sich in der Praxis allerdings überschneiden können:

- *Feststellung/Identifizierung krimineller Absichten bzw. Personen*: Durch die Beobachtung von Nutzerprofilen verdächtiger Personen sollen deren Pläne rekonstruiert und kriminelle Absichten antizipiert werden. Über Querverweise, Kontakt- oder Freundeslisten können möglicherweise Komplizen ermittelt und kriminelle Netzwerke aufgedeckt werden. Verdächtige bzw. deren Taten können so nicht nur durch eigenen Inhalt identifiziert werden, sondern ggf. auch durch den Inhalt der Peers, also von Menschen mit gemeinsam geteilten Interessen. Grundsätzlich gilt, dass die Sichtbarkeit sozialer Bindungen eine wichtige Quelle für Ermittler darstellt (Trottier 2012). Daraus folgt auch, dass durch ein gesetzlich verordnetes Abschalten einschlägiger Internetseiten bzw. Nutzerprofile erhebliche Informationslücken für die polizeiliche Gefahrenabwehr bzw. Strafverfolgung entstehen könnten.
- *Einblick in Gruppen*: Durch die Beobachtung nutzergenerierter Inhalte besteht die Hoffnung, das Verhalten bestimmter Gruppen, die für die Polizei von Interesse sind (z. B. gewaltbereite Fangruppen im Fußball), besser vorhersehen zu können: Welche Themen entwickeln sich? Wie werden flüchtige Ereignisse aufgegriffen? Welche Meinungsführerschaften lassen sich erkennen? Welche Aktionen sind geplant und welche Verabredungen werden ggf. von gegnerischen Gruppierungen getroffen, die zu Gewalt führen und die öffentliche Ordnung gefährden könnten? Die Herausforderung aus Sicht der Behörden besteht vor allem darin, das richtige Verhältnis zwischen explorativer Beobachtung und verwertbaren Erkenntnissen zu finden, ohne alternative Pfade aufgrund des Selektionszwangs zu ignorieren.

- *Erforschung und Verständnis einzelner Phänomenbereiche*: Gelten soziale Medien insgesamt als Ort, an dem soziale und politische Konflikte ausgetragen und diskursiv bearbeitet werden, besteht die Hoffnung, dass die Analyse solcher Diskurse zu einem besseren Verständnis von Entwicklungen und Phänomenen wie Links-/Rechtsradikalismus, Salafismus-Jihadismus und gewaltbereiten Szenen beitragen kann, indem dadurch Aufschlüsse und Einblicke in Radikalisierungspfade und soziale Bedingungen von Gewalt möglich werden. In diesem Feld besteht allerdings noch erheblicher Forschungsbedarf. Beispielsweise wird im Rahmen des Forschungsprojekts »Propaganda, Mobilisierung und Radikalisierung zur Gewalt in der virtuellen und realen Welt« (PANDORA; Laufzeit 2017 bis 2020) untersucht, welche extremistischen Vorstellungen und Symboliken im Internet und in den sozialen Medien verwendet werden, wie diese zu Radikalisierungen beitragen und welche Effekte Internetpropaganda auf Radikalisierung und Gewaltanwendung in der realen Welt haben.[102]

Im Rahmen schutzpolizeilicher Aufgaben wird die Internetbeobachtung anlassbezogen beispielsweise im Vorfeld von und während Großveranstaltungen (Demonstrationen, Risikospielen im Fußball etc.) genutzt, um den Einsatz besser planen und mögliche Gefährdungssituationen erkennen bzw. einschätzen zu können. Ob einsatzbegleitende manuelle Internetrecherchen auch die Bewältigung von Einsatzlagen des täglichen Polizeidienstes unterstützen können (z. B. Vermisstenfälle, Suizidankündigungen, häusliche Gewalt, Personenfahndungen), wurde im Rahmen des Forschungsprojekts »Sicherheit im Einsatz durch Open Source Intelligence in Einsatzleitstellen« (SENTINEL; Laufzeit 2018 bis 2019) in drei Modellleitstellen (Polizeidirektion Osnabrück, Polizeipräsidium Dortmund und Polizeipräsidium München) untersucht (Epple/Ludewig 2019). Demnach können anlassbezogene Internetrecherchen einsatzrelevante Informationen liefern, die zur effektiven und erfolgreichen Einsatzbewältigung beitragen. Deutlich wurde aber auch, dass der nachhaltige Erfolg der Implementierung maßgeblich davon abhängt, inwieweit solche Verfahren in ein strategisches Gesamtkonzept eingebunden sind. So müssen die notwendigen Rahmenbedingungen festgelegt und die Rollen und Aufgaben der recherchierenden Personen klar geregelt sein (Epple/Ludewig 2020, S. 73 ff.).

Nutzergenerierte Internetinhalte können schließlich auch im Falle von unerwartet eingetretenen Großschadenslagen, Krisen oder Katastrophen einschließlich Amok- oder Terrorlagen wichtige Informationsquellen für polizeiliche und nichtpolizeiliche Einsatzkräfte sein. Dies gilt insbesondere dann, wenn infolge von Infrastrukturschäden betroffene Gebiete bzw. Orte für die Einsatzkräfte nicht oder nur teilweise zugänglich sind (BBK 2017, S. 5). So können die veröffentlichten Inhalte der vor Ort anwesenden Personen zusätzliche Erkenntnisse zur

102 https://sifo.bmbfcluster.de/files/Projektumriss_PANDORA.pdf (31.3.2022)

aktuellen Situation, zu potenziellen Schadensstellen oder sogar Hinweise auf Verletzte oder mögliche Täter liefern. Dabei wird auch von den Sicherheits- und Rettungskräften vielfältig Gebrauch von Twitter und anderen sozialen Netzwerken gemacht, um einerseits Mitteilungen an die Bevölkerung zu geben, andererseits aber auch die Reaktionen darauf zu beobachten, um lagerelevante Hinweise zu erhalten. Hier sind die Grenzen zwischen Öffentlichkeits- und der eigentlichen Sicherheitsarbeit oft fließend.

Herausforderungen und Limitierungen

Eine generelle Herausforderung bei der Internetbeobachtung stellt die Einschätzung der Qualität der gewonnenen Informationen dar. Im Zuge größerer Einsätze, aber auch beispielsweise bei Amok- oder Terrorlagen entstehen und kursieren oft Gerüchte im Internet, sodass aufgrund der mangelnden Zurechenbarkeit glaubhafte von nichtglaubhaften Informationen bzw. Quellen nur schwer unterschieden werden können. Dass es beispielsweise bei Twitter keinen Zwang gibt, Klarnamen zu nutzen, erschwert – trotz Anhaltspunkten für eine seriöse Nutzung – die Unterscheidung von echten und unechten Accounts. Prinzipiell können Inhalte von jedem Akteur erstellt werden, ohne dass sich die Identität der jeweiligen Nutzerin/des jeweiligen Nutzers und seine Intentionen sicher feststellen lassen.

Schwierigkeiten bereiten auch Anonymisierungsdienste[103], die eine Navigation im Internet unter fremder IP-Adresse ermöglichen. Bekannte Beispiele sind das The-Onion-Router-(TOR-)Netzwerk oder das Darknet, die auch von Kriminellen genutzt werden (z. B. für den Onlinehandel mit illegalen Waren oder Dienstleistungen), um die eigene IP-Adresse zu verschleiern. Die Ermittlung der Identität von verdächtigen Personen über eine Bestandsdatenauskunft beim Internetdienstanbieter auf Basis der IP-Adresse (Kap. 5.2.2.3) ist in diesem Fall nicht mehr möglich (Kochheim 2015, S. 451 ff.). Als Ermittlungsansatz bleibt oft nur der Einsatz von nicht offen ermittelnden Polizeibeamten bzw. verdeckten Ermittlern, die unter veränderter Identität versuchen, auf der entsprechenden Plattform Kontakt zur/m verdächtigen Nutzer/in aufzunehmen. Ziel der Maßnahme ist die Informationsbeschaffung oder beispielsweise die Anbahnung von Scheinkäufen, um im Zuge einer fingierten Warenübergabe den Tätern habhaft zu werden.

Wenn BOS Internetplattformen auch zur Interaktion mit der Bevölkerung nutzen, besteht ein Problem darin, dass sich die publizierten Inhalte unkontrolliert verbreitet können. Was sich im Rahmen von Fahndungen als Vorteil einer schnellen Verbreitung erweist, kann zum datenschutzrechtlichen Problem werden,

103 Dabei handelt es sich um Internetdienste, die eine Kontaktanfrage einer Nutzerin/eines Nutzers aufnehmen und dann unter der eigenen IP-Adresse an den Zielserver (bzw. zunächst an eine Kaskade weiterer Anonymisierungsdienste und dann an den Zielserver) weitergeben. Der Zielserver kommuniziert dabei nur mit dem Anonymisierungsdienst, sodass die IP-Adresse der Nutzerin/des Nutzers für den Zielserver (und damit auch für den Internetdienstanbieter des Zielservers) nicht sichtbar ist (Kochheim 2015, S. 451 ff.).

sobald sich ein Verdacht als unbegründet herausstellt, jedoch nicht mehr aus dem Netz gelöscht werden kann.

Schließlich stellt die manuelle Internetbeobachtung aufgrund der schieren Quantität der Daten eine personelle Herausforderung für sämtliche Behörden und Organisationen mit Sicherheitsaufgaben dar. Dadurch sind die Möglichkeiten der manuellen Internetbeobachtung begrenzt, da die Größe eines Phänomenbereichs, einer Szene oder eines Akteursnetzwerks die Intensität der Beobachtung bestimmt. Rein explorative Recherchen, die beispielsweise bestimmten Hypothesen nachgehen, dürften kaum machbar sein, wenngleich sie für einzelne Sicherheitsbehörden entsprechend ihrer jeweiligen Aufgabenfelder auch von Bedeutung sein könnten. Abhilfe sollen hier unterstützende softwarebasierte Systeme schaffen, auf die in Kapitel 4.2 eingegangen wird.

4.1.2 Aktuelle Einsatzpraxis bei den Polizeibehörden des Bundes

Das Bundeskriminalamt, die Bundespolizei und der Zollfahndungsdienst führen im Rahmen der jeweiligen Zuständigkeiten Recherchen im Internet durch. Dies betrifft sowohl für jedermann offen zugängliche Bereiche des Internets (Webseiten, Blogs, Twitter etc.) als auch Inhalte aus Foren oder Gruppen in sozialen Medien oder im Darknet, die nur durch eine Anmeldung zugänglich sind (Bundesregierung 2016b, 2018g, S. 2). Letzteres geschieht auch unter Nutzung pseudonymer Accounts (Fake-Accounts), die etwa durch die Bundespolizei zwischen 2016 und 2017 in 458 Fällen verwendet wurden (Bundesregierung 2017c, S. 1).[104]

Seit 2007 besteht das Gemeinsame Internetzentrum (GIZ) zur Beobachtung, Auswertung und Analyse von Veröffentlichungen mit islamistischen und jihadistischen Inhalten im Internet, an dem neben dem Bundeskriminalamt auch die Generalbundesanwaltschaft sowie die Nachrichtendienste des Bundes beteiligt sind. Ziel der Kooperation ist es, Kompetenzen zu bündeln und den Informationsaustausch zwischen den beteiligten Behörden zu gewährleisten (BfV o.J.), ohne dass allerdings eine strukturelle oder operative Zusammenarbeit etwa zwischen der Generalbundesanwaltschaft und den Nachrichtendiensten stattfindet (Bundesregierung 2016c, S. 2). Die Aufgabe besteht vor allem darin, täglich und anlassunabhängig militantislamistische Propagandaveröffentlichungen von jihadistischen Gruppierungen und Personen in Foren, Internetseiten und sozialen Medien zu beobachten und im Hinblick auf sicherheitsrelevante Aspekte mit Deutschlandbezug zu analysieren. Die gewonnenen Erkenntnisse, Themen und dominanten Diskurse werden in drei verschiedenen Berichtsformen aufbereitet (Bundesregierung 2013a, S. 10 f.; 2018e, S. 6):

104 Für das BKA oder den Zollfahndungsdienst lagen laut Bundesregierung (2017c) keine entsprechenden Zahlen vor. Auskünfte zu neueren Zahlen wurden von der Bundesregierung (2019b, S. 3) als Verschlusssache eingestuft (Einstufungsgrad: VS – Nur für den Dienstgebrauch) und stehen damit für die Öffentlichkeit nicht zur Verfügung.

- GIZlog: 14-tägliche Erscheinung, 268 Ausgaben im Zeitraum 2007 bis 2018;
- GIZ-Spezial: anlassbezogen 280 Berichte im Zeitraum 2007 bis 2018;
- GIZ-Spezial Fokus: anlassbezogen 57 Berichte im Zeitraum 2013 bis 2018.

Nach Vorbild des GIZ wurden ab 2012 durch Bundeskriminalamt, Bundesamt für Verfassungsschutz und Militärischer Abschirmdienst die Kooperationsplattformen »Koordinierte Internetauswertung« für Rechtsextremismus (KIA-R), Linksextremismus (KIA-L) und Ausländerextremismus (KIA-A) eingerichtet (BKA o.J.b). Ende 2019 kündigte die Bundesregierung (2019g, S. 2 f.) vor dem Hintergrund mehrerer rechtsextremistisch motivierter Gewalttaten an, zur Bekämpfung der Hasskriminalität im Internet die Internetbeobachtung durch das BKA sowohl auf der Plattform der Koordinierten Internetauswertung als auch durch eigene Internetrecherchen zu verstärken.

4.1.3 Rechtliche Einordnung

Soweit es sich bei der Internetbeobachtung lediglich um polizeiliche Recherchen in offenen Quellen (allgemein zugängliche Webseiten, Foren oder Inhalte sozialer Medien, die jedem Interessierten offenstehen) handelt, ist die grundsätzliche Zulässigkeit von der Rechtsprechung geklärt. So liegt gemäß Bundesverfassungsgericht (BVerfG, Urteil vom 27.2.2008, Rn. 308 ff.) noch kein Eingriff in das allgemeine Persönlichkeitsrecht vor, wenn eine staatliche Stelle im Internet verfügbare Kommunikationsinhalte erhebt, die sich an jedermann oder zumindest an einen nicht weiter abgegrenzten Personenkreis richten. Die Maßnahmen sind folglich durch Generalklauseln abgedeckt, etwa für den Bereich der Strafverfolgung durch §§ 161, 163 StPO. Dies gilt selbst für die gelegentliche Verwendung von Fake-Accounts (als Ausdruck einer kriminalistischen List) durch nicht offen ermittelnde Polizeibeamte, jedoch laut Bundesverfassungsgericht nur solange, wie staatliche Akteure dabei kein schutzwürdiges Vertrauen des Betroffenen in die Identität und die Motivation seines Kommunikationspartners ausnutzen. Letzteres ist dem verdeckten Ermittler vorbehalten und folglich nur unter den strengeren Anforderungen des § 110a StPO zulässig. Unklar ist jedoch, wo genau der Übergang von der List zur Legende im Sinne des § 110a Abs. 2 StPO stattfindet (Kochheim 2015, S. 534 f.).

4.2 Social Media Intelligence

Sicherheitsbehörden, Rettungsorganisationen, aber auch etwa Public-Health-Institutionen haben in den vergangenen Jahren zunehmend ein Interesse daran entwickelt, Inhalte und insbesondere Dynamiken in sozialen Medien besser zu verstehen und für ihre Zwecke zu gebrauchen. Die wesentliche Herausforderung hierbei besteht in der Bewältigung und Interpretation der schier unendlichen

Menge an Daten, deren Auswertung von Interesse sein könnte. Für den einzelnen Sachbearbeiter ist es praktisch unmöglich, mehr als nur eine kleine Auswahl an Inhalten manuell zu erfassen und auszuwerten, um hierauf aufbauend strategische und taktische Entscheidungen abzuleiten. Abhilfe versprechen hier unterstützende Softwarelösungen im Rahmen der Social Media Intelligence (SOCMINT), mittels derer sich die Daten (teil)automatisiert erfassen, klassifizieren, visualisieren und – je nach Funktionsumfang – auch analysieren lassen.

SOCMINT hat unterschiedliche Ursprünge. Aus der Sicht von Polizei- und Strafverfolgungsbehörden schließt es an die Idee der Open Source Intelligence (OSINT) der Nachrichtendienste an, bei der heterogene Informationen aus frei verfügbaren Quellen gesammelt werden, um daraus relevante Erkenntnisse retrospektiv oder in Echtzeit zu generieren. SOCMINT findet aber auch im Marketingbereich seine Entsprechung: Hier werden mithilfe von Analysetools aus möglichst großen Mengen an nutzergenerierten Internetinhalten Trends ermittelt und Kundenprofile erarbeitet, aus denen sich unternehmenstaktische und -strategische Entscheidungen ableiten lassen.

Ziel der Anwendung softwaregestützter Systeme ist es zunächst, die notwendigen Schritte für die Beobachtung zu vereinfachen und effizienter zu machen, um angesichts knapper Personalressourcen die Potenziale der manuellen Internetbeobachtung besser heben zu können. Weitere Nutzenpotenziale erhoffen sich Sicherheitsakteure von einer (teil)automatisierten Datenerfassung und -auswertung vor allem für die Früherkennung von sicherheitsrelevanten Lagen. Eine mögliche Anwendung wäre beispielsweise die Analyse des Datenverkehrs in sozialen Medien (z. B. Twitter) im Kontext von Großveranstaltungen, um die Erkennung von potenziellen Gefahrensituationen in nahezu Echtzeit zu ermöglichen, was im Vergleich zu herkömmlichen telefonischen Meldewegen viel schnellere Reaktionszeiten erlauben könnte (Omand et al. 2012, S. 805 f.). Wenngleich hierzu zahlreiche Ansätze bereits vorliegen, stellt diese Nutzung jedoch noch Zukunftsmusik dar.

Generell befinden sich entsprechende Softwarelösungen insbesondere im Hinblick auf eine automatisierte Auswertung der Inhalte aus sozialen Medien (und weiteren offen zugänglichen Bereichen des Internets) aktuell in einer frühen Entwicklungsphase. So ist, wie im Folgenden anhand einer exemplarischen Beschreibung eines Prototyps für ein SOCMINT-Softwaresystem gezeigt wird, der Leistungsumfang derzeit noch beschränkt. Dementsprechend steht auch die praktische Anwendung solcher Instrumente am Anfang, sodass die Internetbeobachtung durch Polizeibehörden in Deutschland – soweit bekannt – meist noch manuell erfolgen dürfte.[105] Ein Vorreiter in diesem Feld ist die Hessische Landespolizei, die seit 2017 eine angepasste, unter dem Namen Hessendata firmierende

105 So nutzte etwa das BKA zumindest bis 2017 für Internetrecherchen Open-Source-Software wie Internetbrowser und Webapplikationen, nicht aber spezielle Softwaretools (Bundesregierung 2017h, S. 3).

Variante der Gotham-Software des US-amerikanischen Herstellers Palantir testet. Die Software soll es ermöglichen, strukturierte wie unstrukturierte Daten verschiedenster Formate und Quellen zu verknüpfen, wobei sich neben Informationen aus verschiedenen polizeilichen Datenbanken auch Daten aus sozialen Medien (etwa die Facebook-Profile von Verdächtigen) einspeisen lassen sollen (letzteres würde jedoch ein Rechtshilfeersuchen an die US-Behörden voraussetzen; Brühl 2018).

4.2.1 Exemplarische Beschreibung aktuell verfügbarer Softwarelösungen

Aktuell verfügbare Softwarelösungen können die Arbeit von menschlichen Analysten zwar unterstützen, sind aber in Bezug auf die automatisierte Datenerfassung und -auswertung noch nicht ausgereift. Sie bieten in der Regel technische Hilfestellung für folgende Aufgaben (Hempel 2016, S. 83 ff.):[106]

- Sammeln von Informationen aus offenen Datenquellen;
- Anreicherung von Daten durch Verknüpfung;
- Filtern von Daten zur schnelleren Verarbeitung;
- Visualisierung von Datensätzen;
- Protokollierung von Ergebnissen für die weitere Verarbeitung.

Dazu stellen die Softwareprodukte eine Reihe von Visualisierungs- und Analysefunktionen zur Verfügung, u. a.:

- Negativ- und Positivfilter für Begriffe oder Hashtags;
- Zeitaufgelöste Darstellungen von Daten wie Hashtags oder Posts und deren Kommentare (Timeline);
- Visualisierung von Verbindungen bzw. Verknüpfungen zwischen Nutzer/innen, Gruppen, Hashtags etc.
- Analysefunktionen, um Datensätze aus verschiedenen Quellen nach gemeinsamen Nutzer/innen zu durchsuchen.

Der typische Ablauf eines ein Ereignis begleitenden Analyseprozesses besteht aus vier Schritten (hier illustriert am Beispiel eines Risikospiels im Fußball):

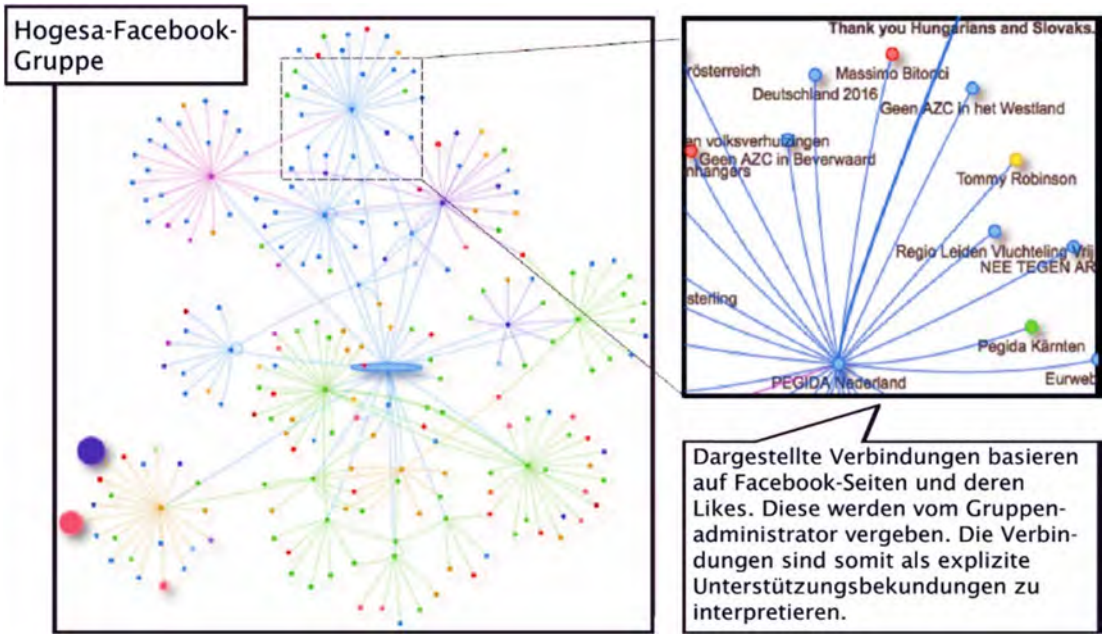
Schritt 1: Exploration

Um die für ein Ereignis potenziell relevanten Internetquellen (Facebook-Gruppen, Twitter-Profile, Foren etc.) zu identifizieren, können Verknüpfungen in

106 Folgende Ausführungen basieren auf einer exemplarischen Systembeschreibung des Softwaredemonstrators »Inspectre« der Munich Innovation Labs GmbH, einem kommerziellen Anbieter für OSINT-Lösungen. Die Systembeschreibung wurde durch Dr. Stephan Taing, der die Entwicklung der Analysesoftware in der Munich Innovation Labs GmbH leitet, im Rahmen des Gutachtens von Hempel (2016, S. 83 ff.) verfasst.

sozialen Netzwerken zwischen verschiedenen Gruppen analysiert werden. Dazu wird ein erster Anknüpfungspunkt benötigt, etwa eine Facebook-Gruppe aus der Hooliganszene. Die Software erlaubt sodann die Darstellung der durch Likes auf Gruppenebene verbundenen Facebook-Gruppen oder Entsprechungen in anderen sozialen Medien (Abb. 4.1).

Abb. 4.1 Analyse der Beziehungen zwischen Facebook-Gruppen vor dem Spieltag: Welche Gruppen sind wie vernetzt?



Quelle: Munich Innovation Labs GmbH

Schritt 2: Vorbereitung auf das konkrete Ereignis

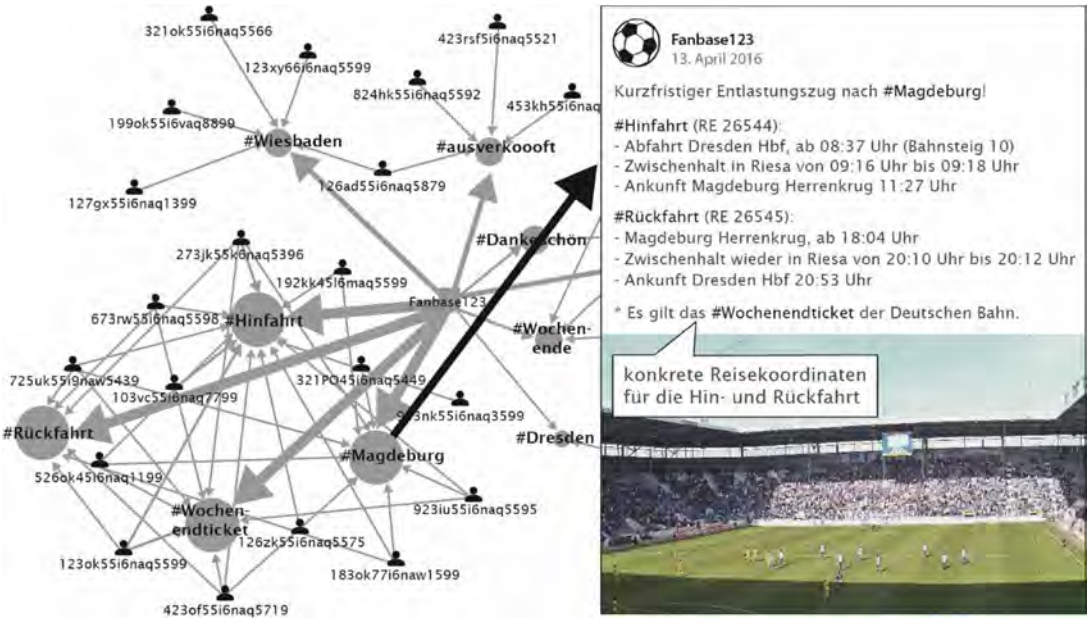
Die Datensätze der als relevant identifizierten Quellen werden heruntergeladen. Diese Grundgesamtheit wird dann verschiedenen Analysen unterzogen. Von Interesse für die Sicherheitsbehörden sind insbesondere

- bestimmende Themen, die durch Schlagwort- und Hashtaganalyse identifiziert werden können;
- Meinungsführer, die durch die Anzahl an Interaktionen ausfindig gemacht werden können;
- verbindende Schlüsselpersonen, die in mehreren Quellen vorkommen und daher von besonderer Relevanz sind;
- Schlüsselorte, die durch Ortserkennung und Kontextanalyse in Erfahrung zu bringen sind.

Schritt 3: während des Ereignisses

Am Tag des Ereignisses werden die Aktivitäten in Echtzeit und mit besonderer Aufmerksamkeit für identifizierte Meinungsführer, Schlüsselpersonen und -orte beobachtet. Ziel dieses Echtzeit-Monitorings sind lagerelevante Informationen, die durch geeignete, von den menschlichen Analysten festzulegende Kriterien herausgefiltert werden. Geeignete Filter können z. B. auf das Aggressionsniveau der Sprache abzielen und nur Nachrichten darstellen, die hinsichtlich dieser Metrik einen gewissen Schwellenwert überschreiten. Auch kann etwa nach konkreten Reiseplänen der einzelnen Fangruppen gesucht werden, was für die Koordination der Einsatzkräfte wichtig sein kann (Abb. 4.2). Der Analyst fasst die als relevant erachteten Informationen zusammen, um damit die Operationsführung zu unterstützen.

Abb. 4.2 Beobachtung von Reisekoordination



Eigene Darstellung nach Munich Innovation Labs GmbH mit Bildmaterial von Goodway (CC-BY-SA-4.0)

Schritt 4: Nachbereitung

Basierend auf den während der Operation aufgetretenen Ereignissen wird in einer Ex-Post-Analyse die Zweckmäßigkeit der gewählten Datenquellen und deren Datenqualität beurteilt, um hierauf aufbauend die Datengrundgesamtheit für das nächste vorzubereitende und zu beobachtende Ereignis anzupassen.

4.2.2 Herausforderungen und aktuelle Entwicklungen

Besteht das Ziel von SOCMINT darin, aus der Fülle an Inhalten und den Dynamiken in den sozialen Medien (und weiteren offenen Internetquellen) nutzbringende Erkenntnisse für die Sicherheitsarbeit abzuleiten, so stellt die große Heterogenität und Volatilität der hier vorliegenden Informationen zugleich die größte Herausforderung für die Entwicklung von robusten Softwarelösungen zur (teil)automatisierten Erfassung und Auswertung solcher Inhalte dar. Soziale Medien generieren nicht immer Informationen bestimmter vergleichbarer Kategorien (z. B. Angaben zu Reiseplänen; Abb. 4.2), vielmehr verändern sich der Inhalt und Kontext der Informationen ständig in Abhängigkeit der Nutzerinteressen und Ereignisse. Auch Quantität und Qualität der Daten sind infolge von Anpassungen (z. B. in Bezug auf die Nutzungsbedingungen) und von technischen Neuerungen (z. B. neue Datenformate) durch die Betreiber der Dienstleistungen einem kontinuierlichen Wandel unterworfen.

Vor dem Hintergrund dieser Herausforderungen wird derzeit intensiv an der Weiterentwicklung entsprechender softwaregestützter Lösungen gearbeitet. Dies betrifft sowohl Prozesse der Datenerfassung und visuellen Aufbereitung als auch die Erarbeitung von Modellen und Analysemethoden zur automatisierten Früherkennung sicherheitsrelevanter Entwicklungen in den Daten. Die Aktivitäten in diesem Feld werden auch im Rahmen der zivilen Sicherheitsforschung des Bundes gefördert, wobei sich hier das Interesse ebenso auf mögliche Auswirkungen solcher Instrumente auf die Gesellschaft und die polizeiliche Arbeit richtet. Exemplarisch seien folgende Projekte genannt:

- Integration vernetzter Daten und prädiktive Analyse zum Schutz vor organisierter Kriminalität (LIDAKRA; Laufzeit 2015 bis 2018):[107] Ziel war es, ein Softwaresystem zu entwickeln, das in einem Verdachtsmoment offene Internetquellen teilautomatisiert durchsuchen und Suchergebnisse zusammenführen kann, um sie mit Tatbeständen der organisierten Kriminalität in Zusammenhang zu bringen. Das Projekt wurde im Januar 2018 mit der Präsentation eines Softwaredemonstrators abgeschlossen. Laut Auskunft des Bundes Deutscher Kriminalbeamter (BDK 2018), der am Projekt beteiligt war, besteht Interesse an einer Fortentwicklung des Softwaredemonstrators.
- Visuelle Entscheidungsunterstützung bei der Auswertung von Daten aus sozialen Netzwerken (INTEGER, Laufzeit 2017 bis 2020):[108] Ziel des Projekts ist es, Anforderungen an eine rechtskonforme, ethisch vertretbare und anwenderfreundliche Softwareplattform zur Unterstützung von Sicherheitsbehörden zu definieren und in einem Leitfaden für die automatisierte Analyse und visuelle Darstellung von Daten zusammenzuführen.

107 https://www.sifo.de/sifo/shareddocs/Downloads/files/projektumriss_lidakra-1.pdf (31.3.2022)
108 https://sifo.bmbfcluster.de/files/Projektumriss_INTEGER.pdf (31.3.2022)

- Analyse extremistischer Bestrebungen in sozialen Netzwerken (X-SONAR; Laufzeit 2017 bis 2020):[109] Es soll die Entwicklung von Radikalisierungsprozessen in sozialen Medien, Blogs und Internetforen untersucht werden, um Radikalisierungsmuster zu identifizieren und Indikatoren zur Früherkennung radikaler Tendenzen zu erarbeiten. Eine spezielle Software soll die Erkennung extremistischer Netzwerkstrukturen und die Einschätzung individueller und kollektiver Radikalisierungsprozesse ermöglichen.

Ein hohes Interesse vonseiten der Sicherheitsakteure sowie die laufenden Forschungs- und Entwicklungsanstrengungen lassen vermuten, dass solche Softwarelösungen zur Unterstützung der polizeilichen Internetbeobachtung künftig zunehmende Verbreitung finden werden.

4.2.3 Rechtliche Einordnung

Während das Bundesverfassungsgericht bei der manuellen Internetbeobachtung keinen Eingriff in das allgemeine Persönlichkeitsrecht konstatiert (Kap. 4.1.3), kommt es im Fall systematischer Datenerhebungen und -auswertungen zu einer anderen Einschätzung. Demnach kann ein Eingriff in das Recht auf informationelle Selbstbestimmung dann vorliegen, wenn im offenen Internet gewonnene Informationen gezielt zusammengetragen, gespeichert und ggf. unter Hinzuziehung weiterer Daten ausgewertet werden (BVerfG, Urteil vom 27.2.2008, Rn. 309). Dies trifft sicherlich auf die softwaregestützte (teil)automatisierte Erfassung und Auswertung von sozialen Medien und anderen offenen Internetquellen im Rahmen der SOCMINT zu. Insofern hat sich hier die Zulässigkeit zunächst nach den allgemeinen Vorschriften zur Verarbeitung personenbezogener Daten in den jeweiligen Fachgesetzen zu richten (z. B. §§ 477 ff. StPO, §§ 9 ff. BKAG, §§ 45 ff. BDSG).

Allerdings könnten solche Softwaresysteme – in Abhängigkeit der weiteren Entwicklungen in Bezug auf die verwendeten Datenquellen und die Leistungsfähigkeit der Algorithmen – künftig in der Lage sein, die Aussagekraft von vermeintlich harmlosen, frei verfügbaren Daten in solchem Maße zu steigern, dass eigenständige grundrechtliche Risiken für die betroffenen Personen geschaffen werden (Kap. 6.2.3). Mögliche Gefahren sehen etwa die Datenschutzbeauftragten des Bundes und der Länder (DSK 2015) darin, dass Daten aus ganz anderen Zusammenhängen verwendet werden könnten, denen kein gefährdendes oder strafbares Verhalten zugrunde liegt. Bürger/innen könnten sich dann nicht mehr sicher sein, welche ihrer Handlungen von der Polizei registriert und nach welchen Kriterien bewertet werden, zumal diese stets nur auf statistischen Erfahrungswerten beruhen, die im Einzelfall nicht zutreffen müssen. Sind zudem die Kriterien und die Funktionsweise der Algorithmen nicht bekannt, so wäre es den

109 https://sifo.bmbfcluster.de/files/Projektumriss_X-SONAR.pdf (31.3.2022)

Betroffenen auch unmöglich, das Ergebnis mit eigenen Angaben zu widerlegen (DSK 2015). Der Einsatz derart fortgeschrittener Softwaretools im Rahmen der SOCMINT dürfte folglich nicht mehr ohne Weiteres auf bestehende gesetzliche Befugnisse gestützt werden.

Eine eigenständige Rechtsgrundlage für die Anwendung derartiger Softwarelösungen wurde erstmalig 2018 durch den Hessischen Gesetzgeber im Zuge der Einführung der Software Hessendata geschaffen.[110] Demnach erlaubt der neue § 25a HSOG den Einsatz von automatisierten Datenanalysen in begründeten Einzelfällen u. a. zur vorbeugenden Bekämpfung von schweren Straftaten (Katalogstraftaten nach § 100a Abs. 2 StPO). Ob diese Befugnis verfassungsrechtlichen Maßstäben genügt, ist allerdings umstritten. So fordert beispielsweise eine 2019 eingelegte Verfassungsbeschwerde angesichts der hohen Eingriffsintensität komplexer Datenanalysen engere Eingriffsschwellen für den Einsatz entsprechender Softwareprodukte (GGF 2019).

4.3 Ansätze des Predictive Policing

Predictive Policing beschreibt die Anwendung softwarebasierter Methoden, die durch automatisierte Auswertung unterschiedlicher Daten Wahrscheinlichkeitsaussagen über das Auftreten bestimmter Kriminalitätsformen in der Zukunft treffen (entweder raumbezogen für ausgewählte Gegenden oder auch personenbezogen), um solche Straftaten durch geeignete präventive Interventionen zu verhindern (Singelnstein 2018, S. 1). Im deutschen Sprachraum wird auch vorhersehende Polizeiarbeit als Synonym für Predictive Policing genutzt (eine Einführung zu Predictive Policing gibt das TAB-Themenkurzprofil Nr. 9; TAB 2016a).

Die Logik von Predictive Policing weist damit große Parallelen zu den Ansätzen der SOCMINT auf, was eine klare Abgrenzung schwierig macht. Zumindest in Bezug auf die hierzulande eingesetzten Verfahren des Predictive Policing lassen sich dennoch zwei wesentliche Unterschiede feststellen:

- Obgleich nicht immer bekannt ist, welche Daten in die Analysen einfließen, beschränken sich die bislang in Deutschland verwendeten Ansätze des Predictive Policing auf die Auswertung nichtpersonenbezogener Daten (Bundesregierung 2018j, S. 2). Hierbei kann es sich prinzipiell um Daten aus Kriminalitätsstatistiken und anderen polizeilichen Datenbanken (z. B. Ort und Zeit begangener Straftaten), aber auch um geografische und Infrastrukturdaten, soziodemografische Daten oder Wetter- und Ereignisdaten handeln (Singelnstein 2018, S. 2; LKA NRW 2018, S. 15).

110 Artikel 3 Nr. 2j Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen vom 25. Juni 2018 (GVBl. S. 302). Eine vergleichbare Eingriffsnorm ist Ende 2019 auch für die Polizei in Hamburg geschaffen worden (§ 49 Gesetz über die Datenverarbeitung der Polizei vom 12. Dezember 2019, HmbGVBl. S. 485)

- Der Datenverarbeitung und den Wahrscheinlichkeitsprognosen liegen spezifische Theorien zugrunde, die die Kriminalitätsentwicklungen auf Grundlage begrenzter Datenquellen evidenzbasiert erklären können sollen. Ein Beispiel sind kriminologische Modelle zur Bestimmung von Nachfolgetaten (Kap. 4.3.2.1). Vorhersagen werden also regelbasiert generiert und das Zustandekommen von Ergebnissen lässt sich – sofern Transparenz gegeben ist – immer noch nachvollziehen. Gleichzeitig beschränkt dies das Einsatzfeld der jeweiligen Methode auf bestimmte Deliktbereiche.

Die Grenzen zwischen SOCMINT und Predictive Policing sind aber fließend. So gewinnen vor allem in den USA personenbezogene Ansätze des Predictive Policing an Bedeutung, um Risikoprofile für einzelne Personen zu erstellen. Neben Vorstrafen und sonstigen polizeilichen Daten werden hier gerade auch Informationen zum sozialen Umfeld von Personen genutzt, die durch die Auswertung sozialer Medien ermittelt werden (Singelnstein 2018, S. 2). Auch in Kanada läuft ein Projekt, in dessen Rahmen Informationen aus sozialen Medien mit Informationen von Sozialämtern und der Polizei verknüpft werden, um anhand bestimmter Risikofaktoren künftig vermisste Kinder oder auch Personen, die Gefahr laufen, entweder Kriminelle oder Opfer von Straftaten zu werden, zu identifizieren (Stockdale 2019). Bezeichnend ist überdies, dass Predictive Policing schon heute oft im Kontext von Big Data diskutiert wird (Merz 2016). Voraussetzung hierfür sind aber nicht vorhandene kriminologische Modelle, vielmehr sollen hier gerade aufgrund der Größe, Heterogenität und Dynamik der Datenbestände Methoden aus dem maschinellen Lernen zum Einsatz gelangen, um die Modelle erst zu erzeugen, mit denen die jeweiligen Vorhersagen zu erzielen wären.

4.3.1 Einbettung von Predictive Policing in die Polizeiarbeit

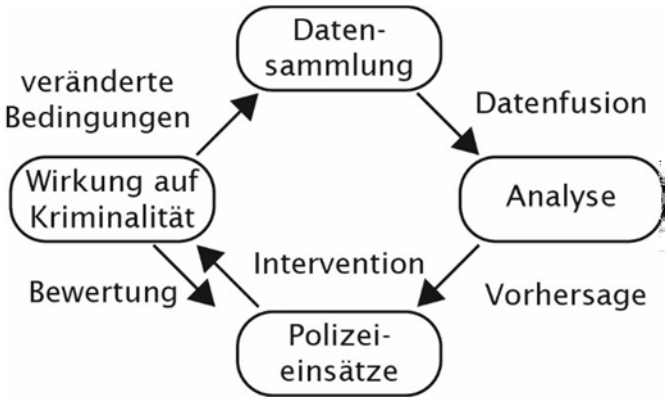
Zu beachten ist, dass das Anliegen, Kriminalität vorherzusagen oder auch Kenntnis von Personen zu haben, von denen entweder eine Gefahr ausgeht oder die Opfer einer Straftat werden könnten, keineswegs neu oder im polizeilichen Kontext überraschend ist. Gefahrenabwehr beinhaltet schon immer einen Vorhersagebedarf, der sich einerseits aus der Aufgabe selbst, andererseits aus den begrenzten Möglichkeiten ergibt, einen Raum etwa durch ständige Polizeipräsenz so zu schützen, dass sich jede denkbare Gefahr verhindern lässt.

Folgerichtig wird Predictive Policing auch unter dem weiter gefassten Paradigma der erkenntnisgestützten Polizeiarbeit (Intelligence Based Policing) verortet (Saunders et al. 2016), das in den 1990er Jahren in den USA entwickelt wurde und inzwischen weite Verbreitung bis in den Bereich der Grenzkontrolle gefunden hat. Nach Ratcliffe (2005, S. 438 f.) zeichnen sich erkenntnisgestützte Polizeistrategien durch drei Aspekte aus: erstens müssen die gesammelten Informationen interpretiert, zweitens muss auf Grundlage dieser Interpretation auf die jeweiligen organisationalen Entscheidungsprozesse eingewirkt und drittens

müssen die Strategien so eingesetzt werden, dass Kriminalität reduziert werden kann. Das entscheidende Merkmal ist, dass die datentechnisch gewonnenen Erkenntnisse zur Entscheidungsfindung eingesetzt werden, um Polizeiarbeit zu priorisieren und so Kriminalität durch einen effektiveren und effizienteren Ressourceneinsatz zu bekämpfen. Dahinter stehen insofern auch ökonomische Abwägungen, den Personaleinsatz durch Technisierung so zu steuern, dass Ressourcen eingespart werden können.

Predictive Policing umfasst somit stets beide Elemente: zum einen eine Prediktionsstrategie in Form theoretisch informierter Vorhersagemodelle und zum anderen eine Präventionsstrategie in Form konkreter polizeilicher Maßnahmen, die auf Erstere aufbauen (Egbert 2018, S. 247). Sind beide Seiten je für sich zu betrachten, nämlich zum einen im Hinblick auf die Güte der datentechnisch generierten Voraussagen und zum anderen im Hinblick auf die Wirksamkeit der konkreten polizeilichen Präventionsmaßnahme, so lassen sich Aussagen über den Nutzen von Predictive Policing erst treffen, wenn gleichzeitig das Zusammenspiel der Datensammlung und -analyse sowie der daran anknüpfenden Polizeieinsätze und ihre Wirkung auf die Kriminalität bewertet werden (Abb. 4.3).

Abb. 4.3 Phasen des Predictive Policing



Eigene Darstellung nach Perry et al. 2013, S. 12

Darüber hinaus besteht ein zweiter Strang der Entwicklung in der räumlichen Darstellung analysierter Daten. Auch hier wird an traditionelle polizeiliche Praktiken angeschlossen, allen voran der Kriminalitätskartierung von Tatorten und der Bestimmung mit Stecknadeln auf Stadtplänen, wo sich die Verbrechen konzentrieren. In Ergänzung zu Ortskenntnissen und Streifenerfahrung bilden Regressionsanalysen der Kriminalitätsdaten und entsprechende Extrapolationen in die Zukunft eine der Methoden, die Wahrscheinlichkeit von Kriminalität zu bestimmen und durch die Ausweisung sogenannter Schwerpunkte auch bis in die öffentliche Wahrnehmung hinein zu markieren. Hier ermöglicht es die Nutzung von Geoinformationssystemen (GIS) die kriminalistische Fallanalysen mit geografischen

und weiteren Informationen (bis hin zu Daten aus sozialen Medien) zu verbinden, um angesichts einer dynamisch sich ändernden Umwelt ein situatives Lagebild herzustellen und die Voraussagen entsprechend auch zu visualisieren.

4.3.2 Anwendungsbeispiele für die Nutzung von Predictive Policing

Heute werden in zahlreichen US-amerikanischen Städten, aber auch in Kanada, Großbritannien oder der Schweiz unterschiedliche softwarebasierte Verfahren des Predictive Policing durch Polizeibehörden eingesetzt oder zumindest erprobt. In Deutschland werden entsprechende Softwarelösungen durch einige Landeskriminalämter entwickelt, getestet oder bereits angewendet (Tab. 4.1), bislang aber nicht durch die Polizeibehörden des Bundes (Bundesregierung 2018j, S. 2).

Tab. 4.1 Einsatz von Verfahren des Predictive Policing bei Landespolizeien (Stand Mitte 2018)

Bundesland/Stadt	seit	Software
Bayern	2015	PRECOPS
Baden-Württemberg	2015 (Probebetrieb)	PRECOPS
Berlin	2016 (Probebetrieb)	KrimPro (Eigenentwicklung)
Brandenburg	geplant	PRECOPS
Hessen	2016	KLB-operativ (Eigenentwicklung)
Niedersachsen	2017 (Probebetrieb)	PreMAP (Eigenentwicklung)
Nordrhein-Westfalen	2015 (Probebetrieb)	SKALA (Eigenentwicklung)

Quellen: Knobloch 2018, S. 14 f.; Singelnstein 2018, S. 1; Hessische Landesregierung 2016; Niedersächsisches Ministerium für Inneres und Sport 2018; Landesregierung Brandenburg 2018; LKA NRW 2018, S. 10; Der Senat von Berlin 2017a

Im Fokus der Anwendungen steht hierzulande bislang die Bekämpfung des Wohnungseinbruchsdiebstahls. Ein Grund für die Fokussierung auf dieses Kriminalitätsphänomen könnte die teilweise intensiv geführte Debatte um einen starken Anstieg des Wohnungseinbruchsdiebstahls sein (Egbert 2018, S. 244). Das »Pre Crime Observation System« (PRECOBS), das die Wahrscheinlichkeit von Wohnungseinbrüchen in bestimmten, räumlich abgrenzbaren Gebieten voraussagen soll, ist die in Deutschland am häufigsten genutzte Prognosesoftware, gefolgt von

einer Reihe von polizeilichen Eigenentwicklungen wie die »Kriminalitätsprognose Wohnraumeinbruch« (KrimPro), das »Predictive Policing Mobile Analytics for Police« (PreMAP) oder das »System zur Kriminalitätsauswertung und Lageantizipation« (SKALA) (Knobloch 2018, S. 14 f.).

Ausgehend von den jeweiligen theoretischen Konzepten werden im Folgenden einige Beispiele für Vorhersagesoftware vorgestellt und – soweit dies anhand von Evaluation und Studien machbar ist – im Hinblick auf ihre Wirkungen diskutiert.

4.3.2.1 Theoretische Grundlagen aktueller Verfahren

Heute eingesetzte Verfahren des Predictive Policing basieren in der Regel auf einem oder mehreren der folgenden kriminologischen Konzepte.

Near-repeat-Hypothese

Die Grundidee der vor allem in Deutschland eingesetzten Prognosesoftware wie »PRECOBS« oder »PreMAP« zur Bekämpfung des Wohnungseinbruchsdiebstahls fußt auf der Near-repeat-Hypothese, die in mehreren wissenschaftlichen Studien bestätigt wurde. Sie besagt, dass im unmittelbaren Umfeld eines bereits erfolgten Einbruchs in der nahen Zukunft mit einem oder mehreren Folgedelikten (»near repeats«) zu rechnen ist. Insbesondere professionell organisierte Wohnungseinbrecher weisen offenbar eine ausgeprägte Delikttreue auf (Schweer 2015). »PRECOPS« definiert als Near-repeat-Areal das Gebiet im Umkreis von 500 Metern vom initialen Ereignis und setzt einen Zeitraum von 7 Tagen für das Eintreten von Folgetaten an (Gerstner 2017, S. 25). Neben Tatort und -zeit entscheiden katalogisierte Deliktmerkmale wie Modus Operandi und Beute, ob ein Alarm ausgelöst wird oder nicht (Schweer 2015). Wenn die Art des Einbruchs oder auch die Beute vom Muster professioneller Wohnungseinbrecher abweichen, sinkt also die Wahrscheinlichkeit und es wird kein Alarm ausgelöst.

Nachbebenvorhersage

Eine mit der Near-repeat-Hypothese vergleichbare Theorie liegt der Nachbebenvorhersage zugrunde. Sie findet insbesondere in dem in den USA genutzten System »PredPol« Anwendung. Ausgangspunkt bildet die Beobachtung, dass kriminelle Handlungen – vergleichbar zu Nachbeben bei großen Erdbeben – zeitliche Folgewirkungen zeigen. So wirken ortsgebundene Straftaten wie Wohnungseinbrüche, Bandengewalt, Autodiebstahl oder Körperverletzung als punktförmige Hintergrundereignisse (Bennett Moses/Chan 2018, S. 808), die wiederum Nachbeben unterschiedlicher Art und Schwere in unmittelbar räumlicher und zeitlicher Nähe nach sich ziehen. Im Unterschied zum Near-repeat-Muster kann

der Delikttyp hier also variieren. Der Algorithmus von »PredPol« erstellt eine eintägige Vorhersage der Kriminalitätsrate an verschiedenen Orten einer Stadt auf Grundlage von bestimmten, zuvor erfassten Verbrechen wie Einbruch, Entwendung von Kfz, Diebstahl aus Kfz oder Raub und bereitet diese mithilfe von Geoinformationssystemen für die Einsatzplanung auf (Hunt et al. 2014). Die Gebiete mit den höchsten prognostizierten Kriminalitätsraten werden als Hotspots in Form von Planquadraten gekennzeichnet.

Analyse von räumlich-zeitlichen Mustern

Greifen die zuvor genannten Ansätzen nur auf phänomenspezifische Falldaten aus polizeilichen Vorgangserfassungssystemen zurück (z. B. Delikttyp, -ort und -zeitpunkt, Beute), ziehen komplexere Vorhersagemodelle weitere Datenquellen heran, um Risikogebiete vorherzusagen. Hierzu zählen z. B. (Perry et al. 2013, S. 44 f.; Singelnstein 2018, S. 2):

- Wetter- und saisonale Daten;
- Ereignisdaten, z. B. zeitliche Nähe zu Sport- oder Kulturveranstaltungen, Terminen von Gehaltszahlungen;
- geografische und Infrastrukturdaten, z. B. Struktur der Nachbarschaft, räumliche Nähe zu Straßen, Einkaufzentren, Gaststätten, Schulen etc., Verkehrsanbindung und -aufkommen;
- demografische und sozioökonomische Daten, z. B. Einwohnerstruktur, Alter, Bildung, Kaufkraft.

Solche Vorhersagemodelle gelangen heute vorrangig in den USA zum Einsatz. Ihnen liegt die Überlegung zugrunde, dass Kriminalitätsmuster durch unterschiedliche zeitliche und räumliche Faktoren beeinflusst werden (Singelnstein 2018, S. 2). Von den in Deutschland genutzten Verfahen bezieht soweit bekannt nur SKALA des Landeskriminalamts Nordrhein-Westfalen neben polizeilichen Vorgangsdaten weitere Datenquellen ein, so u. a. soziodemografische und gebäudespezifische Daten (z. B. Einwohnerstruktur, Kaufkraft, Verkehrsanbindung) (LKA NRW 2018, S. 15).

Risikolisten

Die Analyse von geografischen Daten in Verbindung mit personenbezogenen Informationen u. a. zu Straftaten, Gangmitgliedschaften, Arbeitslosigkeit, Alkohol- und Drogenproblemen, Wohnort, Geschlecht bilden die Grundlage für Risikolisten (Heat Lists), anhand derer analysiert wird, welche Personen künftig Täter oder Opfer einer Straftat werden könnten. Im Unterschied zu den zuvor beschriebenen raumbezogenen Ansätzen handelt es sich hierbei also um eine personenbezogene Herangehensweise. Bekannt wurden Risikolisten insbesondere durch das Prädiktionsprogramm des Chicago Police Department (CPD), das 2013 mit

einem Pilotprojekt startete und inzwischen ein wesentlicher Baustein der prädiktiven Strategie zur Verbrechensbekämpfung des CPDs bildet (City of Chicago 2017). Das vom Illinois Institute of Technology entwickelte Modell baut zunächst auf soziologischen Untersuchungen zu Zusammenhängen zwischen Mordopfern und ihren sozialen Beziehungen auf (dazu und zum Folgenden Saunders et al. 2016, S. 354 ff.). Auf Basis von Verhaftungsdaten wird durch einen Algorithmus das relative Risiko abgeschätzt, dass eine Person zu einem Mordopfer wird oder in einen Mord involviert werden könnte und zwar – soweit bekannt – anhand der Anzahl seiner Verbindungen zu Personen, mit denen diese zuvor inhaftiert war und die später zu einem Mordopfer wurden, sowie zu Personen, die mit anderen Personen verhaftet wurden, die ihrerseits mit einem späteren Mordopfer verhaftet wurden. Der Algorithmus ermittelt den Risikowert pro Person (»heat score«) und erstellt eine Liste von Personen (»persons of interest«), die gemäß der Berechnung eine erhöhte Wahrscheinlichkeit aufweisen, Opfer oder Täter eines Gewaltverbrechens zu werden. Unter Heranziehung weiterer polizeilichen Erkenntnisse u. a. aus der Beobachtung von sozialen Medien bilden diese dann die Grundlage für unterschiedliche Präventionsmaßnahmen, wie z. B. eine Kontaktaufnahme in Fällen von verdächtigem Verhalten bei identifizierten Personen.

4.3.2.2 Herausforderungen und Ergebnisse erster Evaluationen

Ausgangspunkt der aktuell eingesetzten Vorhersagesysteme bildet meist die Annahme rational agierender Akteure, die bekannten Verhaltensmustern folgen und – bevor sie zur Tat schreiten – ihr Entdeckungsrisiko bzw. ihre Erfolgschancen bewerten (TAB 2016a, S. 2 f.). Scheinen diese Rahmenbedingungen für geplante Delikte wie Diebstahl oder Einbruch noch plausibel, ist bei anderen Straftaten und insbesondere bei Gewalttaten, die häufig aus dem Affekt heraus begangen werden, zumindest anzuzweifeln, ob sie als berechenbare und damit vorhersagbare Prozesse verstanden werden können. Aber auch bei geplanten Straftaten dürften zeitlich und räumlich veränderte Bedingungen zu Abweichungen im jeweiligen Tatablauf führen, was eine Vorhersage generell schwierig macht.

Darüber hinaus können durch das Predictive Policing angeleitete Strategien und Taktiken der Polizeiarbeit unter Umständen auch Wirkungen entfalten, die nicht zur Reduktion, sondern zur räumlichen Verdrängung von Kriminalität und/oder zu taktischen Anpassungen im Täterverhalten führen (Rolfes 2017, S. 61). Kriminalitätsmuster entstehen und verändern sich gerade auch aufgrund von Polizeiarbeit, was nicht nur die grundsätzliche Erkennbarkeit von konkreten kriminellen Handlungen, sondern insbesondere deren Voraussage erschwert. Schließlich sind auch mögliche Rückkoppelungseffekte aus der Verbindung von Prognosen und Präventionsstrategien zu beachten: Wenn der Einsatz von Vorhersagesoftware beispielsweise zu einer unverhältnismäßigen Fokussierung auf

bestimmte Räume und Gruppen führt, könnten andere, mindestens ebenso gefährdete Räume und Gruppen möglicherweise aus dem Blickfeld der Polizei geraten. Dies hätte dann auch Auswirkungen auf die Datenbasis für die Vorhersagen (etwa weil durch eine verminderte Streifentätigkeit in den vernachlässigten Gebieten das Dunkelfeld, also die Zahl der polizeilich nicht registrierten Delikte, vergrößert wird), was wiederum die Fixierung der Aufmerksamkeit auf bestimmte Orte und Personengruppen weiter verstärken könnte. In diesem Kontext ist zu beachten, dass polizeiliche Vorgangsdaten die Realität von Kriminalität nie vollständig abbilden können (Knobloch 2018, S. 6). Generell stellt sich somit die Frage, ob bzw. wie Straftaten überhaupt objektiv beschreibbar sind, damit sie zum Gegenstand von datenbasierter Prädiktion werden können.

Vor diesem Hintergrund lassen sich heute gängige Vorhersagesysteme grundsätzlich in zwei Kategorien einteilen:

- Systeme, die beanspruchen, ein breites Spektrum krimineller Handlungen in einem bestimmten Raum vorauszusagen, und
- Systeme, deren Vorhersagen sich auf Straftaten eines bestimmten Delikttyps wie Wohnungseinbrüche oder schwere Straftaten beziehen.

Zur ersten Kategorie gehört insbesondere das in den USA genutzte PredPol, dem die Theorie der Nachbebenvorhersage zugrunde liegt: Unabhängig vom Delikttyp folgen aus einer begangenen Straftat eine oder mehrere andere. Je breiter das Deliktfeld ist, desto höher also ist die Eintrittswahrscheinlichkeiten für Folgetaten. Mit allen Konsequenzen für den konkreten Einsatz bleibt unbestimmt, mit welcher Art von Kriminalität gerechnet werden muss. Wenngleich innerhalb des softwaretechnisch als riskant ermittelten Gebiets, so entscheidet hier – wie bei klassischer Streifentätigkeit auch – letztlich der polizeilich geübte Blick über Verdachtsanlass und Intervention. Es stellt sich also grundsätzlich die Frage, ob es sich hierbei überhaupt noch um eine Vorhersage handelt. Bezeichnend ist, dass erste städtische Polizeibehörden, die die Software angewendet haben, den Einsatz bereits wieder beendet haben und sich wieder auf die Erfahrungen und Kenntnisse von Streifenbeamten verlassen (BondGraham 2015).

Vorhersagesysteme der zweiten Kategorie konzentrieren sich in der Regel auf einen bestimmten Delikttyp, dessen Muster auf die eine oder andere Weise plausibel erklärt werden kann. Alle in Deutschland derzeit eingesetzten Verfahren gehören dieser Kategorie an, wobei hierzulande die Bekämpfung der Wohnungseinbruchskriminalität im Fokus steht. Bisher allerdings konnten noch keine wissenschaftlich-empirisch belastbaren Belege für eine kriminalitätsmindernde Wirkung des Einsatzes solcher Verfahren gefunden werden. Hier aufschlussreich sind insbesondere die beiden umfänglichen Evaluationen zum Probebetrieb von PRECOBS in Baden-Württemberg durch das Max-Planck-Institut für ausländisches und internationales Strafrecht (Gerstner 2017) sowie von SKALA in

Nordrhein-Westfalen durch das hiesige Landeskriminalamt und die Gesellschaft für innovative Sozialforschung und Sozialplanung e. V. (LKA NRW 2018).

Im Pilotprojekt in Baden-Württemberg wurde PRECOBS im Gebiet der Polizeipräsidien Stuttgart und Karlsruhe getestet, der Evaluationszeitraum erstreckte sich über 6 Monate im Winterhalbjahr 2015/2016 (dazu und zum Folgenden Gerstner 2017, S. 85 ff.). Die Evaluation gelangte zu dem Ergebnis, dass kriminalitätsmindernde Effekte wahrscheinlich nur in einem moderaten Bereich liegen und die Fallzahlen allein durch den Einsatz von PRECOBS nicht deutlich reduziert werden konnten. Zwar konnten Indizien für eine Wirksamkeit gefunden werden (in den als »Near-repeat-Arealen definierten Gebieten wurde eine rückläufige Anzahl von Folgedelikten festgestellt), gleichzeitig aber nahm die Gesamtzahl der Wohnungseinbrüche in manchen Gebieten ab (z. B. in Stuttgart), in anderen aber auch zu (z. B. Stadt Karlsruhe). Generell war es nicht möglich, die Entwicklung der Fallzahlen eindeutig auf den Einsatz von PRECOBS zurückzuführen.

In Nordrhein-Westfalen wurde der Einsatz von SKALA im Zeitraum von Mai 2015 bis November 2017 evaluiert, wobei zunächst nur die Kreispolizeibehörden Duisburg und Köln in das Projekt SKALA einbezogen waren und die Kreispolizeibehörden Düsseldorf, Essen und Gelsenkirchen erst ab Januar 2017 hinzukamen. Auch hier konnten keine statistisch belastbaren Ergebnisse gefunden werden, die auf eine Wirkung von SKALA auf die Kriminalitätsentwicklung beim Wohnungseinbruchdiebstahl hindeuten (LKA NRW 2018, S. 34 und 137).

Es ist allerdings zu betonen, dass wissenschaftliche Wirkungsnachweise für Verfahren des Predictive Policing methodisch schwierig zu führen sind. Besondere Herausforderungen bestehen u. a. in der Kontrolle von externen Einflussfaktoren, die ebenfalls Auswirkungen auf die Kriminalitätsentwicklung haben, etwa das Wetter, soziodemografische Faktoren, verändertes Täterverhalten, Wanderungsbewegungen professionell agierender Tätergruppen oder auch andere polizeiliche Maßnahmen (Knobloch 2018, S. 28). Bei den genannten Evaluationen in Baden-Württemberg und Nordrhein-Westfalen waren außerdem die Evaluationszeiträume kurz und die Evaluationsgebiete klein, sodass es aufgrund der geringen Fallzahl schwierig war, potenzielle Effekte des Predictive Policing von zufälligen oder durch externe Faktoren verursachte Schwankungen zu trennen. Schließlich müssen wie bereits erwähnt die softwarebasierten Vorhersagen und die daran anknüpfenden polizeilichen Präventionsstrategien immer im Zusammenhang betrachtet werden. Gründe für ggf. ausbleibende Wirkungen können daher falsche oder unpräzise Prognosen, eine Missdeutung oder Missachtung der Prognosen durch die involvierten Polizeibeamten und/oder eine mangelnde Wirksamkeit der daran anknüpfenden Präventionsstrategien sein (Kriminologisches Forschungsinstitut Niedersachsen 2016, S. 4). Vor diesem Hintergrund sind die Ergebnisse der Wirkungsevaluationen mit Vorsicht zu interpretieren, zugleich besteht noch substanzieller Forschungsbedarf.

4.3.2.3 Ausblick

Bei den derzeit in Deutschland eingesetzten Systemen werden – soweit bekannt – bislang keine personenbezogenen Daten, sondern vor allem Falldaten aus den polizeilichen Vorgangserfassungssystemen eingesetzt, die ggf. durch geografische, infrastrukturelle und soziodemografische Informationen ergänzt werden. Gleichzeitig kann, wie die Beispiele in den USA oder Kanada zeigen, erwartet werden, dass weiterentwickelte Verfahren künftig auch personenbezogene Daten einbeziehen könnten, etwa durch die Kombinationen von Verfahren bzw. Methoden der SOCMINT und des Predictive Policing.

Das Beispiel des Saskatchewan Police Predictive Analytics Lab (SPPAL) in Kanada verdeutlicht in besonderer Weise, in welche Richtungen die aktuelle Entwicklung geht. Es versteht sich selbst als ein operatives Laboratorium mit dem Ziel »die Kapazität zu erhöhen, große Mengen von Polizei- und sicherheitsrelevanten Daten zu integrieren, um prädiktive Modelle und Instrumente zu entwikkeln, die die Polizei- und Partnerbehörden in die Lage versetzen, Risiken für einzelne Personen durch Interventionen zu verringern und so Gemeindesicherheit zu fördern« (TAB-Übersetzung; nach Stockdale 2019, S. 4). Im Rahmen einer Partnerschaft zwischen der Polizei, dem Justizministerium der Provinz und der Universität von Saskatchewan wird ein Verfahren entwickelt, das neben polizeilichen Informationen und historischen Vermisstendaten künftig auch Posts aus sozialen Medien sowie Informationen der Sozialdienste analysieren soll. Ziel ist es, auf Basis von unterschiedlichen Risikofaktoren bei Kindern, die beispielsweise durch häufiges Weglaufen von zu Hause oder auch im Zusammenhang mit häuslicher Gewalt gegenüber den Sozialbehörden oder der Polizei auffällig geworden sind, Vorhersagen zu treffen, ob sie künftig als vermisst gemeldet werden könnten.

4.3.3 Rechtliche Einordnung

Die rechtliche Einordnung von Verfahren des Predictive Policing ist weitgehend ungelöst (dazu und zum Folgenden Hempel/Rehak 2017, S. 124 f.). Soweit die Analyse nur nichtpersonenbezogene Daten einbezieht, liegt der Schluss nahe, dass sie sich außerhalb des grund- und fachrechtlichen Datenschutzes befindet. Dementsprechend wird in der Praxis davon ausgegangen, dass es keiner besonderen gesetzlichen Ermächtigungen für solche Analysen bedarf. Jedoch könnte diese Schlussfolgerung aus mindestens zwei Gründen zu kurz greifen: Erstens besteht, wie in anderen Anwendungsfeldern komplexer Datenverarbeitung auch, die prinzipielle Möglichkeit, aus nichtpersonenbezogenen Daten durch die Verknüpfung mit weiteren (erreichbaren) Daten Informationen über einzelne Personen abzuleiten. So geht es beim Predictive Policing beispielsweise gerade darum, Orte höherer Kriminalitätsbelastung mit möglichst hoher räumlicher Auflösung vorherzusagen. Werden hierbei etwa einzelne Grundstücke markiert, so weisen

die als Ergebnis der Analyse erzeugten Daten einen Personenbezug auf, da die Eigentümer der Grundstücke ohne Weiteres identifizierbar sind. Zweitens sind über den grundrechtlichen Schutz personenbezogener Daten hinaus möglicherweise weitere Gewährleistungen zu beachten. So resultieren aus der Kennzeichnung bestimmter Gebiete als »gefährlich« möglicherweise Stigmatisierungs- und Diskriminierungsrisiken, die einen grundrechtlichen Schutzbedarf anzeigen (etwa indem Personen, die solche Gebiete aufsuchen, sich vermehrten verdachtslosen Personenkontrollen ausgesetzt sehen könnten). Darüber hinaus wird die Frage aufgeworfen, wie derartige softwarebasierte Gefährlichkeitseinschätzungen demokratisch legitimiert werden können, wenn eine umfassende Kontrolle durch die polizeilichen Anwender/innen nicht möglich ist, weil die verwendeten Algorithmen aufgrund von Geschäftsgeheimnissen nicht einsehbar sind und/oder deren innere Logik grundsätzlich nicht nachvollziehbar ist (so etwa im Kontext der Verfahren aus dem maschinellen Lernen).

Angesichts der Entwicklungen in den USA oder Kanada dürfte es aber nur eine Frage der Zeit sein, bis Ansätze des Predictive Policing auch hierzulande personenbezogene Daten als Ausgangsdaten in die Analyse einbeziehen. In diesem Fall liegt ein Eingriff in das Recht auf informationelle Selbstbestimmung vor, sodass sowohl Datenerhebung als auch Datenverarbeitung für Zwecke des Predictive Policing rechtfertigungsbedürftig werden (dazu und zum Folgenden Singelnstein 2018, S. 6 f.). Welche verfassungsrechtlichen Maßstäbe dieser Rechtfertigung zugrunde zu legen sind, ist bislang ungeklärt. Sie hängen jedoch jedenfalls von der Eingriffsintensität ab, die bei Verfahren des Predictive Policing unterschiedlich, je nach Art und Umfang der verarbeiteten Daten, des Inhalts und der Aussagekraft der generierten Prognosen und der Streubreite der Datenerfassung jedoch hoch ausfallen kann. So hat das Bundesverfassungsgericht (BVerfG, Beschluss vom 4.4.2006, 1 BvR 518/02) selbst an die technisch vergleichsweise simple und transparente, insbesondere von einem vorgegebenen Suchraster abhängige Rasterfahndung sehr hohe Anforderungen errichtet. Singelnstein (2018, S. 7) folgert daraus, dass eingriffsintensive Formen des Predictive Policing in jedem Fall hinreichend bestimmter Rechtsgrundlagen bedürften, die deren Einsatz eng begrenzten. Maßgebliche Kriterien für eine Konkretisierung des diesbezüglichen Maßstabs wären die Art der verwendeten Daten und der Anlass für die Einbeziehung der jeweiligen Personen, zudem müssten beliebige Auswertungen ohne Anlass und Zweckbestimmung ausgeschlossen sein. Eine nähere Konturierung der Anlässe und Schutzgüter, die verfassungsrechtlich eine prädiktive Analyse rechtfertigen können, steht jedoch noch aus (Bäcker 2019).

5 Informationstechnische Beobachtung

Beschränken sich Maßnahmen der Internetbeobachtung (Kap. 4) auf die Erhebung von Informationen, die im Internet öffentlich oder zumindest für einen nicht weiter abgrenzbaren Personenkreis frei zugänglich sind, richten sich informationstechnische Beobachtungstechnologien auf solche Daten, die eine Person in der berechtigten Erwartung, dass die Informationen vertraulich bleiben, einem informationstechnischen System anvertraut hat. Hierbei handelt es sich um Inhalte der elektronischen Kommunikation (Telefongespräche, E-Mails, Datenströme zwischen vernetzten Geräten etc.) sowie um die Metadaten der Kommunikation, die im Zuge der Nutzung solcher Dienste anfallen (Telefonnummern, IP-Adressen etc.). Dazu gehören aber auch sämtliche Daten, die eine Person auf ihren Endgeräten wie PC, Smartphone oder Smartwatch bewusst oder unbewusst hinterlässt oder speichert.

Im Kontext der zivilen Sicherheit werden informationstechnische Beobachtungstechnologien heute beinahe ausschließlich im polizeilichen Bereich und hier in erster Linie als Werkzeuge der *heimlichen* Informationsbeschaffung im Bereich der Gefahrenabwehr und Strafverfolgung eingesetzt. Gründe für den polizeilichen Bedarf an verdeckten Ermittlungsmaßnahmen wurden in Kapitel 2.5.2 skizziert. Speziell für informationstechnische Beobachtungstechnologien treten zwei weitere Aspekte hinzu (Hempel/Rehak, S. 138):

- Erstens haben sich im Zuge der Digitalisierung der Gesellschaft neue Deliktformen im Bereich der Cyberkriminalität herausgebildet, deren Bekämpfung den Einsatz von informationstechnischen Beobachtungstechnologien in der Regel voraussetzt. Hier stellt die Beschaffung digitaler Informationen oftmals den einzigen Ermittlungsansatz dar.
- Zweitens verändert die Digitalisierung auch die Art und Weise, wie und mit welchen Mitteln konventionelle Straftaten begangen werden. Nutzen kriminelle Akteure für die Planung und Durchführung von Straftaten stets den neuesten Stand der Informations- und Kommunikationstechnik, so muss sich auch das polizeiliche Handeln hieran ausrichten.

Im Bereich der nichtpolizeilichen Gefahrenabwehr finden informationstechnische Beobachtungstechnologien bislang kaum Anwendung. Eine Ausnahme bildet die Standortbestimmung von Mobilfunkgeräten bei Notrufen (Kap. 3.2.3.1) durch die Funkzellenabfrage. Ein gelegentlicher Anwendungsfall ist überdies die Ortung von verschütteten oder vermissten Personen über deren Mobilfunkgeräte durch IMSI[111]-Catcher, wobei hier die Maßnahmendurchführung meist durch die Polizeibehörden erfolgt, da Feuerwehren oder Rettungsdienste weder über eigene

111 Die IMSI ist eine von den Mobilfunkbetreibern einmalig vergebene Identifizierungsnummer, die auf der SIM-Karte gespeichert ist (Kartennummer).

Geräte noch über die entsprechenden rechtlichen Möglichkeiten für deren Einsatz verfügen. Der Fokus dieses Kapitels richtet sich daher auf die polizeilichen Einsatzfelder von informationstechnischen Beobachtungstechnologien zu Zwecken der Gefahrenabwehr und Strafverfolgung.

Dies soll allerdings nicht implizieren, dass es keine nichtpolizeilichen Anwendungsfelder für informationstechnische Beobachtungstechnologien gäbe. So wird beispielsweise im durch die zivile Sicherheitsforschung des Bundes geförderten Forschungsprojekt »Intelligente Rettung in Smart Homes« (IRiS; Laufzeit 2017 bis 2020) aktuell der Frage nachgegangen, inwieweit digitale Informationen aus Smart-Home-Anwendungen die Einsatzkräfte bei der Menschenrettung und Brandbekämpfung unterstützen können. Konkret wird untersucht, welche Daten aus der Haustechnik und aus vernetzten Geräten wie Rauch- oder Brandmelder zu diesem Zweck passend aufbereitet und der Leitstelle sowie den anrückenden Einheiten zur Verfügung gestellt werden könnten. Darauf aufbauend soll ein Konzept erarbeitet werden, das ein effizienteres Handeln der Rettungskräfte auf Basis dieser Informationen ermöglicht.[112] Weitere (potenzielle) Anwendungsfelder finden sich im Bereich der IT-Sicherheit. In der Cyber-Sicherheitsstrategie 2016 der Bundesregierung beispielsweise wird der Ausbau der Sensorik zur Anomalieerkennung im Internet als wirksames Mittel zur Erhöhung der Datensicherheit im Netz bewertet (BMI 2016, S. 24). Hierbei handelt es sich um Sensoren, die an bestimmten Punkten im Internet zur Erkennung von netzbasierten Angriffen eingesetzt werden, wobei Angriffsmuster als Abweichungen vom Normalzustand erkannt und gemeldet werden (BSI/ConSecur GmbH 2002, S. 6 ff.). Bis zu welcher Tiefe die übertragenen Daten analysiert werden, hängt von der jeweiligen Zielstellung, aber auch von der geltenden Rechtslage ab. Werden nicht nur die verbindungsbegleitenden Metadaten (etwa IP-Adressen, Kap. 5.1.1), sondern auch die Inhalte der Datenpakete analysiert, so wird dies auch als Deep Packet Inspection (DPI) bezeichnet. Bei Internetdiensteanbietern ausgeführt ermöglicht es die DPI im Prinzip, Schadsoftware durch gezielte Inhaltsfilterung aus dem Datenstrom zu entfernen, noch bevor Endkunden damit in Kontakt geraten (Bedner 2009, S. 4 ff.).[113] In Deutschland dürfen Diensteanbieter nach geltender Rechtslage jedoch keine Kommunikationsinhalte zu Zwecken der Störungserkennung und -behandlung erheben oder verwenden (§ 100 Abs. 1 Telekommunikationsgesetz – TKG[114]). Das sehr weite Feld der IT-Sicherheit kann im Rahmen dieses Berichts allerdings nicht weiter behandelt werden.

Das Kapitel 5 ist wie folgt aufgebaut: Zum besseren Verständnis der informationstechnischen Beobachtungstechnologien werden in Kapitel 5.1 zunächst

112 www.sifo.de/de/iris-intelligente-rettung-im-smart-home-2376.html (31.3.2022)

113 Einige Staaten sollen die Technologie gemäß Bedner (2009, S. 16 f.) jedoch auch zur staatlichen Beobachtung und Kontrolle des Internetdatenverkehrs nutzen (z. B. Iran, China).

114 Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 1 des Gesetzes vom 29. November 2018 (BGBl. I S. 2230) geändert worden ist

die grundlegenden Infrastrukturen informationstechnisch vernetzter Systeme skizziert. Der Rekurs auf die technische Architektur soll es auch ermöglichen, die enorme Dynamik der technischen Entwicklungen und die damit einhergehenden Veränderungen bei den relevanten Akteuren in diesem Feld zu verdeutlichen. So sind die Möglichkeiten und Herausforderungen der informationstechnischen Beobachtung immer auch vor dem Hintergrund dieses technischen, infrastrukturellen und akteursbezogenen Wandels zu betrachten, etwa wenn staatliche Stellen zunehmend auf Kooperationen mit privaten Akteuren angewiesen sind.

Darauf aufbauend werden in Kapitel 5.2 die Möglichkeiten und Risiken der informationstechnischen Beobachtung aus der technischen Perspektive beschrieben. Solche Beobachtungsmaßnahmen beinhalten meist nicht den Einsatz technischer Artefakte im gewohnten Sinne, sondern die Anwendung von komplexen softwaregestützten Verfahren. Nachfolgend wird deshalb der Begriff informationstechnische Beobachtungsverfahren verwendet.

Kapitel 5.3 behandelt polizeiliche Anwendungsfelder aus der eingriffsrechtlichen Perspektive. Weil informationstechnische Beobachtungsverfahren in aller Regel personenbezogene Daten zum Gegenstand haben, berührt ihre Anwendung zumindest das Recht auf informationelle Selbstbestimmung. Aufgrund des grundrechtlichen Gesetzesvorbehalts bedarf somit jeder polizeiliche Einsatz einer entsprechenden gesetzlichen Ermächtigungsgrundlage.

In Kapitel 5.4 wird schließlich die polizeiliche Einsatzpraxis von informationstechnischen Beobachtungsverfahren beschrieben und die Frage nach dem Nutzen der Maßnahmen für die Polizeiarbeit aufgegriffen. Bereits an dieser Stelle sei jedoch darauf hingewiesen, dass die Datengrundlage aus öffentlich verfügbaren Quellen äußerst schmal ist und Aussagen insofern nur sehr schwer zu treffen sind.

Auch für dieses Kapitel gilt, dass nachrichtendienstliche Eingriffsbefugnisse und Einsatzpraktiken nicht thematisiert werden. Für die Ausführungen in diesem Kapitel stellte das Gutachten von Hempel und Rehak (2017) die wesentliche Grundlage dar.

5.1 Informationstechnisch vernetzte Systeme: Infrastrukturen und Akteure

Eine kursorische Darstellung der Infrastrukturen informationstechnisch vernetzter Systeme und der zentralen Akteure in diesem Feld ist für das Verständnis der in Kapitel 5.2 dargestellten Verfahren der informationstechnischen Beobachtung wesentlich. Als informationstechnisch vernetzte Systeme können im weitesten Sinne alle Geräte und Anwendungen der IKT verstanden werden einschließlich der Telekommunikationsnetze, über welche die Systeme miteinander kommunizieren.

Der Bereich ist von einer enormen Dynamik gekennzeichnet, die spätestens mit der Kommerzialisierung des Internets und der Öffnung der Telekommunikationsmärkte in der zweiten Hälfte der 1990er Jahre ihren Anfang nahm und immer noch anhält. Der Wandel betrifft sowohl die technischen Infrastrukturen und die damit erbrachten Dienste als auch die Akteure, also die Infrastrukturbetreiber und Diensteanbieter sowie die Nutzer/innen und deren Kommunikationsgewohnheiten: Während sich die Fernkommunikation in Deutschland vor 30 Jahren noch weitgehend auf die analoge Sprachtelefonie beschränkte, die durch ein monopolistisch organisiertes und innerhalb nationalstaatlicher Grenzen agierendes staatliches Unternehmen betriebenen wurde, existiert heute eine Vielzahl an funktional unterschiedlichen, vielfach internetbasierten Informations- und Kommunikationsdiensten, die auf stark fragmentierten, wenngleich oftmals weltweit handelnden Anbieter- und Nutzergruppen basieren. Ein zentraler Treiber dieser Dynamik sind technische Entwicklungen im Bereich der Digitalisierung moderner Gesellschaften. Diese wiederum beruhen nicht zuletzt auf der Bereitschaft der Menschen, immer mehr persönliche Daten informationstechnisch vernetzten Systemen anzuvertrauen.

5.1.1 Transformation der Telekommunikationsnetze

Die Signalübertragung in Telekommunikationsnetzen (TK-Netzen) kann auf verschiede Weise erfolgen. In *leitungsvermittelten* TK-Netzen wird für jeden Kommunikationsvorgang eine physische Verbindung zwischen den Teilnehmer/innen aufgebaut, die für die Dauer des Kommunikationsvorganges bestehen bleibt. Das bekannteste Beispiel ist das klassische, ursprünglich primär für die Sprachübermittlung ausgelegte Telefonnetz. In *paketvermittelten* TK-Netzen werden die Informationen hingegen vor der Übertragung in mehrere Datenpakete aufgeteilt und jeweils mit der Absender- und Empfängeradresse ausgestattet. Die Datenpakete gelangen dann über Vermittlungsstellen (Router) zum Empfänger, wobei jedes Paket in Abhängigkeit der Verfügbarkeit und Auslastung der Router einen anderen Weg durch das TK-Netz nehmen kann. Der Vorteil von paketvermittelten TK-Netzen ist deren Robustheit gegenüber Störungen in Teilbereichen des Netzes, da die Datenpakete diese Bereiche einfach umgehen können (InfoTip Service GmbH o.J.). Das bekannteste paketvermittelte TK-Netz ist das Internet, in dem der Datenaustausch nach den Regeln des Internet-Protokolls (IP) erfolgt, weshalb auch von IP-Datenpaketen oder IP-Adressen gesprochen wird.[115]

Die klassischen leitungsvermittelten Telefonnetze, die paketvermittelten TK-Netze für die Datenübertragung im Internet und weitere TK-Netze (z. B. Kabel-

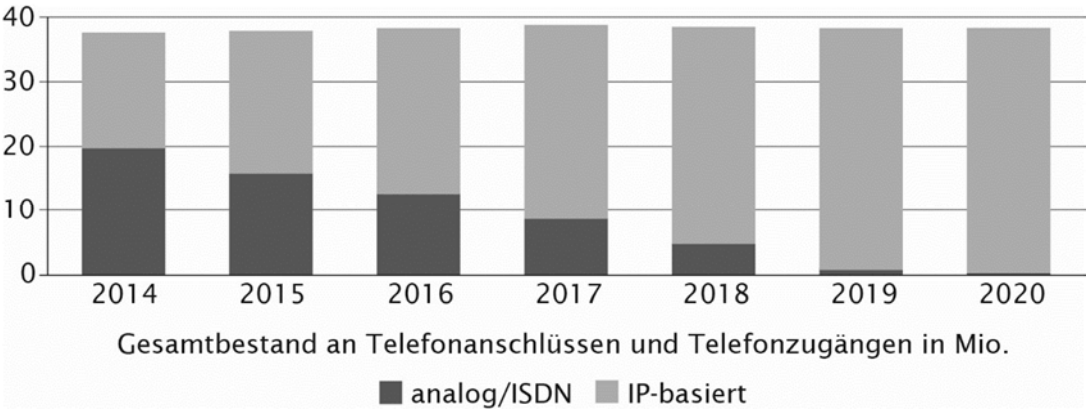
115 Genau genommen handelt es sich beim Internet um einen Verbund vieler unabhängiger Teilnetze (autonome Systeme), die ohne übergeordnete Verwaltung funktionieren, dafür aber alle das Internet-Protokoll als Übertragungsstandard nutzen (Waidner 2014, S. 10 ff.).

fernsehen) wurden lange Zeit parallel zueinander betrieben. Im Zuge der digitalen Transformation und des damit einhergehenden Breitbandausbaus werden die dienstspezifischen Netze allerdings sukzessive durch ein universelles Datennetz ersetzt, über das sämtliche TK-Dienste (Sprache, Bilder/Video, Daten) nach den Regeln des Internet-Protokolls übertragen werden. Kennzeichnend hierfür sind die von den TK-Unternehmen mittlerweile meist standardmäßig angebotenen Bündelprodukte, die auf Grundlage eines Breitbandanschlusses gleichzeitig Internetzugang, IP-basierte Festnetztelefonie (Voice over IP – VoIP), IP-basierter Fernsehempfang und ggf. weitere Angebote wie Clouddienste in einem Vertragsverhältnis bieten (Bundesnetzagentur 2017, S. 23). Dass sich die Umstellung in Deutschland schnell vollzieht, ist beispielsweise an der raschen Verbreitung von IP-basierten Festnetzanschlüssen erkennbar (Abb. 5.1).

5.1.2 Over-the-Top-Kommunikationsdienste

Während früher jeder TK-Dienst sein eigenes Übertragungsnetz hatte, führt die Konvergenz der Netze zu einer Trennung zwischen Dienst und Netz, da nun alle Dienste das universelle IP-basierte TK-Netz für die Datenübertragung nutzen können (Bundesnetzagentur 2017, S. 19). Zugleich werden dadurch neue Dienste ermöglicht, zu deren Verwendung Nutzer/innen lediglich über einen Internetzugang und entsprechende Software auf seinem Endgerät verfügen müssen. Solche Angebote werden in Abgrenzung zu den klassischen TK-Diensten als Over-the-Top-(OTT)-Dienste bezeichnet (Monopolkommission 2015, S. 60 ff.).

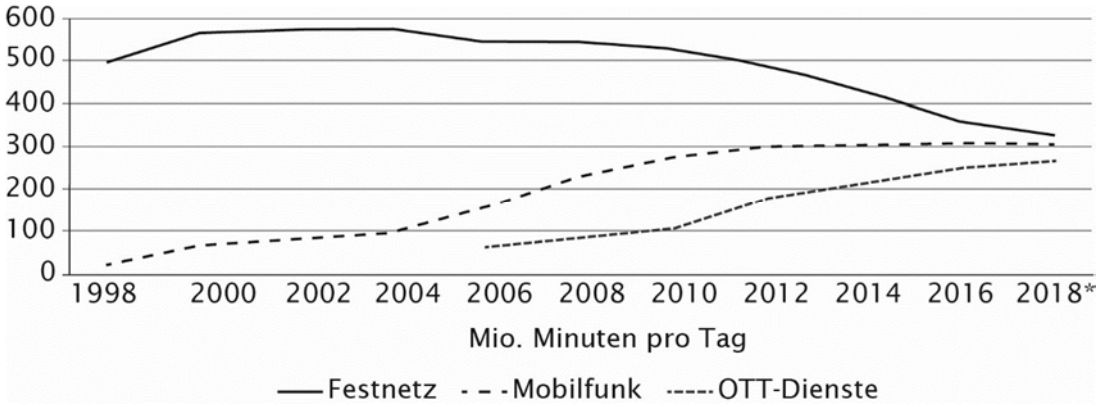
Abb. 5.1 Verteilung zwischen klassischen (analog, ISDN) und IP-basierten Festnetztelefonanschlüssen (VoIP) in Deutschland



Quelle: Bundesnetzagentur (2019, S. 52, 2021, S. 60)

Als OTT-Kommunikationsdienste[116] werden solche Dienste bezeichnet, die mit klassischen TK-Diensten in einer Konkurrenzbeziehung stehen. So wird die klassische SMS zunehmend von Instant-Messaging-Diensten wie WhatsApp oder Telegram Messenger abgelöst, die das Versenden von Kurznachrichten erlauben. Skype, FaceTime, Google Talk etc., die Sprach- bzw. Videoanrufe zwischen den Nutzer/innen dieser Dienste ermöglichen, stehen im Wettbewerb mit der klassischen Sprachtelefonie einschließlich der IP-basierten Festnetztelefonie.[117] Dass klassische TK-Dienste wie SMS oder die Festnetz- bzw. Mobilfunksprachtelefonie gegenüber OTT-Kommunikationsdiensten rasch an Relevanz verlieren, zeigen folgende Zahlen: Wurden 2010 in Deutschland noch täglich über 100 Mio. SMS und nur 1 Mio. WhatsApp-Nachrichten verschickt, waren es 2015 bereits über 660 Mio. WhatsApp-Nachrichten und nur noch knapp 40 Mio. SMS pro Tag (Dialog Consult/VATM 2015, S. 30). Bei der Sprachtelefonie betrug der Anteil der in Deutschland über OTT-Kommunikationsdienste abgewickelten Gesprächsminuten 2006 noch ca. 8 %, 2018 stieg dieser Wert laut Schätzungen von Marktanalysten bereits auf rund 30 % (Abb. 5.2) (Monopolkommission 2015, S. 60 u. 63).

Abb. 5.2 Von Festnetz-, Mobilfunk- und OTT-Anschlüssen abgehende Sprachverbindungsminuten



* Schätzung

Quelle: Dialog Consult und VATM 2018, S. 8

116 In Abgrenzung dazu werden als OTT-Inhaltsdienste solche Dienste bezeichnet, die Inhalte übertragen, z. B. Streamingdienste, soziale Netzwerke, Suchmaschinen oder Onlinehandelsplattformen. Damit ist nicht ausgeschlossen, dass OTT-Inhaltsdienste ebenfalls für Kommunikationszwecke einsetzbar sind (Monopolkommission 2015, S. 60).

117 Viele OTT-Kommunikationsdienste haben ihren Funktionsumfang mittlerweile auf Kurznachrichten, Sprach- bzw. Videotelefonie und Datenübertragung ausgeweitet.

5.1.3 Veränderte Akteurskonstellationen

Mit der Trennung zwischen Dienst und Netz wurde auch die Trennung zwischen Diensteanbieter und Netzbetreiber befördert. Trat vor der Liberalisierung des TK-Sektors in den 1990er Jahren die Deutsche Bundespost noch als alleinige Netzbetreiberin und Diensteanbieterin auf, so sind seitdem zahlreiche Wettbewerber hinzugekommen, die teilweise eigene Netzinfrastrukturen betreiben oder dann im Rahmen der marktlichen TK-Regulierung Komponenten des Netzes von der Deutschen Telekom AG anmieten (Stichwort letzte Meile).[118] Umsätze auf dem Endkundenmarkt erwirtschaften diese Unternehmen mit klassischen TK-Diensten (Telefondienste, SMS, Internetzugang), wobei mit den Erlösen der Netzausbau und -betrieb bzw. die Gebühren für die Nutzung fremder TK-Netze finanziert werden.

Dieses Geschäftsmodell gerät durch das Aufkommen von OTT-Kommunikationsdiensten allerdings zunehmend unter Druck (dazu und zum Folgenden Monopolkommission 2015, S. 62). Die Anbieter von OTT-Kommunikationsdiensten profitieren davon, dass sie ihre Leistungen ohne eigene bzw. angemietete fremde Netzinfrastrukturen anbieten können. Dadurch können sie ihre Leistungen unentgeltlich (in diesem Fall basiert das Geschäftsmodell in der Regel auf Onlinewerbung) oder dann im Vergleich zu klassischen TK-Diensten zu viel niedrigeren Kosten bereitstellen. Zwar könnten auch klassische TK-Unternehmen versuchen, eigene OTT-Kommunikationsdienste anzubieten, um nicht zu reinen Internetdienstanbietern zu werden. Dazu allerdings müsste es ihnen gelingen, in größtenteils bereits besetzte Märkte einzudringen (Bundesnetzagentur 2017, S. 22). Eine weiterhin anhaltende starke Ausbreitung von OTT-Kommunikationsdiensten vorausgesetzt, dürfte der TK-Sektor in Zukunft aus den folgenden drei wesentlichen Akteursgruppen bestehen (Monopolkommission 2015, S. 61):

- Endkunden, die Internetzugänge und OTT-Kommunikationsdienste nachfragen;
- Anbieter von OTT-Kommunikationsdiensten;
- Internetzugangsanbieter, die den technischen Zugang für Endkunden und OTT-Diensteanbieter bereitstellen und die Netzinfrastruktur betreiben.

5.1.4 Implikationen für die Anwendung von informationstechnischen Beobachtungsverfahren

Mit Blick auf die Anwendung von informationstechnischen Beobachtungsverfahren für zivile Sicherheitsaufgaben stellen die beschriebenen technischen und

118 Reseller verzichten ganz auf eigene TK-Netze und kaufen die gesamte Transportleistung bei der Telekom AG ein.

akteursbezogenen Veränderungen im TK-Sektor die Polizei- und Strafverfolgungsbehörden vor diverse Herausforderungen (dazu und zum Folgenden Hempel/Rehak 2017, S. 59 ff.). So führte bereits die Aufhebung des Staatsmonopols in den 1990er Jahren dazu, dass staatliche Stellen fortan in der Regel auf die Kooperation der privaten TK-Unternehmen angewiesen waren, um im Bedarfsfall sicherheitsrelevante Kommunikationsdaten erheben zu können. Diese Zusammenarbeit wurde bzw. wird mit legislativen Mitteln technisch und organisatorisch durchgesetzt, namentlich durch die einschlägigen Vorschriften im Telekommunikationsgesetz.

Aus Sicht der Polizei- und Strafverfolgungsbehörden größere Schwierigkeiten bereitet jedoch die rasante Ausbreitung von OTT-Kommunikationsdiensten, da die ggf. sicherheitsrelevanten Kommunikationsdaten nun zu immer größeren Anteilen bei den Anbietern dieser Dienste beschafft werden müssen. Doch im Unterschied zu den Anbietern der klassischen TK-Dienste, die durch den Betrieb der TK-Netze an den Standort Deutschland gebunden sind, müssen Anbieter von OTT-Diensten weder technische Anlagen (z. B. Server) noch unternehmerische Strukturen in Deutschland (oder in der EU) vorhalten, um ihre Leistungen hierzulande anbieten zu können. Zwar werden die fraglichen Kommunikationsdaten nach wie vor über die TK-Netze der deutschen Infrastrukturbetreiber übertragen, sodass sie von den Polizei- oder Strafverfolgungsbehörden prinzipiell auch bei den Netzbetreibern erhoben werden könnten, weil aber mittlerweile die meisten OTT-Kommunikationsdienste die nutzerseitige Verschlüsselung der zu übertragenden Daten ermöglichen, ist diese Vorgehensweise in der Regel nicht zielführend (dazu Kap. 5.2.1.3).

Die Beschaffung von Kommunikationsdaten bei im Ausland ansässigen Diensteanbietern ist jedoch ungleich aufwendiger als im Falle der hiesigen TK-Unternehmen. Im Bereich der Strafverfolgung beispielsweise verbleiben den Strafverfolgungsbehörden im Wesentlichen zwei Möglichkeiten: die Instrumente der internationalen Rechtshilfe oder Direktanfragen bei den ausländischen Diensteanbietern. Für die Rechtshilfe gibt es innerhalb der Europäischen Union u. a. das Instrument der Europäischen Ermittlungsanordnung in Strafsachen, in deren Rahmen eine Justizbehörde die Justizbehörden in einem anderen Mitgliedstaat auffordern kann, eine Ermittlungsmaßnahme zur Erhebung der fraglichen Daten durchzuführen. Das Verfahren kann allerdings bis zu 120 Tage in Anspruch nehmen (Artikel 12 Richtline 2014/41/EU[119]). Sind Diensteanbieter außerhalb der EU involviert, können ggf. bilaterale Rechtshilfeabkommen zur Anwendung gelangen. Hier von Bedeutung ist insbesondere ein entsprechendes Abkommen zwischen der EU und den USA, wo zahlreiche OTT-Diensteanbieter ihren Sitz haben. In diesem Fall aber dauern die Verfahren laut Auskunft der Europäischen Kommission (2019, S. 1 f.) durchschnittlich zehn Monate, was als zu langwierig für eine effektive Ermittlungsarbeit betrachtet wird. Alternativ können

119 Richtlinie 2014/41/EU über die Europäische Ermittlungsanordnung in Strafsachen

sich die Strafverfolgungsbehörden – sofern andere Staaten dies ausdrücklich erlaubt haben – mit einer Direktanfrage an den ausländischen Diensteanbieter wenden. Direktanfragen sind allerdings an die Freiwilligkeit der Anbieter gebunden; ein Anspruch auf die Herausgabe von Daten besteht nicht (Bundesregierung 2017g, S. 4). So haben beispielsweise US-amerikanische Diensteanbieter den Ersuchen aus der EU in weniger als der Hälfte der Fälle entsprochen. Überdies beschränkt das US-amerikanische Recht die direkte Zusammenarbeit auf Metadaten, Inhaltsdaten dürfen nur in dringenden Fällen eingeholt werden, in denen die Gefahr besteht, dass eine Person zu Tode kommt oder körperlich schwer geschädigt wird (EK 2019, S. 2 f.). Auf EU-Ebene laufen (Stand Ende 2019) diverse Aktivitäten, die auf eine Vereinfachung und Beschleunigung des grenzüberschreitenden Austauschs von elektronischen Beweismitteln sowohl innerhalb der EU als auch auf internationaler Ebene abzielen, so u. a. die Vorschläge der Europäischen Kommission (EK 2018) für eine e-Evidence-Verordnung oder die Aufnahme von Verhandlungen mit den USA für ein neues Abkommen. Ziel ist, den europäischen Strafverfolgungsbehörden unter bestimmten Voraussetzungen die Beschaffung von sicherheitsrelevanten Inhalts- und Metadaten direkt bei den Diensteanbietern zu ermöglichen und zwar bei allen Anbietern mit Sitz in der EU oder den USA, die ihre Dienstleistungen auf dem EU-Markt anbieten (EK 2019, S. 3 ff.). Die Initiativen sind aber nicht unumstritten. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK 2018a) beispielsweise kritisiert vor allem die beabsichtigte Abkehr vom Grundsatz der beidseitigen Strafbarkeit, da die Herausgabe der Daten unabhängig davon zu erfolgen hätte, ob die verfolgte Straftat in dem Land, in dem der Diensteanbieter seinen Sitz hat, überhaupt strafbar ist.

Ob allerdings selbst im Falle einer reibungslos funktionierenden internationalen Zusammenarbeit zwischen den Justizbehörden oder neuer Möglichkeiten für Direktanfragen beim Diensteanbieter eine effektive Ermittlungsarbeit ermöglicht wird, bleibt aus zwei wesentlichen Gründen weiterhin fraglich. Zum einen geht die Ausbreitung von OTT-Kommunikationsdiensten derzeit mit einer weltweiten Konzentration der Diensteanbieter auf einige wenige, oft global tätige und dadurch wirtschaftlich durchaus mächtige private Akteure einher. So stehen beispielsweise hinter den in Deutschland beliebtesten Instant-Messaging-Diensten hauptsächlich die großen US-amerikanischen Internetkonzerne Facebook, Microsoft und Apple.[120] Diese Konzerne haben sich in der Vergangenheit bei verschiedenen Gelegenheiten gegen staatlich angeordnete Datenherausgaben zur Wehr gesetzt, etwa im Fall der Weigerung von Apple, trotz Gerichtsbeschluss dem US-amerikanischen FBI bei der Entschlüsselung des Smartphones einer/s Terrorattentäter/in zu helfen, oder von Microsoft, trotz Gerichtsbeschluss

120 Laut einer Umfrage von Bitkom (2018) sind die fünf beliebtesten Messenger in Deutschland: WhatsApp von Facebook (wird von 81 % der Internetnutzer verwendet), Facebook Messenger (46 %), Skype von Microsoft (24 %), Snapchat von Snap Inc. (15 %) sowie iMessage von Apple (10 %). Alle Unternehmen haben ihren Sitz in den USA.

Kommunikationsdaten einer/s Tatverdächtigen von einem Server in Irland an US-amerikanische Strafverfolgungsbehörden auszuhändigen (Beuth 2016, 2017). Die Gründe für die Konzentration bei den Diensteanbietern und die damit einhergehende Machtfülle einiger Internetkonzerne sind in der Kommerzialisierung des Internets zu suchen: Während klassische TK-Dienste wie auch früh entwickelte OTT-Kommunikationsdienste (z. B. E-Mail) auf offenen technischen Standards sowie einem dezentralen Betrieb der Vermittlungs- und Serverinfrastrukturen basieren und somit allen Marktakteuren zur Verfügung stehen, werden neuere OTT-Kommunikationsdienste als geschlossene Plattformen konzipiert, die nebeneinander existieren und um Nutzer/innen bzw. Marktanteile konkurrieren. Hier bestimmen alleine die Diensteanbieter über die Zugangs- und Nutzungsbedingungen, den Funktionsumfang oder die Sicherheitsstandards und Modalitäten der Datenverarbeitung. Zum Beispiel haben viele Anbieter von OTT-Kommunikationsdiensten mittlerweile eine nutzerseitige Ende-zu-Ende-Verschlüsselung implementiert, wodurch selbst die Diensteanbieter (und folglich auch die Polizei- und Strafverfolgungsbehörden) keinen Zugang mehr zu den Inhaltsdaten im Klartext haben (Kap. 5.2.1.3). Insofern sind es private Akteure, die die Gestaltung informationstechnisch vernetzter Systeme immer stärker prägen und kontrollieren, während staatlichen Sicherheitsakteuren (im Besonderen außerhalb den USA) die Kontroll- und Zugriffsmöglichkeiten auf die Infrastrukturen und Inhalte der Kommunikation immer stärker entzogen werden (Hempel/Rehak 2017, S. 25 u. 61).

Zum anderen existieren in Nischenbereichen neben den kommerziellen Produkten der großen Internetkonzerne verschiedene OTT-Kommunikations-dienste als Open-Source-Lösungen, für welche die zuvor genannten Möglichkeiten der Datenbeschaffung im Wege der internationalen Rechtshilfe oder von Direktanfragen vermutlich geringe Wirkung zeigen. Dasselbe gilt für OTT-Kommunikationsdiente, deren Diensteanbieter ggf. in Ländern mit fragiler Staatlichkeit ansässig sind. Kriminelle könnten ohne Schwierigkeiten auf solche Lösungen zurückgreifen, um ihre Kommunikation zu tarnen.

Für die Polizei- und Strafverfolgungsbehörden sind diese Entwicklungen von großer Tragweite. Denn einerseits können die im stark wachsenden Umfang anfallenden und durch private Diensteanbieter verarbeiteten Kommunikationsdaten für die Gefahrenabwehr und Strafverfolgung von erheblicher praktischer Bedeutung sein, andererseits aber wird der Zugang zu diesen Daten über die Diensteanbieter immer schwieriger. Wie im Folgenden dargestellt wird, setzen Polizei- und Strafverfolgungsbehörden daher zunehmend auf Verfahren der informationstechnischen Beobachtung, die ohne die Kooperation der Diensteanbieter einsetzbar sind, die aber mitunter dem Werkzeugkasten der Hackerszene entstammen bzw. in deren Nähe gehören.

5.2 Verfahren der informationstechnischen Beobachtung

Im Folgenden werden einzelne Verfahren der informationstechnischen Beobachtung aus einer technischen Perspektive dargestellt. Dies schließt eine Beschreibung der Funktionsweisen und Voraussetzungen für den Einsatz der Verfahren als auch eine Diskussion möglicher Gefährdungspotenziale für die IT-Sicherheit entlang der hier relevanten Faktoren Verfügbarkeit, Vertraulichkeit und Integrität ein (Kasten 5.1).

Kasten 5.1 Konzepte der IT-Sicherheit

Die Konzepte der IT-Sicherheit – Verfügbarkeit, Vertraulichkeit und Integrität – beziehen sich allein auf das System und sein technisch korrektes Funktionieren:

- *Verfügbarkeit* bezeichnet die Eigenschaft, den technischen Zugriff auf Systemfunktionen und Daten innerhalb oder zwischen Systemen sicherzustellen, wann immer dieser aus Sicht einer bestimmten Aufgabe notwendig ist.
- *Vertraulichkeit* bezeichnet die Eigenschaft, zwischen befugten und unbefugten technischen Zugriffen auf Systeme oder Daten zu unterscheiden und diese je nach Systemkonfiguration durchzusetzen.
- *Integrität* bezeichnet die Eigenschaft, dass Systeme oder Daten nicht unwillkürlich oder absichtlich verändert werden.

Alle diese Eigenschaften gelten unabhängig voneinander.

Quelle: Hempel/Rehak 2017, S. 137

Zur Gliederung werden die Verfahren danach unterschieden, an welcher Stelle in der Netzarchitektur die Beobachtung der Daten erfolgt:

- während des laufenden Übertragungsvorgangs im TK-Netz;
- beim Diensteanbieter;
- auf dem Endgerät des Kommunikationsteilnehmers.

Für die Darstellung musste ein Kompromiss zwischen der leichten Lesbarkeit und der technischen Detailtiefe gefunden werden. Die Ausführungen beschränken sich daher auf die für das Verständnis und die Diskussion notwendigen technischen Einzelheiten. Diesbezüglich sind insbesondere die Verfahren zur Beobachtung von Daten auf dem Endgerät des Kommunikationsteilnehmers sehr voraussetzungsreich, da diese eine heimliche Installation einer speziellen Beobach-

tungssoftware auf dem Endgerät erforderlich machen. Entsprechend gestalten sich hier die Erläuterungen etwas umfangreicher (Kap. 5.2.3).

Die folgenden Ausführungen basieren in wesentlichen Teilen auf den Kapiteln 3 und 5 im Gutachten von Hempel und Rehak (2017).

5.2.1 Beobachtung während des laufenden Übertragungsvorgangs im TK-Netz

Durch ein TK-Netz übertragene Kommunikationsinhalte können während des Übertragungsvorganges prinzipiell an jeder Stelle auf der Übertragungsstrecke beobachtet werden. Dies gilt auch für die verbindungsbegleitenden Metadaten, beispielsweise bei Telefongesprächen die Rufnummern der beteiligten Anschlüsse oder bei Datenübertragungen im Internet die IP-Adressen des Absenders oder Empfängers.

5.2.1.1 Beobachtung unter Mitwirkung der TK-Netzbetreiber: Telekommunikationsüberwachung

Technisch gesehen am einfachsten setzt die Beobachtung beim Betreiber des zur Datenübertragung genutzten TK-Netzes an. Mithilfe standardisierter Schnittstellen fertigt dieser eine Kopie des fraglichen Datenstroms an, die er an die nachfragende Polizei- oder Strafverfolgungsbehörde in Echtzeit ausleitet oder auf einem Datenträger übergibt. Grundsätzlich sind die Betreiber der TK-Netze, mit denen öffentlich zugänglich TK-Dienste erbracht werden, nach § 110 TKG dazu verpflichtet, auf eigene Kosten technische Einrichtungen zur Umsetzung solcher als Telekommunikationsüberwachung (TKÜ) bezeichnete Maßnahmen vorzuhalten. TKÜ-Maßnahmen können sich auf Festnetz-, Mobilfunk- oder Internetanschlüsse beziehen. In letzterem Fall kann prinzipiell der gesamte über den jeweiligen Anschluss laufende IP-Datenverkehr beobachtet werden, so etwa die Internetaktivitäten der beobachteten Person, aber auch der Datenstrom von internetfähigen Geräten wie beispielsweise intelligente Sprachassistenten oder Smart-Home-Anwendungen. TKÜ-Maßnahmen beeinträchtigen die Vertraulichkeit der übertragenen Daten, nicht aber deren Integrität oder Verfügbarkeit.

Die Beobachtung kann nicht nur auf einen Anschluss bezogen stattfinden (individuelle Maßnahmen), sondern auch gleichzeitig größere Teile des Datenverkehrs in einem TK-Netz zum Gegenstand haben, etwa um mithilfe von Suchbegriffen einzelne Verbindungen mit einschlägigen Inhalten ausfindig zu machen (strategische Fernmeldeaufklärung). Hierbei sind Stellen im TK-Netz von Interesse, an denen möglichst große Datenvolumen übertragen werden, etwa Tiefseekabel oder Internet Exchange Points (IXP), über die Internetzugangsanbieter die Daten ihrer Kunden austauschen (Waidner 2014, S. 12 ff.). Da diese Praktiken

dem Bundesnachrichtendienst vorbehalten sind, wird im Folgenden nicht weiter darauf eingegangen.

5.2.1.2 Beobachtung ohne Mitwirkung der TK-Netzbetreiber

Auch ohne die Mitwirkung der TK-Netzbetreiber lassen sich Inhalts- und Metadaten während des laufenden Übertragungsvorganges im TK-Netz beobachten. Der technische Aufwand ist allerdings höher, zugleich können die Integrität und die Verfügbarkeit der betroffenen informationstechnischen Systeme oder Daten beeinträchtigt werden. Möglich ist dies sowohl in funkgebundenen Netzen (Mobilfunknetze oder lokale Funknetzwerke [Wireless Local Area Network – WLAN]) als auch in leitungsgebundenen Netzen (z. B. durch das heimliche Anzapfen von Glasfaserkabeln mit technischen Hilfsmitteln). Während Ersteres auch von deutschen Polizei- und Strafverfolgungsbehörden praktiziert wird (Kap. 5.4.1.2), gehört Letzteres in den nachrichtendienstlichen Bereich und wird hier nicht weiter vertieft.

IMSI-Catcher: Datenverkehr im Mobilfunknetz abgreifen

Mit einem IMSI-Catcher kann der Funkverkehr eines Mobilfunkgeräts (im Folgenden: Zielgerät) beobachtet werden. Dabei handelt es sich um ein Gerät, das sich als Funkzelle ausgibt. Sobald es in räumliche Nähe zum Zielgerät gebracht wird, überwiegt sein Funksignal jenes der vorhandenen Funkmasten, sodass sich das Zielgerät beim Catcher einbucht. Gegenüber dem Mobilfunknetz gibt sich der Catcher als Mobilfunkgerät zu erkennen und stellt so eine Netzverbindung her. Er ist damit in der Lage, über das Zielgerät geführte Kommunikation durchzuleiten und – von der Zielperson unbemerkt[121] – mitzuschneiden (Abb. 5.3). Ermöglicht wird der Einsatz von IMSI-Catchern erst durch Schwachstellen in den Mobilfunkstandards (z. B. umgehen IMSI-Catcher die Verschlüsselung neuerer Mobilfunkstandards durch Herabstufung auf den älteren und unsicheren GSM-Standard).[122]

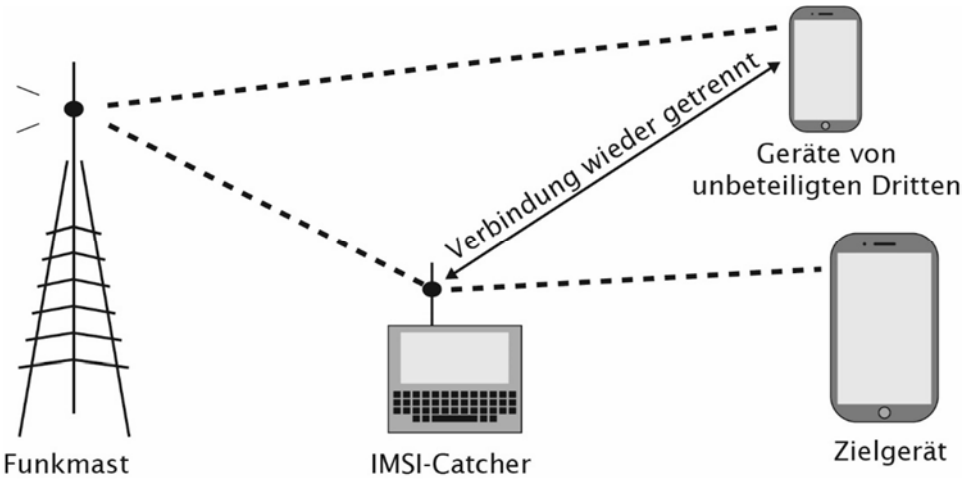
Da bei der Durchleitung des Funkverkehrs Fehler nicht auszuschließen sind, gefährdet der Einsatz eines IMSI-Catchers nicht nur die Vertraulichkeit, sondern ggf. auch die Integrität der über das Zielgerät übertragenen Daten. Außerdem hängt es von der technischen Ausstattung eines IMSI-Catchers ab, ob nur von Mobilfunkgeräten ausgehende Verbindungen durchgeleitet oder zusätzlich auch eingehende Anrufe durchgestellt werden können. Gehört Letzteres nicht zum

121 Allerdings sollen diverse Apps in der Lage sein, IMSI-Catcher zu erkennen, etwa SnoopSnitch für Android (https://opensource.srlabs.de/projects/snoopsnitch, 31.3.2022)

122 Nach Einschätzung der Bundesregierung (2019f, S. 14 f.) ist jedoch absehbar, dass in 5G-Netzen der Einsatz von IMSI-Catchern in derzeitiger Konfiguration nur noch eingeschränkt möglich sein wird.

Funktionsumfang, so ist das Zielgerät von außen nicht mehr erreichbar, sodass auch dessen Verfügbarkeit beeinträchtigt wird.

Abb. 5.3 Funktionsweise eines IMSI-Catchers



Quelle: angepasst nach Hempel/Rehak 2017, S. 89

Gängige IMSI-Catcher haben je nach Sendeleistung einen lokalen Wirkungsradius von 10 bis 100 m. Da sich zunächst alle in seinem Wirkungsbereich befindlichen Mobilfunkgeräte beim IMSI-Catcher einbuchen, betrifft die Maßnahme in der Regel auch Geräte unbeteiligter Dritter. Sofern aber die IMSI des Zielgeräts bekannt ist, kann der Catcher so konfiguriert werden, dass nur die Verbindung zum Zielgerät aufrechterhalten wird. Fremde Mobilfunkgeräte verbinden sich dadurch wieder mit einem regulären Funkmast.

Ein IMSI-Catcher kann auch lediglich zur Ermittlung der IMSI eines Zielgeräts eingesetzt werden, da die IMSI bei jeder Einbuchung an die Funkzelle (und folglich auch an den Catcher) übermittelt wird. Von Nutzen ist dies z. B., wenn – etwa im Bereich der organisierten Kriminalität – Zielpersonen häufig ihre Mobiltelefone wechseln oder gestohlene Geräte bzw. SIM-Karten benutzen (Harnisch/Pohlmann 2009, S. 203). In diesem Fall kann durch Observation zwar festgestellt werden, dass die Zielperson telefoniert, nicht aber unter welcher Rufnummer. Die Kenntnis der IMSI-Nummer erlaubt über eine Bestandsdatenauskunft (Kap. 5.2.2.3) die Ermittlung der Rufnummer des Zielgeräts, um auf dieser Grundlage ggf. weitere Ermittlungsmaßnahmen (z. B. eine TKÜ) durchführen zu können (Parlamentarisches Kontrollgremium 2017, S. 10). Auf ähnliche Weise kann die International Mobile Equipment Identity (IMEI) ermittelt werden, die einmalig für jedes Mobiltelefon vergeben wird (Gerätenummer). Dies ist etwa dann von Bedeutung, wenn eine Zielperson sich verschiedener SIM-Karten und folglich verschiedener IMSI-Kennungen bedient (Harnisch/Pohlmann 2009, S. 204). Schließlich ermöglicht ein IMSI-Catcher die Lokalisation eines Ziel-

geräts, indem er feststellt, ob bzw. wann sich ein Zielgerät in seinem Wirkungsbereich aufhält. Da der Catcher das Zielgerät auffordern kann, regelmäßig Signale auszusenden, ist mithilfe von Richtantennen und Triangulationsmethoden eine präzise Ortung möglich. Für diese Zwecke eingesetzte Catcher verfügen in der Regel nicht über eine Verbindung zum Mobilfunknetz. Die Beeinträchtigung der Verfügbarkeit der eingebuchten Mobilfunkgeräte kann Sekunden bis Minuten (bei der Ermittlung der IMSI) oder auch länger dauern (etwa wenn mehrere Peilungen zur Ortbestimmung durchgeführt werden) (Harnisch/Pohlmann 2009, S. 204).

WLAN-Catcher: Datenverkehr im lokalen Funknetzwerk abgreifen

Die Beobachtung des Internetdatenverkehrs, der über ein drahtloses Funknetzwerk zwischen einem Endgerät und dem lokalen Router übertragen wird, wird als WLAN-Catching bezeichnet. Je nach Sicherheitsvorkehrungen des Zielnetzwerks sind verschiedene Vorgehensweisen zu unterscheiden:

Um den Datenverkehr in einem lokalen Funknetzwerk ohne Sicherheitsvorkehrungen (WLAN ohne WEP- bzw. WPA/WPA2-Verschlüsslung; Daten werden unverschlüsselt zwischen Endgerät und Router übertragen) mitzuschneiden, genügt in der Regel bereits ein handelsüblicher Laptop. Viele WLAN-Adapter bieten zu Test- und Analysezwecke einen Monitormodus, in dem der Adapter nicht nur die an ihn adressierten, sondern alle empfangenen Datenpakete an eine entsprechende Software weiterreicht. Vorausgesetzt, die räumliche Nähe zum Zielnetzwerk ist gegeben, kann der gesamte Datenverkehr aufgezeichnet und analysiert werden, ohne dass eine Verbindung zum Zielnetzwerk aufgebaut werden muss (sog. Sniffen; Ulbrich 2019, S. 106).

Im geschützten Funknetzwerk (WEP- oder WPA/WPA2-Verschlüsselung) werden die Daten zwischen Endgerät und lokalem Router verschlüsselt übertragen. Der durch Sniffen mitgeschnittene Datenstrom liegt dann nur in verschlüsselter Form vor, kann aber bei Kenntnis des WEP- bzw. WPA/WPA2-Schlüssels nachträglich entschlüsselt werden. Ulbricht (2019, S. 80 ff.) skizziert verschiedene Methoden, wie diese Schlüssel auch ohne Wissen der Zielperson erlangt werden können. Dabei gilt der ältere WEP-Sicherheitsstandard als unsicher und kann sehr einfach ausgehebelt werden. Ein WPA/WPA2-Schlüssel lässt sich ggf. aus den mitgeschnittenen Daten[123] mithilfe der Brute-Force-Methode (Kap. 5.2.1.3) in Erfahrung bringen (der Erfolg hängt allerdings von der Komplexität und Länge des gewählten Schlüssels und der Leistungsfähigkeit der eingesetzten Hardware ab). Alternativ lassen sich ggf. vorhandene Schwachstellen im WPA/WPA2-Sicherheitsstandard ausnutzen. Solche Maßnahmen zur Überwin-

123 genauer: aus dem mitgeschnittenen Daten während des Authentifizierungshandshakes zwischen Endgerät und lokalem Router (Ulbrich 2019, S. 91 ff.)

dung der Verschlüsselung gehen fast immer mit Eingriffen in den Datenverkehr der Netzwerkinfrastruktur des Betroffenen einher (Ulbrich 2019, S. 145).

Eine weitere Möglichkeit besteht in Analogie zum Vorgehen beim IMSI-Catcher darin, das Zielnetzwerk zu imitieren, indem ein zusätzlicher WLAN-Zugangspunkt mit denselben Parametern (Name, MAC-Adresse etc.), aber mit stärkerer Sendeleistung anlegt wird. Dieses Netzwerk ist selbst aber nicht verschlüsselt, wodurch ein Mitschneiden des gesamten Datenstroms möglich wird. Allerdings ist bei dieser Maßnahme in der Regel ein (zumindest unbewusstes) Mitwirken der Zielperson notwendig (die Zielperson muss einmalig manuell eine Verbindung mit dem vorgeblich eigenen WLAN herstellen; Ulbricht 2019, S. 103 f.). Ist die Verbindung einmal hergestellt, kann der Datenverkehr nicht nur beobachtet, sondern prinzipiell auch aktiv verändert werden. Dadurch wird nicht nur die Vertraulichkeit, sondern ggf. auch die Integrität der betroffenen Daten beeinträchtigt.

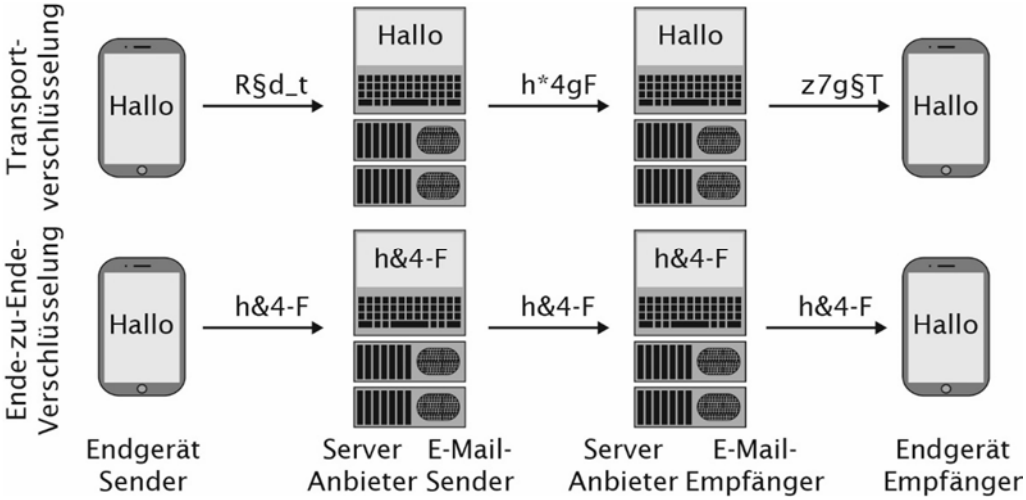
5.2.1.3 Aushebeln von Verschlüsselung

Sichere Verschlüsselungsverfahren für die Speicherung und Übertragung von digitalen Daten gewinnen für den Datenschutz und die Datensicherheit in dem Maße an Bedeutung, wie immer mehr Facetten des persönlichen, sozialen, wirtschaftlichen und politischen Lebens durch die intensive Nutzung von informationstechnischen Systemen geprägt werden.

Für die Verschlüsselung der zu übertragenden Inhaltsdaten (für den Transport notwendige Metadaten wie beispielsweise IP-Adressen können nicht verschlüsselt werden) existieren im Wesentlichen zwei Ansätze (Abb. 5.4):

- Bei der *Transportverschlüsselung* werden die Inhaltsdaten nur für den Transport zwischen einem Client (z. B. Internetbrowser oder E-Mail-Programm auf dem Endgerät der Nutzerin/des Nutzers) und dem Server beim Diensteanbieter verschlüsselt. Vor und nach der Übertragung liegen die Inhaltsdaten im Klartext vor und können im Prinzip beispielsweise vom Diensteanbieter eingesehen werden.
- Einen stärkeren Schutz bietet die nutzerseitige *Ende-zu-Ende-Verschlüsselung*. Hier werden die zu übertragenden Inhaltsdaten noch vor dem eigentlichen Transport manuell durch die Nutzer/innen oder automatisch durch die verwendete Clientanwendung auf dem Endgerät des Senders verschlüsselt und erst auf dem Endgerät beim intendierten Empfänger in gleicher Weise wieder entschlüsselt. Solange die dafür verwendeten Schlüssel alleine im Besitz der beteiligten Kommunikationspartner bleiben, hat niemand entlang der Übertragungsstrecke Einsicht in den Klartext, insbesondere auch nicht die Diensteanbieter.

Abb. 5.4 Transportverschlüsselung vs. Ende-zu-Ende-Verschlüsselung am Beispiel des E-Mail-Versands



Eigene Darstellung

Mittlerweile haben viele OTT-Kommunikationsdienste – auch als Reaktion auf die Enthüllungen der Abhörpraktiken durch US-amerikanische und weitere Nachrichtendienste durch Edward Snowden im Jahr 2013 – eine Ende-zu-Ende-Verschlüsselung fest eingebaut (z. B. Signal, WhatsApp, iMessage) oder bieten diese zumindest optional an (z. B. Telegram Messenger, Facebook Messenger, PGP bei E-Mail) (Stand Februar 2019).

Die Ende-zu-Ende-Verschlüsselung der Datenübertragung durch OTT-Kommunikationsdienste stellt Polizei- und Strafverfolgungsbehörden allerdings vor Herausforderungen, da auch Kriminelle zunehmend davon Gebrauch machen, um ihre Kommunikation zu schützen (Rat der Europäischen Union 2017, S. 40). So wurde 2016 auf einer Arbeitstagung des Generalbundesanwalts mit den Generalstaatsanwälten der Länder festgestellt, dass aktuell »nur noch in weniger als 15 % aller Fälle vollständig unverschlüsselte Kommunikation auf Seiten der Beschuldigten durchgeführt wird … Gleichzeitig ist ausweislich von Stichproben des Bundeskriminalamts erkennbar geworden, dass in zwei Drittel der Fälle seitens der Täter bewusst verschlüsselte Kommunikation zur Verschleierung eingesetzt wird« (nach Greven 2017, S. 3). Zwar kann auch in diesem Fall der Datenstrom während des laufenden Übertragungsvorganges beim TK-Netzbetreiber durch eine TKÜ beim Internetanschluss oder durch WLAN-Catching mitgeschnitten werden, allerdings liegt dieser dann in verschlüsselter Form vor und ist nur von Nutzen, wenn die Entschlüsselung der Inhalte ohne Kenntnis der Schlüssel gelingt (*Brechen* von Verschlüsselung). Dies ist angesichts der heute eingesetzten starken Verschlüsselungsverfahren in der Regel jedoch nur mit einem enormen Zeit- und Ressourcenaufwand bzw. oft auch gar nicht zu leisten (Kasten 5.2). Die Problematik, dass für Sicherheitsbehörden nutzbare Informations-

quellen durch Verschlüsselung zunehmend versiegen, wird im Bereich der zivilen Sicherheit bereits seit rund 40 Jahren unter dem Stichwort »going dark« diskutiert (Schulze 2017, S. 24).

Kasten 5.2 Brechen von Verschlüsselung

Bei der Brute-Force-Methode werden alle möglichen Zeichenkombinationen ausprobiert, bis der passende Schlüssel gefunden wird. Erfolgversprechend ist dies nur bei sehr einfachen Verschlüsselungsverfahren bzw. Passwörtern. Starke Verschlüsselungsverfahren, wie der bei vielen OTT-Kommunikationsdiensten angewendete Advanced-Encryption-Standard (AES) 256, können bei heutiger Computertechnik – wenn überhaupt – nur unter extremem Zeitaufwand (Monate bis Jahre) und erheblicher Rechenleistung (Cluster von Hochleistungsrechnern) entschlüsselt werden. Eine Variante ist die Wörterbuchmethode, bei der eine Liste ausgewählter Begriffe zur Schlüsselsuche verwendet wird, um den Suchraum einzugrenzen. Hier von Nutzen sind zusätzliche Informationen zum Schlüssel, etwa der verwendete Zeichensatz, die Passwortlänge oder mögliche Schlüsselsegmente.

Quelle: Rat der Europäischen Union 2017, S. 41 f.

Ein Ansatz, um staatlichen Stellen die Beobachtung sicherheitsrelevanter Kommunikationsinhalte während des laufenden Übertragungsvorganges trotz Verschlüsselung weiterhin zu ermöglichen, ist der Versuch, die Verschlüsselung auszuhebeln. Dafür stehen prinzipiell folgende Möglichkeiten zur Verfügung (Hempel/Rehak 2017, S. 46 ff.):

Regulierung von Verschlüsselung

Anbieter von OTT-Kommunikationsdiensten bzw. Hersteller von Verschlüsselungstechniken könnten gesetzlich dazu verpflichtet werden, spezielle Soft- oder Hardwareschnittstellen in ihre Produkte einzubauen, über die Sicherheitsbehörden einen Zugang auf die unverschlüsselten Kommunikationsinhalte bzw. verwendeten Schlüssel erhielten (Hintertüren). Kritiker verweisen auf das hohe Missbrauchspotenzial von staatlichen Hintertüren durch kriminelle Akteure oder fremde Nachrichtendienste, was die Sicherheit informationstechnischer Systeme prinzipiell schwächen und das Vertrauen der Nutzer in dieselbe beschädigen würde.

Alternativ könnten Anbieter bzw. Hersteller gesetzlich verpflichtet werden, die verwendeten Schlüssel an eine dafür geeignete Stelle (z. B. eine private oder staatliche Schlüsselverwaltung) zu hinterlegen, um sie im Bedarfsfall unter bestimmten Voraussetzungen (z. B. bei einer richterlichen Anordnung) den Sicherheitsbehörden zugänglich zu machen. Dieser Ansatz birgt das Risiko, dass sich

Dritte unbefugt Zugriff auf die zentral hinterlegten Schlüssel verschaffen und somit auf einen Schlag in der Lage wären, sämtliche verschlüsselte Kommunikation mitzulesen (Gesellschaft für Informatik 2015).

In eine andere Richtung zielt der Vorschlag, den Einsatz von Verschlüsselungsverfahren ab einer gewissen Stärke gesetzlich zu verbieten. Die Verbotsgrenze könnte dann erreicht sein, wenn die Verschlüsselung mit staatlichen Ressourcen nicht mehr in einem angemessenen Zeitraum zu brechen wäre. Ein Verbot starker Verschlüsselungsverfahren würde jedoch die Sicherheit informationstechnischer Systeme insgesamt erheblich schwächen (Castro/McQuinn 2016, S. 14).

Die Wirkung regulatorischer Ansätze wird prinzipiell durch den Umstand beschränkt, dass sie bei außereuropäischen Anbietern oder Herstellern bzw. bei Open-Source-Initiativen nur schwer durchsetzbar sind. Kriminelle könnten problemlos auf nichtregulierte Softwareprodukte ausweichen. Zudem kann die Regulierung von Verschlüsselung die Geschäftsmodelle der Diensteanbieter infrage stellen.

Freiwillige Zusammenarbeit zwischen staatlichen und privaten Akteuren

Als Alternative zu gesetzlichen Verpflichtungen könnte eine freiwillige Zusammenarbeit zwischen staatlichen Akteuren und Herstellern bzw. Anbietern von Kommunikationsdiensten oder Verschlüsselungstechniken etabliert werden. Das Spektrum der möglichen Formen ist breit: Es reicht vom einfachen Informationsaustausch, in dessen Rahmen Hersteller bzw. Anbieter die Sicherheitsbehörden mit Wissen über Design und Implementierung der Verschlüsselungsverfahren versorgen, das bei der Entschlüsselung der ausgeleiteten Datenströme von Nutzen sein könnte, über das gezielte Aufspielen einer präparierten Softwareversion des Kommunikationsdienstes auf das Zielgerät im Rahmen einer Softwareaktualisierung bis hin zum Einbau von staatlichen Hintertüren auf freiwilliger Basis. Bezüglich der Gefahren für die IT-Sicherheit gilt analog zu den regulatorischen Ansätzen, dass Formen der freiwilligen Zusammenarbeit die Sicherheit informationstechnischer Systeme ggf. insgesamt schwächen könnten.

Heimliche Schwächung von Verschlüsselungsstandards

Für den Praxiseinsatz müssen Verschlüsselungsverfahren standardisiert werden (Waidner 2014, S. 25). Staatliche Akteure haben prinzipiell die Möglichkeit, an öffentlichen Standardisierungsprozessen mit der Intention teilzunehmen, auf schwächere oder gar fehlerbehaftete Verschlüsselungsstandards hinzuwirken. Ein bekanntes Beispiel war ein von der US-amerikanischen National Security

Agency (NSA) entwickelter Zufallsgenerator[124], der 2006 durch das US-amerikanische National Institute of Standards and Technology nach einem jahrelangen Standardisierungsprozess trotz Bedenken einiger Sicherheitsexperten zum Standard erklärt wurde. Durch die Enthüllungen von Edward Snowden wurde viel später bekannt, dass die NSA absichtlich eine Hintertür in den Zufallsgenerator implementiert hatte.

Staatliches Hacking

Staatliche Akteure könnten sich auch der Mittel bedienen, die üblicherweise von Kriminellen zur Ausführung von Cyberangriffen benutzt werden. Der Aufwand und die Risiken für die IT-Sicherheit hängen von der konkreten Herangehensweise ab.

Ein Beispiel für eine vergleichsweise einfache und risikoarme Maßnahme ist der Versuch, Zugang zu einem Nutzerkonto durch Hinzufügen neuer Endgeräte zu erhalten. Viele OTT-Kommunikationsdienste bieten ihren Kunden die Möglichkeit, den Dienst gleichzeitig auf mehreren Endgeräten (z. B. Smartphone und Laptop) zu verwenden. Dies lässt sich unter Umständen ausnutzen, um heimlich ein weiteres Endgerät auf das Nutzerkonto einer Zielperson anzumelden, über welches dann die gesamte Kommunikation im Klartext mitgelesen werden kann.

Ausgangspunkt für Hackerangriffe auf fremde Datenbestände sind jedoch häufig Schwachstellen in Betriebssystemen, in der Anwendungssoftware oder in Verschlüsselungsalgorithmen und ihren Implementierungen in Protokollen oder Anwendungen. Diese Mittel stehen grundsätzlich auch staatlichen Akteuren offen, um Verschlüsselungstechniken auszuhebeln. Die Ausnutzung von Schwachstellen steht allerdings mit den Zielen der IT-Sicherheit im Widerspruch, wonach Wissen über Schwachstellen unverzüglich mit den Softwareherstellern zu teilen ist, damit sie durch Softwareupdates behoben werden können (dazu Kap. 5.2.3).

5.2.2 Beobachtung beim Diensteanbieter

Verfahren der informationstechnischen Beobachtung, die beim Diensteanbieter ansetzen, können ggf. hier gespeicherte (retrograde) oder in Echtzeit bzw. künftig anfallende Kommunikationsdaten einer Nutzerin/eines Nutzers zum Gegenstand haben und sich sowohl auf Inhalts- als auch auf Metadaten der Telekommunikation beziehen.

124 Zufallsgeneratoren dienen u. a. der Generierung von Zufallsschlüsseln und sind eine kritische Komponente für Verschlüsselungsverfahren (BSI 2017, S. 40).

5.2.2.1 Erhebung von Inhaltsdaten beim Diensteanbieter

Ob Diensteanbieter Inhaltsdaten der Nutzer verarbeiten und ggf. speichern, hängt vom Dienst und dessen technischer Funktionsweise ab. Technisch erforderlich ist dies bei zeitversetzten (asynchronen) Diensten wie SMS, E-Mail oder Instantmessaging, denen in der Regel ein Client-Server-Modell zugrunde liegt (Grünwald/Nüßing 2016, S. 92 f.): Der Absender schickt eine Nachricht zusammen mit der Adresse des Empfängers an einen zentralen Server beim Diensteanbieter. Von dort wird der Nachrichteninhalt entweder direkt an den Empfänger weitergeleitet oder, falls dieser gerade nicht verfügbar ist, solange zwischengespeichert, bis eine Verbindung möglich ist (z. B. SMS, Instant-Messaging). Alternativ werden die Nachrichten (mindestens) solange auf dem Server des Diensteanbieters gespeichert, bis der Empfänger sie dort abruft (z. B. E-Mail). Für synchron ablaufende Dienste wie beispielsweise die Sprachtelefonie kommen neben Client-Server-Modellen auch hybride Peer-to-Peer-Modelle in Betracht: Hier stellt der Server des Diensteanbieters lediglich die für den Verbindungsaufbau erforderlichen Informationen bereit (etwa die Verfügbarkeiten der Nutzer und die IP-Adressen, unter denen sie zu erreichen sind). Die Inhalte der Kommunikation werden dann jedoch ohne weitere Mitwirkung der Diensteanbieter unmittelbar unter den beteiligten Nutzern über das Internet ausgetauscht.

Sofern ein Dienst auf einem Client-Server-Modell basiert, ist es technisch problemlos möglich, die Serversoftware so zu konfigurieren, dass eine Kopie des einem bestimmten Nutzer zugeordneten Datenstroms beispielsweise an einen Server der Polizeibehörden weitergeleitet wird. Ebenso lassen sich in einem Nutzerkonto gespeicherte Inhaltsdaten kopieren und an die nachfragende Stelle übermitteln, beispielsweise in einem E-Mail-Konto abgelegte Nachrichten. Keinen Nutzen haben solche Inhaltsdaten für die Polizei- und Strafverfolgungsbehörden allerdings dann, wenn sie durch den Nutzer mit einer Ende-zu-Ende-Verschlüsselung geschützt wurden (Kap. 5.2.1.3).

5.2.2.2 Erhebung von Metadaten beim Diensteanbieter

Bei jedem Datenübertragungsvorgang fallen notwendigerweise Metadaten an, die der Diensteanbieter verarbeitet und zum Teil – zumindest kurzfristig – auch speichert (z. B. für Abrechnungszwecke oder zur Erkennung und Beseitigung von Systemstörungen). Bei den klassischen TK-Diensten (Telefondienste, SMS, Internetzugang) gehören dazu u. a. die Rufnummern oder IP-Adressen der beteiligten Anschlüsse, die Anfangs- und Endzeiten der Verbindungen oder bei der Mobilfunknutzung auch die Kennungen der verwendeten Funkzellen (Standortdaten). In der Terminologie des TKG werden diese Daten als *Verkehrsdaten* bezeichnet (§ 96 Abs. 1 TKG). Welche Metadaten Anbieter von OTT-Kommunikationsdiensten verarbeiten und ggf. speichern, hängt von seiner technischen Funk-

tionsweise und vom Geschäftsmodell des jeweiligen Dienstes ab. Aus technischen Gründen mindestens notwendig sind die IP-Adressen der beteiligten Kommunikationspartner. Sofern OTT-Kommunikationsdienste rechtlich den Telemediendiensten (TM-Diensten) zugeordnet werden (Kap. 5.3.1.3), wird hier von *Nutzungsdaten* gesprochen (§ 15 Telemediengesetz – TMG[125]).

Metadaten der Telekommunikation können für Polizei- und Strafverfolgungsbehörden von hoher ermittlungspraktischer Bedeutung sein: Mithilfe von Rufnummern, E-Mail- oder IP-Adressen lassen sich (über eine Bestandsdatenauskunft beim Diensteanbieter, Kap. 5.2.2.3) die Personalien der Anschlussinhaber/in feststellen. Bei Straftaten, die mithilfe von Telefon oder Internet durchgeführt werden – z. B. Trickbetrug, Onlinehandel mit illegalen Gütern, Verbreitung von Kinderpornografie – sind dies häufig die einzigen zur Verfügung stehenden Ermittlungsansätze. Im Rahmen der Aufklärung von Strukturen z. B. der organisierten Kriminalität erlauben die Metadaten ggf. die Analyse von Beziehungsnetzen und (über die Nutzungszeiten und -häufigkeiten) von Verhaltensweisen der beobachteten Personen. Bei der Mobilfunknutzung können aus den Standortdaten der verwendeten Funkzellen die ungefähren Aufenthaltsorte von Verdächtigen ermittelt bzw. auch Bewegungsprofilen erstellt werden. Dabei hängt die Genauigkeit der Ortsbestimmung von der Größe der jeweiligen Funkzelle ab: In urbanen Gebieten liegt sie bei einigen zehn (z. B. in Bahnhöfen oder Einkaufspassagen, wo Mikrozellen im Einsatz sind) bis 100 m. Bei Großzellen für die ländliche Flächenversorgung kann die Unschärfe hingegen mehrere Kilometer betragen (Hempel/Rehak 2017, S. 87).

In Bezug auf die Erhebung von Verkehrsdaten der klassischen TK-Dienste haben sich in der polizeilichen Praxis folgende Formen herausgebildet (Hempel/Rehak 2017, S. 96 ff.):

Individualisierte Verkehrsdatenerhebung

Die individualisierte Verkehrsdatenerhebung bezieht sich auf einen bestimmten Telefon-, Mobilfunk- oder Internetanschluss. Die nachfragende Behörde richtet ein Auskunftsverlangen an den entsprechenden TK-Diensteanbieter. Darin enthalten sind die Rufnummer bzw. eine andere Kennung des zu beobachteten Anschlusses sowie der Zeitraum für die Datenerhebung, welcher sich auch auf gespeicherte (retrograde) Verkehrsdaten beziehen kann (dazu Kap. 5.3.1.2).

Nichtindividualisierte Verkehrsdatenerhebung

Bei der nichtindividualisierten Verkehrsdatenerhebung (auch und im Folgenden als Funkzellenabfrage bezeichnet) steht nicht ein einzelner Anschluss im Fokus,

125 Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 1 des Gesetzes vom 28.9.2017 (BGBl. I S. 3530) geändert worden ist

sondern alle während eines bestimmten Zeitraums in einem festgelegten räumlichen Gebiet erfolgte bzw. stattfindende Mobilfunkkommunikation einschließlich SMS und mobiler Internetnutzung. Die Auswertung der so erhobenen Verkehrsdaten können beispielsweise Auskunft darüber geben, welche Mobilfunkgeräte sich zum Zeitpunkt einer Straftatbegehung in der Nähe des Tatorts aufgehalten haben. Über eine Bestandsdatenabfrage beim Diensteanbieter (Kap. 5.2.2.3) können sodann die Personalien der Anschlussinhaber ermittelt werden. Je nach Anzahl und Größe der erfassten Funkzellen kann der Suchraum einzelne Straßen, Straßenzüge oder auch ganze Stadtteile einschließen.

Charakteristisch für eine Funkzellenabfrage ist, dass nicht nur die Verkehrsdaten des Mobilfunkgeräts der Zielperson erfasst werden (wie dies bei der individualisierten Verkehrsdatenerhebung der Fall ist), sondern unvermeidlich auch alle Personen von der Maßnahme betroffen sind, die sich im fraglichen Zeitraum im Empfangsbereich der erfassten Funkzellen aufgehalten und hier ihre Mobilfunkgeräte benutzt haben. Vor allem in urbanen Räumen oder in Situationen größerer Menschenansammlungen (Veranstaltungen, Demonstrationen) kann die Zahl der unbeteiligt Betroffenen durchaus beträchtlich sein (Kasten 5.3).

Kasten 5.3 Funkzellenabfragen der Strafverfolgungsbehörden in Berlin

Für das Berichtsjahr 2016 legte der Senat von Berlin (2017b) dem Berliner Abgeordnetenhaus erstmals eine detaillierte Aufstellung aller durchgeführten Funkzellenabfragen vor. Demnach hatten die Berliner Strafverfolgungsbehörden insgesamt 491 zuvor gerichtlich angeordnete Funkzellenabfragen in insgesamt 432 Ermittlungsverfahren durchgeführt.

Im Rahmen dieser 491 Funkzellenabfragen wurden die Verkehrsdaten von insgesamt 17.888 einzelnen Funkzellen abgefragt. Davon betroffen waren insgesamt 1.911.133 Anschlüsse (im Schnitt 107 Anschlüsse pro Abfrage). Darüber hinaus wurden in 1.765 Fällen alle Funkzellen in einem Postleitzahlgebiet abgefragt. Hiervon waren insgesamt 2.464.546 Anschlüsse betroffen (im Schnitt 1.396 Anschlüsse pro Abfrage). Es wurden gesamthaft 112.204.682 Verkehrsdatensätze erhoben. In Bezug auf die Dauer der Datenerhebung lässt sich der Übersicht folgendes entnehmen: In 49 % der Fälle betrug diese weniger als 1 Stunde, in 47 % zwischen 1 Stunde und 1 Tag und in 4 % der Fälle mehr als einen Tag.

Jede der 491 gerichtlich angeordneten Funkzellenabfragen betraf somit im Schnitt rd. 8.900 Anschlüsse und war mit der Erhebung von rd. 230.000 Verkehrsdatensätzen verbunden. Zu betonen ist allerdings, dass diese Erkenntnisse nicht ohne Weiteres auf weniger dichtbesiedelte Gebiete als das Land Berlin übertragbar sind.

Über das Ende 2018 freigeschaltete »Funkzellenabfragen-Transparenz-System« (FTS) der Berliner Senatsverwaltung[126] können sich Mobilfunknutzer darüber informieren, ob ihr Gerät von einer Funkzellenabfrage erfasst wurde.

Eigene Berechnung nach Daten des Senats von Berlin 2017b

Stille SMS

Bei den bisher beschriebenen Formen der Verkehrsdatenerhebung werden nur Daten erhoben, die durch das Verhalten der zu beobachteten Person anfallen, also wenn Kommunikationsverbindungen aufgebaut oder Funkzellen betreten werden (passive Maßnahmen). Behörden können die zu erhebenden Verkehrsdaten jedoch auch speziell für Beobachtungszwecke erzeugen (aktive Maßnahmen), um aus mehr bzw. in kürzeren Zeitabständen anfallenden Verkehrsdaten ggf. präzisere Ortbestimmungen zu ermöglichen oder Bewegungsprofile der zu beobachtenden Person zu erstellen. Erreicht werden kann dies durch das Versenden von stillen SMS. Dabei handelt es sich um einen besonderen Typ der Kurznachricht, die von Mobilfunkgeräten zwar empfangen wird, jedoch ohne die Nutzer/innen darüber in Kenntnis zu setzen.[127] Gleichwohl bestätigt das Mobilfunkgerät den Empfang einer stillen SMS gegenüber dem Mobilfunknetz, wodurch die gewünschten Verkehrsdaten anfallen und beim Diensteanbieter angefordert werden können.

Da stille SMS sich immer nur auf das Mobilfunkgerät der Zielperson beziehen, sind – im Gegensatz zu einer Funkzellenabfrage – unbeteiligte Dritte davon nicht betroffen.

5.2.2.3 Bestandsdatenauskunft

Von den verbindungsbegleitenden Metadaten der Kommunikation sind schließlich die Bestandsdaten zu unterscheiden, die ebenfalls beim Diensteanbieter vorliegen und sich hier erheben lassen. Hierbei handelt es sich um die Daten aus dem Vertragsverhältnis der Nutzer mit dem Diensteanbieter, wozu u. a. Name und Anschrift des Anschlussinhabers, vergebene Rufnummern bzw. (dynamische) IP-Adressen, aber auch Sicherungs- und Zugriffscodes gehören können, die den Zugang auf Endgeräte (z. B. PIN, PUK) oder externe Speicher (z. B. Cloudspeicher) ermöglichen.

126 https://fts.berlin.de (31.3.2022)

127 Dieser Nachrichtentyp wurde ursprünglich zur Übermittlung von Statusinformationen oder Dienstanweisungen zwischen Mobilfunknetz und -geräten entwickelt.

5.2.3 Beobachtung auf dem Endgerät

Ein zur Aushebelung von Verschlüsselung (Kap. 5.2.1.3) alternativer Ansatz zur Gewährleistung eines staatlichen Zugangs auf durch OTT-Kommunikationsdienste verschlüsselte ermittlungsrelevante Inhalte der Telekommunikation ist deren Beobachtung noch *vor* dem Verschlüsselungsvorgang. Beim Einsatz einer nutzerseitigen Ende-zu-Ende-Verschlüsselung muss der Zugriff folglich noch vor dem Versenden der Daten auf dem Endgerät der zu beobachtenden Person (im Folgenden: Zielperson) erfolgen. Die Beobachtung findet damit an der Quelle der Telekommunikation statt, weswegen sich die Bezeichnung Quellen-TKÜ etabliert hat.[128] Aus Sicht der Polizei- und Strafverfolgungsbehörden ein weiterer Vorteil der Quellen-TKÜ gegenüber der herkömmlichen TKÜ ist, dass damit auch Telekommunikationsvorgänge erfasst werden können, die eine Zielperson über fremde Internetzugangspunkte führt (z. B. über freie WLAN-Hotspots).

Nicht nur die verschlüsselte Datenübertragung stellt Polizei- und Strafverfolgungsbehörden vor Herausforderungen, sondern zunehmend auch die Verschlüsselung von Datenträgern. So sind seit 2014 alle Geräte des Herstellers Apple ab Werk mit einer Datenträgerverschlüsselung ausgestattet, die selbst Apple eigenen Angaben zufolge nicht umgehen kann. Neuere Android-Geräte bieten die Datenträgerverschlüsselung zumindest optional an (Schulze 2017, S. 23). Dadurch sind Polizei- und Strafverfolgungsbehörden beispielsweise oftmals nicht mehr in der Lage, beschlagnahmte Datenträger, PCs oder Smartphones auszuwerten. In solchen Fällen bietet die informationstechnische Beobachtung auf dem Endgerät eine technische Möglichkeit, um hier gespeicherte ermittlungsrelevante Daten bereits vor der Beschlagnahmung zu erheben oder um Passwörter oder Hinweise zu erlangen, die eine spätere Entschlüsselung der Daten ermöglichen sollen (Henzler 2017, S. 6). Für solche Maßnahmen hat sich die Bezeichnung Onlinedurchsuchung etabliert.

Die Beobachtung auf dem Endgerät setzt in der Regel die Installation einer Software auf dem Endgerät der Zielperson voraus, welche die gewünschten Daten sammelt und an die Behörden ausleitet. In der polizeilichen Praxis muss eine entsprechende Software offenkundig *ohne Wissen* der Zielperson auf dessen Endgerät installiert werden können, da anderenfalls keine ermittlungsrelevanten Informationen zu erwarten sind. Dadurch sind diese Maßnahmen im Vergleich zur Beobachtung im TK-Netz oder beim Diensteanbieter technisch viel aufwendiger bzw. komplexer durchzuführen und infolgedessen auch mit höheren Risiken für die IT-Sicherheit der betroffenen Endgeräte und weiterer informationstechnisch vernetzter Systeme behaftet.

128 Prinzipiell können dieselben Daten auch nach der Entschlüsselung auf dem Endgerät des Empfängers beobachtet werden. Da sich die technischen Vorgehensweisen ähneln, wird hierauf im Folgenden nicht gesondert eingegangen.

5.2.3.1 Ausleiten von Kommunikationsinhalten vor dem Übertragungsvorgang (Quellen-TKÜ)

Der Lebenszyklus einer Quellen-TKÜ erstreckt sich über insgesamt sechs Schritte (dazu und zum Folgenden Hempel/Rehak 2017, S. 32 ff. u. 69 ff.):

Analyse des Zielsystems und Erstellung der Quellen-TKÜ-Software

Um verlässlich zu funktionieren, muss eine Quellen-TKÜ-Software möglichst genau auf das Zielsystem zugeschnitten werden. Dies gilt sowohl in Bezug auf den verwendeten OTT-Kommunikationsdienst als auch hinsichtlich der Hardware- (Desktop-PC, Smartphone, verbaute Hardwarekomponenten etc.) und Softwarekonfiguration (Betriebssystem, installierte Anwendungen und Schutzvorrichtungen wie Firewall, Virenscanner) des Zielsystems (Fox 2007, S. 5).

Die notwendige Analyse des Zielsystems kann teilweise aus der Ferne mit Werkzeugen erfolgen, die zur Wartung von informationstechnisch vernetzten Systemen über das Internet entwickelt wurden. Ist beispielsweise die IP-Adresse des Zielsystems bekannt, erlaubt ein Portscanner Rückschlüsse über Betriebssystem und installierte Anwendungen mitsamt Versionsnummern. Invasivere Methoden bauen Verbindungen zu Netzwerkdiensten auf dem Zielsystem auf (z. B. zu einer installierten Fernwartungssoftware), um mithilfe dienstspezifischer Funktionen weitere Einzelheiten über das System abzufragen (das Entdeckungsrisiko ist hier allerdings höher). Zusätzliche Erkenntnisse müssen ggf. mit herkömmlichen Ermittlungsmethoden gewonnen werden. Eine Observation der Zielperson kann etwa Aufschluss über die verwendete Hardware geben. Die Analyse des Zielsystems kann auch zu dem Ergebnis führen, dass eine Quellen-TKÜ mit den verfügbaren technischen Mitteln gar nicht möglich ist (Fox 2007, S. 5 f.).

Aufgrund der Vielzahl an möglichen Systemkonfigurationen ist es praktisch notwendig, für jede Beobachtungsmaßnahme eine eigene Quellen-TKÜ-Software zu erstellen, wobei aber ggf. auf bestehende Softwarekomponenten zurückgegriffen werden kann. Generell dürfte der Entwicklungsaufwand mit steigender Funktionalität, technischer Komplexität und Diversität der Systeme und OTT-Kommunikationsdienste stetig zunehmen. So könnte es auch sein, dass sich der Entwicklungsaufwand regelmäßig als so arbeits- und zeitintensiv erweist, dass die Software bei Fertigstellung bereits veraltet ist bzw. gar nicht mehr benötigt wird, etwa weil der betroffene OTT-Kommunikationsdienst durch Softwareupdates größere Modifikationen erfahren hat, die Zielperson auf einen anderen OTT-Kommunikationsdienst umgestiegen ist oder es letztlich keinen ermittlungsrelevanten Bedarf für den Einsatz der Software mehr gibt (Albrecht/Poscher 2017, S. 40).

Installation der Quellen-TKÜ-Software auf dem Zielsystem

Die heimliche Installation der Software auf dem Zielsystem ist technisch gesehen der aufwendigste Teil einer Quellen-TKÜ-Maßnahme. Folgende Möglichkeiten stehen zur Verfügung (Fox 2007, S. 6 f.; Pfitzmann 2008, S. 68):

- unbewusste konstruktive Mitarbeit der Zielperson;
- Erreichen des physischen Zugriffs auf das Zielsystem;
- Verpflichtung von Diensteanbietern zur Umleitung von Datenströmen;
- Ausnutzung von Schwachstellen in der Software.

Unbewusste konstruktive Mitarbeit der Zielperson

Es können ähnliche Methoden wie bei der Verbreitung von Schadprogrammen (Viren, Trojaner etc.) eingesetzt werden. Dazu zählt beispielsweise das Zusenden von E-Mails mit einer Datei im Anhang, in die die Quellen-TKÜ-Software eingebettet ist. Auch mithilfe präparierter Webseiten oder USB-Sticks kann eine Zielperson ggf. dazu verleitet werden, entsprechende Dateien auf ihr Endgerät zu laden. Beim Öffnen der Dateien (bzw. bereits beim Anschließen des USB-Sticks) wird die Quellen-TKÜ-Software automatisch im Hintergrund auf dem Zielsystem installiert.

Ein Erfolg ist bei allen diesen Methoden keinesfalls sicher. Auch ist nicht auszuschließen, dass die Quellen-TKÜ-Software (oder zumindest Teile davon[129]) auf einem anderen als dem intendierten Endgerät installiert wird bzw. sich gar unkontrolliert weiterverbreitet (Hansen/Pfitzmann 2007). Auf fremden Systemen könnte die speziell auf ein Zielsystem zugeschnittene Software zu Fehlfunktionen führen.

Erreichen des physischen Zugriffs auf das Zielsystem

Zielgenauer und – sofern auf dem Zielsystem kein wirksamer Zugangsschutz wie ein Sperrcode oder Abgleich des Fingerabdrucks eingerichtet ist[130] – vergleichsweise einfach kann die Installation durch einen direkten physischen Zugriff auf das Zielsystem erfolgen. Im Falle von mobilen Endgeräten bieten beispielsweise Sicherheitskontrollen an Flughäfen eine Gelegenheit, das Endgerät unter einem Vorwand kurz zu entwenden, um die Installation durchzuführen. Der Zugriff könnte prinzipiell auch im Rahmen einer heimlichen Wohnungsbetretung bzw. -durchsuchung zu diesem Zweck stattfinden, dafür fehlen aber

129 Die Quellen-TKÜ-Software kann zwar über einen Mechanismus verfügen, der die Identität des Zielsystems prüft und bei negativem Ergebnis die Installation wieder abbricht, dazu allerdings muss zumindest die Softwarekomponente mit diesem Mechanismus installiert und ausgeführt werden.

130 In diesem Fall wären zusätzliche Maßnahmen erforderlich, etwa eine Observation zur Ermittlung des Sperrcodes.

zumindest auf Ebene des Bundes derzeit (Stand Ende 2019) die Rechtsgrundlagen.[131]

Verpflichtung von Internetzugangsanbieter zur Umleitung von Datenströmen

Eine weitere Option ist, den Internetdatenstrom der Zielperson dahingehend zu verändern, dass eine im Internet angeforderte Datei noch während des Herunterladens durch eine mit der Quellen-TKÜ-Software präparierte Kopie ersetzt wird. Dazu müsste beim Internetzugangsanbieter temporär ein Rechner installiert werden, über den der Datenstrom der Zielperson geleitet wird. Hierdurch ist zwar eine zielgenaue Installation möglich (Albrecht/Poscher 2017, S. 44), allerdings kann auch bei dieser Methode nicht gänzlich ausgeschlossen werden, dass sich die präparierte Datei und damit die Quellen-TKÜ-Software unkontrolliert weiterverbreitet.

Ausnutzen von Schwachstellen in der Software

Schließlich kann versucht werden, die Quellen-TKÜ-Software per Fernzugriff über das Internet auf das Zielsystem zu installieren. Möglich wird dies, wenn die auf dem Zielsystem installierte Software (Betriebssystem, Anwendungen, Programmbibliotheken etc.) Schwachstellen aufweist, die ein Eindringen in das System erlauben. Solche Schwachstellen sind keine Seltenheit, da Fehler in der Entwicklung aufgrund der großen Komplexität heutiger Software kaum zu vermeiden sind: Alleine innerhalb 1 Jahres registrierte das BSI (2017, S. 18) in 11 gängigen Softwareprodukten über 1.600 Schwachstellen, wovon über 900 als kritisch eingestuft wurden.[132] (Was allerdings nicht heißen soll, dass sich alle diese Schwachstellen zur Installation einer Quellen-TKÜ-Software ausnutzen ließen.) Hierbei handelt es sich nur um öffentlich bekannte, mittlerweile durch den Hersteller bereits geschlossene Schwachstellen. Hinzu tritt noch eine unbekannte Zahl an unveröffentlichten, noch offenen Schwachstellen. Diese Vorgehensweise setzt voraus, dass Sicherheitsbehörden (bzw. private Dienstleister, die in deren Auftrag handeln) Kenntnisse über die Existenz und die technischen Details von dafür geeigneten Schwachstellen erlangen (dazu Kap. 5.2.3.4).

131 Über eine entsprechende gefahrenabwehrrechtliche Eingriffsbefugnis verfügen beispielsweise die Polizeibehörden von Bayern (§ 45 Abs. 3 S. 5 Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei in der Fassung vom 18.5.2018)

132 Im Auswertungszeitraum September 2016 bis September 2017 waren dies: Adobe Reader (224 geschlossene Schwachstellen, davon 183 kritisch), Flash Player (128, 119), OS X (240, 119), Safari (157, 20), Chrome (100, 1), Linus Kernel (345, 264), Windows (256, 128), Internet Explorer (65, 41), Office (71, 48), Firefox (18, 8), Java Runtime Environment (55, 4); https://www.cert-bund.de/schwachstellenampel (23.11.2017).

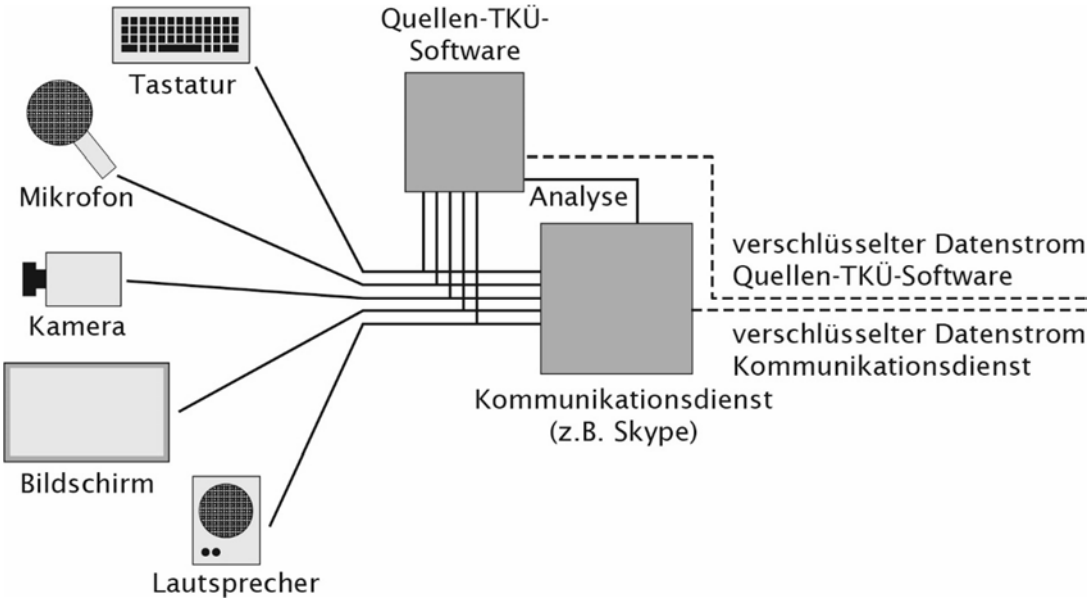
Datenzugriff

Die konkrete Vorgehensweise beim Datenzugriff hängt vom verwendeten OTT-Kommunikationsdienst, dessen Funktionsumfang sowie von den zu beobachtenden Kommunikationsinhalten (Text, Sprache, Video) ab. In Abhängigkeit dieser Faktoren kann der Zugriff auf die noch unverschlüsselten Kommunikationsinhalte auf verschiedene Weisen erfolgen.

Zum Beispiel stellen einige OTT-Kommunikationsdienste Plug-in-Schnittstellen zur Verfügung, die anderen Herstellern die Entwicklung von Zusatzsoftware (Plug-ins) ermöglichen, die in den Kommunikationsdienst eingebunden dessen Funktionalität erweitern (BSI 2017, S. 79). Über diese Schnittstellen erfolgt der Datenaustausch zwischen Kommunikationsdienst und Plug-ins, was sich die Quellen-TKÜ-Software zunutze machen kann (Petri 2012, S. 28).

Ein anderer Ansatz besteht beispielsweise darin, auf die Datenströme der vom Kommunikationsdienst verwendeten Ein- oder Ausgabegeräte zuzugreifen, etwa Tastatur, Mikrofon, Kamera, Bildschirm oder Lautsprecher (Abb. 5.5).

Abb. 5.5 Zugriffmöglichkeiten einer Quellen-TKÜ



Quelle: angepasst nach Hempel/Rehak 2017, S. 78

Dazu muss die Quellen-TKÜ-Software laufend die Systemabläufe analysieren, um Kommunikationsvorgänge rechtzeitig erkennen zu können. Soll beispielsweise eine über Skype geführte Kommunikation beobachtet werden, geht die Software wie folgt vor:

1. Warten, bis eine Skype-Verbindung aufgebaut wird;
2. Ermitteln, welcher Art die Verbindung ist (Text, Sprache, Video);

3. Zugriff auf die jeweiligen Datenströme und Kopie erstellen;
4. Detektieren, wann Verbindung abgebaut wird, um Beobachtung einzustellen.

Eine weitere Zugriffsmöglichkeit besteht bei den vom Kommunikationsdienst verwendeten Verschlüsselungsbibliotheken, die derart verändert werden, dass die Quellen-TKÜ-Software die zu verschlüsselnden Inhalte direkt abrufen kann. Diese Vorgehensweise umgeht das Problem der Kommunikationserkennung des zuvor genannten Ansatzes, allerdings ist sie technisch sehr anspruchsvoll.

Übermittlung der erhobenen Daten an die Polizeibehörden

Die erhobenen Daten werden von der Quellen-TKÜ-Software entweder in Echtzeit oder dann zu festgelegten Zeitpunkten über das Internet an einen Server der Polizeibehörden übermittelt. Damit die ausgeleiteten Daten vor Zugriffen Dritter geschützt sind, müssen sie für den Transport wirksam verschlüsselt werden.

Steuerung und Wartung der Quellen-TKÜ-Software

Ob eine einmal installierte Quellen-TKÜ-Software weitgehend autonom agiert oder aktiv per Fernzugriff von den Polizeibehörden gesteuert wird, hängt von ihrem Funktionsumfang ab. Voraussetzung für eine Fernsteuerung ist allerdings, dass die Quellen-TKÜ-Software bzw. das Zielsystem dauerhaft über das Internet zu erreichen ist, was jedoch nicht garantiert ist.

Im gleichen Maße wie sich Betriebssysteme und Anwendungssoftware durch Updates ständig ändern, so muss sich auch eine Quellen-TKÜ-Software durch das Einspielen von Aktualisierungen anpassen können, damit sie über einen längeren Beobachtungszeitraum zuverlässig funktioniert.

Entfernung der Quellen-TKÜ-Software aus dem Zielgerät

Sobald eine Beobachtungsmaßnahme beendet wird, muss die Quellen-TKÜ-Software deaktiviert und vom Zielsystem entfernt werden. Der Vorgang kann entweder durch Fernsteuerung und/oder automatisch zu einem in der Software festgeschriebenen Zeitpunkt ausgelöst werden. Weil die Verbindung zum Endgerät auch abreißen kann, sollte die Software in der Lage sein, sich nach einem festgelegten Zeitraum ohne Serverkontakt automatisch zu deaktivieren und zu löschen. In Fällen, in denen eine Quellen-TKÜ-Software tief in die Abläufe des Betriebssystems eingreift, wird es allerdings nicht immer möglich sein, die von der Software vorgenommen Veränderungen im Zielsystem vollständig rückgängig zu machen (Freiling 2007, S. 7).

5.2.3.2 Ausleiten von Daten aus informationstechnischen Systemen (Onlinedurchsuchung)

Bei einer Onlinedurchsuchung stehen nicht laufende Kommunikationsinhalte, sondern alle auf einem informationstechnischen System gespeicherten oder verfügbaren Daten im Fokus der heimlichen Beobachtung aus der Ferne. Von der Quellen-TKÜ unterscheidet sich eine Onlinedurchsuchung daher einzig im Datenzugriff (dazu und zum Folgenden Hempel/Rehak 2017, S. 74 ff.).

Datenzugriff bei einer Onlinedurchsuchung

Eine Software für die Onlinedurchsuchung (OD-Software) hat – sofern sie mit den dafür erforderlichen Zugriffrechten ausgestattet ist – prinzipiell Zugriff auf

- alle im Zielsystem gespeicherten Daten,
- alle flüchtigen Daten im Arbeitsspeicher sowie
- auf die Datenströme von Ein- und Ausgabegeräten und weiteren im Zielsystem verbauten Sensoren.

Beim Zugriff auf Datenspeicher kommt eine Komplettübertragung aller auf dem Zielsystem liegenden Daten in der Regel nicht in Betracht, da erstens die Datenmenge zu groß wäre und zweitens übermäßig viele ermittlungsfremde Daten ausgeleitet würden. Daher versucht die OD-Software in einem ersten Schritt, die mutmaßlich ermittlungsrelevanten Daten mithilfe vorher festgelegter Suchkriterien zu identifizieren. Anhand der Metainformationen der gespeicherten Dateien können die zu übermittelnden Daten auf bestimmte Verzeichnisse (z. B. Benutzerverzeichnis), Dateitypen (z. B. Textdokumente, Bild-, Kalender- oder Adressdateien) oder Zeiträume, während derer die Dateien erstellt bzw. geändert wurden, eingegrenzt werden. Textgebundene Dateien können noch auf dem Zielsystem durch eine inhaltliche Stichwortsuche weiter selektiert werden. Bei anderen Medienarten (z. B. Bilder oder Videos) ist dies trotz der Fortschritte in der Objekterkennung (Kap. 3.3.3) ungleich schwerer, weshalb die Bewertung der Relevanz hier erst nach der Ausleitung erfolgen kann. Hinzu kommt, dass zu arbeitsintensive Prozesse der OD-Software das System ungewöhnlich stark auslasten und so letztlich das Entdeckungsrisiko steigern (Albrecht/Poscher 2017, S. 39).

Der Zugriff auf Arbeitsspeicher, Ein- bzw. Ausgabegeräte und Sensoren eröffnet eine Vielzahl weiterer Datenquellen mit diversen Erkenntnismöglichkeiten, u. a.:

- Arbeitsspeicher: Passwörter, flüchtige Daten der Anwendungsprogramme
- Beschleunigungssensoren: Bewegungs- und Verhaltensprofile
- GPS-Sensoren: Lokalisierung
- Tastatur: Passwörter, Benutzernamen, Textdokumente
- Maus/Touchscreen: Zugangscodes wie PINs

- Bildschirm (Screenshot): betrachtete Bilder/Videos, besuchte Webseiten
- Kamera: optische Beobachtung
- Mikrofon: akustische Beobachtung

Zu beachten ist schließlich, dass eine OD-Software nicht nur auf Smartphones oder PCs, sondern im Prinzip auf sämtlichen internetfähigen Geräten per Fernzugriff installiert werden kann, so etwa auch auf intelligenten Sprachassistenten, smarten Haushaltsgeräten oder weiteren Anwendungen des Internets der Dinge.

5.2.3.3 Abgrenzung zwischen Quellen-TKÜ und Onlinedurchsuchung

Verfassungsrechtliche Gründe machen eine strikte Trennung zwischen Maßnahmen der Quellen-TKÜ und der Onlinedurchsuchung notwendig, da Erstere in das Fernmeldegeheimnis und Letztere in das Grundrecht auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme eingreifen, das gegenüber dem Fernmeldegeheimnis ein höheres Schutzniveau gewährleistet. Konkret muss eine Quellen-TKÜ-Maßnahme nach der Rechtsprechung des Bundesverfassungsgerichts (BVerfG, Urteil vom 27.2.2008, 1 BvR 370/07, Rn. 190 ff.) auf die Ausleitung von Daten aus *laufenden* Kommunikationsvorgängen beschränkt bleiben (dazu Kap. 6.1.2.1).

Aus technischer Sicht allerdings ist eine Software, die Inhalte eines laufenden Kommunikationsvorgangs noch auf dem Endgerät zweifelsfrei als solche identifizieren kann, wenn überhaupt nur mit großem Aufwand zu realisieren. In jedem Fall sind in Abhängigkeit des verwendeten OTT-Kommunikationsdienstes und der Vorgehensweise beim Datenzugriff jeweils spezifische technische Lösungen notwendig. Die grundsätzliche Problematik besteht darin, dass eine Quellen-TKÜ-Software immer nur *für den Versand vorgesehene* Daten erfassen kann, da der Zugriff noch vor der Verschlüsselung erfolgen muss. Ob diese Daten *später* tatsächlich verschickt und so zum Inhalt eines laufenden Kommunikationsvorgangs werden, wird in vielen Fällen nur schwer zu bestimmen sein.

Am ehesten dürfte eine Kausalität zwischen Erzeugung, Verschlüsselung und Versand von Daten noch bei der synchronen Sprachtelefonie anzunehmen sein, wo es intuitiv einleuchtet, dass die durch das Mikrofon aufgenommenen Audiodaten an den Empfänger weitergeleitet werden. Bei asynchronen Kommunikationsformen stellt sich die Situation viel schwieriger dar: Bei Instant-Messaging-Diensten beispielsweise können die in ein Textfeld eingegebenen Zeichen nicht einfach durch regelmäßige Screenshots oder das Mitschneiden der Tastaturaktivitäten beobachtet werden, da die Zielperson den Textentwurf auch wieder verändern oder sich gänzlich gegen ein Versenden entscheiden kann. Die Software muss also zuverlässig erkennen können, ob bzw. wann die Zielperson auf den Sendeknopf drückt, um Textnachrichten nur unmittelbar vor dem Verschlüsselungs- und Sendevorgang ausleiten zu können. Die Schwierigkeiten verschär-

fen sich, wenn Verschlüsselung und Versand voneinander unabhängige Vorgänge sind, wie dies etwa bei der nutzerseitigen E-Mail-Verschlüsselung durch PGP der Fall ist. Um der (jederzeit möglichen) Verschlüsselung durch die Zielperson zuvorzukommen, müssten sämtliche E-Mail-Entwürfe fortlaufend von der Quellen-TKÜ-Software erfasst werden. Gleichwohl dürften die Daten vorerst nicht ausgeleitet werden, denn eine so verschlüsselte E-Mail ist zunächst einmal nichts anderes als eine lokal gespeicherte Datei, die schwerlich alleine schon deshalb als Teil eines laufenden Kommunikationsvorgangs begriffen werden kann, weil sie irgendwann später einmal als E-Mail verschickt werden könnte (Hempel/Rehak 2017, S. 119). Eine technische Lösung, um in diesem Fall nur tatsächlich versendete E-Mails auszuleiten, erscheint sehr anspruchsvoll.

Aber selbst bei der synchronen Sprachtelefonie können je nach Zugriffmodalitäten Schwierigkeiten auftreten: Soll etwa der Datenstrom des Mikrofons ausgeleitet werden, so muss die Quellen-TKÜ-Software zuverlässig erkennen können, wann die Audioübertragung durch Betätigen der Stummschaltefunktion unterbrochen wird, da anderenfalls faktisch eine akustische Wohnraumüberwachung stattfindet (Hempel/Rehak 2017, S. 77 ff.).

5.2.3.4 Risiken für die IT-Sicherheit

Beobachtungsmaßnahmen auf dem Endgerät beeinträchtigen infolge der notwendigen Installation einer Beobachtungssoftware zwingend die Integrität des Zielsystems. In Abhängigkeit der konkreten Ausgestaltung und Durchführung solcher Maßnahmen kann die IT-Sicherheit darüber hinaus für weitere informationstechnisch vernetzte Systeme beeinträchtigt werden.

Technische Risiken durch die heimliche Installation

Aus Sicht der IT-Sicherheit richten sich die Bedenken gegen den Einsatz der Quellen-TKÜ oder Onlinedurchsuchung im Besonderen auf den Vorgang der heimlichen Installation der Beobachtungssoftware auf dem Zielsystem. Mit Ausnahme der direkten Installation durch physischen Zugriff auf das Endgerät implizieren alle möglichen Installationswege eine potenzielle Bedrohung für die IT-Sicherheit auch anderer informationstechnischer Systeme. Dies gilt für die Verwendung von präparierten Dateien, die prinzipiell auch fremde Endgeräte erreichen können (und hier ggf. zu Fehlfunktionen und damit zur Beeinträchtigung der Verfügbarkeit führen), im Besonderen aber für die Nutzung von Schwachstellen in der auf dem Zielsystem installierten Software (Kap. 5.2.3.1).

Die Hauptsorge besteht darin, dass in erster Linie unveröffentlichte, auch den Softwareherstellern noch unbekannte Schwachstellen (Zero-Day-Schwachstellen) eingesetzt werden könnten, die der Staat bei sogenannten Schwachstellenbrokern kauft oder durch eigene Analysen findet (Kasten 5.4).

Kasten 5.4 Lebenszyklus einer Schwachstelle in der Software

Viele Softwareschwachstellen werden vom Hersteller entdeckt und mit einem Softwarepatch gleich behoben. Wird eine Schwachstelle jedoch zuerst durch Dritte gefunden, hängt es vom Verhalten des Entdeckers ab, wie ihr Lebenszyklus verläuft und welche Gefährdungen für die IT-Sicherheit der betroffenen Systeme daraus resultieren. Der Entdecker der Schwachstelle hat mehrere Optionen, er kann

1. alle ihm vorliegenden Erkenntnisse veröffentlichen (Full Disclosure),
2. den Hersteller informieren und keine (bzw. nur wenige) Informationen an die Öffentlichkeit geben (Coordinated Disclosure),
3. die Schwachstelle verheimlichen und selbst für Angriffe nutzen (Zero-Day-Schwachstelle)
4. oder die Schwachstelle gegen teilweise hohe Geldbeträge dem Softwarehersteller, kriminellen Akteuren oder staatlichen Stellen (die sie für Beobachtungszwecke nutzen wollen) zum Kauf anbieten (Schwachstellenbroker).

Sobald der Softwarehersteller direkt (Fall 1 und 2) oder indirekt (Fall 3, sobald der Angriff entdeckt wird; Fall 4, wenn ihm entsprechende Informationen zum Kauf angeboten werden) Kenntnis von der Existenz der Schwachstelle erlangt, beginnt er mit der Entwicklung eines Patches zur Behebung der Schwachstelle. Bis der Patch zur Verfügung steht, sind alle Systeme gefährdet, auf denen die fragliche Software läuft. Erst nach Bereitstellung des Patchs und Installation durch den Anwender ist ein System vor Angriffen sicher; ungepatchte Systeme bleiben weiterhin gefährdet.

Fall 1 läuft auf ein Wettrennen zwischen Hersteller und potenziellen Angreifern hinaus, ob die Schwachstelle schneller behoben oder für großflächige Angriffe ausgenutzt werden kann. In Fall 2 steht den Herstellern mehr Zeit für die Entwicklung eines Patchs zur Verfügung, in Fall 3 hingegen gar keine (daher Zero-Day), da die Schwachstelle bereits für Angriffe ausgenutzt wird. Dies macht Zero-Day-Schwachstellen so gefährlich.

Quelle: BSI 2018

Aus der Perspektive der Polizei- und Strafverfolgungsbehörden besteht der Nutzen von Zero-Day-Schwachstellen darin, dass sie über längere Zeiten bestehen und folglich nutzbar bleiben, zumindest solange, wie der Hersteller keine Kenntnisse über deren Existenz erlangt. Daraus aber könnten für die Polizei- oder Strafverfolgungsbehörden Anreize resultieren, das Vorhandensein von Schwachstellen dem Hersteller (und der Öffentlichkeit) vorzuenthalten. Ein solches Szenario wäre zwingend mit hohen Risiken für die IT-Sicherheit insgesamt verbunden, denn geheim gehaltene Softwareschwachstellen können prinzipiell auch von

kriminellen Akteuren oder fremden Geheimdiensten entdeckt bzw. gekauft und für eigene Zwecke missbraucht werden. Außerdem würde dieses Vorgehen die grauen Märkte für solche Schwachstellen zusätzlich befeuern (Kurz et al. 2016, S. 15; Buermeyer 2017a, S. 13 f.).

Häufig außer Acht gelassen wird jedoch, dass zur Installation einer Beobachtungssoftware nicht zwangsläufig eine auf sämtlichen Endgeräten noch offene Zero-Day-Schwachstelle benötigt wird. In Prinzip genügt dazu auch eine öffentlich bekannte, vom Hersteller bereits behobene Schwachstelle, die aber auf dem Zielsystem noch nicht durch die Installation des entsprechenden Patches geschlossen wurde (Kurz et al. 2016, S. 3). Würden Polizei- und Strafverfolgungsbehörden nur solche Schwachstellen nutzen, würde dies den Aufwand für die Durchführung einer Quellen-TKÜ oder Onlinedurchsuchung zwar deutlich erhöhen, da für jede Maßnahme auf dem Zielgerät ggf. noch vorhandene geeignete Schwachstellen gefunden werden müssten. Auch könnte die Zielperson den entsprechenden Patch jederzeit installieren und damit den Erfolg der Maßnahme gefährden. Aus der Perspektive der IT-Sicherheit jedoch würde dies das Gefährdungspotenzial massiv reduzieren.

Grundsätzlich besteht für jede Station im Lebenszyklus einer Softwareschwachstelle ein Zielkonflikt zwischen dem jeweiligen Nutzen zur Durchführung von Beobachtungsmaßnahmen auf dem Endgerät und den Risiken für die IT-Sicherheit (Tab. 5.1).

Im Sinne eines Ausgleichs zwischen den berechtigten Interessen der Gefahrenabwehr und Strafverfolgung einerseits und der IT-Sicherheit andererseits könnte es ein Ansatz sein, die Nutzung von Softwareschwachstellen mit hohem Gefährdungspotenzial für die IT-Sicherheit per Gesetz auszuschließen (dazu zählen im Besonderen Schwachstellen, die dem Hersteller noch nicht bekannt sind). Dies würde die Durchführung von Beobachtungsmaßnahmen auf dem Endgerät zwar wesentlich erschweren, nicht aber verunmöglichen. Weitergehende Vorschläge zur Ausgestaltung eines tragfähigen Umgangs mit Schwachstellen vor dem Hintergrund den kollidierenden Interessen der zivilen Sicherheit einerseits und der IT-Sicherheit andererseits finden sich z. B. in Herpig (2018).

Tab. 5.1 Nutzen und Risiken der Verwendung von Schwachstellen

Station im Lebenszyklus	Perspektive zivile Sicherheit: Nutzen	Perspektive IT-Sicherheit: Gefährdungspotenzial
Schwachstelle öffentlich bekannt; Patch vorhanden	Schwachstelle nur gerätespezifisch und solange nutzbar, wie die Zielperson Gerät nicht patcht. Dies kann jederzeit erfolgen.	keine Gefährdung für gepatchte Systeme (jedoch hohe Gefährdung für ungepatchte Systeme)
Schwachstelle unveröffentlicht, aber dem Hersteller bekannt; Patch noch nicht vorhanden	Schwachstelle für alle Geräte nutzbar, aber nur solange, wie der Hersteller Patch bereitstellt und dieser auf Zielgerät installiert wird. Dieser Zeitraum kann Wochen bis Monate betragen.	keine unmittelbare Gefährdung (bei Teilveröffentlichung ist Gefährdung abhängig von den öffentlich verfügbaren Informationen)
Schwachstelle veröffentlicht (und dem Hersteller bekannt); Patch noch nicht vorhanden	Wie Zeile zuvor. Allerdings zwingt die Veröffentlichung den Hersteller dazu, den Patch möglichst schnell bereitzustellen, was das Zeitfenster für die Nutzung der Schwachstellen reduziert.	temporär kritische Gefährdung bis zum Zeitpunkt der Bereitstellung des Patchs
Schwachstelle wurde von den Sicherheitsbehörden gefunden; Hersteller und/oder Öffentlichkeit wird nicht informiert	Schwachstelle kann für alle Geräte und über einen längeren Zeitraum genutzt werden.	keine unmittelbare Gefährdung. Falls Schwachstelle jedoch zeitgleich von Dritten (Kriminelle, fremde Geheimdienste) gefunden wird, besteht eine anhaltend kritische Gefährdung
Schwachstelle wurde durch Dritte gefunden; Hersteller und/oder Öffentlichkeit wird nicht informiert	Schwachstelle kann für alle Geräte und über einen längeren Zeitraum genutzt werden.	anhaltend kritische Gefährdung, da die Ausnutzung der Schwachstelle durch Dritte wahrscheinlich ist

Eigene Zusammenstellung

Technische Risiken beim Datenzugriff

Die Integrität des Zielsystems kann nicht nur während der Installation der Beobachtungssoftware, sondern – je nach Vorgehensweise – ggf. auch während des Datenzugriffs beeinträchtigt werden (dazu und zum Folgenden Hempel/Rehak 2017, S. 15 f. u. 39 f.). Nutzt eine Quellen-TKÜ-Software beispielsweise Plug-in-Schnittstellen oder Screenshots bzw. greift eine OD-Software auf gespeicherte

Dateien zu, so verhalten sie sich nicht anders als gewöhnliche Anwendungsprogramme. In diesem Fall bleibt die Integrität des Zielsystems beim Datenzugriff gewahrt, allerdings ist auch das Entdeckungsrisiko höher, da die Beobachtungssoftware wie jedes Anwendungsprogramm u. a. im Taskmanager angezeigt wird.

Anders verhält es sich, wenn die Beobachtungssoftware besser getarnt und beispielsweise auf Bereiche im Arbeitsspeicher oder auf Datenströme von Ein- oder Ausgabegeräten zugreifen soll, die gerade von anderen Anwendungsprogrammen verwendet werden. Hierzu muss die Beobachtungssoftware mit erweiterten Privilegien und Zugriffsrechten auf Hardwarekomponenten ausgestattet werden, die üblicherweise den Prozessen des Betriebssystems vorbehalten sind. Dies läuft jedoch einem wesentlichen Schutzkonzept informationstechnischer Systeme entgegen, welches auf eine strikte Trennung zwischen Anwendungsprogrammen und Betriebssystemprozessen setzt: Um zu vermeiden, dass sich die oft parallel laufenden und um Hardwareressourcen konkurrierenden Anwendungsprogramme gegenseitig (unabsichtlich oder intendiert) stören, können Anwendungsprogramme ausschließlich unter Vermittlung des Betriebssystems auf Arbeitsspeicher, Festplatte, Tastatur, Mikrofon etc. zugreifen. In dem Maße, wie eine Beobachtungssoftware dieses Schutzkonzept aushebelt, um an die gewünschten Daten zu gelangen, werden folglich die im Normalfall durch das Betriebssystem garantierte Integrität und Vertraulichkeit des informationstechnischen Systems bzw. der damit verarbeiteten bzw. gespeicherten Daten gefährdet.

Technische Risiken durch fehlerhafte Beobachtungssoftware

Komplexe Softwareprodukte sind grundsätzlich fehlerbehaftet. Bei Maßnahmen der Quellen-TKÜ oder Onlinedurchsuchung tritt hinzu, dass die Softwareentwicklung aus ermittlungstaktischen Gründen regelmäßig unter Zeitdruck erfolgen dürfte, was auch längere Testphasen ausschließt (Hempel/Rehak 2017, S. 70). Außerdem kann die Software nicht unter der exakten Umgebung des Zielsystems getestet werden, über dessen Konfiguration aus Vorermittlungen zwar vieles, aber vermutlich nicht alles bekannt ist. Ob die Software auf dem Zielsystem wie gewünscht funktioniert oder hier zu Fehlfunktionen führt, dürfte sich laut Bogk (2007, S. 16 f.) letztlich erst während des konkreten Einsatzes herausstellen.

5.2.4 Bewertungsmatrix

Auf der Basis der vorangegangenen Kapitel stellt Tabelle 5.2 überblicksartig die verschiedenen informationstechnischen Beobachtungsverfahren zusammen mit einer *qualitativen* Bewertung ihrer jeweiligen Gefährdungspotenziale für die technische IT-Sicherheit einander gegenüber. Zusätzlich werden die Verfahren hinsichtlich ihrer Streubreite, also der Anzahl von Betroffenen, die keinen Anlass für die Beobachtung gegeben haben, beurteilt. Oft hängt das Ausmaß der Be-

einträchtigung der IT-Sicherheit und der Streubreite jedoch von der konkreten Ausgestaltung einer Maßnahme bzw. der technischen Vorgehensweise ab. Für diese Fälle wird eine Spannbreite angegeben (z. B. gering bis mittel).

Tab. 5.2 Bewertungsmatrix für informationstechnische Beobachtungsverfahren

Informationstechnisches Beobachtungsverfahren	Daten		Beeinträchtigung der technischen IT-Sicherheit			Streubreite
	Inhaltsdaten	Metadaten	Verfügbarkeit	Vertraulichkeit	Integrität	
TKÜ	x	x	nicht betroffen	sehr hoch	nicht betroffen	gering
IMSI-Catcher: Ermittlung IMSI/IMEI und Lokalisation		x	hoch	nicht betroffen	nicht betroffen	gering bis mittel
IMSI-/WLAN-Catcher: Inhaltserfassung	x	x	gering bis hoch	sehr hoch	gering bis mittel	gering bis mittel
Aushebeln von Verschlüsselung	x		nicht betroffen	sehr hoch	gering bis hoch	gering bis hoch
Erhebung Inhaltsdaten beim Diensteanbieter	x		nicht betroffen	sehr hoch	nicht betroffen	gering
individualisierte Verkehrsdatenerhebung		x	nicht betroffen	nicht betroffen	nicht betroffen	gering
Funkzellenabfrage		x	nicht betroffen	nicht betroffen	nicht betroffen	mittel bis hoch
stille SMS		x	nicht betroffen	nicht betroffen	nicht betroffen	gering
Quellen-TKÜ	x	x	gering	sehr hoch	sehr hoch	gering
Onlinedurchsuchung	x	x	gering	sehr hoch	sehr hoch	gering

Quelle: angepasst nach Hempel/Rehak 2017, S. 142

5.3 Polizeiliche Anwendungsfelder: eingriffsrechtliche Perspektive

Informationstechnische Beobachtungsverfahren berühren die rechtlich hochgradig sensiblen Felder der grundrechtlichen Privatheitsgarantien. Einschlägig sind insbesondere das Fernmeldegeheimnis (Artikel 10 Abs. 1 GG) sowie die Grund-

rechte auf informationelle Selbstbestimmung und auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als besondere Ausprägungen des allgemeinen Persönlichkeitsrechts (Artikel 2 Abs. 1 i.V.m. Artikel 1 Abs. 1 GG). Nach den verfassungsrechtlichen Maßstäben des Gesetzesvorbehalts und der Normenklarheit bedarf daher jeder staatliche Einsatz informationstechnischer Beobachtungsverfahren bestimmter und normenklarer Ermächtigungsgrundlagen, die dem Gewicht des jeweiligen Grundrechtseingriffs Rechnung tragen (dazu ausführlich Kap. 6).

Für die Polizeibehörden finden sich derartige Ermächtigungsgrundlagen in der bundeseinheitlichen Strafprozessordnung (Strafverfolgung) sowie im Polizeirecht (Gefahrenabwehr), also im Bundeskriminalamtgesetz, im Bundespolizeigesetz und im Gesetz über das Zollkriminalamt und die Zollfahndungsämter sowie in den Polizeigesetzen der Länder.[133] Nachfolgend werden in Kapitel 5.3.1 die strafprozessualen und in Kapitel 5.3.2 exemplarisch für das Bundeskriminalamt die gefahrenabwehrrechtlichen Befugnisse zum Einsatz informationstechnischer Beobachtungsverfahren aufgeführt. Dies schließt auch eine Diskussion einiger bestehender rechtlicher Unklarheiten und Fragestellungen ein, soweit diese sich auf die einzelnen Maßnahmen bzw. Eingriffsbefugnisse beziehen. Für eine Diskussion übergeordneter regulatorischer Fragestellungen im Kontext des Einsatzes von Beobachtungstechnologien im Bereich der zivilen Sicherheit wird auf Kapitel 6 verwiesen.

Die Analysen in diesem Kapitel basieren auf dem Stand der Gesetzgebung zum Zeitpunkt der Fertigstellung dieses Berichts (Anfang 2020). Jüngere Entwicklungen wie etwa die Anpassung der Regelungen zur Erhebung von Bestands- und Nutzungsdaten von TM-Diensten von Ende März 2021[134] oder die umfassende Novellierung des Telekommunikationsgesetzes mit Wirkung zum 1. Dezember 2021[135] konnten daher nicht mehr berücksichtigt werden.

5.3.1 Strafprozessuale Eingriffsbefugnisse

Die strafprozessualen Befugnisse zum Einsatz informationstechnischer Beobachtungsverfahren finden sich in den §§ 100a ff. StPO (Tab. 5.3).

133 Entsprechende Ermächtigungsgrundlagen für die Nachrichtendienste finden sich im Bundesverfassungsschutzgesetz (BVerfSchG), im Bundesnachrichtendienstgesetz (BNDG), im Gesetz über den militärischen Abschirmdienst (MADG), im Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G10) sowie in den Verfassungsschutzgesetzen der Länder. Auf diese wird in diesem Bericht nicht eingegangen.

134 Gesetz zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27.5.2020 vom 30. März 2021 (BGBl. I S. 448)

135 Telekommunikationsmodernisierungsgesetz vom 23. Juni 2021 (BGBl. I S. 1858) sowie Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien vom 23. Juni 2021 (BGBl. I S. 1982)

Tab. 5.3 Strafprozessuale Eingriffsbefugnisse (nach ansteigender Eingriffsschwelle)

Maßnahme*	Ermächtigungsnorm	Eingriffsschwelle (hier: Schwere der Straftat)
Erhebung von Bestandsdaten (Daten nach §§ 95, 111 TKG) beim Diensteanbieter	§ 100j StPO	alle Straftaten
IMSI-Catcher: Ermittlung der IMSI/IMEI und Lokalisierung	§ 100i StPO	Straftat von erheblicher Bedeutung
Erhebung von Verkehrsdaten nach § 96 TKG:	§ 100g StPO	Straftat von erheblicher Bedeutung oder Straftat, die mittels Telekommunikation begangen wurde***
individualisierte Abfrage**	Abs. 1	
Funkzellenabfrage	Abs. 3 S. 1	
TKÜ	§ 100a Abs. 1 S. 1 StPO	schwere Straftat (Katalogstraftaten nach § 100a Abs. 2 StPO)
Quellen-TKÜ	§ 100a Abs. 1 S. 2 u. 3 StPO	schwere Straftat (Katalogstraftaten nach § 100a Abs. 2 StPO)
Onlinedurchsuchung	§ 100b StPO	besonders schwere Straftat (Katalogstraftaten nach § 100b Abs. 2 StPO)
Erhebung von Verkehrsdaten nach § 113b TKG:	§ 100g StPO	besonders schwere Straftat (Katalogstraftaten nach § 100g Abs. 2 StPO)
individualisierte Abfrage	Abs. 2	
Funkzellenabfrage	Abs. 3 S. 2	

* Regelungen für die Erhebung von Bestands- und Nutzungsdaten von TM-Diensten wurden erst mit dem Gesetz zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27. Mai 2020 vom 30. März 2021 (BGBl. I S. 448) eingeführt. Damit zusammenhängende Änderungen des rechtlichen Rahmens konnten nicht mehr berücksichtigt werden. Dies gilt auch für die Novellierung des TKG und weiterer Gesetze durch das Telekommunikationsmodernisierungsgesetz vom 23. Juni 2021 (BGBl. I S. 1858) und das Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien vom 23. Juni 2021 (BGBl. I S. 1982)

** Die Erhebung von Standortdaten nach § 96 TKG ist unter diesen Voraussetzungen nur für künftig anfallende Daten oder in Echtzeit zulässig (§ 100g Abs. 1 S. 4 StPO). Gespeicherte (retrograde) Standortdaten nach § 96 TKG dürfen nur im Falle besonders schwerer Straftaten (Katalogstraftaten nach § 100g Abs. 2 StPO) erhoben werden (§ 100g Abs. 1 S. 3 StPO).

*** Letzteres gilt nicht für die Erhebung von Standortdaten (§ 100g Abs. 1 S. 3 u. 4 StPO) und die Funkzellenabfrage (§ 100g Abs. 3 S. 1 Nr. 1 StPO)

Eigene Zusammenstellung gemäß StPO in der am 26. November 2019 geltenden Fassung

In Abhängigkeit davon, welche Grundrechte berührt werden und wie intensiv der Grundrechtseingriff ist, werden an die Durchführung der Maßnahmen unterschiedlich hohe verfassungsrechtliche Anforderungen gestellt. Zu diesen gehören u. a.:

- ein grundsätzlicher Richtervorbehalt[136];
- Voraussetzungen an den erforderlichen Grad des Tatverdachts und an die Bedeutung der zu verfolgenden Straftat im Verhältnis zur Eingriffsintensität der jeweiligen Maßnahme (Tab. 5.3);
- Pflichten zur nachträglichen Benachrichtigung von Betroffenen (sobald dies den Ermittlungszielen nicht mehr entgegensteht) sowie Löschpflichten für die erlangten personenbezogenen Daten (sobald sie nicht mehr benötigt werden; §§ 101, 101a StPO);
- das Ultima-Ratio-Prinzip für die TKÜ, Quellen-TKÜ, Onlinedurchsuchung sowie die Erhebung von Verkehrsdaten mittels Funkzellenabfrage oder aus der Vorratsdatenspeicherung. Demnach sind diese Maßnahmen nur zulässig, wenn die Zielerreichung auf andere Weise wesentlich erschwert oder aussichtslos wäre;
- Vorschriften zum Schutz des Kernbereichs privater Lebensgestaltung bei der TKÜ, Quellen-TKÜ und Onlinedurchsuchung (§ 100d StPO).

Die Auslegung und konkrete Anwendung dieser Befugnisse in der polizeilichen Praxis werfen unterschiedliche rechtliche Fragestellungen auf, wie dies nachfolgend anhand einiger relevanter Beispiele gezeigt wird.

5.3.1.1 Fehlende Eingriffsnormen

Keine eigenständigen Eingriffsnormen gibt es für die Erhebung von gespeicherten Kommunikationsinhalten beim Diensteanbieter (Kap. 5.2.2.1) sowie für den Einsatz von WLAN-Catchern (Kap. 5.2.1.2) und von stillen SMS (Kap. 5.2.2.2).

Während die Erhebung von Verkehrsdaten, die beim Diensteanbieter gespeichert sind, nach § 100g StPO an enge Voraussetzungen geknüpft ist, errichtet das Strafprozessrecht mangels entsprechender Regelung keine vergleichbar strengen Anforderungen an die Erhebung von beim Diensteanbieter gespeicherte Inhaltsdaten. Letzteres wird in der Praxis auf die Beschlagnahmevorschriften der §§ 94 ff. StPO gestützt, die den Datenzugriff allerdings unter niedrigeren Voraussetzungen zulassen (dazu Kap. 6.1.4).

Sofern beim WLAN-Catching Daten aus laufenden Kommunikationsvorgängen mitgeschnitten werden, so findet dies laut Bundesregierung (2012, S. 16) auf der Grundlage der Befugnisse zur Durchführung von TKÜ-Maßnahmen statt

136 Bei der Bestandsdatenauskunft setzen lediglich Auskunftsverlangen für Sicherungs- und Zugriffscodes auf Endgeräte (z. B. PIN, PUK) oder externe Speicher (z. B. Cloudspeicher) eine richterliche Anordnung voraus (§ 100j Abs. 3 StPO).

(§ 100a StPO). Ähnlich argumentieren Harnisch und Pohlmann (2009, S. 207) für den Einsatz von IMSI-Catchern zum Mitschneiden des Datenverkehrs im Mobilfunknetz. Diese Auffassung ist allerdings nicht unumstritten. Ulbrich (2019, S. 318 f.) beispielsweise argumentiert, dass sich Maßnahmen des WLAN-Catchings dann nicht mehr über § 100a Abs. 1 StPO (in der vor dem 24. August 2017 geltenden Fassung) bzw. als Annexkompetenz davon rechtfertigen ließen, sobald sie mit Eingriffen in den Datenverkehr der Netzwerkinfrastruktur der Zielperson zum Zweck der Überwindung der Verschlüsselung einhergehen (Kap. 5.2.1.2). Ein solches Vorgehen könne nur auf § 100a Abs. 1 S. 2 StPO (in der ab dem 24. August 2017 geltenden Fassung) gestützt werden, der allerdings erst mit der Reform der Strafprozessordnung von 2017 eingeführt wurde (mit der Konsequenz, dass entsprechende Maßnahmen vor 2017 nicht rechtmäßig erfolgt wären). Wenn die Strafverfolgungsbehörden zur Durchführung der Maßnahme einen eigenen WLAN-Zugangspunkts zur Imitation des Zielnetzwerks aufbauen, so bezeichnet dies Ulbrich (2019, S. 320 ff.) als »informationstechnologische Täuschung«, die unter Vorspiegelung falscher technologischer Tatsachen die Zielperson dazu bewegen soll, unbewusst eine (von ihr unbeabsichtigte) Kommunikationsverbindung zu einer staatlichen Stelle herzustellen. Ein solches Vorgehen wäre somit am Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Kap. 6.1.2.1) zu messen. In der Konsequenz ließen sich solche Maßnahmen ausschließlich auf § 100b Abs. 1 StPO (in der ab dem 24. August 2017 geltenden Fassung) stützen und wären entsprechend an höhere Hürden im Vergleich zur TKÜ zu knüpfen (Ulbrich 2019, S. 336). Selbiges würde entsprechend auch für den Einsatz von IMSI-Catchern zum Mitschneiden des Datenverkehrs im Mobilfunknetz gelten.

Der Einsatz von stillen SMS erfolgte laut Bundesregierung (2012, S. 17, 2014b, S. 3) lange Zeit auf der Grundlage der Befugnisse zur TKÜ (§ 100a StPO) bzw. Erhebung von Verkehrsdaten (§ 100g StPO) in Verbindung mit den Ermittlungsgeneralklauseln der §§ 161, 163 StPO. Diese Rechtsauffassung ist jedoch in Teilen der rechtswissenschaftlichen Literatur auf Kritik gestoßen (z. B. Krüger 2012, S. 609 ff.). Problematisiert wurde weniger die Erhebung der Standortdaten beim Diensteanbieter auf Grundlage der §§ 100a, 100g StPO als vielmehr der Vorgang der Datenerzeugung speziell zu diesem Zweck auf Grundlage der Ermittlungsgeneralklauseln §§ 161, 163 StPO: Weil die gezielte Datenerzeugung als Kern der nachfolgenden Datenabfrage anzusehen sei, stelle sie bereits einen intensiven Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar und bedürfe daher einer eigenen Ermächtigungsgrundlage. Dieser Argumentation folgend beschloss der Bundesgerichtshof (BGH, Beschluss vom 8.2.2018, 3 StR 400/17) 2018, dass das Versenden von stillen SMS nicht weiter auf §§ 161, 163 StPO gestützt werden kann, sondern auf der Grundlage von § 100i Abs. 1 Nr. 2 StPO zu erfolgen habe. Denn mit § 100i StPO, der ursprünglich für den Einsatz von IMSI-Catchern eingeführt wurde, existiert laut Gerichtsbeschluss eine

Vorschrift, die Standortermittlungen bei Mobilfunkgeräten durch Einsatz technischer Mittel explizit regelt und somit auch die Versendung von stillen SMS umfasst. Weiter stellte das Gericht klar, dass die Erhebung der so generierten Standortdaten beim Diensteanbieter nicht auf § 100a StPO gestützt werden kann, weil es beim Versand von stillen SMS an einem menschlich veranlassten Informationsaustausch fehlt, auf dessen Schutz das Fernmeldegeheimnis abzielt. Die Rechtsgrundlage für die Erhebung der maschinell erzeugten Standortdaten ist daher § 100g Abs.1 StPO. In der Praxis wird der Einsatz von stillen SMS durch diesen Gerichtsbeschluss vereinfacht, da die Eingriffsvoraussetzungen der kombinierten Anordnung nach § 100i Abs. 1 i.V.m § 100g Abs. 1 StPO niedriger liegen als bei einer Anordnung nach § 100a i.V.m §§ 161, 163 StPO (Tab. 5.3).

5.3.1.2 Erhebung von Verkehrsdaten beim Diensteanbieter

In der Terminologie der Strafprozessordnung und des Telekommunikationsgesetzes wird zwischen Verkehrsdaten nach § 96 TKG und Verkehrsdaten nach § 113b TKG differenziert:

- Verkehrsdaten nach § 96 TKG sind solche, die Diensteanbieter zu geschäftlichen Zwecken erheben und ggf. speichern, z. B. für Abrechnungs- oder Wartungszwecke (Kap. 5.2.2.2). Die zu geschäftlichen Zwecken gespeicherten Verkehrsdaten werden von den Unternehmen aus datenschutzrechtlichen, aber auch aus wirtschaftlichen Gründen zeitnah wieder gelöscht.
- Verkehrsdaten nach § 113b TKG dagegen werden von den Diensteanbietern unabhängig von ihren Geschäftsinteressen aufgrund einer gesetzlichen Pflicht für einen bestimmten Zeitraum gespeichert, um sie im Bedarfsfall den Strafverfolgungsbehörden zugänglich zu machen (Vorratsdatenspeicherung).

Vertreter der Strafverfolgungsbehörden verweisen regelmäßig auf den hohen praktischen Nutzen von retrograden Verkehrsdaten für die Ermittlungsarbeit (z. B. BKA 2018), da es häufig Vorgänge aufzuklären gilt, die in der Vergangenheit liegen. Allerdings würden die nach § 96 TKG zu geschäftlichen Zwecken gespeicherten Verkehrsdaten aus den zuvor genannten Gründen oft nicht mehr zur Verfügung stehen, wenn sich Strafverfolgungsbehörden mit einem Auskunftsersuchen an die Diensteanbieter wendeten. Dies hat zur Einführung der Vorratsdatenspeicherung geführt, die aufgrund der großen Streubreite – die Diensteanbieter speichern die Verkehrsdaten aller Nutzer – zu einem der umstrittensten informationstechnischen Beobachtungsverfahren gehört. Die vom Gesetzgeber erstmalig 2008 aufgrund einer europäischen Richtlinie[137] eingeführte Vorratsdatenspeicherung (Speicherdauer 6 Monate) wurde vom Bundesverfas-

137 Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG

sungsgericht (BVerfG, Urteil vom 2.3.2010, 1 BvR 256/08, Leitsatz 5) denn auch als ein besonders schwerer Grundrechtseingriff qualifiziert und in ihrer damaligen gesetzlichen Ausgestaltung (allerdings nicht grundsätzlich) als verfassungswidrig erklärt. Das Gericht erachtete u. a. die eingriffsrechtlichen Voraussetzungen zur Erhebung der zu diesem Zweck gespeicherten Verkehrsdaten als zu niedrig. Darüber hinaus erklärte der Gerichtshof der Europäischen Union (EuGH, Urteil vom 8.4.2014, C-293/12 und C-594/12 – Digital Rights Ireland u. a.) im Jahr 2014 die Richtlinie, die den Vorschriften über die Vorratsdatenspeicherung zugrunde lag, wegen eines Grundrechtsverstoßes für nichtig.

Bei der 2015 erneut beschlossenen Einführung der Vorratsdatenspeicherung[138] wurde die Erhebung der nach § 113b TKG gespeicherten Verkehrsdaten daher an deutlich engere Voraussetzungen geknüpft (u. a. das Vorliegen einer besonders schweren Straftat), zudem wurden die Speicherdauern reduziert. Konkret sind Anbieter seit dem 1. Juli 2017 nach den §§ 113a, 113b TKG dazu verpflichtet,

- sämtliche Verkehrsdaten für 10 Wochen zu speichern, u. a.
  - bei Telefondiensten die Rufnummern der beteiligten Anschlüsse sowie Zeit und Dauer der Verbindungen,
  - bei SMS die Rufnummern sowie Sende- und Empfangszeit,
  - bei der Internetnutzung die IP-Adressen, die Kennung des Anschlusses sowie Zeit und Dauer der Internetnutzung;
- sowie für die Mobilfunknutzung sämtliche Standortdaten für 4 Wochen vorzuhalten (durch Angabe der benutzten Funkzellen).

Gleichwohl steht die Rechtmäßigkeit der Vorratsdatenspeicherung auch in ihrer gegenwärtigen Ausgestaltung weiter infrage. Der EuGH entschied 2016, dass auch nationale Vorschriften über die Vorratsdatenspeicherung in den Mitgliedstaaten der EU an den Unionsgrundrechten zu messen sind und – wie dies für die nationalen Regelungen in Schweden und Großbritannien, über die der EuGH zu entscheiden hatte, festgestellt wurde – gegen diese verstoßen können. Zwar hat das Urteil keine unmittelbaren Auswirkungen auf die deutschen Regelungen, allerdings stellte der EuGH klar (Urteil vom 21. Dezember 2016, Rs. C-203/15 und C-698/15), dass eine allgemeine und unterschiedslose Vorratsdatenspeicherung mit der Europäischen Grundrechtecharta nicht vereinbar ist. Dem folgten für die deutschen Regelungen in einem verwaltungsgerichtlichen Eilverfahren das Oberverwaltungsgericht für das Land Nordrhein-Westfalen mit Beschluss vom 22. Juni 2017 und im zugehörigen Hauptsacheverfahren das Verwaltungsgericht Köln mit Urteil vom 20. April 2018 (Kasten 5.5). Bis zu einer endgültigen Entscheidung über die Zulässigkeit der deutschen Regelung zur Vorratsdatenspeicherung durch das Bundesverwaltungsgericht sieht die Bundesnetzagentur von

138 Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015, BGBl. I 2015, S. 2218 ff.

Anordnungen und sonstigen Maßnahmen zur Durchsetzung der Speicherverpflichtungen gegenüber allen verpflichteten Unternehmen ab (Stand März 2022).[139] Zur Klärung der Vereinbarkeit der deutschen Regelung mit dem Unionsrecht hat das Bundesverwaltungsgericht (2019) dem EuGH ein Vorabentscheidungsersuchen vorgelegt.

Kasten 5.5 Ist die Vorratsdatenspeicherung unionsrechtswidrig?

Laut einer Entscheidung des Oberverwaltungsgerichts für das Land Nordrhein-Westfalen (Az. 13 B 238/17) ist die Speicherpflicht für Verkehrs- und Standortdaten zumindest in ihrer gegenwärtigen Ausgestaltung in der Folge des Urteils des EuGH vom 21. Dezember 2016 (Rs. C-203/15 und C-698/15) nicht mit Artikel 15 Abs. 1 der Richtlinie 2002/58/EG[140] vereinbar. Denn die Speicherpflicht erfasse pauschal die Daten nahezu aller Nutzer/innen von Telefon- und Internetdiensten. Erforderlich seien nach dem Urteil des EuGH aber Regelungen, die den Kreis der betroffenen Personen von vornherein auf Fälle beschränkten, bei denen ein zumindest mittelbarer Zusammenhang mit der durch das Gesetz bezweckten Verfolgung schwerer Straftaten bzw. der Abwehr schwerwiegender Gefahren für die öffentliche Sicherheit bestehe. Insbesondere könne die anlasslose Speicherung von Daten nicht dadurch kompensiert werden, dass die Behörden nur zum Zweck der Verfolgung schwerer Straftaten bzw. der Abwehr schwerwiegender Gefahren Zugang zu den gespeicherten Daten erhielten und strenge Maßnahmen zum Schutz der gespeicherten Daten vor Missbrauch ergriffen würden. Dieser Rechtsprechung schloss sich im April 2018 auch das Verwaltungsgericht Köln an.

Quellen: Oberverwaltungsgericht für das Land Nordrhein-Westfalen 2017; Verwaltungsgericht Köln 2018

5.3.1.3 Unklare Behandlung von OTT-Kommunikationsdiensten

Ein weitgehend noch ungelöstes Problem stellt die Behandlung von OTT-Kommunikationsdiensten[141] (E-Mail, Instant-Messaging-Dienste etc.) im Strafverfahren dar. Im Kern geht es um die Frage, ob solche Dienste auch unter dem

139 https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/Oeffentliche Sicherheit/Ueberwachung_Auskunftsert/VDS_113aTKG/node.html (31.3.2022)

140 Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)

141 Die rechtlichen Grundlagen für die Behandlung von OTT-Diensten wurden 2021 durch das Gesetz zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27. Mai 2020 sowie durch das Telekommunikationsmodernisierungsgesetz umfassend erneuert. Die hier vorgenommenen Analysen stellen daher nicht mehr den aktuellen Sachstand dar.

strafprozessualen Begriff der Telekommunikation subsumiert werden können und als solche dann auch in den Anwendungsbereich der für Beobachtungsmaßnahmen einschlägigen Eingriffsnormen §§ 100a ff. StPO fallen. Ist dies nicht der Fall, so müssen strafprozessuale Inhalts- oder Metadatenerhebungen bei den Anbietern von OTT-Kommunikationsdiensten auf andere Eingriffsnormen gestützt werden, die aber möglicherweise der Eingriffsintensität der Maßnahmen nicht gerecht werden. Darüber hinaus ist auch die telekommunikationsrechtliche Einordnung von OTT-Kommunikationsdiensten problematisch. Dieses Problem ist für behördliche Datenerhebungen aus solchen Diensten relevant, da sich das Telekommunikations- und das Telemedienrecht in Bezug auf die Anbieterpflichten zur Mitwirkung bei behördlichen Datenerhebungen stark unterscheiden. So sind Anbieter von TK-Diensten gemäß §§ 110 ff. TKG zu weitreichenden technischen Vorkehrungen zur Ermöglichung von TKÜ-Maßnahmen und von Datenübermittlungen verpflichtet. Im Gegensatz dazu dürfen Anbieter von TM-Diensten auf Anfrage der Behörden zwar Auskünfte über Bestands- oder Nutzungsdaten erteilen (§ 14 Abs. 2 u. § 15 Abs. 5 S. 4 TMG), darüberhinausgehende technische Vorbereitungs- und Kooperationspflichten enthält das TMG aber nicht.

Die Schwierigkeiten resultieren aus dem komplexen Zusammenspiel zwischen drei Regelungsregimen – nämlich Strafverfahrensrecht, Telekommunikations- und Telemedienrecht sowie Verfassungsrecht – die möglicherweise für den Begriff der Telekommunikation jeweils unterschiedliche Auslegungen erlauben (dazu und zum Folgenden Bäcker 2019). Beim TK- bzw. TM-Recht, bei dem diese Diskussion vor allem geführt wird, werden OTT-Kommunikationsdienste der überwiegenden Meinung nach nicht als TK-, sondern als TM-Dienste eingestuft, wobei diese Frage allerdings letztinstanzlich noch nicht entschieden wurden (Kasten 5.6). Aus verfassungsrechtlicher Sicht hingegen liegt es nahe, dass zumindest OTT-Kommunikationsdienste, die einer Individualkommunikation zwischen Menschen dienen (E-Mail, Instant-Messaging-Dienste etc.), dem Fernmeldegeheimnis des Artikel 10 GG unterfallen und somit auch zu den besonders schützenswerten Telekommunikationsmitteln gehören.[142] Damit stellt sich die Frage, ob der strafprozessuale TK-Begriff am TK-rechtlichen oder am verfassungsrechtlichen Sprachgebrauch anknüpft, wobei zusätzlich zwischen der Erfassung von Inhalten und von Metadaten der Kommunikation zu unterscheiden ist.

In Bezug auf die Erfassung von Kommunikationsinhalten wird diese Frage selten näher erörtert. Eine verfassungsrechtlich orientierte Auslegung spricht für eine Subsumtion solcher Dienste unter § 100a StPO, da diese Norm dem besonderen grundrechtlichen Schutz des Artikel 10 GG Rechnung tragen soll. Hinzu kommt, dass die Regulierung der Quellen-TKÜ nach § 100a Abs. 1 S. 2

142 Für E-Mails wurde dies auch schon mehrfach gerichtlich festgestellt, z. B. BVerfG, Urteil vom 27.7.2005, 1 BvR 668/04, Rn. 139; Beschluss vom 16.6.2009, 2 BvR 902/06, Rn. 42 ff.

u. 3 StPO wenig Sinn ergäbe, wenn OTT-Kommunikationsdienste (um die es dabei in erster Linie geht) gar keine Telekommunikation im Sinne des Strafverfahrensrechts wären. In diesem Fall würde beispielsweise die Echtzeiterfassung von Inhalten laufender E-Mail-Kommunikation eines Beschuldigten eine TKÜ darstellen, für die die Voraussetzungen von § 100a StPO vorliegen müssten, sodass nach § 100a Abs. 4 StPO auch der E-Mail-Anbieter zur Mitwirkung verpflichtet wäre. Zugleich gilt aber auch, dass der Anbieter keine besonderen technischen Einrichtungen zur Umsetzung solcher Maßnahmen nach §§ 110 ff. TKG bereithalten müsste, da er aus TK-rechtlicher Sicht keinen TK-, sondern einen TM-Dienst betreibt. Folglich wäre eine Inhaltserfassung in Echtzeit beim Diensteanbieter rechtlich zwar möglich, die praktische Durchführung aber häufig schwierig. Anders läge der Fall, wenn sich die Auslegung des strafprozessualen TK-Begriffs stärker am TK-Recht orientierte: Aus der Nichteinstufung eines OTT-Kommunikationsdienstes als TK-Dienst im Sinne des Strafverfahrensrechts folgte unter Umständen die Konsequenz, dass eine Echtzeiterfassung laufender OTT-Kommunikation beim Diensteanbieter mangels gesetzlicher Ermächtigung nicht zulässig wäre.

Andere Fragen und Probleme stellen sich in Bezug auf die Erhebung von Metadaten. Werden OTT-Kommunikationsdienste strafverfahrensrechtlich nicht als TK-, sondern als TM-Dienste einstuft, schließt dies die Anwendung von § 100g StPO, der sich explizit auf Verkehrsdaten im Sinne der TK-Rechts bezieht, aus. Eine eigenständige strafprozessuale Eingriffsnorm, die die Erhebung von Nutzungsdaten von TM-Diensten an vergleichbar enge Voraussetzungen knüpfen würde, existiert jedoch nicht. Da auch das TMG, nach welchem sich die Beauskunftung durch den Diensteanbieter dann richtet, keine besonderen Eingriffsschwellen vorsieht, wird die Erhebung von TM-Nutzungsdaten in der Praxis auf die Ermittlungsgeneralklausel in §§ 161, 163 StPO oder auf die Beschlagnahmevorschriften der §§ 94 ff. StPO gestützt. Diese Normen lassen aber den Datenzugriff unter niedrigeren Voraussetzungen zu, als sie für die Erhebung von Verkehrsdaten nach § 100g StPO zu beachten sind. Eine Differenzierung des Schutzniveaus von Metadaten der Kommunikation in Abhängigkeit von technischen Unterschieden beim verwendeten Telekommunikationsmittel leuchtet aber vor dem Hintergrund der zunehmenden Bedeutung von OTT-Kommunikationsdiensten nicht unmittelbar ein (dazu auch Kap. 6).[143]

143 Ein Beispiel zur Lösung des Problems wäre § 52 BKAG, der TK-Verkehrsdaten und TM-Nutzungsdaten gleichbehandelt und damit die Abgrenzung praktisch obsolet macht (Kap. 5.3.2).

Kasten 5.6 Unterliegen OTT-Kommunikationsdienste dem TKG?

Gemäß § 3 Nr. 24 TKG sind »›Telekommunikationsdienste‹ in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen …«. Laut Grünwald und Nüßing (2016, S. 94 f.) dürfte bereits das Merkmal der Entgeltlichkeit zumindest für solche OTT-Kommunikationsdienste nicht zutreffen, die ohne direkte Zahlungen der Endnutzer an die Anbieter finanziert werden. Auch was das Merkmal der Datenübertragung betrifft, nutzen OTT-Kommunikationsdienste dazu hauptsächlich das Internet, also fremde TK-Netze. Ob ein Dienst an der Übertragung der Signale *überwiegend* beteiligt ist, dürfte damit am ehesten noch für Client-Server-Modelle zutreffen, nicht aber unbedingt für hybride Peer-to-Peer-Modelle (Kap. 5.2.2.1). OTT-Kommunikationsdienste können daher nicht grundsätzlich als TK-Dienste i.S.d. TKG klassifiziert werden (WD 2016b, S. 8). So entschied etwa der Europäische Gerichtshof (EuGH, Urteil vom 13. Juni 2019, C-193/18) im Juni 2019, dass der E-Mail-Dienst Gmail – ein für die Nutzer/innen kostenloser, aber werbefinanzierter Dienst – nicht als TK-Dienst i.S.d. TKG anzusehen ist, weil er keine Signalübertragung umfasst, und revidierte damit die anderslautende Entscheidung des Verwaltungsgerichts Köln (VG Köln, Urteil vom 11. November 2015, Az. 21 K 450/15) von 2015. Ebenfalls im Juni 2019 entschied der EuGH (Urteil vom 5. Juni 2019, C-142/18) in einem anderen Fall, dass ein OTT-Kommunikationsdienst wie Skype mit einer VoIP-Funktion, mit der ein Nutzer einen Festnetz- oder Mobilfunkanschluss anrufen kann, hingegen als TK-Dienst i.S.d. TKG einzustufen ist.

Quellen: Grünwald/Nüßing 2016, S. 93 f.; WAR 2016, S. 1

5.3.1.4 Quellen-TKÜ und Onlinedurchsuchung

Quellen-TKÜ

Eine klare rechtliche Grundlage für den Einsatz von Maßnahmen der Quellen-TKÜ zu Zwecken der Strafverfolgung wurde erst mit der Reform der Strafprozessordnung von 2017 mit § 100a Abs. 1 S. 2 u. 3 StPO geschaffen.[144] Davor war die Zulässigkeit umstritten gewesen, wobei teilweise die Ansicht vertreten wurde, dass die Quellen-TKÜ rechtlich wie eine herkömmliche TKÜ zu behandeln und folglich durch § 100a StPO (a. F.) gedeckt sei (Krauß 2015, S. 119 ff.). Mit der Reform wurde § 100a StPO um spezifische Eingriffsregelungen für die Quellen-TKÜ erweitert. Demnach darf eine Quellen-TKÜ unter denselben eingriffsrecht-

144 Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017. BGBl. 2017 I, S. 3202

lichen Voraussetzungen durchgeführt werden wie eine herkömmliche TKÜ, sofern bestimmte Sicherstellungen technischer Art erfüllt werden. Dazu gehört zum einen die Einschränkung des § 100a Abs. 5 Nr. 1a StPO, nach welcher technisch sicherzustellen ist, dass ausschließlich laufende Telekommunikation ausgeleitet wird. Dies trägt der Forderung des Bundesverfassungsgerichts (BVerfG, Urteil vom 27.2.2008, 1 BvR 370/07, Rn. 190) Rechnung, wonach eine Quellen-TKÜ nur unter dieser Bedingung als Eingriff in das Fernmeldegeheimnis zu werten ist und folglich auch unter denselben Voraussetzungen wie eine TKÜ durchgeführt werden darf. Ob es in der Praxis allerdings immer möglich sein wird, nur solche Daten auszuleiten, die nach ihrer Verschlüsselung auch tatsächlich verschickt werden, ist aus technischen Gründen zumindest anzuzweifeln (Kap. 5.2.3.3).

Zum anderen erlaubt darüberhinausgehend § 100a Abs. 5 Nr. 1b StPO auch die Ausleitung von Inhalten und Umstände der Kommunikation, die »ab dem Zeitpunkt der Anordnung … auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz hätten überwacht und aufgezeichnet werden können«. Dies ermöglicht den Zugriff auf im Zielgerät gespeicherte Inhalte aus *zurückliegenden* Kommunikationsvorgängen, bei denen es sich rein formal nicht mehr um Daten aus einem laufenden Kommunikationsvorgang handelt. Ob dies den zuvor genannten Anforderungen des Bundesverfassungsgerichts an eine Quellen-TKÜ noch gerecht wird, ist umstritten (kritisch z. B. Voßhoff 2017, S. 3; zustimmend z. B. Krauß 2017, S. 7 f.).

Zu den Sicherstellungen technischer Art gehört schließlich, dass die am informationstechnischen System »vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden« (§ 100a Abs. 5 Abs. Nr. 3 StPO). Die gewählte Formulierung legt die Vermutung nahe, dass auch der Gesetzgeber nicht davon ausging, dass eine einmal installierte Quellen-TKÜ-Software in jedem Fall vollständig aus dem betroffenen Endgerät wieder entfernt werden kann (Kap. 5.2.3.1).

Unabhängig von der Frage, ob sich eine Quellen-TKÜ auf Daten laufender Telekommunikation zu beschränken habe, fordern kritische Stimmen deutlich höhere Eingriffsschwellen für die Durchführung einer Quellen-TKÜ als sie für herkömmliche TKÜ-Maßnahmen gelten, so etwa die (ehemalige) Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Andrea Voßhoff (2017, S. 2 f.) oder der Chaos Computer Club (Neumann et al. 2017, S. 10 f.). Begründet wird dies damit, dass die Eingriffstiefe einer Quellen-TKÜ die einer herkömmlichen TKÜ überschreitet, wenn damit verbundene Risiken für die IT-Sicherheit (Kap. 5.2.3.4) und – aufgrund der schwierigen technischen Abgrenzung zu einer Onlinedurchsuchung (Kap. 5.2.3.3) – für die Grundrechte der Betroffenen mitbedacht werden. Höhere Eingriffsschwellen insbesondere in Bezug auf die Schwere der Straftaten seien daher nötig, um zu verhindern, dass künftig Maßnahmen der

Quellen-TKÜ ähnlich häufig eingesetzt werden wie heute herkömmliche TKÜ-Maßnahmen.

Die verfassungsrechtliche Zulässigkeit der neuen strafprozessualen Befugnisse zum Einsatz der Quellen-TKÜ ist Gegenstand mehrerer Verfassungsbeschwerden, die 2018 eingereicht wurden (u. a. von Rechtsanwält/innen, Künstler/innen und Journalist/innen, darunter auch einige Mitglieder des Deutschen Bundestages; Aktenzeichen 2 BvR 897/18, 2 BvR 1797/18, 2 BvR 1838/18, 2 BvR 1850/18, 2 BvR 2061/18).[145]

Onlinedurchsuchung

Mit der Reform der Strafprozessordnung 2017 wurde außerdem die Befugnis zur Durchführung von Onlinedurchsuchungen zu Zwecken der Strafverfolgung eingeführt (§ 100b StPO). Maßnahmen der Onlinedurchsuchung sind verfassungsrechtlich am Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu messen, welches das Bundesverfassungsgericht (BVerfG, Urteil vom 27.2.2008, 1 BvR 370/07) 2008 im Zusammenhang mit dem Einsatz der Onlinedurchsuchung im Bereich der Gefahrenabwehr entwickelte und welches den Grundrechtsschutz des eigenen informationstechnischen Systems besonders hervorhebt (Kap. 6.1.2.1). Folglich errichtete das Bundesverfassungsgericht sehr hohe Hürden für die Durchführung von gefahrenabwehrrechtlichen Onlinedurchsuchungen, u. a. das Vorliegen von tatsächlichen Anhaltspunkten einer konkreten Gefahr für ein überragend wichtiges Rechtsgut (Kap. 5.3.2).[146]

Entsprechend wurde auch der Einsatz der Onlinedurchsuchung zu Zwecken der Strafverfolgung an sehr enge eingriffsrechtliche Voraussetzungen geknüpft, u. a. müssen die Maßnahmen auf Antrag der Staatsanwaltschaft durch die zuständige Kammer des Landgerichts angeordnet werden (§ 100e Abs. 2 StPO) und sind nur in Fällen von besonders schweren Straftaten gemäß Straftatenkatalog des § 100b Abs. 2 StPO zulässig. Gleichwohl gibt es unter Juristen unterschiedliche Ansichten darüber, ob alle im Katalog aufgeführten Straftaten mit den durch das Bundesverfassungsgericht aufgestellten Schranken für die gefahrenabwehrrechtliche Onlinedurchsuchung (konkrete Gefahr für ein überragend wichtiges Rechtsgut) korrespondieren (zustimmend z. B. Krauß 2017, S. 9 ff.; kritisch z. B. Buermeyer 2017b, S. 7 ff., laut welchem Rechtsgüter wie etwa Eigentum oder Vermögen den Einsatz der Onlinedurchsuchung per se nicht rechtfertigen können). Diese Frage dürfte durch das Bundesverfassungsgericht geklärt werden, da sich

145 www.bundesverfassungsgericht.de/DE/Verfahren/Jahresvorausschau/vs_2019/vorausschau_2019_node.html (31.3.2022)

146 Zu den überragend wichtigen Rechtsgütern zählt das Bundesverfassungsgericht (BVerfG, Urteil vom 27.2.2008, 1 BvR 370/07, Leitsatz 2) Leib, Leben und Freiheit der Person, ferner solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.

die zuvor genannten Verfassungsbeschwerden auch auf die neuen strafprozessualen Befugnisse für den Einsatz der Onlinedurchsuchung beziehen.

5.3.2 Gefahrenabwehrrechtliche Eingriffsbefugnisse

Die polizeiliche Gefahrenabwehr ist vorrangig Aufgabe der Bundesländer (Kap. 2.4; zum Abgrenzungsproblem zwischen präventivem und repressivem polizeilichem Handeln siehe Kap. 6.2.1). Entsprechend sind die gefahrenabwehrrechtlichen Befugnisse für den Einsatz informationstechnischer Beobachtungsverfahren in den Polizeigesetzen der Länder geregelt. Eine Übersicht über die einschlägigen Normen ausgewählter Maßnahmen findet sich beispielsweise in der Analyse des Wissenschaftlichen Dienstes (2017b).

Die gefahrenabwehrrechtlichen Befugnisse der Polizeibehörden des Bundes beschränken sich auf spezifische Aufgabenbereiche (Kap. 2.4.2). Zur Erfüllung dieser Aufgaben dürfen Bundespolizei, Bundeskriminalamt und das Zollkriminalamt bzw. die Zollfahndungsämter auch – in unterschiedlichem Umfang – informationstechnische Beobachtungsverfahren einsetzen. Die gefahrenabwehrrechtlichen Eingriffsnormen sind in Tabelle 5.4 exemplarisch für das Bundeskriminalamt aufgeführt, das im Rahmen seiner Aufgaben zur Abwehr von Gefahren des internationalen Terrorismus (§ 5 BKAG) mit den weitreichendsten Befugnissen ausgestattet wurde.

Wie im Strafprozessrecht (Kap. 5.3.1) auch stehen die Maßnahmen (außer bei der Bestandsdatenauskunft[147]) unter einem Richtervorbehalt und kommen nur als Ultima Ratio in Betracht. Außerdem sind Benachrichtigungs- und Löschpflichten (§§ 74, 79 BKAG) und bei Maßnahmen der TKÜ, Quellen-TKÜ und Onlinedurchsuchung Vorschriften zum Schutz des Kernbereichs privater Lebensgestaltung zu beachten (§ 49 Abs. 7, § 51 Abs. 7 BKAG). Schließlich fehlen auch hier eigenständige Eingriffsnormen für die Erhebung von gespeicherten Kommunikationsinhalten beim Diensteanbieter sowie für den Einsatz von WLAN-Catchern oder von stillen SMS.

147 Richtervorbehalt nur bei Auskunftsverlangen für Sicherungs- und Zugriffscodes auf Endgeräte oder externe Speicher (§ 40 Abs. 3 BKAG).

Tab. 5.4 Gefahrenabwehrrechtliche Eingriffsbefugnisse für das BKA (Reihenfolge der Verfahren wie in Tab. 5.3)

Maßnahme*	Ermächtigungsnorm	Eingriffsschwelle (hier: Gefahrenschwelle)
Erhebung von Bestandsdaten (Daten nach §§ 95, 111 TKG) beim Diensteanbieter	§ 40 BKAG	Abwehr von Gefahren durch terroristische Straftaten oder Verhütung solcher Straftaten
IMSI-Catcher: Ermittlung der IMSI/IMEI und Lokalisierung	§ 53 BKAG	wie TKÜ
Erhebung von Verkehrsdaten nach § 96 TKG oder von Telemedien-Nutzungsdaten	§ 52 BKAG	wie TKÜ
TKÜ	§ 51 Abs. 1 BKAG	Abwehr von dringenden Gefahren für besonders wichtige Rechtsgüter durch terroristische Straftaten oder Verhütung solcher Straftaten
Quellen-TKÜ	§ 51 Abs. 2 BKAG	wie TKÜ
Onlinedurchsuchung	§ 49 BKAG	Abwehr von Gefahren für überragend wichtige Rechtsgüter durch terroristische Straftaten oder Verhütung von Schäden für solche Rechtsgüter durch terroristische Straftaten

* Regelungen für die Erhebung von Bestandsdaten von TM-Diensten wurden erst mit dem Gesetz zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27. Mai 2020 vom 30. März 2021 (BGBl. I S. 448) eingeführt. Damit zusammenhängende Änderungen des rechtlichen Rahmens konnten nicht mehr berücksichtigt werden.

Eigene Zusammenstellung gemäß BKAG vom 1. Juni 2017

Es gibt aber auch einige Unterschiede zu den strafprozessualen Regelungen, u. a.:

- Eine den strafprozessualen Regelungen vergleichbare systematische Abstufung der Eingriffsschwellen in Abhängigkeit der jeweiligen Eingriffstiefe der Maßnahmen fehlt. So gelten für den Einsatz von IMSI-Catchern zur Ermittlung der IMSI/IMEI und Lokalisierung, für die Erhebung von Verkehrsdaten nach § 96 TKG sowie für die Durchführung von TKÜ- und Quellen-TKÜ-Maßnahmen dieselben eingriffsrechtlichen Voraussetzungen. In Bezug auf die Gefahrenschwelle sind dies zum einen – rechtsgutbezogen – die Abwehr

einer dringenden Gefahr für besonders wichtige Rechtsgüter[148] im Zusammenhang mit terroristischen Straftaten nach § 5 Abs. 1 S. 2 BKAG und zum anderen – straftatbezogen – die Verhütung von terroristischen Straftaten nach § 5 Abs. 1 S. 2 BKAG. Voraussetzung für eine Onlinedurchsuchung ist dagegen die Abwehr von Gefahren für überragend wichtige Rechtsgüter[149] durch terroristische Straftaten nach § 5 Abs. 1 S. 2 BKAG oder die Verhütung von Schäden für solche Rechtsgüter durch terroristische Straftaten.

- Die Befugnis des BKA zur Erhebung von Verkehrsdaten bezieht sich nur auf Verkehrsdaten nach § 96 TKG, die vom Diensteanbieter zu geschäftlichen Zwecken verarbeitetet werden, nicht aber auf vorratsgespeicherte Verkehrsdaten nach § 113b TKG. Auf Letztere dürfen nach § 113c Abs. 1 Nr. 2 TKG nur Gefahrenabwehrbehörden der Länder bei Vorliegen entsprechender gesetzlicher Bestimmungen zugreifen.
- Für die Funkzellenabfrage fehlt es an einer Legaldefinition, ihre Durchführung basiert auf der Formulierung, dass eine »räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation« für die Anordnung einer Verkehrsdatenerhebung genügt (§ 52 Abs. 3 S. 2 BKAG).

5.4 Polizeiliche Anwendungsfelder: aktuelle Einsatzpraktiken

Öffentlich zugängliche Informationsquellen zur Einsatzpraxis von informationstechnischen Beobachtungsverfahren durch Polizei- und Strafverfolgungsbehörden liegen bis dato – wenige Ausnahmen ausgenommen – nur sehr spärlich vor. Dies gilt für den Bereich der Strafverfolgung, vor allem aber für den Bereich der polizeilichen Gefahrenabwehr.

In Bezug auf die Anwendungshäufigkeit öffentlich gut dokumentiert ist lediglich der strafprozessuale Einsatz von Maßnahmen der TKÜ nach § 100a StPO einschließlich Quellen-TKÜ und der Verkehrsdatenerhebung nach § 100g StPO, für die es bundesweit gesetzliche Berichtspflichten gibt. Die auf dieser Datenbasis erstellten Übersichten werden als TKÜ-Statistik seit 2000 für TKÜ-Maßnahmen und seit 2008 für Maßnahmen der Verkehrsdatenerhebung jährlich durch das Bundesamt für Justiz veröffentlicht.[150] Vor den jüngsten Reformen der Strafprozessordnung verlangten die Berichtspflichten allerdings weder eine Auf-

148 § 51 Abs. 1 Nr. 1 BKAG nennt hier Gefahren für den Bestand oder die Sicherheit des Bundes oder eines Landes, für Leib, Leben oder Freiheit einer Person oder für Sachen von bedeutsamem Wert, deren Erhaltung im öffentlichen Interesse liegt.

149 § 49 Abs. 1 BKAG nennt hier Gefahren für Leib, Leben oder Freiheit einer Person oder für solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt.

150 Die TKÜ-Statistik ist abrufbar unter www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung_node.html (31.3.2022)

schlüsselung nach TKÜ- bzw. Quellen-TKÜ-Maßnahmen noch eine Differenzierung danach, ob es sich um eine individualisierte Verkehrsdatenerhebung oder Funkzellenabfragen handelte.[151] Dies wurde erst mit den Reformen der Strafprozessordnung von 2015 und 2017 umgesetzt, in deren Rahmen zusätzlich gesonderte Berichtspflichten für die Erhebung von Verkehrsdaten nach § 96 TKG bzw. nach § 113b TKG verankert wurden (§ 101b Abs. 2 u. 5 StPO). Mit der Einführung der strafprozessualen Onlinedurchsuchung wurde schließlich auch eine jährliche Berichtspflicht für diese Maßnahme implementiert (§ 101b Abs. 3 StPO). Die Statistiken nach den neuen Berichtspflichten wurden für die Verkehrsdatenerhebung erstmalig für das Berichtsjahr 2018 und für die TKÜ/Quellen-TKÜ bzw. Onlinedurchsuchung erstmalig für das Berichtsjahr 2019 erstellt.[152]

Berichtspflichten für den gefahrenabwehrrechtlichen Einsatz informationstechnischer Beobachtungsverfahren wurden im Zuge der Reform des Bundeskriminalamtsgesetzes von 2017 festgeschrieben: Nach § 88 BKAG muss das Bundeskriminalamt alle 2 Jahre die Bundesregierung und den Deutschen Bundestag u. a. darüber unterrichten, in welchem Umfang von welchen Befugnissen aus Anlass welcher Art von Verdachtslagen Gebrauch gemacht wurde. Die ersten beiden Berichte liegen für den Berichtszeitraum von Mai 2019 bis April 2021 vor (Bundesregierung 2019h, 2021a). Der Gesetzgeber erfüllte damit eine Forderung des Bundesverfassungsgerichts (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, Rn. 142 f.), das gesetzlichen Berichtspflichten als notwendig ansah, »um eine öffentliche Diskussion über Art und Ausmaß der auf diese Befugnisse gestützten Datenerhebung … zu ermöglichen und diese einer demokratischen Kontrolle und Überprüfung zu unterwerfen«.

Weil es mit Ausnahme der strafprozessualen TKÜ und Verkehrsdatenerhebung sowie ersten Berichterstattungen durch das BKA gemäß § 88 BKAG an amtlichen Statistiken zur Anwendungshäufigkeit weitgehend fehlt, basieren die Ausführungen in diesem Kapitel im Wesentlichen auf öffentlich verfügbaren Informationen aus Parlamentsdokumenten, im Besonderen aus Antworten der Bundesregierung oder von Landesregierungen auf entsprechende parlamentarische Anfragen. Gleichwohl erlauben auch diese Informationsquellen oftmals nur sehr fragmentarische Einblicke in die polizeiliche Einsatzpraxis: Zum einen stuft etwa die Bundesregierung diesbezügliche Auskünfte zum Teil als Verschlusssache ein, da befürchtet wird, dass deren Veröffentlichung Rückschlüsse auf Vorgehensweisen, Fähigkeiten und Methoden der Sicherheits- und Strafverfolgungsbehörden erlauben könnten, was von Nachteil für die Aufgabenerfüllung der durchführenden Stellen und damit für die Interessen der Bundesrepublik Deutschland wäre (z. B. Bundesregierung 2019c, S. 1 f.). Zum anderen erlauben die Regierungsantworten kein einheitliches Bild über die Einsatzpraktiken vor allem bei den

151 Vergleiche § 100b Abs. 5 u. 6 StPO in der vor dem 24. August 2017 geltenden Fassung sowie § 100g Abs. 4 StPO in der vor dem 18. Dezember 2015 geltenden Fassung.

152 §§ 12 und 16 Einführungsgesetz zur Strafprozessordnung, das zuletzt durch Artikel 8 des Gesetzes vom 17. August 2017 (BGBl. I S. 3202) geändert worden ist.

Landespolizeien, da entweder entsprechende Anfragen in den Landesparlamenten ausblieben oder die Berichterstattung sehr uneinheitlich erfolgte. Aus diesem Grund liegt der Schwerpunkt dieses Kapitels auf dem Einsatz informationstechnischer Beobachtungsverfahren durch die Polizei- und Strafverfolgungsbehörden des Bundes. Schließlich finden sich zu einigen informationstechnischen Beobachtungsverfahren gar keine belastbaren Informationen zu den Fallzahlen, beispielsweise für die Erhebung von Kommunikationsdaten beim Diensteanbieter auf Grundlage von Ermittlungsgeneralklauseln (z. B. §§ 161, 163 StPO) oder Beschlagnahmevorschriften (z. B. §§ 94 ff. StPO).

In noch weit geringerem Maße als verlässliche Angaben zur Anwendungshäufigkeit der Maßnahmen durch Polizei- und Strafverfolgungsbehörden finden sich (aktuelle) empirische Untersuchungen oder auch nur belastbare Aussagen zum Nutzen von informationstechnischen Beobachtungsverfahren für die Gefahrenabwehr oder Strafverfolgung. So erachtet beispielsweise die Bundesregierung den Einsatz der Maßnahmen zwar grundsätzlich als wesentlich für die Aufklärung von Straftaten – so etwa von IMSI- oder WLAN-Catchern, von stillen SMS oder von Funkzellenabfragen (Bundesregierung 2019c, S. 6 f. u. 10; 2017d, S. 5; 2015c, S. 13). Eine darüberhinausgehende Bewertung des Nutzens sei jedoch in der Regel nicht möglich, was wie folgt begründet wird (z. B. Bundesregierung 2019c, S. 7): »[D]ie Aufklärung von Straftaten bzw. die Abwehr von Gefahren [ist] abhängig von verschiedenen Faktoren. Welche Maßnahmen wesentlich zur Aufklärung einer Straftat oder zur Abwehr einer Gefahr beigetragen haben, ist von Fall zu Fall unterschiedlich und kann in vielen Fällen nicht genau bestimmt werden.« Dieser Aussage ist nur bedingt zuzustimmen. So wurden in Deutschland in der Vergangenheit systematische empirische Untersuchungen durchgeführt, um den Nutzen der strafprozessualen TKÜ und der Verkehrsdatenerhebung für die Ermittlungsarbeit und für den weiteren Verfahrensverlauf (Anklage, Verurteilung etc.) qualitativ und quantitativ zu bewerten (Albrecht et al. 2003; Albrecht et al. 2008). Auch wenn diese Untersuchungen schon älteren Datums sind, haben sie doch gezeigt, dass es methodisch zwar aufwendig und komplex, aber durchaus möglich ist, Effizienznachweise für einzelne Maßnahmen der informationstechnischen Beobachtung zu führen.

5.4.1 Anwendungspraxis in der Strafverfolgung

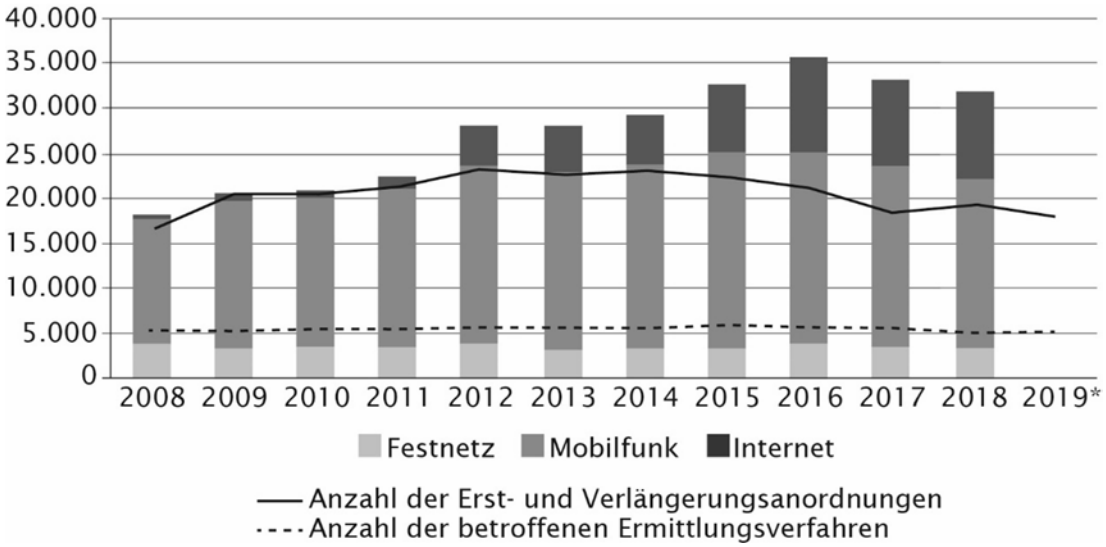
Dieses Kapitel gibt unter dem Eindruck einer sehr schmalen Datengrundlage einen Überblick über aktuelle Anwendungspraktiken von informationstechnischen Beobachtungsverfahren im Bereich der Strafverfolgung, wobei der Schwerpunkt auf den Einsatz solcher Verfahren durch Polizeibehörden des Bundes liegt. Vielfach hat sich die Darstellung auf die Angabe von Einsatzhäufigkeiten zu beschränken (der Datenstand bezieht – soweit möglich – die Berichtsjahre bis und mit 2020 ein), da darüberhinausgehende Informationen (z. B. technische

Verfahrensweisen) oder Nutzenbewertungen (öffentlich zugänglich) nicht vorliegen. Die nachfolgenden Ausführungen orientieren sich in Bezug auf die Reihenfolge der Verfahren an Kapitel 5.2.

5.4.1.1 Einsatz von TKÜ-Maßnahmen

Über die Anzahl der durch Strafverfolgungsbehörden des Bundes und der Länder angeordneten TKÜ-Maßnahmen nach § 100a StPO gibt die seit 2000 jährlich vom Bundesamt der Justiz veröffentlichte TKÜ-Statistik[153] Auskunft (Abb. 5.6).

Abb. 5.6 Einsatzhäufigkeit der TKÜ im Bereich der Strafverfolgung



* Ab 2019 werden die Anordnungen nicht mehr getrennt nach Anschlussart ausgewiesen.

Eigene Darstellung nach Daten der TKÜ-Statistik

Seit 2012 ist ein deutlicher Anstieg von TKÜ-Maßnahmen bei Internetanschlüssen festzustellen, was mit der seither steigenden Nutzung von OTT-Kommunikationsdiensten korrespondiert (Abb. 5.2 in Kap. 5.1.2). Die Anzahl der jährlichen TKÜ-Anordnungen (Erst- und Verlängerungsanordnungen) erreichte zwischen 2012 und 2014 mit rd. 23.000 ein Maximum und nimmt seither tendenziell wieder leicht ab. Auch die Zahl der Ermittlungsverfahren, die davon Gebrauch machten, blieb vergleichsweise stabil im Bereich von jährlich 5.100 bis 5.900 (Abb. 5.6). Daran gemessen werden TKÜ-Maßnahmen nicht häufiger und –

153 Berichtspflichten nach § 100b Abs. 5 u. 6 StPO (in der vor dem 27.8.2017 geltenden Fassung) bzw. § 101b StPO (in der am 27.8.2017 verkündeten Fassung). Die Statistiken sind abrufbar unter www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung.html (31.3.2022)

zumindest im Vergleich zur Gesamtzahl der 2015 von deutschen Staatsanwaltschaften eingeleiteten Ermittlungsverfahren von rd. 5,2 Mio. (Statistisches Bundesamt 2018, S. 317) – auch nur vergleichsweise selten eingesetzt.

Der Nutzen von TKÜ-Maßnahmen für die Strafverfolgung wurde umfänglich in einer am Max-Planck-Institut für ausländisches und internationales Strafrecht durchgeführten empirischen Studie von Albrecht et al. (2003) untersucht. Allerdings liegen hier die Untersuchungszeiträume weit in der Vergangenheit (Kasten 5.7).

Kasten 5.7 Studie von Albrecht et al. (2003) zum Nutzen der TKÜ in der Strafverfolgung

Im Rahmen der Untersuchung wurden die Akten von 523 Verfahren mit TKÜ-Maßnahmen aus dem Jahr 1998 ausgewertet sowie Praktiker (Polizeibeamte, Staatsanwälte und Richter) befragt. Zur Beurteilung der Effizienz von TKÜ-Maßnahmen wurde zwischen ihrem Erkenntniswert im Ermittlungsverfahren und ihrem Beweiswert in der Anklage unterschieden.

Bezüglich des Erkenntniswertes waren den Akten für etwa 60 % der untersuchten Verfahren Hinweise auf mindestens einen Ermittlungserfolg durch TKÜ zu entnehmen. Die dadurch gewonnenen faktischen Hinweise bezogen sich am häufigsten auf Erkenntnisse neuer Straftaten Dritter (25 % der Hinweise), dienten als Grundlage für neue Ermittlungsansätze (z. B. Durchsuchungen, Zeugenvernehmungen) wegen Katalogstraftaten (24 %), führten zur Selbstbelastung der Beschuldigten (19 %) oder gaben Anhaltspunkte auf neue Straftaten bereits Beschuldigter (11 %). Bezogen auf die Straftaten war die relative Erfolgsquote bei den Katalogstraftaten Geld- und Wertpapierfälschung, schwerer Menschenhandel, schwerer Bandendiebstahl, Erpressung, Geldwäsche und Verstößen gegen das Betäubungsmittelgesetz höher als etwa bei Mord und Totschlag oder Delikten gegen die persönliche Freiheit.

Als Beweismittel in der Anklage wurden durch die TKÜ gewonnene Erkenntnisse relativ selten verwendet. Allerdings blieben sie laut den Studienautoren in Gestalt anderer Sachbeweise, die erst durch die Erkenntnisse aus der TKÜ erlangt wurden, und/oder dadurch motivierter Geständnisse häufig auch über das Ermittlungsverfahren hinaus »in unsichtbarer Form« relevant.

Quelle: Albrecht et al. 2003, S. 364 ff. u. 463

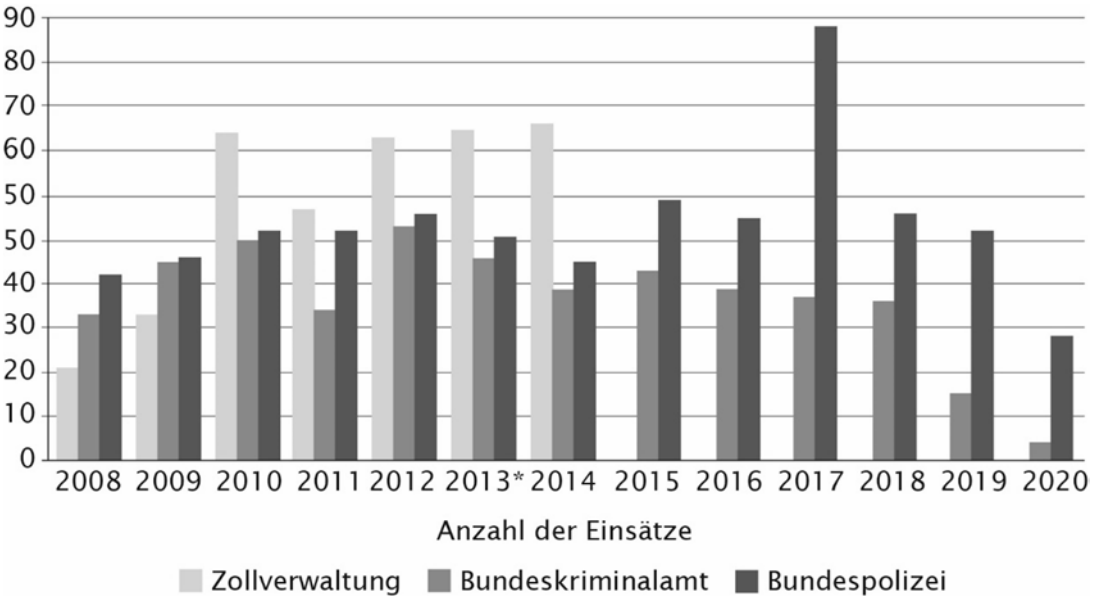
Im Ergebnis wurde die TKÜ insgesamt als wichtiges und unabdingbares Ermittlungsinstrument eingeschätzt, das vor allem im Bereich der Transaktionskri-

minalität[154] grundlegende Erfolge erzielt. Deutlich wurde zugleich, dass die TKÜ als alleiniges Erkenntnis- und Beweismittel keine Rolle spielt (Albrecht et al. 2003, S. 463). Aktuellere Studien mit vergleichbarem inhaltlichem und methodischem Umfang sind keine bekannt. Diese wären aber angesichts des sich seitdem stark veränderten Kommunikationsverhaltens und -aufkommens sehr wünschenswert.

5.4.1.2 Einsatz von IMSI- und WLAN-Catchern

Zur Anwendungspraxis von IMSI-Catchern durch die Polizeibehörden des Bundes erlauben die Antworten der Bundesregierung (2021b, 2020b, 2019j, 2019c, 2018c, 2018d, 2017e, 2017d, 2016a, 2016d, 2015b, 2015c, 2014a, 2013b) auf entsprechende Kleine Anfragen einige Rückschlüsse (Abb. 5.7).

Abb. 5.7 Einsatzhäufigkeit von IMSI-Catchern durch die Polizeibehörden des Bundes



* Für 2013 wurde aufgrund fehlender Zahlen der Mittelwert aus 2012 und 2014 gebildet.

Quellen: Bundesregierung 2013b, 2014a, 2015b, 2015c, 2016a, 2016d, 2017d, 2017e, 2018c, 2018d, 2019c, 2019j, 2020b u. 2021b

154 Kriminelles Verhalten, das sich durch Kommunikation, Handel und Organisation auszeichnet und/oder gewerbs- bzw. bandenmäßig begangen wird (z. B. Handel mit Betäubungsmitteln und Waffen, Menschenhandel, gewerbsmäßiger Diebstahl, gewerbsmäßige Hehlerei) (Albrecht et al. 2003, S. 9 f.).

Soweit daraus hervorgeht wurden IMSI-Catcher hier überwiegend in strafprozessualen Ermittlungsverfahren eingesetzt. Das Bundeskriminalamt verwendete die Geräte zwischen 2008 und 2020 im Schnitt rund 36-mal pro Jahr (seit 2012 mit abnehmender Tendenz). Etwas häufiger wurden IMSI-Catcher durch die Bundespolizei angewendet (im Schnitt 53-mal pro Jahr). Die Zollverwaltung setzte IMSI-Catcher zwischen 2008 und 2014 durchschnittlich 58-mal pro Jahr ein (seit 2015 werden Zahlen für den Zoll nicht mehr in offener Form mitgeteilt). Vereinzelt wurden IMSI-Catcher auch zur Suche von vermissten oder suizidgefährdeten Personen eingesetzt. In Bezug auf die Einsatzform gibt die Bundesregierung (2019c, S. 6 f.) an, dass IMSI-Catcher lediglich zur Ermittlung von IMSI-Nummern und der IMEI eingesetzt würden, also nicht zur Beobachtung laufender Mobilfunkkommunikation (Kap. 5.2.1.2).

Systematische empirische Untersuchungen zum Nutzen von IMSI-Catchern für die Strafverfolgung liegen (soweit bekannt) keine vor. Die Bundesregierung (2019c, S. 6 f.) stellt fest, dass der Einsatz eines IMSI-Catchers ein wesentlicher Ausgangspunkt für weitere Maßnahmen (z. B. Erhebung von Verbindungsdaten, Ortungsmaßnahmen, Internetrecherchen) sei, durch welche Sachverhalte inhaltlich weiter aufgeklärt werden könnten. Ob IMSI-Catcher (oder andere Maßnahmen) wesentlich zur Aufklärung von Straftaten beitrügen, sei von Fall zu Fall unterschiedlich und könne in vielen Fällen nicht genau bestimmt werden.

Aus den Angaben der Bundesregierung geht ferner hervor, dass WLAN-Catcher durch die Polizeibehörden des Bundes seit 2015 nicht angewendet werden, mit Ausnahme von drei Einsätzen im Jahr 2016, einem Einsatz im Jahr 2018 und zwei Einsätzen im Jahr 2019 durch das Bundeskriminalamt.

5.4.1.3 Aushebeln von Verschlüsselung

Zwar darf verschlüsselte Kommunikation, die während des Übertragungsvorganges durch TKÜ-Maßnahmen oder den Einsatz von IMSI- bzw. WLAN-Catcher rechtmäßig ausgeleitet wurde, von den Behörden auch entschlüsselt werden (Bundesregierung 2015a, S. 3 f.), allerdings sind die Möglichkeiten hierzu aus unterschiedlichen Gründen beschränkt:

- *Praktische Gründe*: Die hier typischerweise eingesetzten Verschlüsselungsverfahren lassen sich mit der Brute-Force-Methode in angemessener Frist nicht brechen (Kap. 5.2.1.3). Bei der Ende-zu-Ende-Verschlüsselung bleiben die verwendeten Schlüssel zudem im Besitz der Kommunikationspartner. Die Ermittlung des Schlüssels beispielsweise im Wege einer Bestandsdatenauskunft (§ 100j StPO) oder eines Herausgabeverlangen (§ 95 StPO) beim Diensteanbieter ist daher nicht möglich.
- *Rechtliche und ermittlungstaktische Gründe*: Rechtlich besteht derzeit keine Handhabe, Beschuldigte zur Herausgabe der verwendeten Schlüssel zu

zwingen (Bundesregierung 2016e, S. 4). Dies würde überdies den Zielen einer verdeckten Ermittlung entgegenstehen.

- *Politische Gründe*: Die Bundesregierung hat sich mit den 1999 beschlossenen »Eckpunkten der deutschen Kryptopolitik« gegen jegliche Schwächung, Modifikation oder Verbote von Verschlüsselung oder ein Kompromittieren von Sicherheitsstandards bekannt. Daran hält die Bundesregierung (2018o, S. 4) nach wie vor fest.

Gleichzeitig wurde bereits in den »Eckpunkten der deutschen Kryptopolitik« festgehalten, dass »[d]urch die Verbreitung starker Verschlüsselungsverfahren … die gesetzlichen Befugnisse der Strafverfolgungs- und Sicherheitsbehörden zur Telekommunikationsüberwachung nicht ausgehöhlt werden [dürfen]« (Bundesregierung 2001). Unter den zuvor genannten Beschränkungen verbleiben von den in Kapitel 5.2.1.3 skizzierten prinzipiellen Möglichkeiten zur Aushebelung von Verschlüsselung die freiwillige Zusammenarbeit zwischen staatlichen und privaten Akteuren sowie die Anwendung von Methoden des staatlichen Hackings. In Bezug auf ersteres begrüßt die Bundesregierung (2015a, S. 5) »jedwede[n] Dialog mit Internet-Diensteanbietern, um nach Möglichkeiten zu suchen den unterschiedlichen Bedürfnissen im Verhältnis Datenschutz zu Gefahrenabwehr und Strafverfolgung gerecht zu werden«.

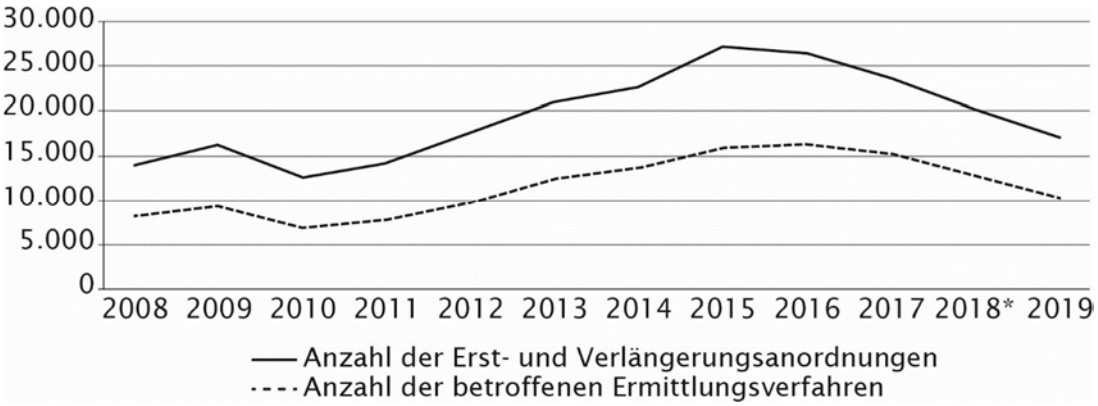
In Bezug auf Methoden des staatlichen Hackings können laut Bundesregierung (2015a, S. 4) »je nach Anwendungsfall gängige Werkzeuge nach dem Stand der Technik zum Einsatz kommen.« Um welche technischen Methoden es sich hierbei handelt, darüber gibt die Bundesregierung (2016f, S. 5) öffentliche keine Auskunft. Medienberichten zufolge soll sich etwa das Bundeskriminalamt mehrfach Zugang zu Nutzerkonten des OTT-Kommunikationsdienstes Telegram verschafft haben, indem neue Endgeräte angemeldet wurden (Kap. 5.2.1.3) (Lipp/Hoppenstedt 2016b). Ob ein solches Vorgehen durch § 100a StPO gedeckt wäre, ist umstritten. Kritiker sehen für eine TKÜ, die unter Zuhilfenahme einer Identitätstäuschung vorgenommen wird, die Erfordernis für eine spezielle Rechtsgrundlage (Lipp/Hoppenstedt 2016a).

5.4.1.4 Erhebung von Verkehrsdaten beim Diensteanbieter

Über die Einsatzpraxis der individualisierten Verkehrsdatenerhebung nach § 100g Abs. 1 u. 2 StPO bei den Strafverfolgungsbehörden des Bundes und der Länder gibt die seit 2008 jährlich vom Bundesamt der Justiz veröffentlichte

TKÜ-Statistik Auskunft.[155] Zwischen 2010 und 2015 ist sowohl die Zahl der jährlich erfolgten Anordnungen (Erst- und Verlängerungsanordnungen) als auch die Zahl der Ermittlungsverfahren, in denen Verkehrsdaten erhoben wurden, deutlich angestiegen (Abb. 5.8). Ab 2016 ist wieder ein Rückgang sowohl bei den Anordnungen als auch bei den Ermittlungsverfahren festzustellen. Für das Berichtsjahr 2019 liegen auch erstmals verlässliche Zahlen in Bezug auf die Art der abgefragten Verkehrsdaten vor. Demnach bezogen sich 13.160 Anordnungen auf Verkehrsdaten nach § 96 StPO sowie 3.833 Anordnungen auf Verkehrsdaten nach § 113b StPO.

Abb. 5.8 Einsatzhäufigkeit der individualisierten Verkehrsdatenerhebung im Bereich der Strafverfolgung



* Angaben unvollständig. Die dargestellten Werte entsprechendem Mittelwert aus 2017 und 2019.

Eigene Zusammenstellung mit Daten aus der TKÜ-Statistik

In Relation zum Einsatz der TKÜ wurden Verkehrsdaten im Jahr 2019 in knapp doppelt so vielen Ermittlungsverfahren erhoben. Während die Zahl der Ermittlungsverfahren mit TKÜ-Maßnahmen im Zeitverlauf vergleichsweise stabil geblieben ist (Kap. 5.4.1.1), hat sich die Zahl der Ermittlungsverfahren mit Verkehrsdatenerhebung zwischen 2010 und 2019 um 50 % erhöht. Dies lässt generell auf eine steigende Bedeutung von Verkehrsdaten für die Strafverfolgung schließen (Kap. 5.2.2.2).

155 Berichtspflichten nach § 100g Abs. 4 StPO in der vor dem 18. Dezember 2015 geltenden Fassung. Diese beziehen sich nur auf die individualisierte Verkehrsdatenerhebungen nach § 100g Abs. 1 StPO (a.F.) und umfassen folglich keine Funkzellenabfragen nach § 100g Abs. 2 S. 2 StPO (a.F.). Ab dem Berichtsjahr 2018 gilt eine Berichtspflicht, die nach den verschiedenen Maßnahmen (individualisierte Abfrage von Verkehrsdaten nach § 96 TKG bzw. nach § 113b TKG, Funkzellenabfrage) differenziert. Infolge der gesetzlichen Änderungen kam es für das Erhebungsjahr 2018 allerdings zu einer uneinheitlichen Erhebungspraxis, sodass die Angaben unvollständig sind. Die Statistiken sind abrufbar unter www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung.html (31.3.2022).

Der Nutzen der Verkehrsdatenerhebung für die Strafverfolgung wurde in einer Reihe von empirischen Studien am Max-Planck-Institut für ausländisches und internationales Strafrecht evaluiert, allerdings sind die Studien bereits älteren Datums. Albrecht et al. (2008) gelangten in ihrer Untersuchung zu dem Ergebnis, dass die Verkehrsdatenerhebung ein nur bedingt erfolgreiches Ermittlungsinstrument darstellt, da die damit verfolgten Ermittlungsziele in rund zwei Dritteln der Fälle nicht erreicht werden konnten (Kasten 5.8). Waren die Maßnahmen allerdings erfolgreich, so konnten dadurch wichtige Hinweise erlangt werden, was in diesen Fällen in höheren Anklagequoten resultierte (Albrecht et al. 2008, S. 411 f.).

Kasten 5.8 Studie von Albrecht et al. (2008) zum Nutzen der Verkehrsdatenerhebung in der Strafverfolgung

Für die Untersuchung wurden Akten zu 467 Verfahren mit insgesamt 1.257 Beschlüssen zur Verkehrsdatenerhebung aus den Jahren 2003 und 2004 ausgewertet, Staatsanwälte schriftlich befragt sowie Experteninterviews geführt (u. a. mit Richtern, Polizeibeamten, Vertreter von Telekommunikationsunternehmen). Als Effizienzindikatoren wurden mit der Maßnahme erzielte Ermittlungserfolge sowie der Verfahrensausgang herangezogen.

Die in den Akten dokumentierten, mit der Verkehrsdatenerhebung verfolgten Ermittlungsziele waren die Identifizierung noch ungekannter Täter (40 %), die Ermittlung weiterer Tatverdächtiger (30 %) oder die Beweissicherung (26 %). Sonstige Ziele (5 %) bezogen sich etwa auf die Ermittlung von Liefer- und Absatzwegen, des Tatorts oder von Bandenstrukturen. Für 43 % der Beschlüsse konnten den Akten Erfolgseinschätzungen entnommen werden. Bei diesen wurde die Verkehrsdatenerhebung in 18 % der Fälle als erfolgreich, in 17 % der Fälle als bedingt erfolgreich und in 65 % der Fälle als nicht erfolgreich eingeschätzt.

In Bezug auf den Verfahrensausgang zeigte sich, dass in Fällen, in denen die Verkehrsdatenerhebung als erfolgreich eingestuft wurde, die Anklagequote im Vergleich zur anderen Fallgruppe deutlich erhöht war. Von Praktikern hervorgehoben wurde vor allem der Nutzen von Verkehrsdaten zur Erwirkung von Geständnissen bei Beschuldigten sowie zur Verdachtserhärtung, um dann andere Maßnahmen durchführen zu können (z. B. Durchsuchungen).

Quelle: Albrecht et al. 2008, S. 403 f. u. 411 f.

Die Datenbasis in der Untersuchung von Albrecht et al. (2008) bezog sich auf einen Zeitraum vor der ersten Einführung der Vorratsdatenspeicherung im Jahr 2008 (Kap. 5.3.1.2). Albrecht et al. (2011) befassten sich in einer Folgestudie speziell mit dem Nutzen von vorratsgespeicherten Verkehrsdaten (bzw. mit den Auswirkungen durch deren Wegfall der Vorratsdatenspeicherung nach dem

Urteil des Bundesverfassungsgerichts von 2010) für die Strafverfolgung. Die Studie lieferte keine eindeutigen Ergebnisse. So konnten mit quantitativen Methoden keine Belege dafür gefunden werden, dass in ausgewählten Deliktbereichen vor, während oder nach der Phase mit Vorratsdatenspeicherung Veränderungen in den Aufklärungsquoten eingetreten wären. Albrecht et al. (2011, S. 218 ff.) schränkten die Belastbarkeit der Ergebnisse allerdings ein, da nur eine sehr unsichere quantitative Datengrundlage zur Verfügung stand. Im Kontrast dazu ließen qualitative Befunde aus Interviews mit Praktikern (Polizeibeamte, Staatsanwälte, Richter etc.) auf einen hohen Nutzen der Vorratsdatenspeicherung für die Strafverfolgung schließen. So schätzte beispielsweise die überwiegende Mehrzahl (85 %) der befragen Polizeibeamten die praktischen Auswirkungen des Wegfalls der Vorratsdatenspeicherung auf die Ermittlungsarbeit als hoch bzw. sehr hoch ein (Albrecht et al. 2011, S. 135).

Untersuchungen jüngeren Datums zum Nutzen der Verkehrsdatenerhebung für die Strafverfolgung liegen (soweit bekannt) in publizierter Form nicht vor. Der Wissensstand ist somit auch vor dem Hintergrund der grundlegenden Veränderungen in den Kommunikationstechniken und -gewohnheiten der letzten Jahre insgesamt als sehr lückenhaft zu bewerten.

Spezialfall Funkzellenabfrage

Die Funkzellenabfrage wird in Deutschland seit spätestens 2005 zu Strafverfolgungszwecken eingesetzt (Weichert 2005). Verfügbare Informationen zur Einsatzpraxis stammen bislang hauptsächlich aus Regierungsantworten auf parlamentarische Anfragen. Die von der Bundesregierung für die Polizeibehörden des Bundes berichteten Zahlen zur Anwendungshäufigkeit sind in Tabelle 5.5 aufgeführt.[156] Ins Auge sticht insbesondere die hohe Zahl an Einsätzen durch das Bundeskriminalamt im Jahr 2017.[157] Bei der Bundespolizei waren die Fallzahlen bis 2017 rückläufig, sind aber 2018 und 2019 wieder angestiegen. Für die Behörden der Zollverwaltung zeichnet sich ein abnehmender Trend ab.

Eine gesetzliche Berichtspflicht für den Einsatz der Funkzellenabfrage zu Zwecken der Strafverfolgung wurde erst 2015 eingeführt und galt erstmalig für das Berichtsjahr 2018. Infolge der gesetzlichen Änderungen kam es 2018 allerdings zu unvollständigen Angaben aus einigen Bundesländern.[158] Ohne die Angaben aus den Bundesländern Bremen, Mecklenburg-Vorpommern, Rheinland-Pfalz, Saarland und Sachsen wurden in den übrigen elf Bundesländern und durch

156 Die Angaben erlauben keine Aufschlüsselung danach, ob es sich um strafprozessuale oder gefahrenabwehrrechtliche Maßnahmen handelte.

157 Laut einer Vermutung von Monroy (2018) könnte dies mit den Ermittlungen zu den am 19. Juni 2017 an 13 Orten in Deutschland verübten Brandanschlägen auf Kabelschächte entlang von Bahnanlagen in Verbindung stehen.

158 Die Statistiken sind abrufbar unter www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung.html (31.3.2022).

die Generalbundesanwaltschaft 2018 insgesamt ca. 8.300 Anordnungen zur Durchführung von Funkzellenabfragen in ca. 7.500 strafprozessualen Ermittlungsverfahren verfügt. Verlässliche Zahlen liegen erstmalig für 2019 vor, in dem insgesamt 10.412 Anordnungen in 9.455 Ermittlungsverfahren berichtet wurden.

Tab. 5.5 Einsatzhäufigkeit von Funkzellenabfragen durch die Polizeibehörden des Bundes

	2014	2015	2016	2017	2018	2019	2020
Bundeskriminalamt	10	12	2	525	22	3	1
Bundespolizei	< 100	< 91	69	54	154	167	77
Zollverwaltung	127	72	169	96	74	65	k.A.

Quellen: Bundesregierung 2014a, 2015b, 2015c, 2016a, 2016d, 2017d, 2017e, 2018c, 2018d, 2019c, 2019j, 2020b u. 2021b

Am Beispiel der Funkzellenabfrage wird nachfolgend die vor der Einführung der gesetzlichen Berichtspflicht problematische empirische Datenlage zur Einsatzpraxis in den Bundesländern illustriert. Die Tabelle 5.6 fasst die Ergebnisse einer Auswertung öffentlich verfügbarer Quellen (vorrangig Antworten von Landesregierungen auf parlamentarische Anfragen) von Schulzki-Haddouti (2017) für die Länder Sachsen, Schleswig-Holstein, Nordrhein-Westfalen und Niedersachsen zusammen, die um entsprechende verfügbare Informationen für das Land Berlin erweitert wurden. Die Angaben sind nur bedingt miteinander vergleichbar, da ihnen unterschiedliche Bezugsgrößen zugrunde liegen: Die Landesregierungen von Sachsen und Berlin gaben die Zahl der Ermittlungsverfahren mit Funkzellenabfragen bekannt, jene von Schleswig-Holstein und Nordrhein-Westfalen die Anordnungshäufigkeiten und für Niedersachsen wurde die Zahl an Auskunftsersuchen bei Netzbetreibern berichtet. Der Zusammenhang zwischen diesen Zahlen ist einzelfallabhängig, Vergleiche sind daher kaum möglich.[159] Insoweit erlauben die vorhandenen Daten lediglich folgende Schlussfolgerungen: Zum einen hat der Einsatz der Funkzellenabfrage in einigen Bundesländern in den letzten Jahren stetig zugenommen, zum anderen wird die Maßnahme durch Landespolizeibehörden deutlich häufiger eingesetzt als durch die Polizeibehörden des Bundes.

159 Die aus Niedersachsen berichteten Zahlen sind vermutlich durch 4 (Anzahl der Netzbetreiber) zu teilen, um die Zahl der angeordneten Funkzellenabfragen anzunähern.

Tab. 5.6 Einsatzhäufigkeit von Funkzellenabfragen in ausgewählten Bundesländern

Bundesland	2013	2014	2015	2016
Sachsen (Anzahl Ermittlungsverfahren)	284	257	360	371
Nordrhein-Westfalen (angeordnete Funkzellenabfragen)	4.145	4.682	6.426	7.249
Schleswig-Holstein (angeordnete Funkzellenabfragen)	441	569	825	866
Niedersachsen (Anfragen bei Netzbetreibern)			20.168	19.020
Berlin (Anzahl Ermittlungsverfahren)		500	256	432

Quellen: Schulzki-Haddouti 2017 und darin enthaltene Quellen; Der Senat von Berlin 2017b, S. 2

Die Angaben der Landesregierungen lassen lediglich auf eine steigende Bedeutung der Funkzellenabfrage als Ermittlungswerkzeug schließen, bieten darüberhinausgehend aber keine wesentlichen Erkenntnisse zum Nutzen für die Strafverfolgung. Zwar wurden für ausgewählte Fallkomplexe durchaus Aufklärungserfolge dokumentiert (Kasten 5.9).

Kasten 5.9 Bundesweite Raubstraftatenserie auf Lebensmittelmärkte

2014 und 2015 kam es in sechs Bundesländern zu einer Serie von Überfällen auf Lebensmittelmärkte. In mehreren Fällen wurden Schüsse auf Personen oder Sachen abgegeben. In Hannover wurde ein Opfer im Dezember 2014 durch zwei Schüsse tödlich verletzt. Vor dem Hintergrund der Ermittlungshypothese, dass der Täter die jeweiligen Tatorte im Vorfeld ausgekundschaftet hatte, wurden gezielte Funkzellenauswertungen initiiert. Im Rahmen eines Schnittmengenabgleichs der Funkzellendaten wurde eine eindeutige Seriennummer (IMEI) festgestellt, die an fünf Tatorten registriert wurde. Weitere Ermittlungen ergaben Bezüge zu acht Tatorten. Nach Lokalisierung des Mobilfunkgeräts konnte der Täter schließlich festgenommen werden.

Quellen: Niedersächsisches Ministerium für Inneres und Sport 2017, Jüttner 2016

Zudem wurde in Nordrhein-Westfalen, das als einziges Land Einblicke in die betroffenen Straftatengruppen gewährte, der häufigere Einsatz der Funkzellenabfrage von einem Anstieg der Aufklärungsquote im Bereich des Bandendiebstahls begleitet. Ob allerdings ein kausaler Zusammenhang zwischen dem Einsatz der Funkzellenabfrage und der höheren Aufklärungsquote besteht, wurde mangels entsprechender wissenschaftlicher Studien bisher nicht nachgewiesen (Schulzki-Haddouti 2017).

Spezialfall stille SMS

Für den Einsatz von stillen SMS gibt es keine gesetzlichen Berichtspflichten. Die Gesamtzahl der durch das Bundeskriminalamt und die Bundespolizei jährlich versendeten stillen SMS lässt sich den Antworten der Bundesregierung auf Kleine Anfragen entnehmen (Zahlen seit 2014 in Tab. 5.7).

Tab. 5.7 Anzahl jährlich durch die Polizeibehörden des Bundes versandte stille SMS

	2014	2015	2016	2017	2018	2019	2020
Bundespolizei	108.241	73.536	139.926	73.722	89.644	47.930	101.117
Bundeskriminalamt	61.571	139.305	63.372	45.578	52.325	41.240	44.444

Quellen: Bundesregierung 2014a, 2015b, 2015c, 2016a, 2016d, 2017d, 2017e, 2018c, 2018d, 2019c, 2019j, 2020b u. 2021b

Angaben über die Anzahl der Ermittlungsverfahren und insbesondere der betroffenen Personen liegen mangels entsprechender statistischer Erfassung nur sehr vereinzelt vor. Zum Beispiel waren von den im 1. Halbjahr 2014 durch das Bundeskriminalamt versandten 34.656 stillen SMS 122 Personen in 58 Ermittlungsverfahren betroffen (Bundesregierung 2014a, S. 9). Demnach entfielen durchschnittlich auf jede Zielperson über 280 und auf jedes Ermittlungsverfahren knapp 600 stille SMS. Davon abgesehen erlauben die Angaben der Bundesregierung keine weiteren Rückschlüsse auf die Einsatzpraxis oder den Nutzen der Maßnahmen für die Ermittlungsarbeit.

5.4.1.5 Einsatz von Quellen-TKÜ und Onlinedurchsuchung

Trotz der damals noch umstrittenen Rechtslage (Kap. 5.3.1.4) wurde die Quellen-TKÜ auch schon vor August 2017 zu Zwecken der Strafverfolgung angewendet. Bei den Strafverfolgungsbehörden des Bundes wurde die Maßnahme bis 2011

durch das BKA in 10 Strafermittlungsverfahren (wobei es zur Aufbringung der Quellen-TKÜ-Software in 6 Fällen, zur Datenausleitung in 4 Fällen kam) und durch den Zollfahndungsdienst in 13 Strafermittlungsverfahren (wobei die Aufbringung der Software in 12 Fällen, die Ausleitung von Daten in 7 Fällen gelang) eingesetzt (Bundesregierung 2011, S. 11 ff.). Auf Ebene der Bundesländer sind beispielsweise die Aktivitäten der bayerischen Strafverfolgungsbehörden vergleichsweise gut dokumentiert, die zwischen 2008 bis 2011 insgesamt 23 solcher Maßnahmen durchführten (Petri 2012, S. 5). Eine der hier verwendeten Quellen-TKÜ-Software wurde 2011 durch den Chaos Computer Club (CCC 2011) analysiert und aufgrund von »groben Design- und Implementierungsfehlern« massiv kritisiert. Bund und Länder sahen sich dadurch veranlasst, »bis auf Weiteres auf die Durchführung von Quellen-TKÜ-Maßnahmen zu verzichten« (Bundesregierung 2013c, S. 6) sowie Mindeststandards (standardisierende Leistungsbeschreibung) für die Entwicklung und den Einsatz von Quellen-TKÜ-Software zu entwickeln (Bundesregierung 2018f, S. 7).

Zur Anwendungspraxis seit 2011 gibt es vonseiten der Bundesregierung oder -behörden keine aufschlussreichen öffentlichen Informationen mehr. Dies gilt bereits für die Fallzahlen und erst recht für weitere Auskünfte etwa in Bezug auf die technische Durchführung oder den Erfolg der Maßnahmen sowie generell für den Nutzen der Quelle-TKÜ für die Strafverfolgung. So stufte die Bundesregierung (z. B. 2018b, 2018f u. 2018l) die Antworten auf entsprechende parlamentarische Anfragen als Verschlusssache (Einstufungsgrad: VS – Nur für den Dienstgebrauch) ein, sodass sie der Öffentlichkeit nicht zugänglich sind.[160] Begründet wurde dies damit, dass bereits eine Veröffentlichung der Fallzahlen Rückschlüsse auf die quantitativen Leistungsfähigkeiten der durchführenden Stellen zulassen könnte, was eine schwerwiegende Beeinträchtigung der Ermittlungsfähigkeit der Behörden zur Folge haben könnte (Bundesregierung 2018p, S. 3 u. 6). Ab dem Berichtsjahr 2019 geben die nach § 101b Abs. 2 Nr. 4 StPO jährlich zu veröffentlichenden Statistiken zumindest Auskunft darüber, wie häufig Maßnahmen der Quellen-TKÜ im Bereich der Strafverfolgung eingesetzt werden. Demnach wurden im Jahr 2019 insgesamt 31 Maßnahmen richterlich angeordnet. Durch die Strafverfolgungsbehörden des Bundes und der Länder tatsächlich durchgeführt wurden jedoch nur drei Eingriffe.[161]

Ebenfalls seit dem Berichtsjahr 2019 wird jährlich über den Umfang des Einsatzes der Onlinedurchsuchung auf Grundlage der im August 2017 geschaffenen Befugnisse durch die Strafverfolgungsbehörden des Bundes und der Länder Auskunft gegeben (Berichtspflichten gemäß § 101b Abs. 3 StPO). Laut Statistik

160 Teilweise werden die erbetenen Auskünfte selbst in eingestufter Form nicht oder nicht vollständig erteilt, wenn die Informationen weitgehende Rückschlüsse auf die technischen Fähigkeiten, die technische Ausstattung und das Know-how der Sicherheitsbehörden zulassen (z. B. Bundesregierung 2018l, S. 5).

161 Die Statistiken sind abrufbar unter www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung.html (31.3.2022).

wurden 2019 in 21 Ermittlungsverfahren insgesamt 22 Erstanordnungen (und 11 Verlängerungsanordnungen) erteilt, wovon jedoch nur 12 Eingriffe auch tatsächlich durchgeführt wurden.

Schließlich gibt die Bundesregierung (2019e, S. 38 ff.) öffentlich auch keine Auskunft darüber, inwieweit die Strafverfolgungsbehörden des Bundes in der Lage sind, entsprechende Beobachtungssoftware auf weiteren informationstechnisch vernetzten Systemen (wie z. B. Smart-Home-Anwendungen; Kap. 5.2.3.2) zu installieren.

5.4.2 Anwendungspraxis in der Gefahrenabwehr

Das Bundeskriminalamt kam seiner Berichtspflicht gemäß § 88 BKAG bisher 2019 und 2021 nach. Die Berichte wurden als Bundestagsdrucksache durch die Bundesregierung (2019h u. 2021a) veröffentlicht. Demnach schloss das Bundeskriminalamt im Rahmen der Aufgaben zur Abwehr von Gefahren des internationalen Terrorismus (§ 5 BKAG) im Berichtszeitraum vom 25. Mai 2018 bis 30. April 2021 insgesamt drei Gefahrenabwehrvorgänge ab.[162] Im Rahmen dieser Vorgänge wurden von den in Tabelle 5.4 aufgeführten informationstechnischen Beobachtungsverfahren die in Tabelle 5.8 aufgeführten Maßnahmen durchgeführt.[163] Eine Differenzierung der Maßnahmen nach TKÜ oder Quellen-TKÜ wurde dabei nicht vorgenommen. Über den etwaigen Nutzen der einzelnen Maßnahmen ist dem Bericht nichts zu entnehmen.

Von diesem Bericht abgesehen liegen zur Anwendungspraxis informationstechnischer Beobachtungsverfahren im Bereich der polizeilichen Gefahrenabwehr bisher weder amtliche Übersichten noch aussagekräftige Informationen aus parlamentarischen Anfragen an die Bundesregierung oder an Landesregierungen vor, da die Antworten in der Regel nur in eingestufter Form übermittelt werden. Einige Rückschlüsse auf die langjährige Anwendungspraxis erlaubt zumindest für das Bundeskriminalamt und auf einer aggregierten Ebene der »Evaluationsbericht zu den §§ 4a, 20j, 20k des Bundeskriminalamtgesetzes« (Albrecht/Poscher 2017). Der Bericht wurde gemäß Artikel 6 des Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt[164] 5 Jahre nach Inkrafttreten der entsprechenden Eingriffsnormen am 1. Januar 2009 durch Albrecht und Poscher (2017) erarbeitet und liegt als Bundestagsdrucksache 18/13031 vor. Demnach schloss das Bundeskriminalamt von 2009 bis Ende 2015 insgesamt 16 Gefahrenabwehrvorgänge ab (ein weiterer befand sich noch in Bearbeitung). Die Anwendungshäufigkeiten der im Zuge dieser Vorgänge vorgenommen informationstechnischen Beobachtungsverfahren sind in Tabelle 5.9 aufgeführt.

162 Über Maßnahmen aus noch laufenden Gefahrenabwehrvorgängen wurde nicht berichtet.
163 Über Maßnahmen der Bestandsdatenauskunft nach § 40 BKAG wurde nicht berichtet.
164 BGBl. I 2008, 3083

Tab. 5.8 Anwendung von Maßnahmen im Rahmen der Aufgaben zur Abwehr von Gefahren des internationalen Terrorismus (§ 5 BKAG)

Maßnahme	Berichtszeitraum Mai 2018 bis April 2019	Berichtszeitraum Mai 2019 bis April 2021
IMSI-Catcher: Ermittlung der IMSI/IMEI (§ 53 Abs. 1 Nr. 2 BKAG)	für 1 Zielperson	für 2 Zielpersonen
IMSI-Catcher: Lokalisierung (§ 53 Abs. 1 Nr. 2 BKAG)	für 1 Zielperson	für 7 Zielpersonen (22 Mobilfunkkarten)
Erhebung von Verkehrs- oder Nutzungsdaten (52 BKAG)	für 7 Anschlüsse/Kennungen/Benutzerkonten	für 57 Anschlüsse/Kennungen/Benutzerkonten
TKÜ (§ 51 BKAG)	für 7 Anschlüsse/Kennungen/Benutzerkonten	für 65 Anschlüsse/Kennungen/Benutzerkonten
Onlinedurchsuchung (§ 49 BKAG)	0	0

Eigene Zusammenstellung nach Bundesregierung 2019h u. 2021a

Tab. 5.9 Einsatzhäufigkeit von Beobachtungstechnologien im Bereich der Gefahrenabwehr durch das Bundeskriminalamt (2009 bis 2015)

Maßnahme nach Bundeskriminalamtgesetz (BKAG; a. F.)	aggregierte Häufigkeit	betroffene Vorgänge
§ 20g Abs.2 Nr. 2: Bildaufnahmen/akustische Überwachung außerhalb Wohnung	19	9
§ 20g Abs. 2 Nr. 3: Observation mit sonstigen technischen Mitteln	22	6
§ 20h: Wohnraumüberwachung	4	3
§ 20k: Onlinedurchsuchung	5	1
§ 20l Abs. 1: TKÜ	397	13
§ 20l Abs. 2: Quellen-TKÜ	7	2
§ 20m: Verkehrsdatenerhebung	322	13
§ 20n: IMSI-Catcher	18	9

Quelle: Albrecht/Poscher 2017, S. 21

Da der Evaluationsbericht auch Auskunft über die Anwendungshäufigkeit von sensorbasierten Beobachtungstechnologien (Bild- und Tonaufnahmen, Kap. 3) gibt, bietet sich hier ein Vergleich der unterschiedlichen technischen Beobachtungsmaßnahmen an. Nicht möglich waren laut Albrecht/Poscher (2017, S. 14) hingegen einzelfallbezogene Analysen zur Anwendungspraxis, insbesondere solche zur Bewertung des Erkenntnisgewinns durch die Einzelmaßnahmen, da entweder die zu den Vorgängen gehörenden Akten oder Datenbestände bereits gelöscht bzw. vernichtet wurden waren oder der Zugang zu den Informationen gesperrt war.

Weitaus am häufigsten wurden Maßnahmen der TKÜ und Verkehrsdatenerhebung durchgeführt, sowohl in Bezug auf die aggregierte Einsatzhäufigkeit als auch auf die Anzahl betroffener Vorgänge. Bezogen auf die Fallzahlen steht die TKÜ mit 397 Anwendungen noch vor der Verkehrsdatenerhebung mit 322 Anwendungen. Ungefähr zwei Drittel aller TKÜ-Maßnahmen und Verkehrsdatenerhebungen gehen lediglich auf 2 Vorgänge zurück, in denen insgesamt 14 Personen als potenziell Verdächtige im Fokus standen. Soweit sich dies aus den aggregierten Häufigkeiten ableiten lässt, scheint – anders als im Bereich der Strafverfolgung (Kap. 5.4.1.4) – der Stellenwert der Inhalts- gegenüber der Verkehrsdatenbeobachtung für die polizeiliche Gefahrenabwehr etwas höher zu liegen. Dies ist plausibel dadurch erklärbar, dass der individuellen und inhaltsbezogenen Informationsgewinnung etwa für die Gefahrenabschätzung herausragende Bedeutung zukommt (Albrecht/ Poscher 2017, S. 21 f.).

Alle anderen technischen Beobachtungsmaßnahmen kamen in weit geringerem Maße zum Einsatz, so im Besonderen die Quellen-TKÜ (7 Anordnungen in zwei Vorgängen) und die Onlinedurchsuchung (5 Anordnungen in einem Vorgang). Nähere Details zur Maßnahmendurchführung werden nur zur Onlinedurchsuchung genannt (Albrecht/ Poscher 2017, S. 22 f. u. 38 f.): Demnach wurde in vier der fünf angeordneten Maßnahmen entsprechende Software auf Zielsysteme installiert, offenbar aus der Ferne. Nur eine der angeordneten Maßnahmen führte letztlich dazu, dass Daten von insgesamt zwei Zielsystemen (stationärer PC und Notebook) ausgeleitet werden konnten. Es wurden rund 70.000 Inhalte erhoben, bei denen es sich weitgehend um Bildschirminhalte (Screenshots) sowie Tastatur- bzw. Mausaktivitäten handelte. Verfahrensrelevante Daten wurden dabei nicht erlangt (Hauptziel der Maßnahme war die Ermittlung von Passwörtern, um auf E-Mail-Postfächer der Zielpersonen zuzugreifen).

Die geringen Fallzahlen für die Quellen-TKÜ und Onlinedurchsuchung sprechen einerseits dafür, dass das Bundeskriminalamt die Maßnahmen sehr zurückhaltend und nur als letztes Mittel einsetzte. Dazu beigetragen haben dürfte sicherlich der Umstand, dass die gesetzeskonforme Durchführung der Maßnahmen in der Praxis äußerst aufwendig, zeitintensiv und oft von technischen Schwierigkeiten begleitet ist (Kap. 5.2.3). Jedenfalls haben sich im Vorfeld der Einführung der Eingriffsnormen teilweise gehegte Befürchtungen, dass es in der Folge zu einem

massiven Einsatz solcher Methoden kommen könnte, zumindest für den Zeitraum bis Ende 2015 nicht bestätigt. Andererseits ist auch zu beachten, dass die im Berichtszeitraum erfassten Maßnahmen alle vor 2012 durchgeführt wurden, also noch vor dem in Reaktion auf die Enthüllungen des Chaos Computer Clubs angestoßenen Prozess zur Entwicklung von Mindeststandards für die Entwicklung und den Einsatz von Quellen-TKÜ-Software (Kap. 5.4.1.5). Inwieweit folglich der Verzicht auf weitere Maßnahmen nach 2011 schlicht darauf zurückzuführen ist, dass keine diese Standards erfüllende Software zur Verfügung stand, kann an dieser Stelle mangels belastbarer Quellen nicht beantwortet werden.

6 Grundlegende regulatorische Fragestellungen

Die folgenden Ausführungen bieten einen Überblick über wichtige regulatorische Fragestellungen, die sich aufgrund der zunehmenden Verbreitung und technischen Weiterentwicklung von Beobachtungstechnologien stellen, wobei der Schwerpunkt auf dem Einsatz solcher Technologien durch Polizeibehörden zu Zwecken der Gefahrenabwehr und Strafverfolgung liegt. Teilweise handelt es sich um neue Fragen, teilweise stellen sich bereits bekannte Fragen heute verschärft oder anders akzentuiert. Die Rechtsfragen werden nach Normebenen (Verfassungsrecht und einfaches Recht) und Rechtsgebieten (Eingriffsrecht und Datenschutzrecht) eingeteilt, wobei sich allerdings Überschneidungen ergeben. Aufgrund der Komplexität der hier relevanten rechtlichen Materie können die folgenden Ausführungen weder einen Anspruch auf Vollständigkeit erheben noch abschließende Bewertungen von offenen Rechtsfragen bieten.

Das Kapitel basiert in ganz wesentlichen Teilen auf zwei rechtlichen Analysen von Prof. Dr. Matthias Bäcker, Dr. Alexander Dix und Prof. Dr. Gerrit Hornung sowie von Prof. Dr. Matthias Bäcker. Die Analysen wurden im Zuge der Gutachten von Hempel (2016, S. 149 ff.) sowie von Hempel und Rehak (2017, S. 116 ff.) erstellt.

Die Analysen in diesem Kapitel basieren auf dem Stand der Gesetzgebung zum Zeitpunkt der Fertigstellung dieses Berichts (Anfang 2020). Jüngere Entwicklungen wie etwa die Anpassung der Regelungen zur Erhebung von Bestands- und Nutzungsdaten von TM-Diensten von Ende März 2021 oder die umfassende Novellierung des Telekommunikationsgesetzes mit Wirkung zum 1. Dezember 2021 und damit zusammenhängende Rechtsfolgen konnten daher nicht mehr berücksichtigt werden.

6.1 Verfassungsrecht

Die verfassungsrechtlichen Anforderungen setzen dem behördlichen Einsatz polizeilicher Beobachtungstechnologien einen Rahmen, ohne diesen Einsatz selbst zu ermöglichen. Hierzu bedarf es – zumindest in der Regel – noch gesetzlicher Ermächtigungen im polizeilichen Eingriffsrecht, also im Polizei- oder Strafverfahrensrecht. Diese Ermächtigungen müssen ihrerseits verfassungsrechtlichen Anforderungen genügen.

Im Folgenden werden grund- und menschenrechtliche Vorgaben an polizeiliche Beobachtungspraktiken dargestellt. Dabei werden nicht nur die Grundrechte des Grundgesetzes, sondern teilweise auch andere Grundrechtskataloge im europäischen Mehrebenensystem mit einbezogen. An dieser Stelle hingegen nicht

erörtert werden verfassungsrechtliche Vorgaben, die sich aus der bundesstaatlichen Ordnung der Gesetzgebungs- und Verwaltungskompetenzen ergeben, beispielweise die Fragen, inwieweit die Regelungskompetenz des Bundes für das Strafverfahrensrecht landesrechtliche Eingriffsermächtigungen sperrt oder mit welchen Aufgaben und Befugnissen der Bund seine Polizeibehörden (u. a. Bundeskriminalamt und Bundespolizei) ausstatten darf.

6.1.1 Grundrechtliches Mehrebenensystem

Der polizeiliche Einsatz von Beobachtungstechnologien zu Zwecken der Gefahrenabwehr und Strafverfolgung unterfällt mehreren Grundrechtskatalogen, die nebeneinander anzuwenden sind. Dies verursacht allerdings materielle Abstimmungsschwierigkeiten zwischen den verschiedenen Grundrechtsordnungen, die auch eine institutionelle Komponente haben.

Wie jede deutsche hoheitliche Stelle sind auch Polizeibehörden gemäß Artikel 1 Abs. 3 GG an die *Grundrechte des Grundgesetzes* gebunden. Zum staatlichen Einsatz von Beobachtungstechnologien liegt mittlerweile eine reichhaltige Rechtsprechung des Bundesverfassungsgerichts vor, das dazu berufen ist, diese Grundrechte letztverbindlich zu konkretisieren. In seinem Urteil zum BKAG hat das Gericht es unternommen, die bis dahin ergangene Rechtsprechung systematisch aufzubereiten und zu konsolidieren (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09).

Daneben sind gesetzliche Regelungen zum staatlichen Einsatz von Beobachtungstechnologien an der *Europäischen Menschenrechtskonvention*[165] (EMRK) zu messen, die innerstaatlich in Deutschland zwar formal nur den Rang eines einfachen Bundesgesetzes hat, durch das Bundesverfassungsgericht aber auf eine quasi- oder semiverfassungsrechtliche Ebene gehoben wurde. Völkerrechtlich ist die Bundesrepublik ohnehin vollumfänglich verpflichtet, die Konvention einzuhalten. Dies wird vom Europäischen Gerichtshof für Menschenrechte überwacht, der gleichfalls schon zahlreiche Urteile zu sicherheitsbehördlichen Beobachtungspraktiken gefällt hat.

Schließlich ist der polizeiliche Einsatz von Beobachtungstechnologien spätestens seit Mai 2018 in der Regel auch an den *Grundrechten der EU-Grundrechtecharta*[166] (GRCh) zu messen, da seitdem die Richtlinie (EU) 2016/680 Mindestanforderungen für den Datenschutz bei Polizei und Strafjustiz festlegt. Polizeiliche Datenverarbeitungen fallen aufgrund der Richtlinie in den Anwendungsbereich des Unionsrechts und damit auch der Grundrechtecharta. Zur Auslegung der Richtlinie und der Grundrechte der Charta ist letztverbindlich der EuGH

165 Konvention zum Schutz der Menschenrechte und Grundfreiheiten vom 4. November 1950, zuletzt geändert mit Wirkung zum 1. Juni 2010 durch das Protokoll Nr. 14 vom 13. Mai 2004

166 Charta der Grundrechte der Europäischen Union, ABl. EU 2012, C 326, S. 391

berufen, der in seiner jüngeren Rechtsprechung gerade in Bezug auf den Datenschutz strenge Anforderungen an hoheitliche Eingriffsmaßnahmen errichtet hat.

Die parallele Anwendung dieser Grundrechtsschichten so zu ordnen, dass insgesamt kohärente und wirksame Bindungen der hoheitlichen Gewalt im sehr grundrechtssensiblen Bereich staatlicher Beobachtungsmaßnahmen bestehen, stellt eine Herausforderung dar. Im Folgenden wird dies exemplarisch aufgegriffen – eine systematische Erörterung (auch) aus Mehrebenenperspektive ist hier jedoch nicht möglich.

6.1.2 Differenzierter Schutz der Privatheit

Derzeit werden die Privatheit des Einzelnen und die Vertraulichkeit seiner Kommunikationsbeziehungen durch ein komplexes Geflecht unterschiedlicher Grund- und Menschenrechte geschützt. Nicht vollständig geklärt ist, welche Folgen die grundrechtliche Einordnung einer Beobachtungsmaßnahme für die Anforderungen hat, die an diese Maßnahme zu stellen sind. Hingegen ist absehbar, dass die Zuordnungs- und Bewertungsprobleme sich im Laufe der technischen Entwicklung und in Anbetracht veränderter Kommunikationsgewohnheiten noch verschärfen werden. Dies gilt insbesondere für die spezifischen Garantien der Privatheit. Teilweise klärungsbedürftig ist auch deren Verhältnis zu weiteren Grundrechten, die in bestimmten Fallkonstellationen gleichfalls die Vertraulichkeit bestimmter Kommunikationsbeziehungen schützen können.

6.1.2.1 Spezifische Privatheitsgarantien

Die in Deutschland bedeutsamsten Grundrechtskataloge enthalten allesamt spezifische Garantien der Privatheit, differenzieren deren Schutz allerdings in sehr unterschiedlichem Maße. Die Europäische Menschenrechtskonvention schützt die Privatheit pauschal als Unterfall eines übergreifenden Rechts auf Achtung des Privat- und Familienlebens (Artikel 8 EMRK). Die Charta der Grundrechte der Europäischen Union greift dieses Recht auf (Artikel 7 GRCh) und enthält darüber hinaus ein eigenständiges Grundrecht auf Schutz personenbezogener Daten (Artikel 8 GRCh). Das Grundgesetz schützt die Privatheit durch zahlreiche Gewährleistungen. Neben den besonderen Garantien der Unverletzlichkeit der Wohnung (Artikel 13 GG) und des Fernmeldegeheimnisses (Artikel 10 GG) ist insbesondere das allgemeine Persönlichkeitsrecht zu nennen (Artikel 2 Abs. 1 i.V.m. Artikel 1 Abs. 1 GG), das eine Vielzahl von Ausprägungen erfährt, z. B. das Recht auf informationelle Selbstbestimmung, die Garantie der Privatsphäre, die Vertraulichkeit des nichtöffentlich gesprochenen Wortes oder das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Kasten 6.1).

Kasten 6.1 Wesentliche grundgesetzliche Privatheitsgarantien im Kontext des staatlichen Einsatzes von Beobachtungstechnologien

Die *Unverletzlichkeit der Wohnung* schützt die räumliche Sphäre, in der sich das Privatleben entfaltet. Der Schutzbereich umfasst auch den physischen Zugang zu informationstechnischen Systemen, soweit sie innerhalb dieser Räume betrieben werden, nicht jedoch den virtuellen Zugriff auf diese Systeme aus der Ferne (BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07, Rn. 195).

Das *Fernmeldegeheimnis* schützt »das Vertrauen des Einzelnen darin, dass eine Fernkommunikation, an der er beteiligt ist, nicht von Dritten zur Kenntnis genommen wird«, wobei nicht nur die Inhalte der Telekommunikation, sondern auch ihre Umstände geschützt sind (BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07, Rn. 183 u. 290). Es ist immer dann einschlägig, wenn Daten während des laufenden Übertragungsvorgangs im Telekommunikationsnetz beobachtet werden.

Das *Recht auf informationelle Selbstbestimmung* ist das Recht des Einzelnen gegenüber dem Staat und seinen Einrichtungen, über die Preisgabe, Erhebung und Verwendung seiner personenbezogenen Daten grundsätzlich selber bestimmen zu können. Es wurde 1983 durch das Bundesverfassungsgericht (BVerfG, Urteil vom 15. Dezember 1983, 1 BvR 209, 269, 362, 420, 440, 484/83) im Volkszählungsurteil aus dem allgemeinen Persönlichkeitsrecht abgeleitet, welches sich wiederum aus Artikel 2 Abs. 1 GG und Artikel 1 Abs. 1 GG ableitet.

Ebenfalls aus dem allgemeinen Persönlichkeitsrecht abgeleitet ist das *Recht auf Vertraulichkeit des nichtöffentlich gesprochenen Wortes*. Es gewährleistet die Selbstbestimmung über die eigene Darstellung der Person in der Kommunikation mit anderen. Es findet einen Ausdruck in der Befugnis des Menschen, selbst und allein zu entscheiden, ob sein Wort auf einen Tonträger aufgenommen und damit möglicherweise Dritten zugänglich werden soll (BVerfG, Urteil vom 9. Oktober 2002, 1 BvR 1611/96, Rn. 28 ff.).

Das *Grundrecht auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* wurde 2008 durch das Bundesverfassungsgericht (BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07) im Urteil zur Onlinedurchsuchung entwickelt. Notwendig wurde dies, da die Onlinedurchsuchung Schutzlücken offenbarte: Weder berührt sie die Unverletzlichkeit der Wohnung noch das Fernmeldegeheimnis. Auch geht der Datenzugriff bei einer Onlinedurchsuchung »in seinem Gewicht für die

Persönlichkeit des Betroffenen über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinaus«, da es der potenziell erzielbare Datenbestand ermöglicht, »einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten« (BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07, Rn. 200 u.203).

Quelle: Kochheim 2015, S. 524 ff.

Der differenzierte Schutzansatz des Grundgesetzes wird vielfach für vorzugswürdig gegenüber einem generalklauselartigen Schutz der Privatheit durch eine übergreifende Gewährleistung gehalten, da er eine präzisere Entfaltung der grundrechtlichen Schutzgehalte ermöglicht. Nach diesem Verständnis markieren Grundrechte, die bestimmte Rückzugsbereiche oder Kommunikationsmittel besonders schützen, einen erhöhten Schutzbedarf, dem durch erhöhte Anforderungen an hoheitliche Eingriffe Rechnung zu tragen ist. Dementsprechend hebt das Bundesverfassungsgericht den grundrechtlichen Schutz der Wohnung, der Telekommunikation und des eigenen informationstechnischen Systems besonders hervor und knüpft entsprechende hoheitliche Eingriffe an hohe verfassungsrechtliche Hürden. Demgegenüber gewährleistet beispielsweise das Recht auf informationelle Selbstbestimmung ein geringeres Schutzniveau, entsprechend sind hier auch die Eingriffsschwellen niedriger.

Der differenzierte Ansatz setzt allerdings voraus, dass sich die unterschiedlichen Gewährleistungen der Privatheit klar voneinander abgrenzen lassen. Dies ist vor allem für die Privatheit kommunikativer Beziehungen problematisch. Die Abgrenzung war vergleichsweise gut zu leisten, solange sich kommunikative Privatheit auf zwischenmenschliche Kommunikation beschränkte, die über funktional klar definierte Kommunikationsmedien geführt wurde. Angesichts der heute zu beobachtenden Konvergenz der Kommunikationsmittel und der Tendenz zu einer Welt allgegenwärtiger Informationstechnik, in der immer mehr Geräte informationstechnische Komponenten enthalten, die über das Internet mit anderen informationstechnischen Systemen kommunizieren, ist dies zunehmend fragwürdig. So bereitet für das Grundgesetz die Abgrenzung des Fernmeldegeheimnisses vom Recht auf informationelle Selbstbestimmung einerseits und vom Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme andererseits erhebliche Schwierigkeiten. Dies wird nachfolgend ausführlicher am Beispiel der informationstechnischen Beobachtung von Inhalten der Telekommunikation aufgezeigt.

Grundrechtlicher Schutz von Inhalten der Telekommunikation: Abgrenzungsprobleme in zeitlicher Hinsicht

Im geltenden Recht nimmt der Schutz der *laufenden* Telekommunikation eine Sonderstellung ein. Ausgangspunkt ist das grundrechtlich verankerte Fernmeldegeheimnis, das der besonderen Verwundbarkeit der technisch vermittelten Fernkommunikation Rechnung tragen soll, die sich aus dem (heimlichen) Hinzutreten eines Kommunikationsintermediärs ergibt. Hingegen ist das Risiko, dass der Kommunikationspartner Inhalte der Kommunikation (freiwillig oder unfreiwillig) preisgibt, nicht Gegenstand des Fernmeldegeheimnisses, sondern unterfällt nur dem Recht auf informationelle Selbstbestimmung, das als abgeleitetes Recht gegenüber dem Fernmeldegeheimnis ein niedrigeres Schutzniveau gewährleistet. Dementsprechend bindet das geltende Eingriffsrecht staatliche Zugriffe auf laufende Kommunikationsvorgänge an strenge Voraussetzungen, die über die allgemeinen Anforderungen an die Erhebung personenbezogener Daten deutlich hinausgehen.

Die eingriffsrechtlichen Regelungen beruhen auf der Prämisse, dass sich die Inhalte der laufenden Telekommunikation als Gegenstand der Beobachtung in zeitlicher Hinsicht von anderen kommunikationsbezogenen Daten abgrenzen lassen. Für hergebrachte Formen der Telekommunikation bereitet die Zuordnung in laufende Vorgänge keine größeren Probleme: Ein Telefongespräch beginnt, wenn der angerufene Teilnehmer den Anruf annimmt, und endet, sobald einer der Teilnehmer das Gespräch beendet. Bei den funktional weniger klar definierten OTT-Kommunikationsdiensten (Kap. 5.1.2) kann die zeitliche Abgrenzung laufender Kommunikationsinhalte hingegen in beide Richtungen erhebliche Schwierigkeiten bereiten.

Problematisch ist zum einen, wann ein Vorgang der Telekommunikation endet. So wurde lange darüber diskutiert, ob E-Mails, die bei einem E-Mail-Anbieter gespeichert sind, auch dann noch durch das Fernmeldegeheimnis geschützt sind, wenn der Empfänger den Inhalt der E-Mails bereits gelesen hat. Der Disput wurde erst durch das Bundesverfassungsgericht (BVerfG, Urteil vom 2. März 2006, 2 BvR 2099/04) entschieden und zwar dahingehend, dass das Fernmeldegeheimnis einen zeitlich unbegrenzten Schutz für Kommunikationsinhalte gewährt, solange sich diese im Telekommunikationsnetz (also auch beim E-Mail-Anbieter) befinden, nicht jedoch, wenn sich diese nach Abschluss der Übertragung im Herrschaftsbereich eines Kommunikationsteilnehmers befinden. In der Folge greift der behördliche Zugriff auf gespeicherte E-Mails bei einem E-Mail-Anbieter in das Fernmeldegeheimnis ein. Sind dieselben E-Mails auch lokal auf dem Rechner des Empfängers gespeichert und werden dort – etwa im Rahmen einer Hausdurchsuchung – erhoben, so wird hingegen lediglich das Recht auf informationelle Selbstbestimmung berührt.

Zum anderen kann auch der Beginn eines Kommunikationsvorgangs schwierig zu bestimmen sein. Dies zeigt sich insbesondere dann, wenn Kommunika-

tionsinhalte vor dem Versand verschlüsselt werden und der Zugriff daher im Rahmen einer Quellen-TKÜ auf dem Endgerät erfolgen soll (Kap. 5.2.3). Nach der Rechtsprechung des Bundesverfassungsgerichts (BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07, Rn. 190 ff.) hat sich eine Quellen-TKÜ hinsichtlich der erhobenen Daten auf Inhalte der *laufenden* Telekommunikation zu beschränken. Nur unter dieser Maßgabe wertet das Bundesverfassungsgericht eine Quellen-TKÜ als einen Eingriff in das Fernmeldegeheimnis, der dann unter den Voraussetzungen einer herkömmlichen TKÜ durchgeführt werden darf. Anderenfalls handelt es sich um eine Onlinedurchsuchung, an die das Gericht höhere verfassungsrechtliche Anforderungen stellt, die eher den Anforderungen an eine Wohnraumüberwachung entsprechen. Wie allerdings in Kapitel 5.2.3.3 dargelegt, überzeugt eine unterschiedliche Behandlung von Quellen-TKÜ und Onlinedurchsuchung aus technischer Sicht nicht durchweg, da der Verschlüsselungs- und Übertragungsvorgang nicht immer als Einheit betrachtet werden kann und daher schwer zu bestimmen ist, welche Daten nach der Verschlüsselung tatsächlich übertragen und damit zum Inhalt eines laufenden Kommunikationsvorgangs werden. Bei seiner Konstruktion einer verfassungsrechtlich privilegierten Quellen-TKÜ ging das Bundesverfassungsgericht möglicherweise unausgesprochen von der synchron ablaufenden Sprachtelefonie aus, bei der es intuitiv eher einleuchtet, Verschlüsselung als Teil des Versands zu begreifen. Den heute üblichen multifunktionalen OTT-Kommunikationsdiensten wird diese Vorstellung jedoch nicht mehr gerecht.

Die Schwierigkeit, laufende Kommunikationsinhalte in zeitlicher Hinsicht überzeugend abzugrenzen, verweist auf ein tieferliegendes Bewertungsproblem. So erscheint es grundsätzlich fraglich, die Sensibilität von Inhalten der Telekommunikation danach zu bemessen, ob sie gerade Teil eines laufenden Kommunikationsvorganges sind oder nicht. Dies führt dazu, dass dieselben Inhalte mal stärker, mal schwächer geschützt werden, je nachdem, ob sie gerade übertragen werden (mit der Folge, dass das Fernmeldegeheimnis greift) oder sich im Herrschaftsbereich des Kommunikationsteilnehmers befinden, wo – je nach Zugriffsmodalitäten – entweder das hohe Schutzniveau des Grundrechts auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gilt (beim Zugriff durch eine Onlinedurchsuchung) oder nur der einfache Schutz des Rechts auf informationelle Selbstbestimmung gewährleistet ist (beim einmaligen Zugriff im Rahmen einer Beschlagnahme). Hinzu kommt, dass angesichts der zunehmenden Funktionalität und Komplexität vernetzter informationstechnischer Systeme die Vorstellung überholt ist, der Einzelne könne in jedem Fall noch die Kontrolle darüber behalten, wo sich seine Daten gerade befinden und wie oft und in welchem Umfang sie zwischen seinen Endgeräten und den Servern der Diensteanbieter übertragen werden (ggf. auch nur zu Sicherungszwecken). Wer nicht auf die Nutzung moderner elektronischer Kommunikationsmittel verzichten will oder kann, muss sich zwangsläufig auf technische Prozesse verlassen,

deren Wirkungsweise er im Einzelnen nicht überschauen und die er allenfalls rudimentär beherrschen kann.

Grundrechtlicher Schutz von Inhalten der Telekommunikation: Abgrenzungsprobleme in sachlicher Hinsicht

Nicht nur in zeitlicher, auch in sachlicher Hinsicht bereitet die Abgrenzung des grundrechtlichen Schutzes für Inhalte der Telekommunikation erhebliche Schwierigkeiten. Insbesondere das Fernmeldegeheimnis schützt nach hergebrachter Doktrin nur die Inhalte einer laufenden Individualkommunikation. Diese Voraussetzung ist weitgehend unproblematisch, solange Fernkommunikation über unterschiedliche, technisch und funktional klar definierte und damit abgrenzbare Dienste vermittelt wird: Geschützt ist etwa das Telefongespräch, nicht jedoch die Ausstrahlung eines Radioprogramms. Unter den heutigen technischen Bedingungen ist eine Unterscheidung zwischen Diensten der Individual- und Massenkommunikation häufig nicht mehr überzeugend zu leisten. So sind OTT-Kommunikationsdienste in der Regel multifunktional und lassen sich zur 1-zu-1- ebenso wie zur 1-zu-x-Kommunikation nutzen. Auch finden sich Zwischenformen, die sich der trennscharfen Einordnung als Individual- oder Massenkommunikation von vornherein entziehen, z. B. Profile oder Gruppen auf sozialen Netzwerken, bei denen der Zugriff auf das Profil bzw. die Gruppe insgesamt oder auch Zugriffe auf einzelne Informationen feingranular gesteuert werden können.

Nicht nur die Unterscheidung zwischen Individual- und Massenkommunikation bereitet Probleme, sondern auch die Frage, ob der Schutzbereich des Fernmeldegeheimnisses auf die Kommunikation zwischen Menschen beschränkt bleibt, oder auch Kommunikationsvorgänge zwischen Menschen und Maschinen (Aufruf einer Webseite, Suchanfragen im Internet, Datenspeicherung in der Cloud) oder zwischen Maschinen (z. B. vernetzte informationstechnische Geräte im Smart Home) umfasst. Für die Praxis ist diese Frage hochrelevant, weil sie darüber entscheidet, ob unter den Voraussetzungen einer TKÜ bei einem Internetanschluss Behörden nur Zugriff auf klassische, zwischen Personen ausgetauschte Kommunikationsinhalte (IP-Telefonie, E-Mail, Instant-Messaging etc.) erhalten sollen oder auch auf den gesamten über den Internetanschluss laufenden IP-Datenverkehr. In letzterem Fall können (sofern keine Verschlüsselung verwendet wird) nicht nur sämtliche Internetaktivitäten des Betroffenen erfasst werden, sondern darüber hinaus auch der Datenverkehr aller mit dem Internet verbundenen Geräte. Angesichts der heutigen Bedeutung des Internets in allen Lebensbereichen sowie der zunehmend massenhaften Verbreitung solcher Geräte unter dem Stichwort Internet der Dinge und der ihnen typischen Funktionalitäten (z. B. intelligente Unterhaltungselektronik, Steuerung von Haustechnik oder Haushaltsgeräten) dürften die hier generierten Datenströme regelmäßig sehr tiefgehende Einblicke in das Leben einer Person ermöglichen. Bei manchen Geräten (internetfähiges Spielzeug, intelligente persönliche Assistenten wie Alexa oder

Siri, vernetzte Medizinprodukte) können auch die (thematisch bestimmte) Privatsphäre oder sogar der unantastbare Kernbereich privater Lebensgestaltung betroffen sein, etwa wenn Ton und Bilder in der Wohnung aufgezeichnet werden oder wenn die Geräte Informationen über höchstpersönliche Bereiche wie Äußerungen innerster Gefühle oder Ausdrucksformen der Sexualität speichern. Insofern können Zugriffe auf den gesamten laufenden IP-Datenverkehr unter Umständen auch in das Grundrecht der Unverletzlichkeit der Wohnung und/oder in das Recht auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme eingreifen, die gegenüber dem Fernmeldegeheimnis ein höheres Schutzniveau errichten.

In diesem Zusammenhang von Bedeutung ist ein Beschluss des Bundesverfassungsgerichts (BVerfG, Beschluss vom 6. Juli 2016, 2 BvR 1454/13) von 2016. Demnach fallen auch nutzerseitige Abrufe von Informationen aus dem Internet (Webseitenaufrufe, Suchanfragen etc.) in den Schutzbereich des Fernmeldegeheimnisses, sodass behördliche Zugriffe auf solche Informationen unter den Voraussetzungen einer TKÜ (§ 100a StPO) erfolgen können.[167] Zwar erkennt das Gericht (BVerfG, Beschluss vom 6. Juli 2016, 2 BvR 1454/13, Rn. 26 ff. u. 49) die unterschiedliche Natur der Internetnutzung zur Kommunikation im sozialen Sinne und zum Zwecke des Surfens an und ermahnt Ermittlungsbehörden und Gerichte, im Einzelfall eine Verhältnismäßigkeitsabwägung zwischen einer Internetüberwachung und einer beispielsweise auf die Ausleitung des Telefon- und E-Mail-Verkehrs beschränkte TKÜ vorzunehmen. Einigen Kommentatoren geht diese Aufforderung allerdings nicht weit genug, vielmehr fordern sie die Schaffung einer eigenständigen Eingriffsnorm für die Internetüberwachung mit entsprechend höheren Eingriffsschwellen im Vergleich zur herkömmlichen TKÜ. Begründet wird dies damit, dass bei der sozialen Kommunikation Betroffene bewusst und freiwillig Wissen gegenüber Dritten offenbaren würden (z. B. in einem Telefongespräch), während die Internetnutzung zu nichtkommunikativen Zwecken (Informationsbeschaffung, Unterhaltung) keine Interaktion mit Dritten erfordere und daher ihrer Natur nach (wenn auch nicht immer dem Inhalt nach) privater und infolgedessen besonders schützenswert sei (Hiéramente 2016, S. 451 ff.).

In der Praxis ist es aber regelmäßig sehr schwierig, Inhalte zwischenmenschlicher von anderen Formen der Telekommunikation abzugrenzen, da internetbasierte Dienste häufig kommunikative und nichtkommunikative Komponenten vereinen oder sich zumindest für eine Kommunikation zwischen Menschen zweckentfremden lassen. Cloudspeicherdienste beispielsweise dienen auf den ersten Blick nicht der zwischenmenschlichen Kommunikation, indem aber

167 Das Gericht begründet dies u. a. mit der technikorientierten Definition des in den jeweiligen Eingriffsnormen verwendeten Begriffs der Telekommunikation: Gemäß § 3 Nr. 22 TKG umfasst Telekommunikation den »technischen Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen« – mitunter also auch die Fernkommunikation zwischen Mensch und Maschine.

gespeicherte Daten mit Dritten geteilt werden, können sie gleichfalls zum Gegenstand einer Fernkommunikation zwischen zwei Menschen werden. Ob ein Kommunikationsvorgang viele, zwei, einen oder keinen menschlichen Teilnehmer hat, dürfte sich daher oftmals erst bei der Analyse der Daten, also erst nachdem die Daten ausgeleitet wurden, feststellen lassen.

Die hier angerissenen Probleme, bei modernen Formen der Telekommunikation die Inhalte in zeitlicher und sachlicher Hinsicht abzugrenzen, werfen die grundlegende Frage auf, ob der grundrechtliche Schutz elektronischer Kommunikationsinhalte ggf. neu zu konzipieren wäre, indem nach technisch und sozial anschlussfähigeren und normativ überzeugenderen Kriterien für die Sensibilität digitaler Inhalte gesucht wird. Benötigt werden Kriterien für die Bemessung der Eingriffsintensität behördlicher Beobachtungen, die sich einerseits von der hergebrachten Abgrenzung nach Herrschaftssphären des Betroffenen lösen und andererseits der Vielschichtigkeit von Telekommunikation in Bezug auf die beteiligten Teilnehmer (seien dies Menschen oder Maschinen) Rechnung tragen. Bislang fehlt es hierzu jedoch weitgehend an konzeptionellen Vorarbeiten. Ein konsistenter und handhabbarer Satz trennscharfer alternativer Intensitätskriterien ist weder in der Rechtsprechung noch in der Literatur erkennbar.

6.1.2.2 Weitere Gewährleistungen

Neben spezifischen Privatheitsgarantien kann der staatliche Einsatz von Beobachtungstechnologien weitere Grundrechte berühren, etwa die freie Meinungsäußerung, die Religionsfreiheit, die Versammlungsfreiheit oder die Presse- und Rundfunkfreiheit. Diese Grundrechte markieren gleichfalls besondere Schutzbedürfnisse.

Auch diesbezüglich ergeben sich im Lichte neuer Kommunikationsmittel und -formen sowie entsprechender Beobachtungsmöglichkeiten neue Herausforderungen. Dies betrifft beispielsweise den Zuschnitt der Privilegien der hergebrachten Massenmedien, die zur Gewährleistung der Presse- und der Rundfunkfreiheit einen erhöhten Schutz beruflicher Vertrauensverhältnisse gegen hoheitliche Beobachtung umfassen. Schon heute hat sich nämlich die klassische Rolle der Massenmedien als Vermittler der öffentlichen Kommunikation relativiert, da beispielsweise manche Blogs oder Twitter-Profile eine nicht minder hohe Zahl an Leser/innen erreichen. Es stellt sich die Frage, ob, unter welchen Voraussetzungen und inwieweit von Grundrechts wegen die hergebrachten Medienprivilegien auf die Betreiber von netzbasierten Kommunikationsformaten erstreckt werden müssen, die gleichfalls zur öffentlichen Meinungsbildung beitragen, ohne notwendigerweise im hergebrachten Sinn journalistisch zu arbeiten oder über redaktionelle Strukturen herkömmlichen Zuschnitts zu verfügen.

6.1.3 Kriterien für die Eingriffsbegründung

Steht fest, welches Grundrecht durch eine staatliche Beobachtungsmaßnahme berührt wird, so muss untersucht werden, ob bzw. mit welcher Intensität die Maßnahme in dieses Grundrecht eingreift.

Für die Gewährleistungen der Privatheit geht die Rechtsprechung einerseits von einem weiten Eingriffsbegriff aus, der grundsätzlich jede hoheitliche Kenntnisnahme grundrechtlich geschützter Persönlichkeitsäußerungen rechtfertigungsbedürftig macht. Da zugleich insbesondere das Recht auf informationelle Selbstbestimmung alle personenbezogenen Daten in seinen Schutzbereich aufnimmt, führt dies zu einer Ubiquität des Grundrechtsschutzes. Es stellt sich insofern die Frage, ob auf diese Weise die privatheitsbezogenen Grundrechte nicht entwertet werden. Denn es liegt nahe, dem universellen Rechtfertigungsbedarf mit ebenso universellen Rechtfertigungsformeln zu begegnen, die dann wiederum herangezogen werden können, um den Grundrechtsschutz auch in wirklich problematischen Situationen zu relativieren.

Andererseits ist es der Rechtsprechung bislang nicht gelungen, allgemein akzeptierte Kriterien zur Einengung des Grundrechtsschutzes zu finden. Hierfür exemplarisch ist die Frage zu nennen, ob die grundrechtlichen Gewährleistungen der Privatheit vor einer hoheitlichen Kenntnisnahme öffentlich zugänglicher Daten schützen. Nach der Rechtsprechung lässt sich diese Frage nicht pauschal beantworten, wie einige Beispiele zeigen:

- So hat das Bundesverfassungsgericht (BVerfG, Beschluss vom 23. Februar 2007, 1 BvR 2368/06) die dauerhafte stationäre Videobeobachtung im öffentlich zugänglichen Raum jedenfalls dann, wenn das gewonnene Bildmaterial gespeichert wird, ohne Weiteres als Grundrechtseingriff qualifiziert. Eine Unterscheidung von (personenbeziehbaren) Übersichtsaufnahmen und der gezielten Beobachtung einzelner Personen ist in dieser Rechtsprechung nicht angelegt.
- Wird hingegen eine stationäre Videobeobachtung im öffentlich zugänglichen Raum mit Verfahren der automatisierten Bildauswertung (Kap. 3.3) verknüpft und derart ausgestaltet, dass die Aufnahmen in Nichttrefferfällen unmittelbar nach der Auswertung gelöscht werden, so erkannte das Bundesverfassungsgericht (BVerfG, Urteil vom 11. März 2008, 1 BvR 2074/05 zum automatisierten Kfz-Kennzeichenabgleich) darin bis vor Kurzem nur in Trefferfällen einen Grundrechtseingriff. Ende 2018 korrigierte das Gericht (BVerfG, Beschluss vom 18. Dezember 2018, 1 BvR 142/15. Rn. 45 ff.) seine bisherige Rechtsprechung dahingehend, dass in solchen Fällen immer in Grundrechte eingegriffen wird, unabhängig davon, ob ein Treffer vorliegt oder nicht (Kap. 3.5.5.2).
- In Bezug auf öffentlich zugängliche Inhalte im Internet hat das Bundesverfassungsgericht festgehalten, dass eine Kenntnisnahme dem Staat grundsätzlich

nicht verwehrt sei. So würden staatliche Stellen nicht in Grundrechte eingreifen, wenn sie im Internet verfügbare Inhalte erheben, die sich an jedermann oder zumindest an einen nicht weiter abgegrenzten Personenkreis richteten. Dies gelte auch dann, wenn auf diese Weise im Einzelfall personenbezogene Informationen erhoben würden. Allerdings könne ein Eingriff in das Recht auf informationelle Selbstbestimmung dann vorliegen, wenn solche allgemein zugängliche Informationen gezielt zusammengetragen, gespeichert und ggf. unter Hinzuziehung weiterer Daten ausgewertet würden und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergebe (BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07, Rn. 304 ff.). Kriterien dafür, wann eine solche Gefahrenlage anzunehmen ist, stehen aber weitgehend noch aus.

6.1.4 Kriterien für die Eingriffsintensität

Um die grund- und menschenrechtlichen Anforderungen an den behördlichen Einsatz einer bestimmten Beobachtungstechnologie abzuleiten, muss bestimmt werden, wie intensiv die Maßnahme in das betroffene Grundrecht eingreift. In der Rechtsprechung wird dazu ein Bündel von Kriterien herangezogen, die allerdings teilweise umstritten sind und vor dem Hintergrund des technischen und sozialen Wandels einer kritischen Evaluation bedürfen.

Umstritten ist beispielsweise die Auffassung des Bundesverfassungsgerichts, die Eingriffsintensität nehme zu, wenn eine Beobachtungsmaßnahme breit streut, also – zunächst – eine Vielzahl von Personen erfasst, an deren Mehrheit kein behördliches Interesse besteht.[168] In der Rechtsprechung und Literatur wird das Kriterium der Streubreite vielfach auf einen Einschüchterungseffekt großflächig wirkender Beobachtungsmaßnahmen zurückgeführt.[169] Kritiker des Streubreitenkriteriums verweisen jedoch auf den noch lückenhaften wissenschaftlichen Erkenntnisstand über mögliche Einschüchterungseffekte (dazu Kap. 7.1), wodurch die Rechtsprechung mit »Vermutungen über die möglichen Wirkungen« von Beobachtungsmaßnahmen (Trute 2009, S. 98), mindestens aber mit großzügigen Extrapolationen arbeite. Anderer Ansicht nach lasse sich das Streubreitenkriterium allerdings über Einschüchterungseffekte hinaus auch mit der Erwägung begründen, dass breit streuende Beobachtungsmaßnahmen ein besonderes Prognoserisiko schafften. Beispielsweise könnten menschliche oder algorithmenbasierte Fehler bei der Datenauswertung dazu führen, dass Personen in den behördlichen Fokus geraten, die dafür gar keinen Anlass gegeben haben. In solchen Fällen setze sich die Streubreite in Folgemaßnahmen gegenüber diesen Betroffenen fort,

168 Ständige Rechtsprechung, zuletzt aufgegriffen in BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 101

169 So auch das Bundesverfassungsgericht (BVerfG, Urteil vom 15. Dezember 1983, 1 BvR 209, 269, 362, 420, 440, 484/83, Rn. 154) im Volkszählungsurteil von 1983 zur Begründung des grundrechtlichen Datenschutzes überhaupt.

was wiederum als Steigerung der Eingriffsintensität der Beobachtungsmaßnahme zu bewerten sei (Bäcker 2015, S. 270 ff.).

Einer kritischen Evaluation bedarf die Frage der Eingriffsintensität insbesondere für Beobachtungsmaßnahmen, welche die Telekommunikation zum Gegenstand haben. Teils setzt sich hier die Schwierigkeit fort, netzbasierte Kommunikationsdienste den verschiedenen Gewährleistungen kommunikativer Privatheit zuzuordnen (Kap. 6.1.2.1). Teils aber bestehen auch im Rahmen der einzelnen Gewährleistungen Bewertungsprobleme. Beispielsweise entschied das Bundesverfassungsgericht, dass Inhalte von E-Mails, die sich im Telekommunikationsnetz befinden, durch das Fernmeldegeheimnis zeitlich uneingeschränkten Schutz genießen (Kap. 6.1.2.1). Doch während die Echtzeiterhebung von Inhalten von E-Mails beim Diensteanbieter laufende Kommunikationsvorgänge betrifft und nur unter den hohen Voraussetzungen einer TKÜ (§ 100a StPO) erfolgen kann, verzichtete das Bundesverfassungsgericht in einem Urteil von 2009 darauf, dieselben strengen Maßstäbe an die Erhebung von beim Diensteanbieter gespeicherten Nachrichten zu knüpfen. Hier erachtete das Gericht (BVerfG, Urteil vom 16. Juli 2009, 2 BvR 902/06, Rn. 69) die Eingriffsnormen zur Sicherstellung und Beschlagnahme (§§ 94 ff. StPO) als ausreichend, die lediglich den Anfangsverdacht einer Straftat voraussetzen. Zur Begründung verweist das Gericht u. a. darauf, dass die Beschlagnahme gegenüber dem Betroffenen offen erfolge, was allerdings in der Praxis allenfalls ausnahmsweise der Fall sein dürfte. Unabhängig davon leuchtet in Bezug auf die Sensibilität der betroffenen Kommunikationsinhalte eine Unterscheidung danach, ob die staatliche Kenntnisnahme aus technischer Sicht während eines Übermittlungsvorgangs oder während einer – immer noch der Übertragungsstrecke zuzuordnenden – Zwischenspeicherung stattfindet, nicht unmittelbar ein (Bäcker 2019).

Das Fernmeldegeheimnis schützt überdies nicht nur die Inhalte der laufenden Telekommunikation, sondern auch deren Umstände, also die Verkehrsdaten, die bei der Erbringung des Telekommunikationsdienstes anfallen. Allerdings genießen Verkehrsdaten nach verbreiteter Auffassung, die sich teils auch in der Rechtsprechung des Bundesverfassungsgerichts und des EuGH widerspiegelt, einen weniger weitreichenden Schutz als Inhaltsdaten. Zum Ausdruck kommt dies beispielsweise in der Strafprozessordnung, welche die Erhebung von Verkehrsdaten (im Sinne von § 96 TKG) beim Diensteanbieter an niedrigere Eingriffsvoraussetzungen knüpft als die Erhebung von Inhaltsdaten im Rahmen der TKÜ (Tab. 5.3 in Kap. 5.3.1).[170] Historisch erklärt sich diese Position daraus, dass der Schutz der Umstände der Telekommunikation als abgeleiteter Schutz konzipiert wurde. Danach sind die Kommunikationsumstände darum schutzbedürftig, weil aus ihnen ggf. Rückschlüsse auf die Telekommunikationsinhalte gezogen bzw. solche Inhalte bestimmten Personen zugeordnet werden können. Diese Erkenntnis trifft zwar immer noch zu, schöpft jedoch den Erkenntniswert von Verkehrsdaten nicht

170 Nicht so aber beispielsweise das BKAG (Tab. 5.4, Kap. 5.3.2).

annähernd aus. Heute ermöglichen Verkehrsdaten unter Umständen die Ermittlung von Aufenthaltsorten einer Person, die Erstellung individueller Bewegungs- oder Verhaltensprofile oder die Analyse komplexer Beziehungsnetze (was beispielsweise für die Bekämpfung von organisierter Kriminalität von Bedeutung sein kann). Die Aussagekraft von Verkehrsdaten kann somit unabhängig von den Inhalten sein und teilweise über den möglichen Erkenntnisgewinn aus der Analyse von Inhaltsdaten sogar hinausgehen. Vor diesem Hintergrund erscheinen Verkehrsdaten nicht weniger schutzbedürftig als Inhaltsdaten.

6.1.5 Diskriminierungsschutz: blinder Fleck des Sicherheitsverfassungsrechts?

Anders als in anderen Jurisdiktionen spielen die grundrechtlichen Diskriminierungsverbote in der verfassungsrechtlichen Diskussion zum staatlichen Einsatz von Beobachtungstechnologien in Deutschland bislang kaum eine Rolle. Dies mag auch mit dem hiesigen hohen Stellenwert und dem beträchtlichen Schutzniveau des grundrechtlichen Datenschutzes zusammenhängen, mit dessen Hilfe sich viele Schutzbedürfnisse abbilden lassen, die anderenorts vor allem als Gleichbehandlungsproblem gesehen würden.

Allerdings könnten grundrechtliche Diskriminierungsverbote künftig im Zusammenhang mit der zunehmenden polizeilichen Nutzung von Verfahren der automatisierten Datenauswertung an Bedeutung gewinnen, etwa im Kontext der Videobeobachtung (Gesichtserkennung, Situation- und Verhaltensanalysen; Kap. 3.3), der Internetbeobachtung (teilautomatisierte Social Media Intelligence; Kap. 4.2) oder der Ansätze des Predictive Policing (Kap. 4.3). Sowohl bei der Auswahl von Kriterien, die zur Beobachtung von polizeilich relevanten Sachverhalten oder Personen herangezogen werden sollen, als auch bei der Entwicklung der Algorithmen bzw. von Modellen des maschinellen Lernens kann es zu Diskriminierungen kommen (Kap. 3.3.8.2). Sollten derartige Systeme künftig beispielsweise zur Personenfahndung in Echtzeit oder für die Erstellung individualisierter Risikobewertungen eingesetzt werden, stellen sich völlig neuartige Grundrechtsfragen.

6.1.6 Polizeiliche Planungshandlungen

Das polizeiliche Eingriffsrecht regelt derzeit neben den Aufgaben der Polizei in erster Linie einzelne polizeiliche Maßnahmen, wozu auch technische Beobachtungsmaßnahmen zählen. Die taktischen Vorentscheidungen, die einzelnen Maßnahmen vorausliegen und sie miteinander verknüpfen, sind als solche kein Thema des Eingriffsrechts. Für polizeiliche Planungshandlungen enthalten die Polizeigesetze und die Strafprozessordnung nur insoweit rudimentäre Regelungen, als es um die Verarbeitung personenbezogener Daten geht. Diesem Regulierungs-

ansatz liegt die Annahme zugrunde, dass die Regulierung einzelner Maßnahmen ausreicht, um polizeiliche Verfahren wirksam anzuleiten und in einem rechtsstaatlich angemessenen Rahmen zu halten. Zudem wird vorausgesetzt, dass das polizeiliche Planungsstadium – abgesehen von datenschutzrechtlichen Aspekten – keine grundrechtliche Relevanz hat.

Neue Kriminalitätsformen, geänderte Gefährdungsbewertungen, die zunehmende Ausrichtung der Polizeiarbeit auch auf die vorbeugende Verbrechensbekämpfung und nicht zuletzt die neuen Möglichkeiten der (heimlichen) informationstechnischen Beobachtung tragen zum Ausbau und zur Vertiefung proaktiver polizeilicher Handlungskonzepte bei, die jenseits von Einzelfällen auf eine fortlaufende Kriminalitätskontrolle gerichtet sind (Kap. 2.5.2; Bäcker 2015, S. 53 ff. u. 64 ff.). Diese Handlungskonzepte eröffnen der Polizei die Möglichkeit, ihre Verfahren in weit größerem Maß selbst zu gestalten, als dies nach den hergebrachten, an konkreten sozialen Konflikten ausgerichteten Präventionsansätzen der Fall ist: Die Polizei kann hier strategisch bestimmen, welchen Risikofaktoren sie sich widmet und welche kriminalpräventiven Erfolge sie anstrebt. Einzelne Eingriffsmaßnahmen erhalten ihren Sinn deshalb durch vorgelagerte planerische Entscheidungen, die diese Maßnahmen vorstrukturieren und verknüpfen. Zu nennen sind hier etwa längerfristige heimliche Beobachtungen krimineller Strukturen oder Milieus mit dem Ziel, gegen sie möglichst nachhaltig vorzugehen, oder die Einrichtung von stationärer polizeilicher Videobeobachtung an kriminalitätsbelasteten Orten.

Allerdings können bereits von der polizeilichen Planungsphase Risiken für Grundrechtseingriffe ausgehen, weil hier ggf. getroffene Vorentscheidungen auf der Ebene der einzelnen Eingriffsmaßnahmen als Sachzwänge wirken können, die sich kaum noch in Frage stellen lassen (z. B. im Kontext von Lagebildern oder sonstigen Gefahrenbewertungen, die der Planung zugrunde liegen). Insofern wird verschiedentlich die Frage aufgeworfen, ob grundrechtliche Anforderungen nicht erst an die einzelnen polizeilichen Eingriffsmaßnahmen, sondern darüber hinaus auch bereits an das polizeiliche Planungsstadium (über datenschutzrechtliche Aspekte hinaus) gestellt werden sollten (z. B. Bäcker 2015, S. 290 ff.). Eine Anforderung könnte beispielsweise darin bestehen, dass die einzelnen Maßnahmen an eine vorab festgelegte, allerdings für Anpassungen offene Präventionsstrategie mit einem übergeordneten Präventionsziel ausrichtet werden müssten; die Präventionsstrategie könnte dann einen rechtlich verbindlichen Rahmen für die einzelnen Maßnahmen bilden.

6.1.7 Inpflichtnahme privater Akteure zur Sicherheitsgewähr

Für die Bewältigung der Sicherheitsarbeit nimmt der Staat auch nichtstaatliche Akteure und insbesondere private Unternehmen in die Pflicht. Im Kontext einiger Beobachtungstechnologien ist er auf eine Mitwirkung Privater sogar angewiesen,

beispielsweise bei einigen informationstechnischen Beobachtungspraktiken im Telekommunikationsnetz (Kap. 5.2.1.1, 5.2.2) oder im Rahmen der Nutzung von privatem Bild- oder Videomaterial zu Zwecken der Gefahrenabwehr oder Strafverfolgung (Kap. 3.4.2.4).

Eine solche Inpflichtnahme Privater zur Sicherheitsgewähr ist aus grundrechtlicher Sicht vor allem dann problematisch, wenn sie einen Zielkonflikt zwischen unterschiedlichen Sicherheitsanliegen erzeugt. Ein Beispiel hierfür bietet die Regulierung von Verschlüsselung (Kap. 5.2.1.3), wo der Zielkonflikt darin besteht, dass einerseits Schutzmechanismen umgangen werden sollen, die staatlichen Beobachtungsmaßnahmen entgegenstehen, andererseits diese Schutzmechanismen aber ein essentieller Bestandteil für eine sichere Kommunikation im Internet darstellen. Zumindest in Deutschland ist die hohe gesellschaftliche Bedeutung leistungsfähiger Verschlüsselung weitgehend anerkannt, sodass es aktuell keine politischen Bestrebungen für eine gezielte Schwächung von Verschlüsselung gibt (Kap. 5.4.1.3). Für andere Zielkonflikte hingegen ist umstrittener, wie eine tragfähige Lösung aussehen könnte. Exemplarisch sei hier der Dauerstreit um die Vorratsdatenspeicherung von Verkehrsdaten der Telekommunikation genannt, der auch nach Entscheidungen zahlreicher deutscher und europäischer Gerichte bisher noch nicht nachhaltig befriedet werden konnte (Kap. 5.3.1.2).

Aus Sicht der in die Pflicht genommenen Unternehmen ist schließlich auch die Frage bedeutsam, wer die Kosten der Inpflichtnahme zu tragen hat. Grundrechtlich relevant ist diese Frage z. B. in Bezug auf die verfassungsrechtlich garantierte Berufsfreiheit und die unternehmerische Freiheit. Das Bundesverfassungsgericht hat eine entschädigungslose Inpflichtnahme in weitem Umfang gebilligt und die Unternehmen auf die Möglichkeit verwiesen, die Kosten auf ihre Kunden abzuwälzen. Ob der EuGH diese Position teilt, bleibt allerdings abzuwarten.

6.2 Eingriffsrecht (Strafprozess- und Polizeirecht)

Durch die grundrechtlichen Vorgaben des europäischen Mehrebenensystems (Kap. 6.1.1) besteht ein differenziertes System von Anforderungen an die Sicherheitsbehörden in Bezug auf die Informationserhebung und -verarbeitung sowie auf das Handeln aufgrund der so gewonnenen Erkenntnisse. Da die Erhebung und Verwendung personenbezogener Daten – im Regelfall – zumindest einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstellen, greift der Gesetzesvorbehalt: Jeder staatliche Eingriff in grundrechtlich geschützte Rechtspositionen bedarf bestimmter und normenklarer Ermächtigungsgrundlagen, die dem Gewicht des Eingriffs Rechnung tragen und insbesondere den Grundsatz der Verhältnismäßigkeit (auch als Übermaßverbot bezeichnet) beachten. Nach diesem Grundsatz muss ein Grundrechtseingriff immer einem legitimen Zweck dienen und das gewählte Mittel zur Erreichung des Zwecks muss

geeignet, erforderlich (d. h. der Zweck darf nicht mit Maßnahmen geringerer Eingriffsintensität vergleichbar effektiv zu erreichen sein) und verhältnismäßig im engeren Sinne sein. Das Gebot der Verhältnismäßig im engeren Sinne (auch als Gebot der Angemessenheit bezeichnet) verlangt vom Gesetzgeber, dass zwischen der Schwere des Eingriffs in die Grundrechte potenziell Betroffener auf der einen Seite und der Pflicht des Staates zum Schutz der Grundrechte auf der anderen Seite ein Ausgleich zu schaffen ist (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09 Rn. 93 u. 98).

In Deutschland finden sich derartige Eingriffsgrundlagen in zwei großen Rechtsbereichen: im Polizeirecht (präventive Abwehr von Gefahren einschließlich Straftaten) und im Strafprozessrecht (repressive Aufklärung begangener Straftaten).[171] Beide Bereiche werden durch neue Informations- und Kommunikationstechnologien herausgefordert, weil sie zum einen organisationsrechtlich von zwar in Grenzbereichen umstrittenen, herkömmlich aber doch relativ stabilen Kompetenzbereichen ausgehen und zum anderen unterschiedliche Normschichten aufweisen, die aus verschiedenen Epochen der Sicherheitsregulierung stammen. Diese Epochen unterscheiden sich nicht nur – faktisch – hinsichtlich der jeweils als modern verstandenen Beobachtungstechnologien, sondern auch – rechtlich – hinsichtlich des Verständnisses darüber, welche Anforderungen das Grundgesetz an die Bestimmtheit und den Detailgrad der gesetzlichen Ermächtigungsgrundlagen stellt.

6.2.1 Abgrenzung präventives und repressives Handeln

Bei der Abgrenzung von präventivem und repressivem Handeln handelt es sich um eine klassische Problemstellung des Sicherheitsrechts, die dieses in die zwei Bereiche des Polizei- und Strafprozessrechts unterscheidet. Während das präventive Handeln vorrangig auf die Abwehr drohender Gefahren (für die öffentliche Sicherheit, teilweise auch für die öffentliche Ordnung) gerichtet ist, dient repressives Handeln (insbesondere) der strafrechtlichen Sanktionierung begangenen Unrechts. Die Abgrenzung der beiden Bereiche ist insbesondere für polizeiliches Handeln problembehaftet, weil Polizeibehörden regelmäßig sowohl für die Gefahrenabwehr als auch für die Strafverfolgung zuständig sind. Der Einsatz von Beobachtungstechnologien führt hier regelmäßig zu spezifischen Herausforderungen, weil sie je nach Einsatzszenario flexibel zu unterschiedlichen Zwecken eingesetzt werden können und Beobachtungssituationen infolgedessen häufig nicht eindeutig einem bestimmten Aufgabenbereich zuzuordnen sind (beispielsweise kann die stationäre polizeiliche Videobeobachtung sowohl der Gefahrenabwehr als auch der Strafverfolgung dienen).

171 Auf entsprechende Eingriffsbefugnisse für die Nachrichtendienste wird hier nicht eingegangen.

Der Einsatz von Beobachtungstechnologien kann daher die genannte Zweiteilung des deutschen Sicherheitsrechts vor Probleme stellen. Diese beginnen bereits bei den Handlungskompetenzen, weil verfassungsrechtlich der Bereich der Gefahrenabwehr (bis auf wenige spezifische Aufgabenfelder wie der Grenzschutz) grundsätzlich den Ländern, dagegen der Bereich der Strafverfolgung dem Bund zugewiesen ist (Kap. 2.4). Werden neue Eingriffsbefugnisse für den Einsatz von Beobachtungstechnologien geschaffen, so muss stets die Zuständigkeit geklärt werden.[172]

Geht es um die Anwendung bestehenden Rechts, ist ebenfalls zu bestimmen, welchem Regelungsregime (Polizeigesetze der Länder, Strafprozessordnung des Bundes) die jeweiligen Maßnahmen unterfallen. So unterscheiden sich die Befugnisse zum präventiven bzw. repressiven Einsatz von Beobachtungstechnologien teilweise nicht nur im Detail – z. B. in Bezug auf die Abstufung der Eingriffsvoraussetzungen in Abhängigkeit von der Schwere des Grundrechtseingriffs (Kap. 5.3) –, sondern auch grundsätzlich (so waren beispielsweise Regelungen zum automatisierten Kfz-Kennzeichenabgleich lange Zeit nur in einigen Landespolizeigesetzen enthalten, während entsprechende strafprozessuale Regelungen erst in jüngster Zeit eingeführt wurden[173]). Auch die verfahrensrechtlichen Vorgaben weichen teilweise ab, etwa hinsichtlich der vorherigen oder nachträglichen Information der Adressaten des staatlichen Handelns und mitbetroffener Dritter. Schließlich bestehen Unterschiede bei den institutionellen Rahmenbedingungen (vor allem hinsichtlich der Verfahrensherrschaft von Polizei oder Staatsanwaltschaft).

Aufgrund der regelmäßig problematischen Abgrenzung wäre eine Vereinheitlichung der Eingriffsbefugnisse für unterschiedliche Aufgabenbereiche zu prüfen. Solange entsprechende Unterschiede bestehen, stellt sich verfassungsrechtlich außerdem die komplexe Frage der Zweckbindung bzw. der Anforderungen an eine zulässige Zweckänderung bei der Verarbeitung von Informationen.

6.2.2 Einfachgesetzliche Zulässigkeit der Erhebung öffentlich zugänglicher Daten

Auch auf einfachgesetzlicher Ebene, also im Polizei- und Strafprozessrecht, wirft die Zulässigkeit der Erhebung und Verwendung öffentlich zugänglicher Daten Rechtsfragen auf. Geht man beispielsweise davon aus, dass die staatliche Erhebung öffentlich zugänglicher Inhalte im Internet in Grundrechte eingreift (also

172 Beispielsweise erklärte das Bundesverfassungsgericht (BVerfG, Beschluss vom 18. Dezember 2018, 1 BvR 142/15, Rn. 54 ff.) die Befugnis zum automatisierten Kfz-Kennzeichenabgleich im Bayerischen Polizeirecht in Teilen für verfassungswidrig, insoweit die Maßnahme unmittelbar zum Grenzschutz eingesetzt wird, weil dies gegen die ausschließliche Gesetzgebungskompetenz des Bundes für den Grenzschutz verstößt.

173 Artikel 1 Nr. 29 Gesetz zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften vom 25.6.2021 (BGBl. I, S. 2099)

laut Bundesverfassungsgericht ggf. in Fällen des zielgerichteten Zusammentragens und Auswertens von Informationen, Kap. 6.1.3), müssen diese Maßnahmen Ermächtigungsgrundlagen im jeweiligen Eingriffsrecht finden. So ist davon auszugehen, dass Formen der Internetbeobachtung wie die Social Media Intelligence (Kap. 4.2) in der polizeilichen Praxis künftig an Bedeutung gewinnen werden, da angesichts der zunehmenden Nutzung sozialer Netzwerke immer mehr Bereiche menschlicher Kommunikation für Beobachtungstechnologien offen liegen. Dabei verhalten sich polizeiliche Beobachter oftmals wie private Internetnutzer auch, sodass man ihren Aktionen häufig nicht ansieht, dass sie zu staatlichen Zwecken erfolgen. Das daraus entstehende Informations- und Transparenzungleichgewicht kann nicht ohne Auswirkungen auf die Anwendung der bestehenden, oftmals generalklauselartigen Ermächtigungsgrundlagen (z. B. §§ 161 u. 163 StPO, § 14 BPolG) bleiben, auf die »Onlinestreifen« derzeit gestützt werden. Werden die so erhobenen Informationen zum Gegenstand komplexer Analyseverfahren, wirft dies weitere rechtliche Fragen auf, die im nachfolgenden Kapitel umrissen werden.

6.2.3 Verfahren der automatisierten Datenauswertung

Die in den vergangenen Jahren erzielten substanziellen Fortschritte bei Verfahren der automatisierten Datenauswertung insbesondere auch durch Methoden des maschinellen Lernens (Kap. 3.3) eröffnen einerseits neue Möglichkeiten der Datenauswertung für polizeiliche Zwecke, werfen andererseits aber auch neue grund- und eingriffsrechtliche Fragen auf.

So ist der Bereich der nachgelagerten Datenauswertung bislang eine Art blinder Fleck des Eingriffsrechts: Während sowohl die Polizeigesetze als auch die Strafprozessordnung zahlreiche und detaillierte Regelungen zur Erhebung und Speicherung von Informationen enthalten, stellen beide Teile des Eingriffsrechts nur wenige Regelungen bezüglich der Auswertung der erhobenen Informationen bereit. Problematisch wird dies insbesondere, wenn durch den Einsatz von Verfahren der automatisierten Datenauswertung der durch die Datenerhebung gegebene Grundrechtseingriff erheblich intensiviert wird, wodurch ggf. zusätzliche eigenständige grundrechtliche Risiken geschaffen werden. In solchen Fällen kann die nachträgliche Auswertung des erhobenen Materials nicht mehr nur als logische Folge der Datenerhebung betrachtet werden, die ohne Weiteres auf die gesetzliche Ermächtigung zu dieser Erhebung gestützt werden könnte.

So ist beispielsweise unbestritten, dass Bildaufnahmen, die etwa im Rahmen der Strafverfolgung unter bestimmten Voraussetzungen nach § 100h Abs. 1 Satz 1 Nr. 1 StPO hergestellt werden dürfen, dann auch betrachtet, intern weiterverarbeitet und als Beweismittel genutzt werden dürfen. Unklar ist hingegen, ob diese Befugnis zur Datenerhebung auch den Einsatz komplexer Analyseverfahren, beispielsweise von Verfahren zur automatisierten Gesichtserkennung,

umfasst (Kap. 3.5.5.1). Ein weiteres Beispiel ist die Erhebung von Verkehrsdaten der Telekommunikation nach § 100g Abs. 1 StPO: Die Maßnahme kann das Ziel haben, einmalig den Aufenthaltsort einer Person festzustellen, es können mit Analyseverfahren aus Verkehrsdaten jedoch auch Bewegungs- und Verhaltensprofile oder soziale Beziehungsnetze über längere Zeiträume umfassend beobachtet werden. Das geltende Recht bindet beide Formen der Auswertung an dieselben Eingriffsschwellen zur Erhebung von Verkehrsdaten.

Nach den verfassungsrechtlichen Maßstäben des Gesetzesvorbehalts und der Normenklarheit stellt sich die Frage, ob (bzw. unter welchen Voraussetzungen) es spezieller Ermächtigungsgrundlagen für die nachträgliche Auswertung der erhobenen Daten bedarf. Wird dies grundsätzlich bejaht, müsste eine solche Datenauswertung (in Abhängigkeit vom Erhebungszweck) tatbestandlich in sinnvollem Ausmaß ermöglicht und zugleich angemessen begrenzt werden. Wichtig wäre eine differenziertere Regulierung, die für unterschiedliche Auswertungsformen der erhobenen Daten jeweils spezifische Eingriffsschwellen vorsähe, da eine pauschale Bemessung der Eingriffsschwellen für eine Datenerhebung am Gewicht eines gedachten maximal eingriffsintensiven Auswertungsvorgangs die Leistungsfähigkeit der Gefahrenabwehr und Strafverfolgung mindern könnte (ein Beispiel für einen solchen Ansatz wird in Kapitel 6.3.2 vorgestellt). Da automatisierte Verfahren zur Datenauswertung nicht fehlerfrei arbeiten, wäre insbesondere auch ein rechtsverträglicher Umgang mit Fehlalarmen (Kap. 3.5.2.2) zu entwickeln.

Es bedarf daher einer Untersuchung der grundrechtlichen und sonstigen verfassungsrechtlichen Anforderungen an den Einsatz von Verfahren der automatisierten Datenauswertung für polizeiliche Zwecke wie auch einer Erörterung der eingriffsrechtlichen Regelungsoptionen. Die Diskussion hierzu steht allerdings noch am Anfang.

6.2.4 Regulierung der Kooperation zwischen Polizeibehörden und privaten Akteuren

Im Sicherheitsbereich hat sich seit Längerem eine Vielzahl an formellen und informellen Kooperationsformen herausgebildet, in denen die Sicherheitsbehörden mit privaten Sicherheitsakteuren zusammenarbeiten (Kap. 2.4.3). Hieraus resultieren verfassungs-, sicherheits- und datenschutzrechtliche Probleme. Fraglich ist, ob zumindest weitreichende und institutionalisierte Kooperationsformen, die auch Elemente der Inpflichtnahme privater Akteure umfassen (Kap. 6.1.7), nicht als solche schon regulierungsbedürftig sind, weil sie zu besonderen Grundrechtsgefährdungen für die betroffenen privaten Akteure führen können (z. B. in Bezug auf die Berufsfreiheit, die unternehmerische Freiheit oder das Eigentum). Bei weitgehend freiwilligen Kooperationsarrangements stellt sich häufig das Problem der Letztverantwortlichkeit. So könnte der Wissensvorsprung der Betreiber in

privaten Großanlagen (z. B. in Fußballstadien) so weit gehen, dass die Sicherheitsbehörden als ausführende Stellen der privaten Betreiber erscheinen – umgekehrt könnten letztere ihre Ressourcen den Behörden im Extremfall zur selbstständigen Verplanung und Nutzung bereitstellen und dann gewissermaßen zu Werkzeugen des Staates werden. Hier könnten durch die Zuweisung klarer rechtlicher Verantwortlichkeiten alle an der Kooperation beteiligten Akteure an Handlungssicherheit gewinnen.

Weitere Besonderheiten werden durch Formen der Kooperation aufgeworfen, die in starkem Maße auf den Einsatz von Beobachtungstechnologien abstellen. Dies betrifft nicht nur den Austausch personenbezogener Daten, sondern insbesondere die Befugnisse zur Datenauswertung und die Frage der Letztentscheidung über den Inhalt der gewonnenen Informationen. Es ist sicherzustellen, dass die in umfassenden Kooperationsbeziehungen bereitgestellten Daten hinreichend verlässlich sind (in Bezug auf die Integrität, Authentizität und Verfügbarkeit). Bei der Bewertung können private Sicherheitsakteure einerseits über mehr bereichsspezifisches Vorwissen als die Polizei verfügen und deshalb etwa die Gefährlichkeit einer Person besser einschätzen (z. B. im Kontext gewaltbereiter Fußballfans). Andererseits dürfen staatliche Stellen derartige Bewertungen nicht ungeprüft übernehmen, weil die privaten Akteure ggf. Partikularinteressen verfolgen und die Übernahme so gewonnener Erkenntnisse in staatliche Datenbestände erhebliche Grundrechtseingriffe für die Betroffenen Personen nach sich ziehen kann (z. B. wenn eine Gefahrenbewertung durch private Akteure eine Übernahme in eine Gewalttäterdatei zur Folge hätte).

6.2.5 Regulierung des behördlichen Zugriffs auf private Datenbestände

Indem die Digitalisierung mittlerweile sämtliche Lebensbereiche durchdringt, verfügen private Betreiber solcher Dienste und Lösungen über umfassende Datenbestände, die nicht nur für ihre eigenen kommerziellen Zwecke, sondern auch für Sicherheitsbehörden von erheblichem Interesse sein können. Die Regulierung des behördlichen Zugriffs auf solche privaten Datenbestände ist derzeit in den Polizeigesetzen und der Strafprozessordnung jedoch nur fragmentarisch geregelt. Bestimmungen finden sich nach geltendem Recht entweder für bestimmte Sonderfälle – insbesondere für Telekommunikationsdaten (Kap. 5.3) – oder nur in sehr allgemeiner Form. So erfolgt der Zugriff in der Praxis häufig auf der Grundlage von Generalklauseln (z. B. §§ 161, 163 StPO) oder von allgemeinen Befugnissen zur Sicherstellung bzw. Beschlagnahme (z. B. §§ 94 ff. StPO).

Behördliche Zugriffe auf private Daten auf der Grundlage allgemeiner Befugnisse – also ohne explizite gesetzliche Regelung – können jedoch dann rechtsstaatlich bedenklich werden, wenn davon komplexe Bestände mit sensiblen Daten betroffen sind. Dies gilt umso mehr, wenn durch die Erhebung und Ver-

knüpfung von Daten aus unterschiedlichen Datenbeständen zusätzliche Gefahren für die Persönlichkeitsrechte betroffener Personen entstehen. Explizit geregelt ist dies für den praktisch nicht sonderlich relevanten Fall der Rasterfahndung (z. B. §§ 98a f. StPO). Bislang fehlt es aber an konsensfähigen Kriterien für eine grundrechtsschonende Ausgestaltung des behördlichen Zugriffs auf private Datenbestände.

6.3 Datenschutzrecht

Das Datenschutzrecht konkretisiert den grund- und menschenrechtlichen Schutz der informationellen Selbstbestimmung. Es enthält ein inzwischen relativ stabiles Set von Regelungsprinzipien, denen die staatliche Datenverarbeitung genügen muss, um rechtmäßig zu sein: Nach dem Verbotsprinzip bedarf jede Verarbeitung von personenbezogenen Daten einer Einwilligung des Betroffenen oder einer gesetzlichen Grundlage. Daten dürfen nur zu hinreichend bestimmten Zwecken verwendet werden; Zweckänderungen sind legitimationsbedürftig. Die Datenverarbeitung ist strikt auf die zum jeweiligen Zweck erforderlichen Daten begrenzt und muss für die Betroffenen transparent sein. Vorgaben für den technischen und organisatorischen Rahmen von Datenverarbeitungsprozessen werden errichtet, damit diese Prozesse von vornherein möglichst datenschutzverträglich gestaltet werden. Die Betroffenen haben eine feste Gruppe spezifischer Rechte (etwa auf Auskunft und, wenn die Datenverarbeitung rechtswidrig ist, auf Löschung). Schließlich bedarf es einer Kontrolle durch unabhängige Datenschutzbehörden.

Der seit Mai 2018 geltende Rechtsrahmen des Unionsrechts setzt EU-weit einheitliche Mindestanforderungen für die staatliche Verarbeitung von personenbezogenen Daten im Allgemeinen (durch die Europäische Datenschutzgrundverordnung) und für Zwecke der polizeilichen Gefahrenabwehr und Strafverfolgung im Besonderen (durch die Richtlinie [EU] 2016/680). Das neue europäische Datenschutzregime löste für die Gesetzgeber des Bundes und der Länder einen umfassenden Anpassungsbedarf im nationalen Recht aus. Der Prozess der Anpassung ist teilweise bereits abgeschlossen (auf Bundesebene z. B. durch das neue BDSG oder das neue BKAG), teilweise aber auch noch im Gange (z. B. für die Strafprozessordnung, Stand Oktober 2019).

Im Rahmen der Umsetzung wurde der Datenschutz beispielsweise beim Bundeskriminalamt deutlich ausgebaut: Neben notwendigen Anpassungen in Bezug auf die datenschutzrechtlichen Begrifflichkeiten und Kategorisierungen von Betroffenen und Daten, wurden u. a. die Kontrollmöglichkeiten des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit gestärkt sowie Protokollierungsvorschriften zum Zweck der Datenschutzkontrolle eingeführt bzw. ausgebaut. Außerdem muss das Bundeskriminalamt durch technische und organisatorische Vorkehrungen sicherstellen, dass die Datenschutzgrund-

sätze und die Anforderungen an die Datensicherheit beachtet werden. Schließlich wurden die Rolle des behördlichen Beauftragten für den Datenschutz des Bundeskriminalamtes und die Rechte der Betroffenen gestärkt.174

Eine vertiefende Analyse der Auswirkungen des neuen Datenschutzrechts auf die in diesem TAB-Bericht dargestellten polizeilichen Beobachtungspraktiken kann in Anbetracht des noch jungen, in Teilen noch nicht konsolidierten Rechtsrahmens, aber auch aufgrund der äußerst komplizierten Rechtsmaterie an dieser Stelle nicht geleistet werden. Im Folgenden soll daher auf zwei grundsätzliche Problemfelder des hergebrachten Datenschutzes eingegangen werden, die ihren Ursprung in den datenschutzrechtlichen Regelungsprinzipen haben und die vor allem auch in Bezug auf künftige Anwendungsszenarien für Beobachtungstechnologien durch Polizeibehörden von Bedeutung sind.

6.3.1 Sachlicher Anwendungsbereich des Datenschutzrechts

Der Begriff des personenbezogenen Datums markiert eine starre Grenze des Datenschutzrechts: Die Verarbeitung personenbezogener Daten unterliegt grundsätzlich vollständig der datenschutzrechtlichen Regulierung, die Verarbeitung nichtpersonenbezogener Daten überhaupt nicht.

Dieser Regelungsansatz kann unter den gegenwärtigen technischen und sozialen Bedingungen Unter- oder Überregulierungen verursachen: Eine Unterregulierung entsteht, wenn Datenverarbeitungen aus dem sachlichen Anwendungsbereich des Datenschutzrechts herausgenommen werden, obwohl sie Risiken für die informationelle Selbstbestimmung der Betroffenen oberhalb einer Erheblichkeitsschwelle begründen und deshalb ein datenschutzspezifisches Schutzbedürfnis besteht. Allerdings ist der Personenbezug von Daten gerade im Zusammenhang mit modernen Beobachtungspraktiken vielfach sehr schwierig zu beurteilen. So ermöglichen es komplexe Datenauswertungsverfahren – ggf. unter Einbezug weiterer Informationsquellen – zunehmend, Daten auf einzelne Personen zu beziehen, die früher als anonym angesehen worden wären. Beispielsweise verarbeiten aktuelle Formen des Predictive Policing nur vermeintlich nichtpersonenbezogene Daten, sodass solche Datenverarbeitungen nach gegenwärtigem Recht weder einer Rechtfertigung durch Einwilligung oder gesetzliche Ermächtigung bedürfen noch irgendwelchen Lösch- oder Auskunftspflichten gegenüber den Betroffenen unterliegen. Es erscheint aber durchaus plausibel, dass in vielen Fällen (ggf. auch zu einem späteren Zeitpunkt) ein Personenbezug mit Hilfe von Analysewerkzeugen und Zusatzinformationen aus öffentlichen und nichtöffentlichen Quellen (z. B. Melde- oder Fahrzeugregister) prinzipiell hergestellt werden könnte. Wird auf solche Daten das Datenschutzrecht erst angewandt, wenn der Personenbezug hergestellt wurde, so können

174 Vergleiche dazu den Gesetzentwurf der CDU/CSU-Fraktion und der SPD-Fraktion (2017, S. 77 f).

bereits irreversible Beeinträchtigungen entstanden sein. Aber auch die Verarbeitung von dauerhaft nichtpersonenbezogenen Daten wirft Fragen auf. Ermöglicht etwa ein internetbasierter Kommunikationsdienst eine Beteiligung unter einem Pseudonym, das weder der Anbieter noch Dritte der dahinterstehenden Person zuordnen können, so liegt eine Einstufung der bei der Nutzung anfallenden Daten als nichtpersonenbezogen zumindest nahe. Gleichwohl kann die Person über ihr Pseudonym z. B. zum Gegenstand einer gezielten polizeilichen Beobachtung in Internet werden und sich dadurch in ihrer Freiheit und Privatheit eingeschränkt fühlen.

Bei einem zu weiten Verständnis von Personenbezug droht allerdings eine Überregulierung. Diese entsteht, wenn Verarbeitungen personenbezogener Daten in den sachlichen Anwendungsbereich des Datenschutzrechts fallen, obwohl sie keine signifikanten Risiken für die informationelle Selbstbestimmung der Betroffenen begründen. Durch Überregulierung könnten Datenverarbeitungen unnötig behindert bzw. einschränkt werden, weil sie dann durchweg einer Einwilligung der Betroffenen oder einer gesetzlichen Grundlage bedürften und die Verantwortlichen zudem die prozeduralen Schutzvorkehrungen des Datenschutzrechts zu beachten hätten, z. B. Informations-, Benachrichtigungs- und Dokumentationspflichten. Dies könnte sich auch nachteilig auf den Einsatz von Beobachtungstechnologien im Bereich der zivilen Sicherheit auswirken. Beispielsweise lassen sich Geodaten mit entsprechendem Zusatzwissen vielfach auf natürliche Personen zurückführen, etwa die Eigentümer bestimmter Grundstücke. Müssten Sicherheitsakteure vor einer Verarbeitung von Geodaten alle potenziell identifizierbaren Personen benachrichtigen oder wären sie durchweg Auskunftsansprüchen solcher Personen ausgesetzt, könnte dies komplexere Verarbeitungen solcher Daten zum Zweck der Sicherheitsgewähr (etwa bei der Analyse der räumlichen Kriminalitätsverteilung in einer Stadt) quasiprohibitiv erschweren. An die Stelle einer angemessenen Regulierung solcher Datenverarbeitungen träte dann ihre faktische Verhinderung durch unpassende und unangemessene rechtliche Vorgaben (Bäcker 2019).

Um das Problem drohender Unter- und Überregulierungen abzuwenden, wird in jüngerer Zeit vermehrt diskutiert, ob der gegenwärtige Grundansatz des Datenschutzrechts (Verbotsprinzip) durch einen neuen Ansatz ersetzt werden sollte, der von den Risiken einer Datenverarbeitung ausgeht. Diese Position hat durch den neuen europäischen Rechtsrahmen einen gewissen Auftrieb erhalten, der zwar das hergebrachte Verbotsprinzip beibehält, jedoch bestimmte Schutzvorkehrungen nur für riskantere Datenverarbeitungen fordert. Eine systematische Untersuchung zu dieser Frage steht allerdings bislang noch aus.

6.3.2 Datenschutzgerechte Gestaltung von Beobachtungstechnologien

Das neue europäische Datenschutzrecht errichtet ausdrückliche Pflichten zum Datenschutz durch Technikgestaltung (Privacy by Design) und durch datenschutzfreundliche Voreinstellungen (Privacy by Default) – sowohl für die Verarbeitung personenbezogener Daten im Allgemeinen (Artikel 25 Datenschutz-Grundverordnung) als auch speziell zu Zwecken der Gefahrenabwehr und Strafverfolgung (Artikel 20 Richtlinie [EU] 2016/680). In der Folge hat sich beispielsweise die Datenverarbeitung für polizeiliche Zwecke »an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu verarbeiten. Personenbezogene Daten sind zum frühestmöglichen Zeitpunkt zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verarbeitungszweck möglich ist« (§ 71 BDSG).

Auf der einen Seite können Pflichten für eine datenschutzgerechte Technikgestaltung bei der Anwendung von Beobachtungstechnologien dazu beitragen, die Intensität des Eingriffs in das Recht auf informationelle Selbstbestimmung zumindest in bestimmten Einsatzkontexten abzumildern. So existieren beispielweise für die Videobeobachtung verschiedene technische und organisatorische Ansätze für eine datenschutzgerechte Gestaltung (Kees 2015, S. 77 ff.): Der beobachtete Bereich kann eingeschränkt werden (z. B. durch physische Blenden, durch Unterbinden von Schwenk- oder Zoomfunktionen in vorher festgelegten Bereichen), personenbezogene Daten im Bildmaterial können softwarebasiert unkenntlich gemacht werden (z. B. Gesichter oder menschliche Körper durch Verpixelung) oder durch Zugriffsbeschränkungen kann das Risiko des Datenmissbrauchs reduziert werden.

Auf der anderen Seite allerdings steht die mit solchen Pflichten verbundene Informationsreduktion in vielen Fällen in Konflikt mit dem eigentlichen Beobachtungsziel. Zum Beispiel würde der Nutzen der Videobeobachtung im öffentlich zugänglichen Raum für die Strafverfolgung durch die Unkenntlichmachung von Gesichtern bzw. Körpern stark reduziert werden. Auch ist grundsätzlich fraglich, wie ein Datenschutz durch Technikgestaltung bei solchen Beobachtungstechnologien aussehen könnte, die prinzipiell auf eine möglichst umfassende Datenerhebung abstellen, um daraus mit modernen Methoden der Datenanalyse unbekannte Zusammenhänge zu erkennen (etwa Ansätze des Predictive Policing). Schließlich ist auch zu bedenken, dass sich Verfahren der Datenverarbeitung ständig weiterentwickeln, sodass die eingesetzten datenschutzfördernden Techniken permanent auf ihre Wirksamkeit hin überprüft werden müssen. So könnten künftig Personen in Videoaufnahmen ggf. nicht mehr nur über einen Gesichtsabgleich, sondern auch anhand ihres Ganges oder von Farbkombinationen ihrer Kleidung identifiziert werden (Kees 2015, S. 116). Der jewei-

lige Stand der Technik ist von ähnlich großer Bedeutung wie beim Einsatz von Verschlüsselungstechnik.

Insbesondere vor dem Hintergrund neuer Beobachtungsmöglichkeiten mithilfe komplexer Datenverarbeitung können die vorhandenen, allgemein formulierten Pflichten eine datenschutzgerechte Technikgestaltung kaum wirksam anleiten bzw. bedürfen einer – ggf. spezifisch auf bestimmte Beobachtungsverfahren bezogenen – Konkretisierung, um operabel zu werden. Es sind unterschiedliche Modelle denkbar, die bessere Orientierung bieten könnten. Rossnagel et al. (2011) etwa schlagen für die automatisierte Videobeobachtung mit Verhaltensanalyse und Personenerkennung in Echtzeit (Kap. 3.3.4 u. 3.5) einen stärker nach Eingriffsstufen differenzierten Ansatz vor. Im 3-Stufen-Modell wird der Eingriff in das Grundrecht auf informationelle Selbstbestimmung abhängig vom Grad der Feststellung einer Gefahr auf jeder Stufe so gering wie möglich gehalten (Roßnagel et al. 2011, S. 695 ff.):

- *Stufe 1 »Allgemein beobachtende Überwachung«*: Es findet eine allgemeine Beobachtung aller Personen statt mit dem Ziel, möglichst frühzeitig auffällige Situationen zu erkennen. Dazu ist es nicht notwendig, die aufgenommenen Personen individualisiert oder identifiziert darzustellen. Auf einem Monitor können die aufgenommenen Personen und ihre Bewegungen stilisiert dargestellt werden, etwa in Form von Strichmännchen. Aufnahmen, auf denen kein auffälliges Verhalten erkannt wurde, werden umgehend gelöscht.
- *Stufe 2 »Gezielte Personenüberwachung«*: Der Übergang in die zweite Stufe erfolgt entweder automatisch (Software erkennt auffällige Situation) oder manuell (Videobeobachter erkennt auffällige Situation). Personen, deren Verhalten auffällig ist, werden gezielt auf ihrem weiteren Weg beobachtet. Die Aufnahmen werden aufgezeichnet, um ggf. nachträglich das Entstehen der Gefahr oder Straftat nachverfolgen zu können. Allerdings soll das Kamerasystem Aufnahmen des Gesichts oder anderer biometrischer Merkmale vermieden, wodurch noch keine Daten für eine mögliche Identifikation erfasst werden. Die Aufnahmen werden unmittelbar nach der Feststellung durch den Beobachter, dass weder eine Gefahr entstanden ist noch eine Straftat begangen wurde, gelöscht.
- *Stufe 3 »Personenerkennung«*: Der Übergang in die dritte Stufe erfolgt entweder automatisch (Software erkennt gefährliche Situation) oder manuell (Videobeobachter erkennt gefährliche Situation). In der Regel ist das Einschreiten von Sicherheitskräften erforderlich. Die dritte Stufe dient der weiteren Beobachtung (z. B. durch die Einsatzleitung), vor allem aber der Beweissicherung. Zu diesem Zweck werden die Bilder einschließlich biometrischer Merkmale der verdächtigen Person in hoher Qualität angezeigt und gespeichert. Eine Identifizierung (z. B. durch Abgleich mit einer Fahndungsdatenbank) erfolgt aber nicht automatisch, sondern nur durch eine sich an die Beobachtung anschließende ausdrückliche Entscheidung eines veran-

twortlichen Experten. Ob die Identifizierung zulässig ist, richtet sich nach den jeweiligen Eingriffsermächtigungen im Polizei- oder im Strafprozessrecht. Die Videoaufnahmen werden solange aufbewahrt, bis die Gefahrenabwehr oder die Strafverfolgung abgeschlossen sind, oder sich herausstellt, dass weder eine Gefahr vorlag noch eine Straftat verübt wurde.

Ob und inwieweit sich dieses Modell allerdings auf andere Beobachtungstechnologien übertragen lässt und welcher Modifikationen es dafür ggf. bedarf, bleibt zu diskutieren.

7 Gesellschaftliche Auswirkungen technisierter Beobachtung

Der Einsatz von Beobachtungstechnologien im Bereich der zivilen Sicherheit ist immer mit gesellschaftlichen Auswirkungen verbunden. Dazu gehören die intendierten Wirkungen der jeweiligen Beobachtungspraktiken – bei der offenen Videobeobachtung im öffentlich zugänglichen Raum beispielsweise verhaltensbeeinflussende Wirkungen im Hinblick auf eine Abschreckung von potenziellen Straftäter/innen und eine Steigerung des Sicherheitsempfindens der Bürger/innen (Kap. 3.4.4) –, aber auch potenzielle unerwünschte Wirkungen. Im Fokus öffentlicher und politischer Debatten stehen insbesondere mögliche Einschüchterungseffekte im Kontext von breit streuenden Beobachtungstechnologien, deren Einsatz typischerweise eine Vielzahl von Personen betrifft, die selbst keinen Anlass für die Beobachtung gegeben haben. Der diesbezügliche empirische Wissensstand ist, wie im nachfolgenden Kapitel 7.1 gezeigt wird, allerdings noch unbefriedigend.

Der Einsatz von Beobachtungstechnologien hat aber nicht nur Auswirkungen auf die beobachteten Personen, sondern ebenfalls auf die sie benutzenden Sicherheitsakteure. Auch hier gilt, dass den erwünschten Wirkungen (z. B. Unterstützung der Sicherheitsarbeit, Erhöhung der Ressourceneffizienz) unerwünschte bzw. unerwartete Effekte gegenüberstehen können, die den eigentlich intendierten Sicherheitsgewinn unter Umständen auch wieder schmälern. Mögliche Auswirkungen auf die Anwender von Beobachtungstechnologien spielen im öffentlichen und politischen Diskurs bislang nur eine untergeordnete Rolle. Sie sind Thema in Kapitel 7.2.

In den Debatten um den Einsatz von Beobachtungstechnologien durch Polizeibehörden zu Zwecken der Gefahrenabwehr und Strafverfolgung bildet schließlich das Spannungsverhältnis zwischen den Werten der Sicherheit und der Freiheit eine herausragende Rolle. Es ist eine schwierige Aufgabe, diese beiden Werte miteinander in Einklang zu bringen. Einige der zentralen Fragestellungen und Herausforderungen, die sich in diesem Zusammenhang stellen, werden in Kapitel 7.3 diskutiert.

7.1 Psychische Wirkungen technisierter Beobachtung

Intuitiv erscheint es naheliegend, dass das Wissen, beobachtet zu werden, sich auf die Psyche und das Verhalten der beobachteten Personen auswirkt. So richtet sich das eigene Verhalten und Handeln in den meisten sozialen Situationen an den Erwartungen aus, welche andere an einen herantragen. Fühlt ein Mensch sich unbeobachtet, wiegt er sich in der Annahme, dass niemand weiß, wie er sich

verhält. Dies setzt Handlungsmöglichkeiten frei, denen unter Beobachtung ggf. nicht mehr nachgegangen werden kann, ohne gewisse Sanktionen, Verletzungen oder Schamgefühle befürchten zu müssen (IZEW 2017, S. 78). Allerdings erweist sich der wissenschaftliche Nachweis dieser Annahme als schwierig, da das Phänomen der Beobachtung gerade im gesamtgesellschaftlichen Kontext sehr komplex ist (dazu und zum Folgenden IZEW 2017, S. 28 ff.): Beobachtung ist nicht lediglich ein unabhängiger Faktor, der einen bestimmten direkten psychischen Effekt bei den Beobachteten hervorruft. Stattdessen spielen auch die Einstellung der Beobachteten zu der beobachtenden Instanz sowie die mit der Beobachtung verfolgten Ziele eine entscheidende Rolle. Dies trifft insbesondere auch auf den Anwendungskontext der zivilen Sicherheit zu, wo der Einsatz von Beobachtungstechnologien häufig in einen Diskurs eingebettet ist, dessen zentrale Frage lautet, inwieweit der Staat als Garant von Sicherheit auftreten soll und kann. Es sind also immer die Voraussetzungen und Bedingungen der Beobachtung zu berücksichtigen, was die Ergründung der psychischen Effekte von Beobachtung umso schwieriger macht.

Zusätzliche methodische Herausforderungen stellen sich bei Formen der Beobachtung, die subtil oder heimlich erfolgen. Bei der Videobeobachtung im öffentlich zugänglichen Raum beispielsweise markieren Kameras oder Hinweisschilder zwar die Beobachtung, gleichwohl ist nicht nachvollziehbar, ob die Bilder durch einen Menschen zeitgleich ausgewertet, lediglich gespeichert oder gar nicht aufgezeichnet (Kameraattrappe) werden. Andere Formen der Beobachtung, vor allem solche der Internet- oder informationstechnischen Beobachtung, finden häufig ohne Wissen der Beobachteten statt. Ob und wann jemand beobachtet wird, kann kaum überprüft werden – im Bewusstsein bleibt einzig die Möglichkeit, dass man beobachtet werden *könnte* (IZEW 2017, S. 28).

Dies veranlasste etwa Lüdemann und Schlepper (2011, S. 125 f.) zu der Hypothese, dass technisierte Beobachtungspraktiken einen generellen Kontrollverlust bei den Bürger/innen zur Folge haben, der nicht in Protest, sondern in Apathie kulminiert. Diese Vermutung ließ sich jedoch im Rahmen einer Telefonerhebung (repräsentative Stichprobe von 2.176 Personen aus dem gesamten Bundesgebiet) nicht untermauern, stattdessen zeigte sich, dass Akzeptanz oder Ablehnung von Beobachtung davon abhing, welche subjektiven Kosten und welchen Nutzen sich die Befragten davon versprachen. Eine vergleichbare Untersuchung von Turow et al. (2015) in den USA (Telefonerhebung mit repräsentativer Stichprobe, n = 1.506) ließ hingegen den Schluss zu, dass die Nutzer/innen von digitalen Diensten in Bezug auf den Schutz ihrer Daten vor fremder Kenntnisnahme vielmehr resigniert hatten: Die Weiternutzung der Dienste erfolgte nur, weil Widerstand zwecklos und unpraktisch erschien.

Nicht nur solche widersprüchlichen Forschungsergebnisse machen eine Bewertung möglicher psychischer und sozialer Effekte von (staatlicher) Beobachtung schwierig, sondern auch der Umstand, dass es diesbezüglich vor allem im

Kontext der Internet- und informationstechnischen Beobachtung bislang nur wenige systematische Untersuchungen gibt. Das mögliche Ausmaß des staatlichen Einsatzes solcher Beobachtungstechnologien drang einer breiten Öffentlichkeit vor allem durch die Aufdeckung der Aktivitäten einiger Nachrichtendienste der USA und weiterer Staaten durch Edward Snowden im Sommer 2013 ins Bewusstsein. In der Folge hat sich das wissenschaftliche Interesse am Thema zwar stark erhöht, der bisher erreichte Forschungsstand ist aber immer noch unzureichend und in Teilen eben auch uneindeutig.

Vor diesem Hintergrund stellt dieses Kapitel den Stand der Forschung zu möglichen psychischen und sozialen Auswirkungen technisierter Beobachtung dar. In Kapitel 7.1.1 werden zunächst einige einschlägige Studien diskutiert, die sich unabhängig vom speziellen Anwendungskontext der zivilen Sicherheit mit möglichen unbewussten Effekten technisierter Beobachtung auf den Menschen beschäftigt haben. Vorbehaltlich des noch lückenhaften Forschungsstandes deuten die hier vorliegenden Forschungsergebnisse auf mögliche Auswirkungen technisierter Beobachtung auf die menschliche Psyche und individuelle Verhaltensweisen hin, die gerade auch im Hinblick auf den Einsatz von Beobachtungstechnologien im Rahmen der zivilen Sicherheit bedeutsam sein könnten. Daran anknüpfend werden anhand exemplarischer Studien die jeweiligen Wissensstände zu möglichen psychischen und sozialen Auswirkungen der Videobeobachtung (Kap. 7.1.2) sowie der Internet- und informationstechnische Beobachtung (Kap. 7.1.3) vorgestellt.

Die Auswahl und Auswertung der vorgestellten Studien erfolgte durch die Autor/innen des Gutachtens des Internationalen Zentrums für Ethik in den Wissenschaften (IZEW 2017, S. 28 ff.), auf dem die folgenden Ausführungen in wesentlichen Teilen fußen. Kriterien für die Auswahl der Studien waren u. a. die wissenschaftliche Validität, die exemplarische Aussagekraft für das Verständnis möglicher psychischer Effekte von Beobachtung sowie die Bedeutung einzelner Studien für die wissenschaftliche und öffentliche Diskussion. Bei letzteren Studien korrespondieren Bedeutung für den Diskurs und wissenschaftliche Validität nicht immer – das allgemeine Interesse an den Untersuchungen ist jedoch ein indirekter Hinweis darauf, dass noch keine anderen belastbareren Umfrage- und Forschungsergebnisse vorlagen.

7.1.1 Unbewusste psychologische Effekte von Beobachtung

Evolutionstheoretische und psychologische Theorien sowie (spieltheoretische) Versuche legen nahe, dass Menschen kooperativer, sozialer und großzügiger handeln, wenn andere Menschen ihr Handeln beobachten und bewerten können. Dies wird u. a. darauf zurückgeführt, dass sie mit direkten Folgen für ihren Ruf und ihr Ansehen innerhalb einer Gesellschaft oder Gruppe rechnen (Sparks/Barclay 2013, S. 317). Seit Ende der 1980er Jahre befasst sich die psychologische

Forschung mit der Frage, ob dieser Effekt auch *unbewusst* auftritt, also insbesondere in Situationen, in denen die Beobachtung nicht durch direkte zwischenmenschliche Interaktion gekennzeichnet ist, sondern lediglich durch Symbole markiert wird. Diese Frage ist auch für den Anwendungskontext der zivilen Sicherheit von Bedeutung: Fördern bereits subtile Hinweise auf Beobachtung durch unbewusste Reaktionen kooperatives oder prosoziales Verhalten, so wäre dies ein wichtiger sozialpsychologischer Erklärungsansatz für eine mögliche kriminalpräventive Wirkung von offenen Beobachtungsmaßnahmen wie beispielsweise die Videobeobachtung im öffentlich zugänglichen Raum (selbst wenn es sich hierbei nur um Kameraattrappen handelte).

Eine in diesem Zusammenhang häufig rezipierte und über Fachkreise hinaus bekannte Studie ist die von Bateson et al. (2006), in deren Rahmen der Effekt von über einer freiwilligen Kaffeekasse aufgehängten Bildern von Augenpaaren auf die Zahlungsmoral der Kaffeetrinker untersucht wurde (Methode: 10-wöchiges Experiment mit 48 Mitarbeiter/innen eines Psychologieinstituts, die darüber nicht informiert wurden). Als Ergebnis wurde festgestellt, dass in Wochen, in denen Augenbilder aufgehängt waren, im Schnitt über 2,7-mal mehr Kaffeegeld bezahlt wurde als in Wochen, in denen Blumenbilder an der Wand hangen. Die Studienautor/innen erklärten dies damit, dass (bereits) Bilder von Augenpaaren das Gefühl hervorrufen könnten, beobachtet zu werden, was die Teilnehmer/innen aus dem Bedürfnis heraus, von anderen als sozial eingestellt wahrgenommen zu werden, zu kooperativem Verhalten motiviert habe. Abstrakter könnte dies auch so interpretiert werden, dass Personen sich einer (vorgestellten) sozialen Norm anpassen, wenn sie sich beobachtet fühlen. Allerdings sind diese Ergebnisse weder verallgemeinerbar noch repräsentativ, da die Studie diverse methodische Mängel aufweist (u. a. kleine Stichprobe, kurze Versuchsdauer, unzureichende Kontrolle anderer Einflussfaktoren).

Seitdem durchgeführte, methodisch ausgereiftere Studie zeichnen ein uneinheitliches Bild: Sparks und Barclay (2013) kamen beispielsweise bei einem ähnlichen Versuch zu dem Ergebnis, dass Personen sich dann großzügiger gegenüber Fremden zeigten, wenn sie impulshaften Augenabbildungen ausgesetzt waren (Methode: computerbasierter Versuch mit 188 Teilnehmer/innen, die im Rahmen eines Diktatorspiels Geldbeträge untereinander zuteilten). Dass es zwischen den Teilnehmer/innen, denen entweder gar keine oder dauerhaft Bilder von Augenpaaren gezeigt wurden, keinen Unterschied gab, erklärten die Studienautoren damit, dass Menschen mit der Zeit lernen, solche künstlichen Hinweise auf Beobachtung zu ignorieren. Auf den Anwendungskontext der zivilen Sicherheit übertragen würde dies bedeuten, dass die präventive Wirkung von offenen Beobachtungsmaßnahmen durch Gewöhnungseffekte mit der Zeit wieder abnehmen könnte.

Demgegenüber konnten Northover et al. (2017) im Rahmen einer Metaanalyse von insgesamt 27 solcher Augenexperimente (Gesamtzahl der Teilnehmer/

innen: 19.512) keine statistisch signifikanten Effekte einer vermeintlichen Beobachtung auf die Großzügigkeit der Betroffenen feststellen und zwar sowohl an der Höhe gespendeter Geldbeträge gemessen als auch in Bezug auf die Wahrscheinlichkeit, dass Personen sich unter gefühlter Beobachtung großzügiger zeigen. Allerdings sind auch dieser Metastudie methodische Mängel vorzuwerfen. So wurden die Ergebnisse der berücksichtigten Studien zusammengefasst und vereinfacht, wodurch unter Umständen solche kontext- und studienspezifischen Faktoren verdeckt wurden, die Vorbedingungen für den Nachweis entsprechender Effekte sind.

Der Wissensstand zur Frage, ob unbewusst wahrgenommene Symbole der Beobachtung kooperatives und prosoziales Verhalten fördern können, ist somit noch nicht gefestigt. Auch ist nicht klar, ob die Ergebnisse bisheriger, vornehmlich als computer- oder rollenspielbasierte Experimente durchgeführte Studien ohne Weiteres auf den Anwendungskontext der zivilen Sicherheit übertragbar sind. Hierzu ist weitere Forschung notwendig, die insbesondere auch hier vorherrschende Bedingungen (z. B. Anonymität im öffentlichen Raum) und Zwecke der Beobachtung (z. B. Verhütung und Verfolgung von Straftaten) adäquat berücksichtigt.

7.1.2 Psychische Auswirkungen von Videobeobachtung

Die möglichen psychischen Auswirkungen von Videobeobachtung sind im Vergleich zu anderen Formen technisierter Beobachtung im zivilen Sicherheitsbereich verhältnismäßig gut erforscht. Die Wirkung der Videobeobachtung im öffentlich zugänglichen Raum auf das Sicherheitsempfinden der beobachteten Personen wurde bereits in Kapitel 3.4.4.3 diskutiert, wobei der bisheriger Erkenntnisstand zeigt, dass dieser positive Effekt nicht überschätzt werden sollte.

Weitere psychische Auswirkungen von – auch automatisierter – Videobeobachtung sind Gegenstand aktueller Forschung. Dafür exemplarisch wird im Folgenden das Forschungsprojekt »Mustererkennung und Video Tracking: sozialpsychologische, soziologische, ethische und rechtswissenschaftliche Analysen« (MuViT, Laufzeit 2010 bis 2013) vorgestellt (Ammicht Quinn et al. 2015), das mehrere technische Forschungsprojekte zu Mustererkennungstechniken im Rahmen der zivilen Sicherheitsforschung des Bundes interdisziplinär begleitete (dazu und zum Folgenden IZEW 2017, S. 41 ff.).

Im Rahmen des Forschungsprojektes wurden experimentelle Untersuchungen unter Laborbedingungen durchgeführt, die überprüfen sollten, welche Auswirkungen (vermeintliche) automatisierte Videobeobachtung auf das Erleben und Verhalten von Personen hat. Dazu hatten 190 Probanden am Computer bestimmte Aufgaben zu lösen, während sie teils offenkundig videobeobachtet wurden. Darüber hinaus wurden einige besonders stark auf die Beobachtung aufmerksam gemacht, z. B. durch Hinweisschilder und auffällige Kamerabewegungen. Auch die

Dauer der Beobachtung variierte. Die Probanden wurden daraufhin zu emotionalen Aspekten, dem Bewusstsein der Beobachtung und zur Selbstaufmerksamkeit befragt. Außerdem wurde ihr Verhalten ausgewertet, wobei besondere Aufmerksamkeit auf Verhaltensweisen wie Vermeiden beobachteter Räume, achtloses Wegwerfen von Müll, Betrugsversuche oder gegenseitige Unterstützung und Hilfe gelegt wurde.

Ein festgestellter psychischer Effekt bestand darin, dass die Exposition einer Person gegenüber vermeintlicher Videobeobachtung eine gesteigerte Selbstaufmerksamkeit bewirkte: Personen, die sich beobachtet wähnten, nahmen sich selbst verstärkt wahr, was als unangenehm empfunden werden kann. Zudem führte das Gefühl, Videobeobachtung ausgesetzt zu sein, auf der subjektiven Erlebensebene zu einem gesteigerten Stresslevel. Diese Auswirkung trat bei vermeintlicher intelligenter Videobeobachtung verstärkt auf (Ammicht Quinn et al. 2015, S. 17 u. 19). Dieses gesteigerte Stresslevel resultierte in einer Verhaltensmodifikation, die sich vorrangig dadurch ausdrückte, dass betroffene Personen Orte mit sehr auffälliger Beobachtung mieden. Dieser Effekt zeigte sich besonders bei Probanden, denen erklärt wurde, wie intelligente Videobeobachtung funktioniert (Ammicht Quinn et al. 2015, S. 20).

Die experimentellen Untersuchungen demonstrierten aber auch, dass bestimmte Effekte der Videobeobachtung auf die Psyche möglicherweise überschätzt werden. Dies zeigte sich insbesondere im Hinblick auf den Einschüchterungseffekt, der (staatlichen) Beobachtungspraktiken häufig attestiert wird. Ein solcher Effekt konnte nicht nachgewiesen werden, wenn die Versuchspersonen lediglich das Gefühl hatten, videobeobachtet zu werden. Ein Einschüchterungseffekt trat erst dann auf, wenn zusätzliche Faktoren wie beispielsweise Sanktionsmechanismen hinzukamen, wenn also mögliche Konsequenzen des eigenen Handelns aufgezeigt wurden (Ammicht Quinn et al. 2015, S. 20; Strack/Markel 2013, S. 19). Daneben konnte auch ein recht schneller Gewöhnungseffekt festgestellt werden: Die Verhaltensmodifikation infolge der Videobeobachtung nahm ab, wenn die Probanden dieser über längere Zeit ausgesetzt waren (Ammicht Quinn et al. 2015, S. 20).

Festzuhalten bleibt, dass (automatisierte) Videobeobachtung zwar durchaus gewisse psychische Effekte hat, darunter eine gesteigerte Selbstaufmerksamkeit, ein erhöhtes Stresslevel und eine Verhaltensmodifikation in Form der Vermeidung beobachteter Räume. Ein Einschüchterungseffekt entsteht aber vermutlich nicht isoliert, sondern nur im Zusammenspiel mit anderen Faktoren, insbesondere Sanktionsmechanismen. Entscheidend ist zudem auch die Erwartungshaltung der Betroffenen: Persönliche Annahmen über die Wirkungsweise (automatisierter) Videobeobachtung beeinflussen die eigene Reaktion darauf (Ammicht Quinn et al. 2015, S. 17).

7.1.3 Psychische und soziale Auswirkungen von Internet- und informationstechnischer Beobachtung

In Bezug auf mögliche Auswirkungen einer staatlichen Internet- oder informationstechnischen Beobachtung auf die menschliche Psyche und individuelle Verhaltensweisen liegt es einerseits nahe, zwischen beiden Formen der Beobachtung zu unterscheiden: Die Internetbeobachtung beschränkt sich auf solche Daten, die Personen im Wissen darum, das die Daten durch Dritte einsehbar sind, ins Internet gestellt haben (Kap. 4). Es darf also angenommen werden, dass Internetnutzer bei der Veröffentlichung persönlichkeitssensibler Daten auf Webseiten oder in sozialen Medien auch unabhängig von einer potenziellen staatlichen Kenntnisnahme eine gewisse Vorsicht walten lassen. Demgegenüber richten sich informationstechnische Beobachtungsverfahren auf solche Daten, die Personen in der berechtigten Erwartung einem informationstechnischen System anvertraut haben, dass die Informationen vertraulich bleiben (Kap. 5). Misstrauen die Nutzer solcher Dienste und Systeme dieser Vertraulichkeitsgarantie, scheint die Vermutung gerechtfertigt, dass dies erheblichen Einfluss auch ihre Nutzungsgewohnheiten hat.

Andererseits lässt sich im Hinblick auf die möglichen Erkenntnisgewinne (und damit auch auf mögliche Folgewirkungen für die beobachteten Personen) auch eine gewisse Konvergenz zwischen beiden Beobachtungsformen feststellen: Indem Personen in wachsendem Umfang Informationen über sich und ihr Leben – Identitäten, Beziehungen, persönliche Vorlieben und Ansichten etc. – im Internet veröffentlichen, stehen Sicherheitsakteuren durch die Internetbeobachtung prinzipiell immer mehr personenbezogene Daten von Bürger/innen für ihre jeweiligen Beobachtungsinteressen zur Verfügung. In Kombination mit technischen Hilfsmitteln, die derzeit zur besseren Erfassung, Visualisierung und Auswertung solcher Daten entwickelt werden (Kap. 4.2), werden so individuelle Interessen und Gewohnheiten in neuer, umfassender Weise sichtbar. Auch bei der informationstechnischen Beobachtung beschränken sich die Möglichkeiten längst nicht mehr nur auf die zwischenmenschliche elektronische Kommunikation (Telefongespräche, E-Mails etc.). Die Erfassung und Auswertung von Internetdatenströmen erlauben im Wechselspiel mit der Nutzung des Internets und seiner zahllosen Dienste in sämtlichen Lebensbereichen eine neue Qualität *potenzieller* Beobachtung. Das Spektrum der im Prinzip beobachtbaren Lebensaspekte einer Person reicht hier von persönlichen Interessen und Vorlieben (z. B. durch die Auswertung von besuchten Webseiten oder Suchanfragen im Internet) über Gewohnheiten (z. B. durch Auswertung der Daten von smarten Haushalts- oder Unterhaltungsgeräten) bis hin zu höchstpersönlichen Lebensbereichen wie die Wohnung (z. B. durch Auswertung der Daten von persönlichen Sprachassistenten) oder Gesundheitsdaten (z. B. durch Auswertung der Daten von vernetzten Medizinprodukten). In einer digitalen Gesellschaft existieren folglich mannig-

faltige Quellen für die Beobachtung persönlichkeitssensibler Daten. In Verbindung mit den technischen Möglichkeiten für die Datenauswertung kann daraus eine Informationsfülle entstehen, die dazu geneigt ist, das Leben des Einzelnen in einem zuvor unbekannten Ausmaß abzubilden (Heesen 2012, S. 239).

Zwar lässt sich einwenden, dass solche Formen staatlicher Beobachtung in Deutschland und anderen Rechtsstaaten in der Regel nur unter sehr engen rechtlichen Voraussetzungen und insbesondere unter Beachtung des Grundsatzes der Verhältnismäßigkeit möglich sind. Gerade aber weil solche Maßnahmen typischerweise ohne Wissen der Betroffenen stattfinden, können Nutzer nicht überprüfen, ob (durch wen und zu welchem Zweck auch immer) ihre Internet- oder Kommunikationsaktivitäten beobachtet werden – im Bewusstsein bleibt einzig die Möglichkeit, dass man beobachtet werden *könnte*. Dies kann unter Umständen ein permanentes diffuses Gefühl der Verunsicherung auslösen, vor allem auch deshalb, weil Nutzer subjektiv kaum einschätzen können, welchen Verdacht sie erregen müssen, um potenziell staatlichen Beobachtungsmaßnahmen ausgesetzt zu werden (Staben 2016, S. 158). In diesem Zusammenhang einschneidend waren zweifellos die Enthüllungen von Edward Snowden im Jahr 2013, als erstmals das tatsächliche Ausmaß staatlicher Internet- und/oder informationstechnischer Beobachtung in das Bewusstsein der breiten Öffentlichkeit drang: Mag es sich hierbei auch vorrangig um die Aktivitäten einiger Nachrichtendienste der USA und weiterer Staaten gehandelt haben, die nach ganz anderen Motivationen und Regeln handeln als die im vorliegenden Bericht adressierten deutschen Polizei- und Strafverfolgungsbehörden, so hat sich seither der gesellschaftliche und politische Diskurs zum staatlichen Einsatz solcher Beobachtungstechnologien insgesamt nachhaltig verändert.

In der Folge der Snowden-Enthüllungen sind mögliche Auswirkungen der (staatlichen) Internet- und/oder informationstechnischen Beobachtung auf die Psyche und das individuelle Verhalten der Nutzer auch ins Zentrum wissenschaftlicher Aufmerksamkeit gerückt. Ausgangspunkt ist die Hypothese, dass dadurch das Gefühl einer ubiquitären Überwachung entstehen kann – mit entsprechenden handlungspsychologischen Folgen. Vergleichsweise noch harmlose Auswirkungen könnten dabei in individuellen Bemühungen zur Wiederherstellung oder Stärkung des Schutzes der eigenen Daten bestehen (z. B. durch Anpassung der Datenschutzeinstellungen in den jeweiligen Diensten oder die Verwendung verschlüsselter Kommunikationsdienste). Vermutet werden aber auch gravierendere Folgen durch mögliche Abschreckungs- oder Lähmungseffekte (Chillingeffekte), die von Änderungen im Onlineverhalten über Nutzungseinschränkungen bis hin zu Effekten der Selbstzensur im Rahmen der Nutzung solcher Dienste reichen könnten.

Im Folgenden werden bisher erzielte relevante Studienergebnisse kurz vorgestellt. Die Ausführungen basieren in wesentlichen Teilen auf dem Gutachten des IZEW (2017, S. 47 f.). Bereits an dieser Stelle sei jedoch darauf hingewiesen,

dass die bisherigen Forschungsergebnisse, die sich auf die psychischen Wirkungen von Beobachtungspraktiken vorrangig durch (ausländische) Nachrichtendienste beziehen, nicht vorbehaltlos auf die Beobachtungspraktiken durch deutsche Polizei- und Strafverfolgungsbehörden übertragen lassen. Stattdessen ist zu konstatieren, dass genau zu letzterem Anwendungskontext Untersuchungen und gesicherte Aussagen zu möglichen psychischen Wirkungen fehlen, sodass hierzu noch erheblicher Forschungsbedarf besteht.

7.1.3.1 Verhaltensänderungen infolge der Snowden-Enthüllungen

Eine relevante Forschungsfrage lautet, ob Nutzer ihr Verhalten infolge des neuen Bewusstseins über die Qualität staatlicher Internet- und informationstechnischer Beobachtung durch die Snowden-Enthüllungen verändert bzw. eingeschränkt haben. Die massiven gesellschaftlichen und politischen Reaktionen im Nachgang der Enthüllungen legen solche Verhaltensanpassungen nahe.

Bereits wenige Wochen nach Bekanntwerden der nachrichtendienstlichen Beobachtungspraktiken führte das Deutsche Institut für Vertrauen und Sicherheit im Internet (DIVSI 2013) eine erste repräsentative Onlinebefragung unter 2.016 Internetnutzern ab 16 Jahren in Deutschland durch. Obschon immerhin 68 % der Befragten die Enthüllungen bekannt waren, waren die Effekte überraschend gering: Über die Hälfte (53 %) der Befragten gab an, ihr Onlineverhalten gar nicht verändert zu haben, während nur 18 % das Verhalten im Internet etwas bzw. sehr verändert hatten. Verhaltensänderungen dieser Gruppe beinhalteten u. a.:

- besser darauf achten, welche privaten Informationen Onlinediensten zur Verfügung gestellt werden (73 %);
- soziale Netzwerke weniger nutzen (39 %);
- mobile Endgeräte weniger nutzen (21 %);
- weniger online sein (13 %).

Zugleich sprachen aber auch insgesamt 50 % der Befragten den deutschen Sicherheitsbehörden das Recht auf den Zugriff privater Daten zu (12 % ja sicher; 38 % eher schon), während dies für ausländische Sicherheitsbehörden nur 14 % bejahten.

Eine ähnliche Befragung im Folgejahr der Snowden-Enthüllungen (DIVSI/ dimap GmbH 2014) bestätigte diesen generellen Befund (Telefoninterviews mit 1.007 Personen ab 16 Jahren in Deutschland): Kannten hier bereits 80 % der Befragten die Enthüllungen, gab nur etwa jeder Vierte (23 %) an, sein Verhalten bei der Telefon- oder Internetnutzung in Reaktion darauf verändert zu haben und dies, obwohl die Mehrheit (56 %) davon ausging, dass »jeder von uns« abgehört werde. Für dieses zunächst wenig konsequent erscheinende Verhalten lieferte die Befragung zwei mögliche Erklärungen: Zum einen gaben 30 % an, dass sie

bereits vor den Enthüllungen sehr vorsichtig waren, und zum anderen sagte knapp die Hälfte der Befragten (44 %), es interessiere sie nicht, ob sie abgehört würden, da sie »nichts zu verbergen« hätten.

Auch in anderen Ländern wurden eher geringe Auswirkungen der Snowden-Enthüllungen auf das Nutzungsverhalten festgestellt. In den USA beispielsweise ergab eine ähnliche Umfrage von Rainie und Madden (2015, S. 17 f.) folgende Ergebnisse (n = 475): Hatten hier 87 % der Befragten von den staatlichen Beobachtungspraktiken gehört, gaben von diesen nur 25 % an, ihr Verhalten bei der Nutzung von (Mobil)Telefonen, E-Mail, Suchmaschinen oder sozialen Medien verändert zu haben (etwa indem private Dinge weniger offen in sozialen Netzwerken diskutiert wurden). Immerhin 34 % dieser Personen hatten Maßnahmen zum besseren Schutz ihrer Daten vor staatlicher Beobachtung ergriffen (z. B. durch Anpassung von Datenschutzeinstellungen in sozialen Medien). Personen, die ihr Verhalten nicht in nennenswerter Form geändert hatten, nannten als mögliche Gründe u. a. (Rainie/Madden 2015, S. 19):

- »I really don't worry about government monitoring since they would have no interest in what I'm doing. I'm more cautious about what I post and say for personal reasons.«[175]
- »I actually haven't changed anything, at least consciously. I forget that I might be monitored, to be honest.«[176]
- »I haven't changed it much simply because I don't feel it's worth the effort.«[177]

In Bezug auf die Aussagekraft solcher Umfragen ist einschränkend zu sagen, dass die Ergebnisse ausschließlich auf Selbstaussagen und -einschätzungen beruhen. Somit ist schwer zu beurteilen, ob die Befragten ehrliche und ausreichend reflektierte Auskünfte erteilten. So könnten Befragte auch dazu neigen, gesellschaftlich legitimierte bzw. wünschenswerte Antworten zu geben, die nicht unbedingt der eigenen Meinung entsprechen müssen (IZEW 2017, S. 55). Nichtsdestotrotz verweisen die Umfrageergebnisse übereinstimmend darauf, dass, obwohl sich eine deutliche Mehrheit über die Möglichkeit staatlicher Beobachtung ihrer privaten Daten durchaus bewusst ist, nur ein relativ kleiner Teil der Nutzer/innen – zumindest in der eigenen Wahrnehmung – sein Verhalten in Reaktion darauf angepasst hat (wenngleich ein Teil der Nutzer/innen ggf. bereits vor den Snowden-Enthüllungen entsprechende Vorsichtsmaßnahmen ergriffen hatte). Dies mag angesichts der (damaligen) allgemeinen Empörung über das Ausmaß der nachrichtendienstlichen Beobachtung etwas überraschen. Jedoch scheint der Umgang mit staatlichen Beobachtungspraktiken von einer gewissen Passivität und Gleich-

175 »Ich mache mir keine Gedanken über staatliche Überwachung, da die Regierung kein Interesse an meinen Aktivitäten hätte. Dass ich vorsichtiger bin, was ich veröffentliche oder sage, hat persönliche Gründe.« (TAB-Übersetzung)

176 »Ich habe nichts verändert, zumindest nicht bewusst. Um ehrlich zu sein, ich vergesse es, dass ich überwacht werden könnte.« (TAB-Übersetzung)

177 »Ich habe nichts verändert, weil es – um es einfach auszudrücken – nach meinem Gefühl den Aufwand nicht wert ist« (TAB-Übersetzung)

gültigkeit geleitet, wobei diese nach dem Motto »ich habe nichts zu verbergen« oder »für meine Daten interessiert sich der Staat nicht« stillschweigend toleriert werden. Diese Argumentation ist aber aus mindestens vier Gründen als problematisch anzusehen (IZEW 2017, S. 83 f.):

- Menschen können auch Dinge verbergen wollen, die nicht sicherheitsrelevant, sondern einfach nur privat sind.
- Das Argument befördert die massenhafte Offenlegung von individuellen Daten und dadurch die Bildung von Stereotypen. Dadurch werden Rückschlüsse auf Individuen nach dem Muster »Menschen wie …« ermöglicht, was die Privatheit Dritter verletzt.
- Es besteht die Gefahr, dass Beobachtung dort, wo sie ihren Zweck aus dem Auge verliert, zum Selbstzweck wird. Denn dass jemand »nichts zu verbergen« hat und eine Beobachtung daher toleriert, bedeutet deshalb nicht zugleich auch, dass er oder sie etwas offenzulegen hätte und eine Beobachtung daher sinnvoll und gerechtfertigt ist. Grundsätzlich sind nicht die Bürger gegenüber dem Staat in der Rechtfertigungspflicht (was das Argument »ich habe nichts zu verbergen« faktisch darstellt), sondern umgekehrt hat der Staat Eingriffe in die Privatheit von Fall zu Fall zu begründen und zu rechtfertigen.
- Schließlich ist Gleichgültigkeit gegenüber staatlichen Beobachtungsmaßnahmen auch insofern gefährlich, als dass Beobachtungstechnologien immer auch missbraucht werden könnten.

7.1.3.2 Auswirkungen auf das Suchverhalten im Internet

Neben solchen Umfragen, die immer nur subjektive Wahrnehmungen abbilden können, beschäftigten sich andere Studien mit objektiv messbaren Verhaltensänderungen. So haben beispielsweise Marthews und Tucker (2017) potenzielle Lähmungseffekte durch Beobachtung untersucht, indem sie das Suchverhalten im Internet vor und nach den Snowden-Enthüllungen in den USA und 40 weiteren Ländern (u. a. auch Deutschland) mithilfe von Google-Trends[178] miteinander verglichen. Gemessen wurde die Veränderung in der Zahl an Suchanfragen nach ausgewählten, als sensibel eingeschätzten Begriffen vor und nach den Enthüllungen. Dazu zählten zum einen regierungssensible Begriffe, in deren Zusammenhang Probleme mit staatlichen Autoritäten erwartet werden können (z. B. »dirty bomb«, »anthrax«), zum anderen persönlichkeitssensible Begriffe, bei denen jemand entsprechende Suchanfragen unter Umständen auch gegenüber Freunden, der Familie oder dem Arbeitgeber geheim halten möchte (z. B. »abortion«, »coming out«, »suicide«). Wichtige Ergebnisse der Studie waren (Marthews/Tucker 2017, S. 19 f. u. 26 ff.): Nach den Enthüllungen wurde in den USA ein Rückgang

178 Google-Trends ist ein Onlinedienst, in dessen Rahmen Google Informationen zur Nutzung seiner Suchfunktion bereitstellt (https://trends.google.de/trends; 31.3.2022).

von 4 % bei Suchanfragen nach solchen Begriffen festgestellt, die als besonders regierungs- und persönlichkeitssensibel eingeschätzt wurden. In den anderen untersuchten Ländern wurde weniger nach regierungssensiblen Begriffen gesucht, hier fiel der Rückgang im Vergleich zur USA aber etwas geringer aus. Interessanterweise wurden die stärksten Lähmungseffekte nicht in Ländern gemessen, die traditionell im Fokus US-amerikanischer Nachrichtendienste liegen (z. B. China, Iran), sondern in Partnerländern der USA (u. a. in Deutschland).

Penney (2016) untersuchte in einer vergleichbaren Studie die Nutzung von 48 englischsprachigen Wikipedia-Seiten zu politisch brisanten Begriffen (z. B. »Biological Weapon«, »Jihad«) vor und nach den Snowden-Enthüllungen. Auch diese Untersuchung stellte nach Bereinigung der Ergebnisse (u. a. durch Weglassen von Ausreißerwerten) einen substanziellen Lähmungseffekt fest, indem die Zugriffzahlen auf die untersuchten Wikipedia-Seiten unmittelbar nach den Enthüllungen um 25 % sanken (Penney 2016, S. 151 ff.). Auch in der Langzeitperspektive (16 Monate nach den Enthüllungen) konnte noch eine konstante Abnahme der Besucherzahlen festgestellt werden.[179]

Beide Studien weisen allerdings einige konzeptionelle und methodische Schwächen auf (IZEW 2017, S. 52 ff.): Die Studie von Marthews und Tucker (2017) kann etwa im Hinblick auf den verwendeten Datensatz kritisiert werden, da Google-Trends nur bereits bereinigte Daten zu Suchanfragen zur Verfügung stellt.[180] Außerdem wird die Art der erwarteten Probleme mit staatlichen Autoritäten nicht konkretisiert und es bleibt unbeantwortet, ob Nutzer bestimmte Begriffe bewusst oder unbewusst vermieden. Die Gründe für verändertes Nutzungsverhalten und die Auswirkungen von Beobachtung auf die Psyche bleiben daher vage. Penney (2016) kann vor allem in Bezug auf den Umgang mit Ausreißerwerten kritisiert werden. So wurden Zugriffszahlen auf Wikipedia-Seiten zur Terrororganisation Hamas, die infolge des damals eskalierenden Nahostkonflikts drastisch zunahmen, nachträglich nicht berücksichtigt. Das Weglassen von Ausreißerwerten ist problematisch, weil gerade sie darauf hindeuten könnten, dass die möglichen Gründe für Lähmungseffekte und Motivationen zu politischer Beteiligung weitaus komplexer sein könnten, als es die Studie zu erklären vermag. Ein grundsätzlicher Kritikpunkt betrifft die Tatsache, dass durch die Auswertung von aggregierten Häufigkeitszahlen ggf. verdeckt wird, dass als Folge der Beobachtung sich bestimmte Personen weniger, andere aber möglicherweise häufiger über bestimmte sensible Themen im Internet informieren.

179 Dabei ist die Abnahme nicht auf eine geringere Wikipedia-Nutzung insgesamt zurückzuführen, da die Zugriffszahlen auf englischsprachige Seiten im untersuchten Zeitraum stetig zunahmen.

180 Über die Methodik hinter Google-Trends gibt das Unternehmen wenig Auskunft. Google reagiert aber auf unregelmäßige Suchaktivitäten (z. B. automatisierte Suchanfragen mit dem Ziel, die Ergebnisse zu verfälschen). Diese werden jedoch nicht grundsätzlich herausgefiltert, da dies die Erkennung entsprechender Aktivitäten und Herausfilterung aus anderen Google-Diensten erschweren würde. Aus diesem Grund stellen die Daten gemäß Google (o. J.) »kein exaktes Abbild der Suchaktivitäten« dar.

Geben also beide Studien erste objektiv messbare Hinweise auf die Existenz von Abschreckungs- bzw. Lähmungseffekten im Zusammenhang mit staatlichen Beobachtungspraktiken im Internet, so werfen sie gleichzeitig hinsichtlich einer Ausdifferenzierung der Gründe für verändertes Nutzungsverhalten und der genauen psychischen Wirkweisen von Beobachtung eine Reihe von Forschungsfragen auf, die genauer untersucht werden müssen.

7.1.3.3 Auswirkungen auf die Meinungsäußerung im Internet

Andere einschlägige Umfragen und Studien untersuchten potenzielle Abschreckungs- bzw. Lähmungseffekte auf die Bereitschaft zur freien Meinungsäußerung im Internet. Neben möglichen Nutzungseinschränkungen geht es hier also um die Frage, ob staatliche Beobachtung auch zu Effekten der Selbstzensur bei den Nutzern führt.

In diesem Zusammenhang sehr häufig angeführt werden die Ergebnisse einer Onlineumfrage von PEN America (2015), einer Schriftstellervereinigung, die sich für freie Meinungsäußerung einsetzt. Die Umfrage, an der 772 Schriftsteller/innen aus 50 Staaten teilnahmen, stieß auch in der Öffentlichkeit auf große Resonanz. Demnach betrieb ein großer Teil der Schriftsteller/innen aus Angst vor staatlicher Beobachtung Selbstzensur, wobei es offenbar einen Unterschied machte, ob sie in freien, teilweise freien oder unfreien Staaten beheimatet waren. Beispielsweise vermieden oder erwogen es 31 % der Schriftsteller/innen in freien Staaten, 38 % in teilweise freien Staaten und 68 % in unfreien Staaten, bestimmte Themen in Telefongesprächen oder E-Mails anzusprechen.

Andere, nicht auf eine bestimmte Gruppe fokussierte Umfragen deuten indes an, dass das Bewusstsein von Beobachtung nur im Zusammenspiel mit anderen Faktoren die Bereitschaft zur freien Meinungsäußerung vermindert. So zeigte die medial ebenfalls breit rezipierte Umfrage von Amnesty International (2015) unter insgesamt 15.000 Personen in 13 Ländern (u. a. Deutschland), dass die Bereitschaft, Regierungskritik in sozialen Medien, E-Mails oder Telefonaten zu üben, lediglich bei 13 % der Befragten sinken würde, wenn ihre Internet- und Kommunikationsaktivitäten staatlich erfasst würden. Für die Mehrheit (60 %) würde sich dadurch nichts ändern. Zugleich gaben 16 % der Befragten an, dass die Beobachtung dazu führe, die Regierung eher mehr zu kritisieren. In Deutschland gaben 15 % der Befragten an, dass Beobachtung ihre Bereitschaft zu Regierungskritik mindere, und etwa gleich viele, dass dies ihre Bereitschaft steigere. Ist auch die Aussagekraft dieser Umfrage aus diversen Gründen kritisch zu hinterfragen[181], so deuten die Ergebnisse zumindest an, dass das Bewusstsein von Beobachtung die Bereitschaft zur Regierungskritik je nach Kontext auch steigern kann. Dies

181 Beispielsweise wird nicht offengelegt, nach welchen Kriterien die Teilnehmer der Umfrage ausgewählt wurden. Auch beruht sie auf Selbstaussagen, deren Wahrheitsgehalt – wie beschrieben – kaum überprüfbar ist (IZEW 2017, S. 55).

widerspricht der allgemeinen These der Abschreckungs- bzw. Lähmungseffekte durch Beobachtung und kann gewissermaßen als inverser Chillingeffekt angesehen werden. Die Umfrage bietet jedoch keine Erklärung für diese Reaktionen auf Beobachtung.

Erste Erklärungsansätze für dieses Verhalten liefert möglicherweise eine Studie von Stoycheff (2016), deren zentrale Erkenntnis ist, dass das Bewusstsein der Beobachtung nur im Zusammenspiel mit anderen Faktoren die Bereitschaft zur Meinungsäußerung verändert. Konkret wurde untersucht, wie die Faktoren Bewusstsein und Akzeptanz von Beobachtung die individuelle Bereitschaft, politische Meinungen in sozialen Medien zu veröffentlichen, beeinflussen. Um dies zu überprüfen, wurde 255 Studienteilnehmern ein fiktiver Facebook-Post einer Nachrichtenagentur vorgelegt, der erneute US-Luftangriffe gegen den Islamischen Staat im Irak ankündigte. Der Hälfte der Teilnehmer wurde davor gesagt, dass sie staatlicher Internetbeobachtung ausgesetzt seien. Das Experiment zeigte dabei Folgendes:

- Teilnehmer, die die staatliche Beobachtung ablehnten, zeigten eine unverändert hohe Bereitschaft zur Meinungsäußerung, unabhängig davon, ob sie von einer Beobachtung ausgingen oder ob ihre Meinung der Mehrheits- oder Minderheitsmeinung entsprach.
- Bei Teilnehmern, die staatliche Beobachtung akzeptierten oder zumindest tolerierten, verringerte das Bewusstsein, beobachtet zu werden, signifikant die Bereitschaft, Minderheitsmeinungen zu vertreten. Mehrheitsmeinungen wurden dagegen bereitwillig kundgetan, insbesondere von solchen Teilnehmern, die der Aussage »Die Regierung kann mein Verhalten beobachten, da ich nichts zu verbergen habe« zustimmten.

Obschon auch diese Untersuchung methodische Mängel aufweist (u. a. nichtrepräsentative Onlineumfrage, Selbstaussagen), deuten die Ergebnisse an, dass ein Lähmungseffekt durchaus existiert, allerdings ggf. nur bei Personen, die staatliche Beobachtung tolerieren oder sogar begrüßen. Hier führt der Lähmungseffekt unter Umständen zu einem sozial konformen Verhalten, bei dem Minderheitsmeinungen unterdrückt, während Mehrheitsmeinungen verstärkt werden. Die Studienautorin sieht in diesem Verhalten eine potenzielle Gefahr für demokratische Systeme, da staatliche Beobachtung die Offenlegung von Minderheitsmeinungen einschränken könnte (Stoycheff 2016, S. 307).

Als eine mögliche Erklärung dafür, dass der Lähmungseffekt bei Personen, die staatliche Beobachtung ablehnen, geringer ausfällt, vermutet Stoycheff (2016, S. 305) ein hohes Bildungsniveau bei dieser Gruppe, wodurch diese Personen entweder unabhängig von den Umständen dazu bereit sind, ihre Meinung kundzutun, oder dies generell nie tun, weil sie stets davon ausgehen, beobachtet zu werden. Interessanterweise aber konnte Penney (2017) in einer Untersuchung keine statistisch signifikanten Zusammenhänge zwischen dem Auftreten von Läh-

mungseffekten auf die freie Meinungsäußerung im Internet unter staatlicher Beobachtung mit Einflussgrößen wie Geschlecht, Bildungs- und Einkommensniveau oder die Internetaffinität der Studienteilnehmer/innen feststellen (Onlineumfrage mit 1.212 Teilnehmer/innen, allerdings nicht repräsentativ). Einen moderaten Einfluss hatte einzig das Alter der Teilnehmer/innen, wobei der Lähmungseffekt umso größer ausfiel, je jünger die Befragten waren (Penney 2017, S. 16 ff.). Insgesamt ist somit die wissenschaftliche Erkenntnislage zum Auftreten von Lähmungseffekten und zu möglichen Ursachen dafür noch sehr lückenhaft.

7.1.4 Zwischenfazit

Im Zusammenhang mit dem Einsatz von Beobachtungstechnologien für zivile Sicherheitsaufgaben werden handlungspsychologische Folgewirkungen für die Betroffenen vermutet. Der Forschungsstand hierzu ist allerdings noch nicht weit fortgeschritten.

Im Vergleich zu anderen Beobachtungstechnologien verhältnismäßig gut erforscht sind mögliche psychische Auswirkungen der offenen Videobeobachtung. Hier zeigt sich, dass Videobeobachtung zu einer gesteigerten Selbstaufmerksamkeit, einem erhöhten Stresslevel und Verhaltensmodifikationen, insbesondere in Form der Vermeidung beobachteter Räume, führt. Jedoch legt es der aktuelle Forschungsstand nahe, solche möglichen Effekte nicht zu überschätzen. So treten Einschüchterungseffekte ggf. nur dann auf, wenn zur Beobachtung noch andere Faktoren wie etwa die Androhung von Sanktionen hinzukommen. Auch stellen sich bei den Beobachteten möglicherweise schnell Gewöhnungseffekte ein.

In Bezug auf die Internet- und/oder informationstechnische Beobachtung ist festzustellen, dass es klare Anhaltspunkte für Chillingeffekte gibt, also für Verhaltensanpassungen und Einschränkungen der eigenen Handlungen als Reaktion auf die staatliche Beobachtung. Diese Abschreckungs- und Lähmungseffekte beziehen sich dabei sowohl auf das Suchverhalten der Nutzer im Internet als auch auf ihre Bereitschaft zur freien Meinungsäußerung. Fraglich bleibt aber, ob diese Befunde, die vorrangig im Zusammenhang mit Beobachtungspraktiken durch (ausländische) Nachrichtendienste stehen, sich auch auf Beobachtungspraktiken durch andere (deutsche) Sicherheitsakteure übertragen lassen. Gleichzeitig weisen selbst breit rezipierte Studien oft methodische und konzeptionelle Schwächen auf und die Forschungslage bleibt hinsichtlich ihrer Befunde uneindeutig. Unklar ist etwa, ob die gefundenen Abschreckungs- und Lähmungseffekte nur aus Angst vor staatlichen Sanktionen auftreten oder eine allgemeinere Folge von staatlicher Beobachtung sind. Auch gibt es empirische Hinweise auf inverse Chillingeffekte, etwa in Form einer gesteigerten Bereitschaft zur Regierungskritik trotz staatlicher Beobachtung, wobei Erklärungen für dieses Verhalten noch weitgehend fehlen. Hier ergibt sich für die nächste Zukunft das Forschungsdesiderat, die genauen Mechanismen der psychischen Auswirkungen technisierter Beobachtung auf

individueller Ebene besser zu verstehen. Weitere Forschung in diesem Feld könnte schließlich dazu beitragen, weitere mögliche handlungspsychologische Folgen einer im Zuge der Digitalisierung zunehmend ubiquitären Beobachtung nicht nur durch staatliche Sicherheitsakteure, sondern auch durch Unternehmen und Privatpersonen zu erkennen und zu untersuchen.

7.2 Auswirkungen auf die Technologieanwender

Bisher standen mögliche Auswirkungen von technisierter Beobachtung auf die von der Beobachtung potenziell betroffenen Personen im Fokus. Der Einsatz von Beobachtungstechnologien im Sicherheitsbereich hat aber auch Auswirkungen auf die sie benutzenden Sicherheitsakteure. Dazu zählen insbesondere die Einsatzkräfte der Behörden und Organisationen mit Sicherheitsaufgaben, die die Technologien unmittelbar anwenden, etwa Feuerwehrleute, Polizeibeamte oder im Rettungsdienst tätige Personen, aber auch beispielsweise das Sicherheitspersonal bei kritischen Infrastrukturen (z. B. Verkehrsbetriebe). Anwender im weiteren Sinne sind darüber hinaus auch sämtliche Personen im Sicherheitsbereich, deren berufliche Tätigkeit mit Beobachtungstechnologien bzw. den damit gewonnenen Informationen im Zusammenhang steht, beispielsweise Staatsanwälte, Richter oder Akteure auf Behördenebene, die für Beschaffung, Planung oder Controlling verantwortlich sind.

In politischen und öffentlichen Diskursen spielen mögliche Auswirkungen von Beobachtungstechnologien auf die Technologieanwender bislang eine untergeordnete Rolle. Dabei zeigt sich in anderen Sicherheitskontexten, dass Technisierungsstrategien durch unerwünschte bzw. unerwartete Wirkungen auf die Technologieanwender damit eigentlich intendierte Sicherheitsgewinne auch wieder schmälern oder gänzlich zunichtemachen können. Strohschneider (2010, S. 163 ff.) verweist in diesem Zusammenhang auf das Beispiel der Seefahrt, die im ersten Jahrzehnt des 21. Jahrhunderts – eine Dekade, in der zahlreiche Sicherheitstechniken wie elektronische Navigationshilfen und Seekarten oder automatisierte Schiffsidentifizierung und Strandwarnsysteme eingeführt wurden – einen weitaus höheren Verlust an Schiffen im Vergleich zum Anstieg des internationalen Seefrachtverkehrs hinnehmen musste, als im Jahrzehnt davor. Ein aktuelles Beispiel stellen womöglich die beiden Abstürze eines Flugzeugs vom Typ Boeing 737 Max im Oktober 2018 bzw. März 2019 dar. Deren Ursachen werden in einer Fehlfunktion eines neuen Sicherheitssystems vermutet, das eigentlich einen möglichen Strömungsabriss durch Absenken der Flugzeugnase verhindern soll. Wird das System mit fehlerhaften Sensordaten versorgt, kann es sich grundlos einschalten und auf diese Weise Piloten, die unzureichend auf diese Situation vorbereitet sind, in eine kritische Lage bringen (Frommberg 2019). In diesem Zusammenhang sagte etwa der Luftfahrtexperte Giemulla (2019): »Die Piloten gehen eigentlich davon aus, jedenfalls leider heute viele moderne Piloten, dass

sie gar nicht mehr das Flugzeug fliegen, sondern dass es die Maschine tut, was ja tatsächlich der Fall ist. Das heißt, viele Piloten verstehen sich eigentlich nur als Knöpfchendrücker und Bediener eines technischen Geräts. Da kommt die Fähigkeit des persönlichen Fliegens oftmals zu kurz und soll ja auch gar nicht der Regelfall sein. Das soll ja wenn überhaupt in einem Notfall gemacht werden … Das Problem ist, dass das natürlich nicht in einer ganz ruhigen Situation passiert. … Ausgerechnet in einer solchen Situation soll … mir völlig klar sein, in welcher Fluglage die Maschine ist, was ich tun muss«.

Die Frage, inwieweit unerwünschte Effekte der Mensch-Maschine-Interaktion das Ziel einer Steigerung von Sicherheit durch Technisierung konterkarieren können, stellt sich auch beim Einsatz von Beobachtungstechnologien. Im Folgenden wird dies anhand einiger Thesen bzw. Phänomene aus der Ingenieurspsychologie und der Human-Factors-Forschung, die sich dem besseren Verständnis und der Optimierung der Mensch-Maschine-Interaktion widmet, diskutiert. Aufgrund der Vielfalt an möglichen Einsatzformen von Beobachtungstechnologien im zivilen Sicherheitsbereich haben die folgenden Anführungen allerdings nur exemplarischen Charakter.

7.2.1 Vertrauen in Technik

Aus der Human-Factors-Forschung bekannt ist der Complacency-Effekt (Selbstgefälligkeit). Der Psychologe Strohschneider (2010, S. 165) beschreibt den Effekt als »vom Vertrauen in die Technik überzeugtes Zurücklehnen«, das dann entsteht, wenn Technikanwender acht- und sorglos werden, gewissermaßen von der Haltung geprägt »Ach, auf mich und meine Achtsamkeit kommt es ja nicht mehr so an, die Technik regelt das schon alleine«. Ein übersteigertes Vertrauen in die Funktions- und Leistungsfähigkeit der Technik ist daher unerwünscht, weil es zu Nachlässigkeit führen kann. Genauso gilt es aber, ein zu geringes Maß an Vertrauen zu vermeiden, das in einer mangelnden Nutzung resultiert (Kees 2015, S. 131). Eine kritische Folge eines übersteigerten Vertrauens in Sicherheitstechnologien sieht Strohschneider (2010, S. 165 f.) in einer Abnahme des Situationsbewusstseins bei den Anwendern, weil diese dann auf die Nutzung von Informationen aus anderen Quellen oder Sinneskanälen verzichten könnten (»das System wird mich schon alarmieren, wenn was los ist«). Entstehen dann aber tatsächlich kritische Situationen, die rasches Handeln erfordern, geht viel Zeit verloren, um die fehlenden Informationen für ein adäquates Lagebild zu beschaffen.

Ein übersteigertes Vertrauen in die Funktions- und Leistungsfähigkeit von Beobachtungstechnologien erhöht das Risiko für mangelndes Situationsbewusstsein im besonderen Maße, da der Zweck von Beobachtungstechnologien gerade in der Bereitstellung von Informationen für die Lagebeurteilung und Risikobewertung liegt. Die Technisierung von Beobachtung geht aber notwendigerweise mit einer Reduktion der Komplexität und des Informationsgehalts des

beobachteten Raumes einher, sodass Beobachtungstechnologien immer nur einen eingeschränkten Ausschnitt der Realität erfassen und darstellen können. Ein paradigmatisches Beispiel hierfür ist die Videobeobachtung im öffentlich zugänglichen Raum, in deren Rahmen vorher ausgewählte Risikoräume in Ausschnitten (abhängig von den örtlichen Gegebenheiten und der Wahl der Kamerapositionen) als zweidimensionale Bilder mit einer bestimmten Qualität auf Bildschirmen im Kontrollraum dargestellt werden. Den Videobeobachtern fehlen damit wichtige Informationen, die für die Kontextualisierung der Bilder und die frühzeitige Erkennung sicherheitskritischer Situationen wichtig sein könnten (Kees 2015, S. 23 f.), angefangen von Ereignissen im nicht videobeobachteten Bereich über Geräusche und andere Sinneseindrücke bis hin zu atmosphärischen Eindrücken der Situation vor Ort. Dies gilt es insbesondere etwa dann zu berücksichtigen, wenn der Nutzen der Videobeobachtung gegenüber alternativen Sicherheitslösungen (z. B. den Einsatz von Sicherheitspersonal vor Ort) abzuwägen ist.

Neue Brisanz erhalten derartige Aspekte aktuell infolge der Entwicklungen im Bereich der künstlichen Intelligenz und des maschinellen Lernens, aus denen Systeme hervorgehen, die dem Menschen assistieren sollen (z. B. im Bereich der Robotik oder des autonomen Fahrens), während ihnen oft eine eigene Autorität, Neutralität und Glaubwürdigkeit zugeschrieben wird (IZEW 2017, S. 68). Auch Beobachtungstechnologien mit automatisierter Datenauswertung wird teilweise eine technische Überlegenheit gegenüber menschlichen Beobachtern attestiert, etwa im Kontext der automatisierten Videobeobachtung in Bezug auf die Schnelligkeit, Zuverlässigkeit oder Objektivität bei der Erkennung von polizeilich gesuchten Personen anhand ihrer Gesichter (Kap. 3.5) bzw. von Gefahrensituationen anhand des Verhaltens der videobeobachteten Personen (Kap. 3.3.4) oder im Kontext des Predictive Policing in Bezug auf das Auffinden neuer, für den Menschen nicht erkennbarer Zusammenhänge in großen Datenmengen (Kap. 4.3). Es ist gerade dieses Versprechen auf einen grundlegenden Qualitätssprung im Sicherheitshandeln, das automatisierte Beobachtungstechnologien für Sicherheitsakteure so attraktiv macht (IZEW 2017, S. 90). Verlieren aber die Anwender das Bewusstsein für die Grenzen und Limitationen solcher Beobachtungstechnologien, kann dies dazu führen, dass potenziell sicherheitskritische Situationen, die die Technologie nicht erkennt, auch von den Anwendern übersehen werden, oder dass algorithmenbasierte Interpretationen und Empfehlungen akzeptiert werden, ohne sie durch Hinzuziehen anderer relevanter Informationsquellen auf ihre Richtigkeit oder zumindest Plausibilität hin zu überprüfen (Kees 2015, S. 132).

Nun könnte man ein übersteigertes Vertrauen in die Technik zu einem individuellen Problem erklären, welches – einmal erkannt – durch geeignete Maßnahmen (z. B. Sensibilisierung der Anwender) wieder entschärft werden kann. Das Problem wiegt vor allem im Kontext von Beobachtungstechnologien mit automatisierter Datenauswertung allerdings schwerer. Denn Sicherheitsakteure, die im Einsatzkontext mit den Ergebnissen automatisierter Beobachtungstech-

nologien konfrontiert sind, stehen immer dann vor einer problematischen Entscheidungssituation, wenn die technikbasierten Handlungsempfehlungen den eigenen Erfahrungen, Intuitionen oder Präferenzen widersprechen. Folgen sie in dieser Situation der eigenen Intuition und stellt sich dies nachträglich als die falsche Entscheidung heraus, stehen sie unter hohem Druck, da Sicherheitsakteure im besonderen Maße in der Verantwortung stehen, ihre Handlungen gegenüber Vorgesetzten, der Politik oder der Öffentlichkeit zu rechtfertigen. Solchen Situationen können Sicherheitsakteure vermeintlich am einfachsten dadurch entgehen, indem sie den Empfehlungen der Beobachtungstechnologie »blind« Folge leisten (IZEW 2017, S. 91).

7.2.2 Mangelndes Systemverständnis

Die erfolgreiche Nutzung technischer Sicherheitssysteme setzt Systemverständnis voraus. So offenkundig dies ist, so zentral ist dieser Aspekt für die Human-Factors-Forschung. Probleme werden insbesondere dann gesehen, wenn neue komplexe Systeme installiert werden, ohne gleichzeitig die Anwender durch Ausbildung und Training optimal auf deren Einsatz vorzubereiten. So reichen Systemkenntnisse, die den Technologieeinsatz in Routinesituationen erlauben, nicht aus, um auch Ausnahmesituationen sicher bewältigen zu können. Mögliche Gründe für ein mangelhaftes Systemverständnis bei den Anwendern gibt es viele, angefangen von der zunehmenden Verfügbarkeit preiswerter komplexer Sicherheitssysteme, die dazu verleitet, diese auch dort zu installieren, wo eine entsprechende Schulung der Anwender als zu aufwendig erachtet wird, bis hin zu eher technologiegetriebenen Innovationspfaden in der Sicherheitsindustrie. Gehen aber Neuentwicklungen nicht auf die Bedürfnisse der Anwender zurück, sind diese wenig motiviert, sich damit intensiv auseinanderzusetzen bzw. umfangreiche Handbücher durchzuarbeiten (Strohschneider 2010, S. 167 f.).

In Bezug auf den Einsatz von Beobachtungstechnologien (und generell von Sicherheitstechnologien) im Bereich der zivilen Sicherheit relativiert sich das Problem eines mangelnden Systemverständnisses. So sind regelmäßige Schulungs- und Trainingsmaßnahmen ein integraler Bestandteil der Arbeit von Einsatzkräften und zwar nicht nur vor dem Hintergrund der ständigen Weiterentwicklung der Technik, sondern gerade auch deshalb, weil hier die Bewältigung von Ausnahmesituationen zum Alltag gehört. Gleichwohl können auch hier besondere Umstände dazu führen, dass die Ausbildung der Anwender der Einführung neuer, komplexer Beobachtungstechnologien hinterherhinkt. Hier zu nennen sind etwa Änderungen in den rechtlichen Rahmenbedingungen, die plötzlich neue Einsatzmöglichkeiten eröffnen und/oder zu einer raschen Verbreitung der praktischen Anwendung führen. Ein Beispiel hierfür sind die 2017 eingeführten strafprozessualen Befugnisse für Maßnahmen der Quellen-TKÜ und Onlinedurchsuchung zu Zwecken der Strafverfolgung (Kap. 5.3.1.4). Die Durchführung

der Maßnahmen ist technisch derart komplex, dass sie nur von Spezialisten geleistet werden kann (Kap. 5.2.3). Auch wenn es in den Polizeibehörden entsprechende Fachleute geben mag, so ist zu bedenken, dass auch Staatsanwälte und Richter, die solche Maßnahmen beantragen, anordnen und kontrollieren sollen, sich ein Systemverständnis aneignen müssen, das zumindest so weit reicht, dass ein rechtskonformer Einsatz der Maßnahmen gewährleistet werden kann (Buermeyer 2017b, S. 19). Ein weiteres Beispiel in diesem Zusammenhang sind Beobachtungstechnologien mit automatisierter Datenauswertung auf der Grundlage von Modellen aus dem maschinellen Lernen, deren innere Logik selbst von den Entwicklern, geschweige denn von den Anwendern, nicht nachvollzogen werden kann (Kap. 3.3.8.2). Liegen aber keinerlei Informationen vor, wie ein Algorithmus zu seinen Ergebnissen gelangt, bestehen für die Anwender auch keine Möglichkeiten, algorithmenbasierte Empfehlungen verlässlich auf ihre Korrektheit hin zu überprüfen (IZEW 2017, S. 90 f.).

Der Ausbildungs- und Trainingsbedarf darf aber auch im Kontext (vermeintlich) einfach anwendbarer Beobachtungstechnologien nicht unterschätzt werden. Beispielhaft sei hier auf die polizeiliche Videobeobachtung in Nordrhein-Westfalen verwiesen, die durch Glaubitz et al. (2018) evaluiert wurden. Die im Rahmen der Evaluation befragten Videobeobachter bezeichneten die initialen Schulungen einheitlich als sehr kurz. Zwar wurde angeführt, dass die Bedienung der (schwenk- und zoomfähigen) Kameras intuitiv und damit eine längere Schulung nicht notwendig sei, es gab aber auch kritische Stimmen. So wurde ein Videobeobachter damit zitiert, dass die Beschulung ca. eine Stunde gedauert habe, wobei die Technik erklärt wurde, »aber nicht … wie man wirklich damit … umzugehen hat, [das] musste man sich so selbst beibringen« (Glaubitz et al. 2018, S. 34). Es wäre aber bedenklich, die erforderlichen Kompetenzen eines Videobeobachters auf die technische Bedienung der Kameras zu beschränken. Die Komplexität seiner Tätigkeit ergibt sich vielmehr aus der Notwendigkeit, die auf seinen Monitoren dargestellten Räume durch die erneute Anreicherung mit Informationen zu rekontextualisieren (Kap. 7.2.1; Kees 2015, S. 24). Dazu ist Wissen über den beobachteten Raum notwendig, vor allem aber auch praktisches Erfahrungswissen, dass nur durch intensives Training und den Austausch mit erfahrenen Videobeobachtern aufgebaut werden kann.

7.2.3 Schwächung des subjektiven Kompetenzempfindens

Arbeitspsychologische Theorien gehen meist davon aus, dass ein hohes subjektives Kompetenzempfinden, also das subjektive Zutrauen in die eigenen Fähigkeiten, ein wichtiger Faktor für die Motivation und Leistung von Mitarbeitern darstellt. Gerade der Einsatz von komplexen Sicherheitssystemen kann aber dazu führen, dass das Kompetenzempfinden geschwächt wird, zum einen infolge des bereits erwähnten mangelnden Systemverständnisses (Kap. 7.2.2), zum anderen,

indem immer mehr Aspekte der eigentlichen Sicherheitsarbeit an die Systeme abgegebenen werden und der aktiv handelnde Mensch auf die eingeschränkte Aufgabe der Kontrolle der Systeme und Überprüfung von Systemmeldungen verwiesen wird. Mögliche Auswirkungen auf den Systemanwender reichen vom Verlust an kritischer Aufmerksamkeit über die Suche nach alternativen Quellen für das subjektive Kompetenzempfinden (z. B. durch gegenseitige Bestätigung im Kollegenkreis) bis hin zu Motivationslosigkeit, Langeweile oder die Flucht in Tagträume und Phantasietätigkeit. Offensichtlich konterkarieren solche Folgen die eigentlich intendierten Sicherheitsgewinne. Sie sind aber nicht als Ausdruck menschlicher Schwäche zu interpretieren, sondern als Resultat von Technisierungsstrategien, die unzureichend auf die Bedürfnisse der Anwender eingehen (Strohschneider 2010, S. 169 f.).

In diesem Kontext sind vor allem Beobachtungstechnologien mit automatisierter Datenauswertung zu problematisieren, die algorithmenbasierte Handlungsempfehlungen liefern. Ein Beispiel ist die Videobeobachtung in Kombination mit Gesichtserkennungssystemen zur Personenfahndung in Echtzeit (Kap. 3.5): Aufgrund messtechnischer und weiterer Gründe ist die Erkennungsleistung solcher Systeme limitiert, sodass immer mit einer bestimmten Anzahl von Fehlalarmen zu rechnen ist. Dabei gilt: Je höher die Erkennungsrate, desto höher auch die Fehlalarmrate (Kap. 3.5.2.2.) Sollten solche Systeme in Zukunft verstärkt in hochfrequentierten öffentlichen Räumen (Bahnhöfe, Flughäfen etc.) zum Einsatz gelangen, so wird die Validierung von Treffermeldungen zu einer wichtigen Tätigkeit der hier eingesetzten Videobeobachter werden. Nimmt diese Aufgabe dauerhaft einen beträchtlichen Teil der Arbeitszeit von Videobeobachtern in Anspruch, könnte dies nicht nur ihr subjektives Kompetenzempfinden schwächen (mit den zuvor angesprochen Auswirkungen und Folgen), auch würden sie dadurch generell weniger Zeit für die eigentliche Sicherheitsarbeit haben.

7.2.4 Verlust von Fähigkeiten

Es gilt dafür Sorge zu tragen, dass die Anwendung von Beobachtungstechnologien nicht dazu führt, wichtige menschliche Fähigkeiten zu beeinträchtigen oder langfristig sogar verkümmern zu lassen. Als Beispiel wird hier die Einführung des teilautomatisierten Grenzkontrollsystems EasyPASS genannt, das auf Flughäfen zum Einsatz kommt und auf einem biometrischen Gesichtsabgleich zur Überprüfung der Identität der Reisenden basiert (Kap. 3.5.4.1). Dadurch sollen manuelle Passkontrollen entfallen, Grenzkontrollbeamte entlastet und der Kontrollvorgang für die Reisenden insgesamt erleichtert und beschleunigt werden. Bei einer automatisierten Passkontrolle werden aber menschliche Fähigkeiten, die zur Überprüfung von Reisedokumenten sowie zur Durchführung von Identitätsüberprüfungen und Einreisebefragungen essenziell sind, nicht mehr abgerufen. Zu diesen gehören u. a. das Deuten und Einschätzen von verbalem und

nonverbalem Verhalten sowie ein ausgeprägtes Wissen über ethnische Merkmale und Charakteristika. Zwar überblicken Grenzbeamte in einer Kontrollbox hinter den Schleusen den Kontrollprozess auch weiterhin, durch die Automatisierung der Passkontrolle gelangen die erwähnten Fähigkeiten aber weitaus seltener zur Anwendung, sodass sie auf Dauer sogar ganz verloren gehen könnten (Hempel 2016, S. 179). Ähnliches darf auch für andere Anwendungskontexte von Beobachtungstechnologien mit automatisierter Datenauswertung angenommen werden: So dürfte beispielsweise ein Videobeobachter, der auf seinem Monitor nur noch von einem Algorithmus ausgewählte Szenen einschließlich expliziter oder impliziter Handlungsempfehlungen angezeigt bekommt (z. B. verdächtige Person erkannt, abgelegter Gegenstand erkannt), kaum dasselbe praktische Erfahrungswissen sammeln bzw. dieselbe Intuition für die Erkennung sicherheitskritischer Situationen entwickeln können wie jemand, der mit konventioneller Videobeobachtung arbeitet. Erfordern dann aber außergewöhnliche Umstände (z. B. besondere Gefahrenlagen) spezielle menschliche Fähigkeiten und Intuitionen, stehen diese ggf. nicht mehr in ausreichendem Ausmaß zur Verfügung.

Nicht nur tätigkeitspezifische Fähigkeiten der Einsatzkräfte können ggf. eingebüßt werden. Auch bereichsübergreifende Kompetenzen, die für eine erfolgreiche Bewältigung schwieriger, nicht entlang der üblichen Routinen zu lösenden Situationen (z. B. größere Schadenslagen) insbesondere auf Ebene der Führungskräfte erforderlich sind, werden durch den Einsatz von Beobachtungstechnologien in vielfältiger Weise beeinflusst. Hier angesprochen sind vor allem kommunikative, organisatorische und strategisch-problemlöserische Fähigkeiten (Strohschneider 2010, S. 170 f.),

- um Ereignisse und kausale Zusammenhänge (verbal oder visuell) darzustellen und zusammen mit anderen Beteiligten ein gemeinsames Lagebild zu erarbeiten (diskursive Kommunikationsfähigkeit),
- um Entscheidungen auch unter Zeitdruck und Unsicherheit zu treffen,
- um konstruktiv mit Informationsüberflutung, aber auch mit unzuverlässiger oder fehlender Information umzugehen
- sowie um neuartige Handlungsalternativen zu entwickeln (Problemlösefähigkeit).

Beispielsweise wird derzeit intensiv an der Entwicklung von mit Kameras und weiteren Sensoren ausgerüsteten unbemannten Fluggeräten geforscht, die bei großen und/oder komplizierten Schadenslagen schnell und ggf. weitgehend automatisiert der Einsatzleitung wichtige Informationen für die Lagebewertung und Maßnahmenplanung liefern sollen (z. B. Überblicksaufnahmen, 3-D-Karten, Position von Personen oder Gefahrenquellen, Kap. 3.1.3). Ohne Zweifel kann die Erhöhung der Informationsdichte die Bewältigung schwieriger Lagen maßgeblich unterstützen, zugleich sind aber auch mögliche unerwünschte Wirkungen zu beachten. In diesem Zusammenhang spricht etwa der Leiter der Feuerwehr- und

Katastrophenschutzschule von Rheinland-Pfalz, Hans-Peter Plattner, von einem »Teufelskreis von Informationsfülle und Bürokratisierung« (Plattner in Hufschmidt et al. 2017, S. 283 f.): Demnach könne ein zunehmender Technikeinsatz auch eine »wahre Flutwelle« von Informationen erzeugen, die Einsatzleitungen und Führungsstäbe zu verarbeiten haben. Dazu sei mehr Personal erforderlich, was wiederum mehr Informations- und Kommunikationstechnik erfordere. Auch könnten Führungsstäbe zum Abwarten auf immer noch genauere Informationen veranlasst werden. So drehe sich eine aufwendige Spirale, ohne letztlich zu einer besseren Führung beitragen zu können.

Der englische Organisationssoziologe Richard McMaster hat die Organisationsstrukturen und Entscheidungsfindungsprozesse während der Flutkatastrophe in England 2007 untersucht (nach Strohschneider 2010, S. 173). Er vertritt die Meinung, dass der Technologieeinsatz eine erfolgreiche Bewältigung von kritischen Lagen sogar behindern kann, wenn er dazu führt, dass die direkte Kommunikation zwischen wichtigen Akteuren der beteiligten Organisationen (Feuerwehr, Rettungsdienste, Katastrophenschutz, Polizei) erschwert wird (etwa durch den Einsatz einer gemeinsamen Informationsplattform). Denn in der Realität seien abweichend von den festgeschriebenen Regeln der interorganisationalen Zusammenarbeit oft ad-hoc-Strukturen nötig, die flexible Reaktionen ermöglichen. Eine wichtige Voraussetzung hierfür sei aber Vertrauen zwischen den Beteiligten, das am besten durch direkte Kommunikation und das Ausdiskutieren von Lageeinschätzungen und Machtfragen hergestellt werden kann.

7.2.5 Einschränkung der Entscheidungs- und Handlungsfreiheit

Die im zivilen Sicherheitsbereich eingesetzten Beobachtungstechnologien mit automatisierter Datenauswertung sind als *Entscheidungsunterstützungssysteme* konzipiert: Die Technologien sollen Sicherheitsakteuren zusätzliche Informationen liefern, nach denen sie ihr Handeln ausrichten können, aber nicht müssen (Zweig 2018, S. 12 ff.). Ein Sicherheitsscanner zur Personenkontrolle beispielsweise weist auf möglicherweise unter der Kleidung versteckte Gegenstände hin, über das weitere Vorgehen aber entscheidet das anwesende Kontrollpersonal (Kap. 3.1.2.3). Davon abzugrenzen sind *autonome Entscheidungssysteme*, die eigenständig Entscheidungen treffen und auf dieser Grundlage Aktionen ausführen (auch als automatische Entscheidungssysteme bezeichnet; Zweig 2018, S. 12 f.). Im vorgenannten Beispiel wäre dies etwa dann der Fall, wenn Sicherheitsscanner als Schleusen konzipiert werden, die nur vom System als ungefährlich eingestufte Personen passieren lassen. Offenkundig können autonome Systeme, die unzuverlässig funktionieren oder fehlerhaft arbeiten, für betroffene Personen unter Umständen gravierende Konsequenzen haben. Ihr Einsatz ist rechtlich daher auch nur unter engen rechtlichen Voraussetzungen möglich (z. B. §§ 37, 54 BDSG).

Auch unter ethischen Gesichtspunkten wird der in vielen Technikfeldern (geplante) Einsatz von autonomen Entscheidungssystemen sehr kontrovers diskutiert, etwa im Zusammenhang mit der Robotik (TAB 2016b), autonomen Fahrzeugen (Ethik-Kommission 2017) oder autonomen Waffensystemen (TAB 2020). Ein wesentlicher Diskursstrang der Debatten beschäftigt sich mit der Frage der Verantwortungszuschreibung, die dann virulent wird, wenn Entscheidungs- und Handlungsfreiheiten vom Menschen auf Maschinen übertragen werden, deren Einsatz dann aber Schäden anrichtet. Denn mit menschlicher Entscheidungs- und Handlungsfreiheit geht für gewöhnlich die Zuschreibung von individueller Verantwortung für eben diese Entscheidungen einher (dazu und zum Folgenden IZEW 2017, S. 89 f.). Damit verbunden gilt auch, dass Menschen für selbstverschuldetes Fehlverhalten zur Verantwortung gezogen werden können. Dies ist eine Maßgabe der Ethik, ebenso wie eine Maßgabe des Rechts. Sobald aber Handeln alleine auf algorithmenbasierten Entscheidungen beruht, ist eine individuelle Verantwortungszuschreibung nicht mehr gegebenen, sodass im Zweifel keine Schuldigen identifiziert werden können und niemand für unrechtmäßige oder unmoralische Handlungen zur Rechenschaft gezogen werden kann. Die Frage der Verantwortung im Kontext von autonomen Entscheidungssystemen ist in vielen Anwendungskontexten ein noch ungelöstes Problem.

Nur auf den ersten Blick stellt sich die Frage der Verantwortungszuschreibung im Kontext des Einsatzes von Beobachtungstechnologien mit automatisierter Datenauswertung im zivilen Sicherheitsbereich nicht: Die durch Algorithmen gewonnenen Erkenntnisse und Handlungsempfehlungen dienen den Sicherheitsakteuren lediglich als Entscheidungshilfe, sodass die Letztentscheidung und damit die Verantwortung für die auf dieser Grundlage getroffenen Maßnahmen einem bzw. mehreren menschlichen Akteuren zugeordnet werden können.[182] Angesichts der großen Fortschritte im Bereich der automatisierten Datenauswertung besteht allerdings die berechtigte Sorge, dass das Prinzip der menschlichen Letztverantwortung auch bei eigentlich als Entscheidungsunterstützungssysteme ausgelegten Beobachtungstechnologien zunehmend untergraben werden könnte. Der Grund dafür ist nicht, dass individuellen Sicherheitsakteuren ihre Handlungen nicht mehr zugeschrieben werden könnten, sondern vielmehr der Umstand, dass Zweifel bestehen, ob ihnen tatsächlich noch Entscheidungs- und Handlungsfreiheit zukommt (IZEW 2017, S. 89 f.). So treten neben einem hohen *Rechtfertigungsdruck* (Kap. 7.2.1) weitere (z. T. bereits erwähnte) Faktoren hinzu, die dazu beitragen können, den Entscheidungsspielraum für die betroffenen Sicherheitsakteure wesentlich zu schmälern (IZEW 2017, S. 91):

182 Prinzipiell gilt dies auch vor dem Hintergrund, dass Behörden und Organisationen mit Sicherheitsaufgaben oft stark hierarchisch organisiert sind, sodass Verantwortung oft über gestaffelte, z. T. lange Befehls- und Kompetenzketten delegiert wird und somit im Nachhinein nicht immer klar zugeordnet werden kann (IZEW 2017, S. 89).

- *Informationsdefizit*: Insbesondere im Fall von Algorithmen aus dem maschinellen Lernen haben Sicherheitsakteure keine Kenntnis darüber, wie die jeweilige Beobachtungstechnologie arbeitet und wie genau Ergebnisse zustande kommen. Insofern besteht auch keine Möglichkeit, algorithmenbasierte Schlüsse verlässlich auf ihre Korrektheit hin zu bewerten.
- *Kapazitätsdefizit*: Die jeweiligen Beobachtungstechnologien suggerieren Sicherheitsakteuren gegenüber eine technische Überlegenheit (z. B. in Bezug auf Schnelligkeit, Zuverlässigkeit oder Objektivität), mit der sie als menschliche Akteure nicht (dauerhaft) mithalten können.
- *Zeitdefizit*: Sicherheitsakteure sind im Einsatzkontext oft zu schnellem, entschiedenem Handeln gezwungen, was die Möglichkeiten der Reflexion und des Abwägens unterschiedlicher Handlungsoptionen einschränkt.

In der Konsequenz könnten die Ergebnisse von automatisierten Beobachtungstechnologien von den betroffenen Sicherheitsakteuren nicht mehr lediglich als Entscheidungshilfe neben anderen Kriterien (insbesondere persönliches Erfahrungswissen) angesehen werden, sondern faktisch als eigenständige, aufgrund ihrer angenommenen Objektivität und Zuverlässigkeit legitime Entscheidungsinstanzen. Eine wirkliche menschliche Letztentscheidung bzw. die Möglichkeit der individuellen Verantwortungszuschreibung wäre in diesem Fall aber nicht (mehr) gegeben. Eine individuelle Verantwortungszuschreibung ist jedoch gerade im Sicherheitskontext von essentieller Bedeutung, da Sicherheitshandeln mitunter tiefgreifende Grundrechtseingriffe legitimieren und somit potenziell weitreichende Konsequenzen für die Betroffenen haben kann. Wie in anderen Feldern auch bleibt hier die schwierige Frage zu diskutieren, wie eine geteilte Verantwortung zwischen Menschen und technischen Systemen genau aussehen könnte. Hierbei kann Verantwortung nicht (allein) den jeweiligen Technologieanwendern zugeschrieben werden. Bei einer Einführung solcher Beobachtungstechnologien müssten daher neue Formen geteilter Verantwortung gefunden werden, die auch andere Akteure (z. B. die beteiligten Unternehmen und Programmierer, die jeweiligen Sicherheitsbehörden) mit einbeziehen (IZEW 2017, S. 91 f.).

7.2.6 Zwischenfazit

Deutlich wird, dass die einfache Formel »mehr Technologie führt zu mehr Sicherheit« aufgrund von nichtintendierten Wirkungen auf die Anwender der Technologien nicht generell gilt. Dies trifft auch auf den Einsatz von Beobachtungstechnologien für zivile Sicherheitsaufgaben zu. Aus der Anwenderperspektive betrachtet ist deren Einsatz dann relativ unproblematisch, wenn sie das menschliche Wahrnehmungs- und Beurteilungsvermögen für Risiken, Gefahren oder Schäden verbessern, die Arbeit von Sicherheitsakteuren unterstützen und nicht behindern sowie Aufwand (z. B. für Ausbildung und Training, Personalbedarf) und erhaltene Unterstützung in einem ausgewogenen, zielführenden Verhältnis

stehen. Zu problematisieren ist der Einsatz allerdings dann, wenn Beobachtungstechnologien eingespielte und zuverlässig funktionierende Routinen und Prozesse verändern, die Fähigkeiten und das Erfahrungswissen der Sicherheitsakteure verdrängen oder die sozialen, kognitiven und motivationalen Voraussetzungen des menschlichen Sicherheitshandeln (negativ) verändern (Strohschneider 2010, S. 174; Hempel 2016, S. 118).

Diesbezüglich sind im Besonderen Beobachtungstechnologien mit automatisierter Datenauswertung kritisch zu reflektieren, die den menschlichen Beobachter bei der Analyse und Interpretation der Beobachtungsdaten unterstützen bzw. solche Aufgaben ganz übernehmen sollen. Dies spricht aber nicht generell gegen die Einführung und Nutzung von automatisierten Beobachtungstechnologien. Vielmehr sollten bei Entscheidungen über deren (künftigen) Einsatz nicht nur technologische Effizienzkriterien und mögliche Auswirkungen auf die beobachteten Personen betrachtet, sondern auch mögliche Effekte auf die sie benutzenden Sicherheitsakteure adäquat einbezogen werden. Dazu ist es notwendig, den Wissenstand über solche Effekte auf- und auszubauen.

7.3 Verhältnis zwischen Sicherheit und Freiheit

Die Herstellung bzw. Gewährleistung von Sicherheit gehört unstrittig zu den Kernaufgaben des modernen Staates. Ohne ein gewisses Maß an Sicherheit lässt sich ein selbstbestimmtes Leben für die einzelnen Bürger/innen und für ein Gemeinwesen insgesamt nur sehr schwer vorstellen bzw. realisieren (IZEW 2017, S. 85). Insofern wird Sicherheit immer auch als Wert verstanden. Zur Werteordnung von freiheitlich verfassten Demokratien gehören zugleich die Grundrechte, die den Freiheitsraum jeder Bürgerin und jedes Bürgers vor Eingriffen durch den Staat schützen. Ist die Herstellung von Sicherheit mit Eingriffen in individuelle Freiheitsrechte verbunden, so ergibt sich aus beiden Werten also ein mitunter sensibles Spannungsverhältnis. Die schwierige und zum Teil sehr kontrovers diskutierte Frage lautet dann, wie beide Ziele bzw. Werte so in Einklang gebracht werden können, dass der eine Wert den anderen nicht überlagert bzw. Sicherheit durch den Staat garantiert werden kann und ein selbstbestimmtes Leben möglich bleibt.

Zu konstatieren ist, dass das Verhältnis beider Werte zueinander je nach Anwendungskontext durchaus unterschiedlich intensiv bzw. kontrovers diskutiert wird. So wird unter diesem Aspekt Sicherheitshandeln im Rahmen der nichtpolizeilichen Gefahrenabwehr oder beispielsweise der polizeilichen Verkehrsüberwachung eher selten kritisch erörtert (z. B. gemessen an der medialen Berichterstattung oder Anzahl von wissenschaftlichen Publikationen zum Thema). Obwohl es auch hier zu Eingriffen in die Privatheitsgarantien (z. B. im Kontext der Ortung verschütteter Personen, Kap. 3.2.1.2) oder die individuelle Handlungsfreiheit (z. B. im Kontext von Evakuationen in Gefahrenlagen oder von Polizeikontrollen im Straßenverkehr) kommen kann, ist in diesen Kontexten

Sicherheit als institutionalisierte Wertvorstellung weitgehend akzeptiert. Sicherheitshandeln gilt hier als zentrales Element einer sozialen Ordnung mit verteilten Rollen und Kompetenzen und beruht auf einem breiten gesellschaftlichen Konsens (IZEW 2017, S. 85; Heesen 2016, S. 50 f.).

Anders verhält es sich im Kontext der Bekämpfung von Kriminalität und Terrorismus (also dem Schutz vor Angriffen Dritter) (IZEW 2017, S. 85 f.). Das schwierige Spannungsverhältnis zwischen Sicherheit und Freiheit bildet hier bis heute einen Schwerpunkt öffentlicher und politischer Debatten bezüglich der Aufgaben des Staates und der Legitimität der hierzu eingesetzten (beobachtungstechnischen) Mittel. Stehen sich meist stark unterschiedliche und zum Teil verhärtete Positionen gegenüber, so hängt ein Aufflammen einer breiteren öffentlichen Debatte allerdings oft von der medialen Präsenz und der konkreten Betroffenheit von sicherheitsrelevanten Ereignisse ab. Nachrichten über die Häufung spezifischer Delikte wie Wohnungseinbrüche oder auch einzelner außergewöhnlich schwerer Straftaten wie Terroranschläge gehen einerseits mit einer Akzeptanz neuer Maßnahmen und erweiterter polizeilicher Einsatzbefugnisse einher, während mögliche Rechtskonflikte durch den Einsatz von (neuen) Beobachtungstechnologien eine verstärkte Ablehnung bewirken können.

Die Aufgabe des Gesetzgebers ist es, für den staatlichen Einsatz von Beobachtungstechnologien die gesetzlichen Grundlagen zu schaffen und zwar so, dass Bürger/innen selbstbestimmt und die Sicherheitsbehörden rechtssicher handeln können.[183] Erscheint diese Aufgabe angesichts der fortschreitenden Technisierung und einer immer komplexer werdenden Technik zunehmend schwieriger lösbar, so unterliegt der Gesetzgeber hierbei zugleich verfassungsrechtlichen Bindungen (Bäcker et al. 2013, S. 9). Zur Klärung des fraglichen Spannungsverhältnisses von Sicherheit und Freiheit bildet der Grundsatz der Verhältnismäßigkeit eines der zentralen Instrumente. Dieser ergibt sich »aus dem Rechtsstaatsprinzip, im Grunde bereits aus dem Wesen der Grundrechte selbst, die als Ausdruck des allgemeinen Freiheitsanspruchs des Bürgers gegenüber dem Staat von der öffentlichen Gewalt jeweils nur so weit beschränkt werden dürfen, als es zum Schutz öffentlicher Interessen unerlässlich ist« (BVerfG, Beschluss vom 15. Dezember 1965, 1 BvR 513/65, Rn. 17).

Der Verhältnismäßigkeitsgrundsatz ist aber nicht nur Verpflichtung, sondern gibt dem Gesetzgeber in seiner konkreten Ausgestaltung gleichzeitig auch ein methodisches Prozedere an die Hand, wie Sicherheit und Freiheit abgewogen werden können, um über die verfassungsrechtliche Konformität von staatlichen Beobachtungspraktiken zu entscheiden. Zur Erinnerung: Ein Grundrechtseingriff ist nach diesem Grundsatz dann verhältnismäßig, wenn er einem legitimen Zweck dient sowie das gewählte Mittel zur Erreichung des Zwecks geeignet, erforderlich und angemessen (verhältnismäßig im engeren Sinne) ist (Kap. 6.2). Wie die Verhältnismäßigkeitsprüfung im Einzelnen zu geschehen hat und ob dies für die

183 Oft und auch beim Einsatz von Beobachtungstechnologien erfolgt der eigentliche Grundrechtseingriff nicht durch das den Eingriff ermächtigende Gesetz selbst, sondern erst durch Anwendung des gewählten Mittels im konkret-individuellen Einzelfall.

geltenden Gesetze immer gelungen ist, wird vor allem im Kontext der Sicherheitsgesetzgebung allerdings oft unterschiedlich beantwortet. Hierfür kennzeichnend ist, dass die Entwicklungen im Bereich der Sicherheitsgesetzgebung zu einer Reihe von verfassungsrechtlichen Entscheidungen geführt haben, in denen wesentliche grund- und freiheitsrechtliche Grenzen staatlicher Eingriffsbefugnisse aufgezeigt wurden (Bäcker et al. 2013, S. 10). Darüber hinaus haben sich innerhalb der Sicherheitsforschung auch neue Forschungsansätze etabliert, so u. a. zur Technikfolgenabschätzung, -bewertung und -gestaltung aus rechtswissenschaftlicher Perspektive (Roßnagel et al. 1993), die interdisziplinär ausgerichtete Sicherheitsethik (Ammicht Quinn 2014) sowie die sozialwissenschaftliche Sicherheitsforschung, die konkrete Anwendungspraktiken und ihre Wechselwirkungen mit institutionalisierten Handlungserwartungen analysiert (Hempel et al. 2019).

Im Folgenden werden die notwendigen Schritte der Verhältnismäßigkeitsprüfung rekapituliert und mit Fokus auf den Einsatz von Beobachtungstechnologien durch Polizeibehörden zu Zwecken der Gefahrenabwehr und Strafverfolgung diskutiert. Dabei soll bzw. kann es nicht darum gehen, sämtliche Argumente und Überlegungen der kontroversen und weit verzweigten Debatte über polizeiliche Beobachtungspraktiken umfassend abzuhandeln (was im Rahmen dieses Berichts auch gar nicht möglich wäre). Vielmehr soll es darum gehen, zentrale Fragen und Herausforderungen für eine Verhältnismäßigkeitsprüfung polizeilicher Beobachtungsmaßnahmen zu thematisieren, die sich im Lichte der Erkenntnisse aus den vorangegangenen Kapiteln ergeben.

7.3.1 Legitimer Zweck und legitimes Mittel

Der Verhältnismäßigkeitsgrundsatz verlangt zunächst, dass vom Staat verfolgte Zwecke und die hierfür eingesetzten Mittel legitim sind. Hierbei gilt, dass der Gesetzgeber bei der Zweckwahl über einen weiten Spielraum verfügt, da er – anders als die jeweils an Gesetz und Recht gebundene Exekutive und Judikative – alleine an das Grundgesetz gebunden ist (Artikel 20 Abs. 3 GG). Abgesehen von der Verfolgung verfassungswidriger Ziele und soweit verfassungsimmanente Schranken (wie z. B. Artikel 13 Abs. 2 ff. GG) berücksichtigt werden, umfassen legitime Zwecke daher im Wesentlichen das gesamte Spektrum der Staatsaufgaben. Ähnliches gilt für das gewählte Mittel,[184] also die konkret getroffene Maßnahme (Wienbracke 2013, S. 147 f.).

Der Schutz der Bevölkerung leitet sich als eine der wesentlichen Verpflichtungen des Staates aus den Grundrechten, insbesondere dem Grundrecht auf Leben und körperliche Unversehrtheit, und dem staatlichen Gewaltmonopol ab (Bäcker et al. 2013, S. 11). Die Zwecklegitimität von Sicherheitsgesetzen wird daher selten infrage gestellt. Durch die existentielle Dimension erscheint

184 Ein Beispiel für ein grundgesetzlich verbotenes Mittel ist die Folter (Artikel 104 Abs. 1 S. 2 GG).

Sicherheit unmittelbar einsichtig und gewinnt mit einem steigenden gesellschaftlichen Sicherheitsbedürfnis (Kap. 2.3) innerhalb der Bevölkerung an Rückhalt.

Dieser Konsens ist jedoch gerade angesichts eines sich wandelnden Sicherheitsverständnisses, das immer neue Gefahren für die Sicherheit in den Blick nimmt, auch kritisch zu reflektieren. Der große Freiraum, der sich dem Gesetzgeber bei der Zweckwahl prinzipiell eröffnet, darf gleichsam nicht automatisch zu immer weitreichenderen Sicherheitsbefugnissen – u. a. zum Einsatz von Beobachtungstechnologien – führen (IZEW 2017, S. 70), sondern es muss immer eine eindeutige und klare Zwecksetzung erkennbar sein. So birgt gerade eine Sicherheitspolitik, die das Präventionsparadigma verstärkt betont, das Potenzial, dass Bedrohungslagen proaktiv konstruiert werden, ohne dass hierfür ausreichende Erkenntnisse oder reale Anlässe vorliegen. Vom Gesetzgeber mit einer konkreten Maßnahme etwaig zu schützende Sicherheitsinteressen vermögen aber Grundrechtseingriffe dann nicht zu legitimieren, wenn diese Interessen gar nicht gefährdet sind (Wienbracke 2013, S. 149).

Wohl gilt Sicherheit immer schon als ein legitimer Zweck, jedoch muss sich mit der Implementierung von Beobachtungstechnologien nicht zwangsläufig, immer und unmittelbar auch ein Sicherheitsgewinn einstellen. Beobachtungstechnologien sind Technologien, die zunächst nicht mehr und nicht weniger intendieren, Sicherheit nach Möglichkeit herstellen und gewährleisten zu wollen. Es kann durchaus noch andere Zwecke für ihre Implementierung geben, die etwa organisatorische Interessen verfolgen (z. B. Ressourceneffizienz bzw. Personal- oder Kosteneinsparungen) und die ggf. sogar als primäre Zwecke zu betrachten sind. Entscheidend ist daher, die Verhältnismäßigkeit des Einsatzes neuer Beobachtungstechnologien stets unter Berücksichtigung *aller* damit verfolgten Zwecke zu prüfen, um so auch Wirkungen und Folgen (z. B. Veränderungen in der organisationalen Praxis) zu berücksichtigen, die unter Umständen auch auf den Zweck der Sicherheit zurückwirken.

7.3.2 Geeignetheit des Mittels

Die Verhältnismäßigkeitsprüfung beginnt mit dem Kriterium der Geeignetheit des Mittels zur Zweckerreichung. Ein Mittel ist geeignet, wenn mit seiner Hilfe der gewünschte Erfolg gefördert werden kann. Dabei muss der erstrebte Erfolg nicht in jedem Einzelfall erreicht werden oder erreichbar sein, die abstrakte Möglichkeit der Zweckerreichung genügt (BVerfG, Beschluss vom 20. Juni 1984, 1 BvR 1494/78, Rn. 60). Zudem räumt das Bundesverfassungsgericht (BVerfG, Urteil vom 22. Mai 1963, 1 BvR 78/56, Rn. 141) dem Gesetzgeber einen weiten Einschätzungs- und Prognosevorrang ein, sodass ein Mittel nur dann an der Eignungsprüfung scheitert, wenn es sich »von vornherein [als] objektiv untauglich« erweist (Wienbracke 2013, S. 150).

Unter diesen Voraussetzungen wird das Eignungskriterium von polizeilichen Beobachtungsmaßnahmen allerdings quasi automatisch erfüllt. Denn kaum

infrage zu stellen ist, dass durch den Einsatz von Beobachtungstechnologien das damit verfolgte Ziel *potenziell* bzw. zumindest *in Einzelfällen* erreicht werden kann (z. B. indem einzelne Täter durch die Videobeobachtung im öffentlich zugänglichen Raum abgeschreckt bzw. ermittelt werden können, Kap. 3.4.4, oder TKÜ-Maßnahmen fallabhängig wichtige Hinweise zur Aufklärung von Straftaten liefern, Kap. 5.4.1.1). Die verfassungsrechtliche Geeignetheitsprüfung reduziert sich insofern im Wesentlichen auf einen Nachweis der *technisch-funktionalen* Eignung der jeweiligen Beobachtungstechnologie. Über den tatsächlichen Nutzen des Technologieeinsatzes für die Kriminalitätsbekämpfung sagt dies allerdings noch sehr wenig aus.

Für die grundsätzlich nur sehr schwer lösbare Aufgabe, den konkreten Sicherheitsnutzen des Einsatzes von Beobachtungtechnologien zu bestimmen, bietet der Verhältnismäßigkeitsgrundsatz daher kaum eine Orientierung. Es stellt sich die Frage, wie die Möglichkeiten für den Gesetzgeber, Aussagen zur Geeignetheit neuer polizeilicher Beobachtungspraktiken zu treffen, verbessert werden können. Ein mögliches Instrument sind Pilotprojekte, in deren Rahmen Daten und Erfahrungen für eine fundiertere Nutzenbewertung vor der eigentlichen praktischen Implementierung einer Beobachtungstechnologie gesammelt werden sollen. Pilotprojekte fanden bzw. finden beispielsweise zum Einsatz von Bodycams (Kap. 3.4.3.3), von automatisierter Videobeobachtung (Kap. 3.3.4 u. 3.5.4.3) oder von Verfahren des Predictive Policing (Kap. 4.3.2) statt, eignen sich aber nicht für alle Beobachtungstechnologien gleichermaßen (so ist ein Pilotprojekt zur Vorratsdatenspeicher nur schwer vorstellbar).

Allerdings sollte auch im Rahmen von Pilotprojekten die Eignungsbewertung für Beobachtungstechnologien nicht allein auf technisch-funktionale Kriterien beschränkt werden. Als paradigmatisches Beispiel hierfür mag die Erprobung der automatisierten Videobeobachtung zur Personenfahndung in Echtzeit im Rahmen des Pilotprojekts »Sicherheitsbahnhof Berlin Südkreuz« dienen. Laut Evaluationsbericht des Bundespolizeipräsidiums (2018) erfolgte die Eignungsbewertung im Wesentlichen anhand der gemessenen Erkennungs- und Fehlalarmraten, auf deren Grundlage dann der Einsatz der Systeme an ausgewählten Bahnhöfen empfohlen wurde (Kap. 3.5.4.3). Bei genauerer Betrachtung hängt der sicherheitsrelevante Nutzen aber von weit mehr Faktoren als nur der Erkennungsleistung der Systeme ab, etwa von spezifischen Verhaltensweisen der gesuchten Personen oder von der Frage, ob bzw. wie viele dieser Personen die videobeobachteten Bereiche überhaupt betreten (Kap. 3.5.3.3). Nicht zuletzt sind auch mögliche Konsequenzen auf die polizeiliche Einsatzpraxis in den Blick zu nehmen, die durch den Technologieeinsatz erhoffte Sicherheitsgewinne unter Umständen auch wieder schmälern können. Dies könnte etwa dann der Fall sein, wenn die Einführung der automatisierten Videobeobachtung sich negativ auf bewährte und zuverlässig funktionierende polizeiliche Einsatzpraktiken und -prozesse auswirkt

oder dazu führt, dass Erfahrungswissen der Polizeibeamten nicht mehr adäquat abgerufen wird (Kap. 7.2).

Deutlich wird, dass die Überprüfung der Geeignetheit des Einsatzes von Beobachtungstechnologien zur Kriminalitätsbekämpfung, obwohl für eine Eignungsprüfung im verfassungsrechtlichen Sinne ausreichend, nicht allein auf die jeweilige technisch-funktionale Eignung einzelner Komponenten reduziert werden kann. Eine Reduktion auf die technische Machbarkeit erscheint umso fraglicher, wenn im Kontext breit streuender Beobachtungstechnologien, wie etwa der automatisierten Videobeobachtung im öffentlich zugänglichen Raum, dem Maßnahmenerfolg in Einzelfällen regelmäßig eine große Zahl an Personen gegenübersteht, die für die Beobachtung keinen Anlass gegeben hat, aber in ihren Grundrechten eingeschränkt werden könnte.

Kasten 7.1 Gesetzgebung auf Probe

Ein anderes gesetzgeberisches Instrument ist die Gesetzgebung auf Probe, also die Einführung neuer Eingriffsbefugnisse für einen befristeten Zeitraum, deren Verlängerung von den Ergebnissen einer Evaluation abhängig gemacht wird. Eine Variante davon sind Eingriffsbefugnisse ohne zeitliche Befristung, für die aber die Durchführung einer Evaluation nach einem festgelegten Zeitraum gesetzlich vorschrieben wird. Die Gesetzgebung auf Probe ist Pilotprojekten im Charakter ähnlich, soll aber die Möglichkeiten für die Geeignetheitsprüfung verbessern, indem diese auf in der Realität gesammelte Daten und Erfahrungen abstellen kann. Das Instrument bietet sich daher vor allem dann an, wenn die Informationsgrundlage für eine Bewertung der Wirkungen (und Folgen) neuer Eingriffsbefugnisse zum Zeitpunkt der Gesetzesverabschiedung nicht ausreichen (Gusy/Kapitza 2015, S. 19 f.). Im Kontext der Sicherheitsgesetzgebung wird das Instrument der gesetzlich vorgesehenen Evaluationspflichten öfter (aber nur zum Teil in Kombination mit einer zeitlichen Befristung der Eingriffsbefugnisse) eingesetzt.[185] Gleichwohl existiert bislang kein konsentiertes Konzept hinsichtlich der Fragen, *ob* und wenn ja, *wie* Sicherheitsgesetze evaluiert werden sollen bzw. können. Oft fehlen in den jeweiligen gesetzlichen Evaluationspflichten denn auch nähere Hinweise zu Inhalten, Kriterien, Methoden und Akteuren der Evaluation (Gusy/Kapitza 2015, S. 27).

185 Beispiele für Sicherheitsgesetze mit Evaluationsvorschriften auf Bundesebene sind das Terrorismusbekämpfungsgesetz (BGBl. 2002, S. 361), das Gesetz zur Ergänzung des Terrorismusbekämpfungsgesetzes (BGBl. I 2007, S. 2) oder das Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt (BGBl. I 2008, S. 3083) (dazu ausführlich WD 2015). Ein Beispiel auf Landesebene ist § 15a PolG NRW (GV. NRW. 2013, S. 375) im Kontext der Videobeobachtung im öffentlich zugänglichen Raum.

7.3.3 Erforderlichkeit des Mittels

Ein Mittel ist erforderlich, »wenn der Gesetzgeber nicht ein anderes, gleich wirksames, aber das Grundrecht nicht oder doch weniger fühlbar einschränkendes [im Folgenden: milderes] Mittel hätte wählen können« (BVerfG, Beschluss vom 16. März 1971, 1 BvR 52, 665, 667, 754/66, Rn. 70). Mit der Prüfung der Erforderlichkeit verbindet sich also erstens die Suche nach milderen Handlungsalternativen und zweitens der Vergleich der Geeignetheit dieser Mittel zur Zweckerreichung (Wienbracke 2013, S. 151).

Der Raum der möglichen Handlungsalternativen zum Einsatz einer bestimmten Beobachtungstechnologie wird zunächst durch andere Beobachtungstechnologien aufgespannt, mit denen das verfolgte Ziel ebenso gut, aber in grundrechtsschonender Weise erreicht werden könnte. Zum Beispiel stehen verschiedene bildgebende Beobachtungstechnologien auf der Basis von IR-Strahlung, THz-Strahlung, Millimeterwellen oder Röntgenstrahlung zur Detektion von verborgenen Gegenständen oder Personen innerhalb von Objekten zur Verfügung, deren Eignung zwar nicht in sämtlichen Einsatzkontexten gleich, aber für die fraglichen Aufgaben ggf. ausreichend vergleichbar sind, sich jedoch in ihrer Eingriffstiefe teilweise unterscheiden (Kap. 3.1.1 u. 3.1.2.2).

Ein anderes Beispiel ist die automatisierte Videobeobachtung, deren Einsatzformen sich in Bezug auf die Erforderlichkeit mit der konventionellen Videobeobachtung, also der Auswertung der Bilder durch einen Videobeobachter, messen lassen müssen. Eine solche Einsatzform ist die bereits erwähnte Videobeobachtung in Verbindung mit einem Gesichtserkennungssystem, die künftig ggf. zur Personenfahndung in Echtzeit beispielsweise an ausgewählten Bahnhöfen eingesetzt werden könnte (Kap. 3.5). Die Menge der in diesem Einsatzkontext anfallenden und in Echtzeit auszuwertenden Videodaten spricht angesichts der begrenzten menschlichen Konzentrations- und Leistungsfähigkeit zunächst für eine mindestens gleich hohe bzw. höhere Wirksamkeit der automatisierten gegenüber der konventionellen Videobeobachtung für die Personenfahndung. Wie bereits angeführt, gibt es aber auch Gründe (z. B. Verhaltensanpassungen der gesuchten Personen), die Zweifel an dieser Annahme rechtfertigen (was die Erforderlichkeit der automatisierten Videobeobachtung wieder infrage stellen würde). Auch hinsichtlich der Frage, welche der beiden Maßnahmen das mildere Mittel darstellt, sind keine einfachen Antworten zu erwarten (IZEW 2017, S. 80 f.): Auf der einen Seite lässt sich argumentieren, dass die automatisierte Videobeobachtung die Aufmerksamkeit der Videobeobachter direkt auf gesuchte Personen lenkt, sodass unbeteiligte Dritte weniger in ihren Privatheitsrechten beeinträchtigt werden. Auf der anderen Seite kann der Einsatz der automatisierten Videobeobachtung – in Abhängigkeit der Zahl der videobeobachteten Personen und der gewählten Einsatzmodalitäten – zu einer hohen Zahl an Fehleralarmen führen (Kap. 3.5.3). Fehlalarme können aber für die betroffenen Personen unter

Umständen weitreichende Konsequenzen haben, etwa in Form von Personenkontrollen oder von Abfragen in polizeilichen Datenbanken. Nun kann zwar argumentiert werden, dass auch menschliche Videobeobachter Personen zuweilen falsch identifizieren. Jedoch scheint die Annahme gerechtfertigt, dass menschliche Fehler(quellen) im Vergleich zu algorithmeninduzierten schneller erkannt und korrigiert werden können. Dies dürfte insbesondere beim Einsatz von Verfahren aus dem maschinellen Lernen zutreffen, bei denen in der Regel selbst die Entwickler (und schon gar die Anwender) nicht nachvollziehen können, wie das Ergebnis zustande gekommen ist (Kap. 3.3.8.2). Dies schränkt die Möglichkeiten für die Fehlererkennung und -korrektur erheblich ein.

Gerade im Kontext von verstärkt technikbasiertem Sicherheitshandeln erscheint es wichtig, die Erforderlichkeit des Technikeinsatzes auch durch die Berücksichtigung nichttechnischer Handlungsmöglichkeiten zu prüfen. Denn festzustellen ist, dass auf Sicherheitsprobleme oft (nur) mit technischen Lösungsansätzen geantwortet wird (dazu und zum Folgenden IZEW 2017, S. 127 ff.). So erscheint insbesondere der Einsatz von Beobachtungstechnologien häufig als notwendige, gewissermaßen logische Lösung für die Eindämmung von Kriminalitätsproblemen. Dabei könnten jedoch alternative Ansätze aus dem Blickfeld geraten, die ggf. weniger stark in Grundrechte eingreifen. So kann beispielsweise die Einführung von polizeilicher Videobeobachtung an gefährdeten Orten als einmalige Erledigung des Kriminalitätsproblems gesehen werden (Matzner 2016, S. 72). Abgesehen von der bisher nicht nachgewiesenen kriminalitätspräventiven Wirkung der Videobeobachtung (Kap. 3.4.4.1) wirkt sie als Symptombekämpfung, die anders als eine Ursachenbekämpfung relativ schnell zu einem Rückgang des Kriminalitätsaufkommens in den beobachteten Räumen führen soll (so die Hoffnung). Alternative, in der Regel personalbasierte Lösungsansätze könnten hingegen stärker auf die sozialen Ursachen von Kriminalität eingehen, ohne (bzw. in einem geringeren Maße) dabei in die Grundrechte Dritter einzugreifen (Ammicht Quinn et al. 2015, S. 23). Dies umfasst etwa Maßnahmen der Sozialpolitik, Sozialarbeit, Erziehung, Pädagogik oder Aufklärung (Gusy 2017, S. 69). Nichttechnische Lösungsansätze sind in der Regel kostenintensiver und oft auch nur in einer längerfristigen Perspektive erfolgsversprechend. Sie aber deshalb als Handlungsalternativen zu technischen Lösungsansätzen außer Acht zu lassen, würde nicht nur dem Sinn von Abwägung widersprechen, sondern könnte auch zu einer Verzerrung hinsichtlich der Zweckbestimmung führen.

Entscheidend im Hinblick auf eine Überprüfung der Erforderlichkeit von Beobachtungstechnologien im Vergleich zu nichttechnischen Ansätzen ist schließlich, dass mithilfe der technisierten Beobachtung zwar die Anzahl der sicherheitsrelevanten Handlungssituationen maßgeblich erhöht werden kann. Diese Situationen müssen dann jedoch ebenfalls in ihrem sinnhaften Zusammenhang nachvollzogen, verstanden, überprüft und ggf. bewältigt werden können. Abzuwägen ist im Hinblick auf die Erforderlichkeit also immer auch, ob die schiere Menge

an technisch beobachtbaren Situationen organisatorisch überhaupt sinnvoll abgearbeitet werden kann, damit sich ein erhöhter Sicherheitsnutzen durch den Einsatz von Beobachtungstechnologien auch tatsächlich einstellen kann.

7.3.4 Angemessenheit des Mittels

Ist die Geeignetheit und Erforderlichkeit des Einsatzes einer Beobachtungstechnologie zu bejahen, muss dieser schließlich auch angemessen (verhältnismäßig im engeren Sinne) sein, um ein Übermaß an Grundrechtseinschränkungen zu verhindern. Ein gewähltes Mittel ist dann angemessen, wenn »die Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe« (BVerfG, Beschluss vom 13. Juni 2007, 1 BvR 1550/03, 2357/04, 603/05, Rn. 125) bzw. positiv formuliert »das Maß der den Einzelnen … treffenden Belastung noch in einem vernünftigen Verhältnis zu den der Allgemeinheit erwachsenden Vorteilen« (BVerfG, Beschluss vom 12. Juni 1987, 2 BvR 1226/83, 101, 313/84, Rn. 133) steht.

Das Kriterium der Angemessenheit stellt oft den schwierigsten und für subjektive Urteile anfälligsten Teil der Verhältnismäßigkeitsprüfung dar. In einem ersten Schritt sind die sich jeweils gegenüberstehenden (Rechts-)Positionen – sowohl die durch den Eingriff belasteten als auch die zu dessen Rechtfertigung bemühten – zu benennen. In einem zweiten Schritt sind die widerstreitenden Interessen gegeneinander abzuwägen. Dabei gilt: Je schwerwiegender eine Grundrechtseinschränkung ist, desto gewichtiger muss auch das mit der Maßnahme zu erreichende Ziel sein. Dabei hat der Gesetzgeber aber auch die Möglichkeit, den Grundrechtseingriff z. B. durch Ausnahmeregelungen abzumildern, um zu vermeiden, dass das verfolgte Schutzziel aufgrund einer unangemessenen Beeinträchtigung der Grundrechte Betroffener zurückstehen muss (Wienbracke 2013, S. 152 f.).

Während die Rechtsgüter, die durch eine Maßnahme geschützt werden sollen, und deren Gewichtigkeit typischerweise feststehen, sind im Vergleich dazu die nachteilig betroffenen Grundrechte und die Schwere der jeweiligen Beeinträchtigungen meist sehr viel schwieriger und aufwendiger zu bestimmen. Entscheidend dabei ist, die Angemessenheitsprüfung nicht nur auf solche Grundrechtswirkungen zu beschränken, die naheliegend sind bzw. sich unmittelbar aus dem technischen Funktionszusammenhang ergeben.

So beinhalten Beobachtungstechnologien, die zu Zwecken der polizeilichen Gefahrenabwehr oder Strafverfolgung eingesetzt werden, sehr häufig die Erhebung und Auswertung von persönlichen Daten. Dies mag der Grund sein, weshalb polizeiliche Beobachtungspraktiken in öffentlichen, politischen, rechtlichen oder auch akademischen Debatten vor allem im Hinblick auf mögliche Eingriffe in grundrechtlich geschützte Privatheitsgarantien (Kap. 6.1.2.1) problematisiert werden. Um den daraus resultierenden Schutzbedarfen Rechnung zu tragen

und damit die Angemessenheit des Einsatzes einer Beobachtungstechnologien herzustellen, werden entsprechende Beobachtungsmaßnahmen im geltenden Eingriffsrecht an hohe Eingriffsvoraussetzungen geknüpft sowie durch verfahrensmäßige, organisatorische oder technische Vorkehrungen zum Datenschutz (z. B. Benachrichtigungs- und Löschpflichten bei Datenerhebungen, Privacy-by-Design-Lösungen wie Piktogramme beim Körperscanner) oder beispielsweise zum Schutz des Kernbereich privater Lebensgestaltung bei TKÜ-Maßnahmen abgemildert. Eine Fokussierung auf Privatheitsfragen kann allerdings auch dazu führen, den Einsatz von Beobachtungstechnologien bereits dann als angemessen zu betrachten, sobald Aspekte des Privatheitsschutzes ausreichende Berücksichtigung gefunden haben (Kees 2015, S. 34). Dass dies aber unter Umständen zu kurz greift, soll im Folgenden anhand einiger Beispiele illustriert werden.

Neben Privatheitsfragen sind beispielsweise mögliche psychische Wirkungen der Beobachtung auf die beobachteten Personen zu erörtern. So werden Abschreckungs- oder Lähmungseffekte (Chillingeffekt) vermutet, die unter Umständen zu Verhaltensanpassungen führen können. Auch das Bundesverfassungsgericht zieht Einschüchterungseffekte zur Bestimmung der Eingriffsintensität von breit streuenden Beobachtungsmaßnahmen heran, so etwa bereits 1983 im Volkszählungsurteil zur Begründung des grundrechtlichen Datenschutzes überhaupt (Kap. 6.1.4). Obschon seit Jahrzehnten thematisiert, ist der empirische Forschungsstand zu möglichen Abschreckungs- oder Lähmungseffekten durch (technisierte) Beobachtung jedoch bis heute sehr unbefriedigend (Kap. 7.1). In der Rechtswissenschaft ist es daher umstritten, inwieweit potenzielle psychische Effekte für die Beurteilung der Angemessenheit staatlicher Beobachtungspraktiken herangezogen werden müssen. Allerdings hat die diesbezügliche Forschung (ausgelöst durch die Snowden-Enthüllungen) seit 2013 stark an Fahrt gewonnen, sodass die hier zu erwartenden Erkenntnisse künftig bei der Angemessenheitsprüfung adäquate Berücksichtigung finden sollten.

Diskriminierungspotenziale spielen in den gegenwärtigen Diskussionen zum staatlichen Einsatz von Beobachtungstechnologien bislang kaum eine Rolle (Kap. 6.1.5). Dabei führen einige Einsatzformen von Beobachtungstechnologien zu einer ungleichen Belastung verschiedener Bevölkerungsgruppen, auch wenn dies nicht immer offensichtlich ist. Ein Beispiel hierfür ist die Videobeobachtung im öffentlich zugänglichen Raum (z. B. an öffentlichen Plätzen oder im ÖPNV), durch welche etwa Obdachlose, für die der öffentliche zugleich der private Raum ist, unter Umständen stärker belastet werden als Passanten bzw. Fahrgäste, die solche Räume nur passieren (IZEW 2017, S. 100). Diskriminierungspotenziale werden aber vor allem im Kontext von Beobachtungstechnologien mit automatisierter Datenauswertung vermutet. Diese können hier zum einen systembedingt auftreten, etwa wenn ein auf Modellen aus dem maschinellen Lernen gestütztes Gesichtserkennungssystem für bestimmte Personengruppen eine verringerte Erkennungsleistung aufweist (Kap. 3.3.8.2). Personen dieser Gruppen wären

folglich häufiger mit (den Folgen von) Fehlalarmen konfrontiert. Zum anderen können bereits bestehende Diskriminierungspotenziale durch den Einsatz von automatisierten Beobachtungstechnologien verstärkt werden. Beispielsweise verweisen Kritiker des Predictive Policing darauf, dass sich in prognostizierten Risikogebieten aufhaltende Personen alleine durch ihre Anwesenheit unter Verdacht geraten könnten (Legnaro/Kretschmann 2015, S. 101). Dies könnte Probleme des Racial Profiling verstärken, da neben äußeren Merkmalen, die eine Person – in Abhängigkeit des jeweiligen Kontextes – als verdächtig erscheinen lassen, noch die Prognose aus dem Predictive Policing als Verdachtsmoment hinzukommt (Egbert 2018, S. 257 f.). Schließlich sind mögliche Rückkoppelungseffekte zu bedenken (Kap. 4.3.2.2): Werden bestimmte Gebiete aufgrund der Vorhersagen aus dem Predictive Policing verstärkt kontrolliert, werden auch mehr Delikte polizeilich registriert, die in polizeiliche Statistiken einfließen. Dadurch lernt der Algorithmus, dass in diesen Gebieten mehr Straftäter/innen aktiv sind, was wiederum die polizeiliche Aufmerksamkeit auf diese Gebiete lenkt. Dies kann letztlich dazu führen, dass Kriminalität ungleichmäßig verfolgt wird (Zweig 2018, S. 27).

Sind bisher überwiegend Beispiele für Grundrechtswirkungen genannt worden, die sich aus der unmittelbaren Beobachtung und den daran anknüpfenden polizeilichen Maßnahmen ergeben, können auch die eigentliche Beobachtung begleitende Maßnahmen Freiheitseinschränkungen begründen. Als Beispiel hierfür soll ein letztes Mal die automatisierte Videobeobachtung in Verbindung mit einem Gesichtserkennungssystem zur Personenfahndung in Echtzeit dienen. Voraussetzung für einen erfolgreichen Einsatz z. B. an einem Bahnhof ist, dass ein möglichst großer Anteil der Bahnhofsbesucher die videobeobachteten Bereiche passiert und dabei möglichst geradeaus in eine der Kameras blickt. Dazu könnte es erforderlich sein, die räumlichen Strukturen im beobachteten Raum anzupassen, z. B. derart, dass möglichst viele Passanten über Rolltreppen geleitet werden, über denen Kameras angebracht sind (Kap. 3.5.3.3). Dies könnte aber bereits als Einschränkung in die Bewegungs- und Handlungsfreiheit der Bahnhofsbesucher gewertet werden.

Auf die genannten und auf weitere mögliche Grundrechtswirkungen des Einsatzes von Beobachtungstechnologien soll an dieser Stelle nicht weiter eingegangen werden. Die Beispiele verdeutlichen aber die Notwendigkeit, das Spektrum der möglichen Auswirkungen staatlicher Beobachtungspraktiken über Fragen des Privatheitsschutzes hinaus zu erweitern, um sie im Rahmen einer adäquaten Verhältnismäßigkeitsprüfung zu berücksichtigen.

7.3.5 Zwischenfazit

Staatliches Sicherheitshandeln in eine angemessene Balance zwischen gesellschaftlichen Sicherheitsbedürfnissen und individuellen Freiheitsrechten zu brin-

gen, ist stets eine große Herausforderung. Der Grundsatz der Verhältnismäßigkeit stellt notwendige Schritte und Prüfkriterien bereit, die zur Herstellung eines ausgewogenen Verhältnisses zwischen den beiden konfligierenden Werten führen sollen. Gerade im Kontext des Einsatzes von Beobachtungstechnologien zu Zwecken der polizeilichen Gefahrenabwehr und Strafverfolgung aber wird deutlich, dass diese Prüfkriterien – zumindest nach bisheriger Anwendungspraxis – zum Teil zu vage sind (z. B. in Bezug auf die Bewertung der Geeignetheit polizeilicher Beobachtungspraktiken) oder große Ermessensspielräume offenlassen (z. B. in Bezug auf die zu berücksichtigenden Grundrechtswirkungen). Dies kann unter Umständen dazu führen, dass staatliche Beobachtungspraktiken, die im verfassungsrechtlichen Sinne als verhältnismäßig gelten (und somit vor dem Bundesverfassungsgericht Bestand haben), nach anderen (z. B. ethischen) Bewertungsmaßstäben ebengerade keinen angemessenen Kompromiss zwischen den Anforderungen an die Sicherheit einerseits und an die Freiheit andererseits herstellen können. Welche Anforderungen in diesem Lichte an eine erweiterte Verhältnismäßigkeitsprüfung im Kontext des Einsatzes von Beobachtungstechnologien zu stellen wären und welche Gestaltungsoptionen daraus resultieren, ist Thema in Kapitel 8.2.

8 Gestaltungsoptionen

Beobachtungstechnologien können das menschliche Wahrnehmungs- und Beurteilungsvermögen für Risiken, Gefahren oder Schäden in vielfältigster Weise erweitern. Entsprechend breit ist das Spektrum der Einsatzmöglichkeiten von Beobachtungstechnologien in ganz unterschiedlichen Bereichen der zivilen Sicherheit. Auch der potenzielle bzw. tatsächliche Nutzen und die Notwendigkeiten des Technikeinsatzes sind oftmals naheliegend, sei es z. B. die Detektion gefährlicher und für den Menschen nicht wahrnehmbarer Substanzen, die Ortung von verschütteten Personen, die Anfertigung von Luftbildern von Katastrophengebieten, die Sichtbarmachung von kriminellen Strukturen oder die Beobachtung und Aufzeichnung von Straftaten aus der Distanz (die diversen Beobachtungstechnologien und Einsatzmöglichkeiten wurden in den Kapiteln 3 bis 5 ausführlich dargestellt). Es gilt, diese grundsätzlichen technischen Potenziale weiterhin nutzbringend und verantwortungsvoll zu heben.

Aus gesellschaftlicher, politischer oder rechtlicher Perspektive ist jedoch nicht alles, was technisch möglich ist, auch in jedem Fall erstrebenswert. Der Einsatz von Beobachtungstechnologien im zivilen Sicherheitsbereich kann auch mit unerwünschten und/oder unbeabsichtigten Wirkungen und Folgen verbunden sein. Diese sind hochgradig abhängig von der betrachteten Beobachtungstechnologie, ihrem Einsatzkontext und der jeweiligen konkreten Anwendungssituation und reichen von unerwünschten Wirkungen auf die beobachteten Personen (z. B. Eingriffe in Grundrechte vor allem im Kontext von polizeilichen Einsatzformen) über technische Risiken (z. B. Gefahren für die IT-Sicherheit) bis hin zu (negativen) Effekten auf die Arbeit der Sicherheitsakteure. Es kann daher auch keine pauschal gültigen Handlungsoptionen für einen sinnvollen Einsatz von Beobachtungstechnologien im zivilen Sicherheitsbereich geben.

Es würde aber den Umfang des vorliegenden Berichts sprengen, für sämtliche der hier behandelten Beobachtungstechnologien und Einsatzfelder spezifische Handlungsoptionen zu formulieren. Ziel ist es vielmehr, im Lichte der in den vorangegangenen Kapiteln gewonnenen Erkenntnisse zentrale Punkte zu resümieren, die bei Überlegungen und Entscheidungen zur Entwicklung, zur Implementierung oder zum Einsatz von Beobachtungstechnologien im Bereich der zivilen Sicherheit Berücksichtigung finden sollten, um einen zielführenden und zugleich gesellschaftlich tragfähigen Umgang mit technisierten Beobachtungspraktiken befördern zu können. Bei den adressierten Akteuren handelt es sich entsprechend um

- die Akteure in der Forschung und Entwicklung, die die Beobachtungstechnologien bereitstellen (sowohl Forschungsförderung als auch Forschende),
- den Gesetzgeber, der im Vorfeld der Implementierung neuer grundrechtsrelevanter Beobachtungsmaßnahmen die gesetzlichen Rahmenbedingungen

schafft (angesprochen sind hier in erster Linie polizeiliche Beobachtungspraktiken), und
- die Akteure der zivilen Sicherheit, die Beobachtungstechnologien operativ einsetzen, also insbesondere die Behörden und Organisationen mit Sicherheitsaufgaben.

8.1 Akteure der Forschung und Entwicklung

Die Erforschung und (Weiter)Entwicklung von Beobachtungstechnologien und deren Anwendungsmöglichkeiten im Bereich der zivilen Sicherheit werden wesentlich durch öffentliche Gelder gefördert. Durch die entsprechenden Förderstrukturen – hier zu nennen ist insbesondere das Rahmenprogramm »Forschung für die zivile Sicherheit« der Bundesregierung – verfügt die Politik über wesentliche Einflussmöglichkeiten, um Zielrichtungen, inhaltliche Prägungen und Prioritätensetzungen in der zivilen Sicherheitsforschung mitzubestimmen.[186]

Der Forschung zu Beobachtungstechnologien ist eine gewisse Techniklastigkeit immanent, weil es um die Entwicklung von technischen Systemen zur Erweiterung des menschlichen Wahrnehmungs- und Beurteilungsvermögens geht. Zugleich besteht die Hoffnung, dass neue Beobachtungstechnologien, die nicht nur technische Ansprüche erfüllen, sondern durch die Einbindung der Ethik sowie der Rechtswissenschaft und der Sozialwissenschaften in die Technikentwicklungsprojekte den konkreten gesellschaftlichen, wirtschaftlichen und rechtlichen Anforderungen gerecht werden, bessere Chancen auf einen erfolgreichen und gesellschaftlich akzeptablen Praxiseinsatz haben. Zwei wesentliche Fragen der Forschungsförderung lauten deshalb, in welchem Stadium der Technikentwicklung der Einbezug von ethischen, sozial- und rechtswissenschaftlichen Aspekten sinnvoll bzw. notwendig ist und wie dies am besten erreicht werden kann.

Nicht nur in den mit Technik befassten Geistes- und Sozialwissenschaften sowie in den Technikwissenschaften selbst, sondern auch in der Förderpolitik besteht mittlerweile ein weitgehender Konsens, dass sich interdisziplinäres Wissen über neue Technologien am effektivsten nutzen lässt, wenn es bereits in der Phase der Technikentwicklung miteinbezogen wird. So verfolgt auch die Bundesregierung (2018k, S. 2) im aktuell laufenden Rahmenprogramm »Forschung für die zivile Sicherheit 2018–2023« das Ziel, »bei der Entwicklung von Sicherheitslösungen gesellschaftswissenschaftliche Fragestellungen von Beginn an [zu] berücksichtig[en]«. Entsprechend werden in der Regel Projektkonsortien gefördert,

186 Ein weiterer Treiber für die Entwicklung von Beobachtungstechnologien und -anwendungen ist die industrielle Forschung ohne staatliche Förderung. Diese wird nicht weiter thematisiert, da hier die politischen Einflussmöglichkeiten beschränkt sind. Politische Gestaltungsoptionen ergeben sich ggf. in der Phase der Beschaffung und Implementierung entsprechender Produkte.

in denen Technikentwickler mit Vertretern aus der Ethik, den Sozialwissenschaften oder der Rechtswissenschaft zusammenarbeiten (IZEW 2017, S. 129 f.).

Hier zum Ausdruck kommt ein Paradigmenwechsel in der öffentlich geförderten Innovationsforschung, weg von der Begleitforschung hin zur integrierten Forschung, die sowohl die Ansätze der Technikgeneseforschung (Rammert 2000) aufgreift als auch durch die Reflexion ethischer, rechtlicher und sozialer Implikationen eine »interpretative Flexibilität« (Bijker 1995) in die Technikentwicklung einbringt. Bestand der Ansatz der Begleitforschung darin, im Rahmen größerer Förderlinien der Technikentwicklung eigenständige begleitende Forschungsprojekte zur Untersuchung von gesellschafts- und/oder rechtswissenschaftlichen Aspekten des Innovationsbereichs zu fördern, verlangt die integrierte Forschung für jedes Technikentwicklungsprojekt eine interdisziplinäre Zusammenarbeit. Wohl sind beide Ansätze interdisziplinär, doch ist die integrierte Forschung besser als die Begleitforschung dazu geeignet, die verschiedenen Disziplinen miteinander zu verzahnen. Das Ziel besteht hier konkret darin, unerwünschte gesellschaftliche Wirkungen einer späteren Technologieanwendung möglichst frühzeitig zu erkennen, um sie durch technische und organisatorische Maßnahmen vermeiden bzw. abmildern zu können (im Kontext von Beobachtungstechnologien beispielweise durch die Umsetzung von Privacy-by-Design-Lösungen). Auf diese Weise sollen die Grundlagen für einen rechtskonformen und gesellschaftlich akzeptablen künftigen Praxiseinsatz gelegt werden (IZEW 2017, S. 130).

Der Ansatz der integrierten Forschung ist daher zu begrüßen und sollte verstärkt und konsequent angewendet werden. Er hat allerdings auch einige Schwächen und es ist bislang unklar, inwieweit er in der konkreten Forschungs- und Entwicklungsarbeit tatsächlich zu einer wirksamen Integration entsprechender Wertfragen führt. Beispielsweise müssen in Entwicklungsprojekten wichtige Entscheidungen über Auswahl und Ausgestaltung der zu entwickelnden Technikkomponenten häufig bereits vor Projektbeginn oder zumindest in einer frühen Projektphase getroffen werden, ohne dass ein Wissen über mögliche technische und nichttechnische Auswirkungen schon vorhanden wäre. Wird dieses Wissen erst während des Projekts erarbeitet, so sind bereits getroffene (technikbezogene) Entscheidungen nur schwer wieder rückgängig zu machen (Fraunhofer INT 2016, S. 81). Aber auch die Auswahl der nichttechnischen Aspekte bzw. der einbezogenen nichttechnischen Disziplinen muss während des Forschungs- und Entwicklungsprozesses offenbleiben, falls sich relevante Fragestellungen bzw. Probleme erst im Zuge der Entwicklung zeigen. Inwiefern integrierte Forschung die in sie gestellten Ansprüche zu erfüllen vermag, hängt damit wesentlich davon ab, wie die interdisziplinäre Zusammenarbeit methodisch operationalisiert und umgesetzt werden kann (Hempel et al. 2019). Speziell im Sicherheitsbereich gehen Entwicklungsprojekte zudem typischerweise von einem konkreten Gefahrenszenario aus, für welches eine Technologie (oder Komponenten davon) als

Unterstützungsinstrument zur Lösung des Sicherheitsproblems entwickelt werden soll. Steht aber eine für einen bestimmten Einsatzzweck entwickelte Beobachtungstechnologie erst einmal zur Verfügung, könnte sie – ggf. in Kombination mit anderen Entwicklungen – auch in anderen Anwendungskontexten eingesetzt werden, für welche aber unter Umständen ganz andere soziale, politische und rechtliche Rahmenbedingungen gelten.[187] Neben der Schwierigkeit, anwendungsübergreifende Aspekte zu berücksichtigen, sind einzelne Technikentwicklungsprojekte schließlich auch selten dazu geeignet bzw. in der Lage, technologieübergreifende Forschungsfragen zu behandeln.

Es ist daher wichtig zu betonen, dass der Ansatz einer integrierten Forschung eine gesellschafts- und rechtswissenschaftliche (Folgen-)Forschung jenseits von interdisziplinär bearbeiteten Einzelprojekten der Technologieentwicklung nicht überflüssig macht. Vielmehr müssen auch disziplinäre Kernfragen gestellt und beantwortet werden, um dieses Wissen sodann in die integrierte Forschung einfließen zu lassen. Im Kontext des Einsatzes von Beobachtungstechnologien gehören hierzu insbesondere die im Folgenden angeführten Forschungsthemen, die sich aus den in diesem Bericht identifizierten Wissenslücken ergeben.[188]

Psychische und soziale Wirkungen technisierter Beobachtung

Der Forschungsstand zu möglichen psychischen und sozialen Wirkungen und Folgen technisierter Beobachtung ist unbefriedigend (Kap. 7.1). Oft weisen die verfügbaren Studien methodische und konzeptionelle Schwächen auf und in der Gesamtschau erscheinen die Ergebnisse uneindeutig. Dies trifft auf Formen der sensorbasierten Beobachtung (z. B. Videobeobachtung), insbesondere aber auch auf Formen der datenbasierten Beobachtung (z. B. Internetbeobachtung) zu. Die empirische Forschung etwa im Zusammenhang mit Beobachtungspraktiken (ausländischer) Nachrichtendienste liefert zwar klare Anhaltspunkte für Chillingeffekte, also Verhaltensanpassungen aufgrund von Beobachtungsmaßnahmen, doch bleibt unklar, ob und inwieweit diese Befunde verallgemeinert und auf andere staatliche oder nichtstaatliche Beobachtungspraktiken übertragen werden können. Gerade Pilotprojekte (wie beispielsweise zum Einsatz automatisierter Videobeobachtung an Bahnhöfen) könnten bzw. hätten hier wichtige Erkenn-

187 Dies wäre etwa der Fall, wenn für Werksfeuerwehren zur Lokalisierung von Gefahrenpotenzialen entwickelte unbemannte Fluggeräte (siehe das Forschungsprojekt »EffFeu«; www.sifo.de/files/Projektumriss_EffFeu.pdf; 30.10.2019) mit Verfahren zur Erkennung interventionsbedürftiger Situation im ÖPNV mithilfe automatisierter Videoanalyse (siehe etwa das Forschungsprojekts »ADIS«; www.sifo.de/1948; 31.3.2022) kombiniert würden, um Gefahrensituationen während Demonstrationen zu erkennen.

188 Programmatisch sieht das aktuelle Rahmenprogramm der zivilen Sicherheitsforschung des Bundes die Bearbeitung solcher übergeordneten Forschungsfragen als Querschnittsthemen zu den drei Programmsäulen »Schutz und Rettung von Menschen«, »Schutz Kritischer Infrastrukturen« und »Schutz vor Kriminalität und Terrorismus« vor (Bundesregierung 2018k, S. 3 f.).

tnisse liefern können, um Vermutungen durch wissenschaftlich belastbares Wissen zu ersetzen.

Forschungsbedarf besteht insbesondere bezüglich der Frage, ob sich mögliche Abschreckungs- und Lähmungseffekte nur mit der Angst vor potenziellen Sanktionen erklären lassen oder sie zugleich auch eine Folge der im Zuge der Digitalisierung zunehmend allgegenwärtigen Beobachtungsmöglichkeiten durch staatliche wie auch durch private Akteure sind. Um dies zu beantworten, müssten die Mechanismen technisierter Beobachtung wesentlich gründlicher als bislang erforscht werden. Gerade im Hinblick auf Chillingeffekte sind als deren Kehrseite dann auch Gewöhnungseffekte zu berücksichtigen (Kap. 7.1.2). Es ist gerade die alltägliche Nutzung von Beobachtungstechnologien aller Art, die zur Normalisierung von technisierter Beobachtung beiträgt, Verhaltensanpassungen aufhebt und das öffentliche Problembewusstsein für mögliche Folgen der Beobachtung ggf. reduziert. Die Gefahr besteht, dass Änderungen im Verhalten nicht mehr als Anpassungen wahrgenommen werden, sondern bereits als alltägliches, allgemein anerkanntes und somit selbstverständliches Handeln gelten.

Auswirkungen auf die Technologieanwender und deren Institutionen

Beobachtungstechnologien für zivile Sicherheitsaufgaben sollen den Wahrnehmungs- und Beurteilungsprozess des Menschen möglichst integrativ unterstützen und den praktischen Anforderungen der Sicherheitsakteure entsprechen. Als Hemmnis für eine an den Bedürfnissen der Nutzer orientierte Entwicklung von Beobachtungstechnologien erweist sich ggf., dass Technologieentwickler die organisationale Praxis zu wenig kennen oder dazu tendieren, die Bedarfe der Nutzer aus ihrer technischen Sicht heraus falsch einzuschätzen. Generell empfiehlt sich daher ein nutzerzentriertes Vorgehen, damit unterschiedliche Perspektiven und Anforderungen einfließen können. Das aktuelle Rahmenprogramm der zivilen Sicherheitsforschung des Bundes unterstützt eine bedarfs- und praxisgerechte Entwicklung von Beobachtungstechnologien, indem die (künftigen) Technologieanwender in den einzelnen Technologieentwicklungsprojekten konsequent eingebunden werden. Darüber hinaus wird die Entwicklung von Trainingsmaßnahmen, Schulungsmodulen und Geschäftsmodellen sowie die Einrichtung von Innovationslaboren, Kompetenzzentren und Spitzenforschungsclustern gefördert (Bundesregierung 2018k, S. 2 f.).

Eine enge Zusammenarbeit zwischen den Entwickler/innen und (künftigen) Anwender/innen ist grundsätzlich dazu geeignet, die Entwicklung praxistauglicher Beobachtungstechnologien zu fördern. Dazu ergänzend ist es aber auch notwendig, solche Auswirkungen auf die Technologieanwender in den Blick zu nehmen, die von den jeweilig involvierten Anwendern nicht bzw. nur schwer zu antizipieren sind. Hier angesprochen sind insbesondere mögliche handlungspsychologische Effekte der Mensch-Maschine-Interaktion, die in anderen sicherheits-

relevanten Kontexten (z. B. in der Luftfahrt) intensiv beforscht werden, im Kontext des Einsatzes von Beobachtungstechnologien aber ein noch weitgehend unbearbeitetes Forschungsfeld darstellen. Hierzu zählen auch (negative) Auswirkungen des Technologieeinsatzes auf die Arbeitsorganisation, den Personaleinsatz oder die jeweiligen Wissensressourcen. So zeigt sich in anderen Sicherheitskontexten, dass solche unerwünschten Wirkungen das Ziel einer Steigerung von Sicherheit durch Technisierung auch konterkarieren können (Kap. 7.2). Die Erforschung der Auswirkungen des Einsatzes von Beobachtungstechnologien auf die Anwender und ihre Institutionen sollte daher zu einem wichtigen Querschnittsthema der zivilen Sicherheitsforschung gemacht werden, um über den Rahmen einzelner Technologieentwicklungsprojekte hinausgehend potenzielle unerwünschte Effekte erkennen und Strategien zu deren Vermeidung entwickeln zu können.

Empirische Wirkungsforschung

Auf den in vielen Fällen unbefriedigenden, oft auch stark veralteten Kenntnisstand zum konkreten sicherheitsrelevanten Nutzen bestehender polizeilicher Beobachtungsmaßnahmen zu Zwecken der Gefahrenabwehr oder Strafverfolgung wurde bereits in diesem Bericht mehrfach hingewiesen. Aber auch im Bereich der nichtpolizeilichen Gefahrenabwehr kann der in der konkreten Einsatzpraxis erzielte Nutzen unter Umständen unter den Erwartungen liegen, beispielsweise wenn der praktische Aufwand für die Implementierung und Anwendung der Beobachtungstechnologie den Nutzen aus dem erhaltenen Erkenntnisgewinn übersteigt oder der Einsatz eingespielte interne Arbeitsprozesse negativ verändert (Kap. 7.2). Die Evaluation des Nutzens technisierter Beobachtungspraktiken im zivilen Sicherheitsbereich stellt daher fortwährend ein wichtiges Forschungsdesiderat dar. Grundsätzlich müssen Evaluationen bestimmte methodische Standards erfüllen, um auch Vergleichbarkeit (und damit Metaevaluationen) zu ermöglichen und bei entsprechenden Erweiterungen des Einsatzes wiederholt werden zu können. Gerade die Reproduzierbarkeit von Ergebnissen muss dabei ein leitendes Kriterium sein.

Aktueller Anwendungsumfang und konkrete Einsatzpraktiken

Wie bereits gezeigt, liegen über das tatsächliche Ausmaß der Anwendung von Beobachtungstechnologien im Bereich der zivilen Sicherheit und die konkreten Einsatzpraktiken – wenn überhaupt – oft nur fragmentierte oder veraltete Informationen vor. Dies betrifft erwartungsgemäß polizeiliche Beobachtungspraktiken zur verdeckten Informationsbeschaffung, für die es gute Gründe gibt, entsprechende Informationen zurückzuhalten. Es trifft aber auch für viele andere technisierte Beobachtungspraktiken zu, für die solche Gründe nicht immer ersichtlich sind, wie beispielsweise die offene Videobeobachtung im öffentlich

zugänglichen Raum. Die Debatten über das Für und Wider des Einsatzes von Beobachtungstechnologien basieren daher oft auf Vermutungen und spekulativen Annahmen hinsichtlich der Technologien und tatsächlichen Einsatzpraxis. Dabei wohnt gerade Beobachtungstechnologien mit automatisierter Datenauswertung wie dem Predictive Policing das Potenzial inne, intransparent zu werden und in ihren immer komplexeren Prozessen selbst für Experten nicht mehr einfach nachvollziehbar zu sein.

Wo dies die Datenlage erlaubt, könnten systematische empirische Erhebungen zum aktuellen Umfang der Anwendung und zur konkreten Einsatzpraxis von Beobachtungstechnologien einen wichtigen Beitrag zur Fundierung der Debatten liefern, um nicht zuletzt auch das Zusammenwirken unterschiedlicher Beobachtungstechnologien und die Auswirkungen dieses Zusammenwirkens besser beurteilen zu können.

Grundlegende Fragestellungen

Nicht zuletzt gilt es, auch grundlegende Fragestellungen und Herausforderungen, die sich im Zusammenhang mit staatlichem Sicherheitshandeln stellen, im Rahmen der (öffentlich geförderten) zivilen Sicherheitsforschung zu bearbeiten: Wie sind Sicherheitsrisiken und -bedrohungen im Lichte gestiegener gesellschaftlicher Sicherheitsbedürfnisse zu bewerten? Sind (technikvermittelte) Sicherheitslösungen immer die richtige Antwort auf (neue) Sicherheitsprobleme? Wie verändert staatliches (und auch nichtstaatliches) Sicherheitshandeln die Gesellschaft? Auch wenn solche Fragestellungen über das Thema Beobachtungstechnologien (und damit den Fokus dieses Berichts) weit hinausgehen, so ist deren Einsatz immer als Teil eines Gesamtkonzepts staatlicher Sicherheitsgewährleistung zu sehen. Für die hier notwendig zu führenden gesellschaftlichen und politischen Diskussionen kann die ethische, sozial- und rechtswissenschaftliche Forschung wichtige Beiträge liefern.

8.2 Gesetzgeber

Die Herstellung von Sicherheit kann mit Eingriffen in individuelle Freiheitsrechte verbunden sein. Die Verantwortung, staatliches Sicherheitshandeln in ein ausgewogenes Verhältnis zwischen Sicherheit und Freiheit zu bringen, fällt vorrangig dem Gesetzgeber zu, der die hierfür notwendigen gesetzlichen Eingriffsbefugnisse zu schaffen hat. Dabei ist der Grundsatz der Verhältnismäßigkeit zu beachten, der verlangt, dass der Staat mit jedem Grundrechtseingriff einen legitimen Zweck mit geeigneten, erforderlichen und angemessenen Mitteln verfolgt (Kap. 6.2). Wie allerdings am Beispiel des Einsatzes von Beobachtungstechnologien durch Polizeibehörden zu Zwecken der Gefahrenabwehr und Strafverfolgung deutlich wurde, erweisen sich die vom Bundesverfassungsgericht ange-

legten Prüfmaßstäbe teilweise als unzureichend, um über die Verhältnismäßigkeit von polizeilichen Beobachtungsmaßnahmen auch nach gesellschaftlichen (z. B. ethischen) Bewertungskriterien entscheiden zu können (Kap. 7.3). Für den Gesetzgeber leiten sich daraus verschiedene Gestaltungsoptionen ab, die im Wesentlichen auf eine Erweiterung der verfassungsrechtlichen Verhältnismäßigkeitsüberprüfung hinauslaufen.

Methoden und Kriterien für eine adäquate Überprüfung der Geeignetheit entwickeln

Im Kontext des Einsatzes von Beobachtungstechnologien reduziert sich die verfassungsrechtliche Geeignetheitsüberprüfung im Wesentlichen auf den Nachweis der technisch-funktionalen Eignung der jeweiligen Beobachtungstechnologie (Kap. 7.3.2). Der sicherheitsrelevante Nutzen von polizeilichen Beobachtungsmaßnahmen hängt jedoch in den allermeisten Fällen von weit mehr Faktoren ab. Dazu zählen z. B. die jeweiligen konkreten räumlichen und sozialen Anwendungskontexte der Beobachtung, das Verhalten der beobachteten Personen oder mögliche Auswirkungen der Maßnahmen auf die bestehenden polizeilichen Einsatzpraktiken und -prozesse. Zu diesen Faktoren liegen vor der Implementierung neuer Beobachtungsmaßnahmen oftmals nur unzureichende bzw. keine praktischen Erfahrungen oder empirischen Daten vor. Durch diesen Informationsmangel wird die Aufgabe, den konkret zu erwartenden Sicherheitsnutzen geplanter Maßnahmen abzuschätzen, erheblich erschwert.

Zur Verbesserung der Informationsgrundlagen stehen dem Gesetzgeber im Wesentlichen zwei Möglichkeiten zur Verfügung. Zum einen können Pilotprojekte zu geplanten Maßnahmen durchgeführt werden, in deren Rahmen Daten und Erfahrungen für eine fundierte Nutzenbewertung vor dem eigentlichen Gesetzgebungsverfahren gesammelt werden. Pilotprojekte fanden bisher meist auf Initiative der Behörden statt, sie können aber prinzipiell auch im gesetzlichen Auftrag erfolgen. Wichtig dabei ist, dass auch im Rahmen von Pilotprojekten die Geeignetheitsüberprüfung nicht – wie zuweilen festzustellen ist – allein auf technisch-funktionalen Kriterien abstellt (Kap. 7.3.2). Zum anderen kann der Gesetzgeber neue Eingriffsbefugnisse für einen befristeten Zeitraum einführen und eine Verlängerung von den Ergebnissen einer durchzuführenden Evaluation abhängig machen (Gesetzgebung auf Probe).[189] Dieses Instrument empfiehlt sich etwa dann, wenn sich Pilotprojekte zur Eignungsüberprüfung nicht anbieten (z. B. im Kontext der Vorratsdatenspeicherung). Zwar sind gesetzliche Evaluationspflichten im Bereich der Sicherheitsgesetzgebung keine Seltenheit, doch ist bislang kein klares Konzept in Bezug auf Kriterien und Methoden der Evaluation erkennbar (Kap. 7.3.2).

189 Eine Variante davon sind Eingriffsbefugnisse ohne zeitliche Befristung, aber mit einer gesetzlich vorgeschriebenen Evaluation nach einem festgelegten Zeitraum.

Daher wären sowohl für Pilotprojekte zu geplanten als auch für nachträgliche Evaluationen zu bestehenden polizeilichen Beobachtungsmaßnahmen zunächst methodische Mindestanforderungen und Maßstäbe für eine adäquate Eignungsüberprüfung zu entwickeln. Methodisch sinnvoll und anzustreben wären Ansätze, die auf die jeweiligen konkreten Einsatzsituationen anwendbar sind und es ermöglichen, die den jeweiligen technischen, rechtlichen, ethischen und sozialwissenschaftlichen Diskursen entstammenden Bewertungsdimensionen nicht nur im Hinblick auf ihre jeweilige Erfüllung oder Nichterfüllung, sondern auch in ihren Wechselwirkungen integriert zu betrachten. Dabei sind in die Analyse auch alle polizeilichen Einsatz- und Organisationsprozesse miteinzubeziehen, die zwar unabhängig von der zu überprüfenden Beobachtungsmaßnahme sind, durch den Technologieeinsatz aber möglicherweise (negativ) beeinflusst werden. Der diesbezügliche Handlungsbedarf ist trotz bestehender Sicherheitsforschung nach wie vor groß.

Daran anknüpfend wären im Fall von Pilotprojekten die jeweiligen Untersuchungskonzepte anzupassen bzw. im Fall von gesetzlichen Evaluationspflichten geeignete gesetzliche Rahmenbedingungen zu schaffen, damit die nötigen praktischen Erfahrungen und empirischen Daten gesammelt werden können.

Handlungsalternativen bedenken

Mit der Prüfung der Erforderlichkeit des Einsatzes einer bestimmten Beobachtungstechnologie zum Zweck der Kriminalitätsbekämpfung verbindet sich stets die Suche nach grundrechtsschonenderen, aber in Bezug auf die Zweckerreichung gleich wirksamen Handlungsalternativen. Neben der Prüfung anderer Beobachtungstechnologien sollten immer auch nichttechnische Handlungsmöglichkeiten mitbedacht werden, die stärker auf die sozialen Ursachen von Kriminalität eingehen (z. B. Maßnahmen der Sozialpolitik, Erziehung oder Aufklärung). Nichttechnische Maßnahmen wirken zwar oft nur langfristig, haben aber im Gegensatz zu Beobachtungstechnologien, die eher der Symptomerfassung bzw. -bekämpfung dienen, das Potenzial, gesellschaftliche Problemlagen zu beseitigen und insofern Sicherheitshandeln im Zeitverlauf obsolet zu machen.

So, wie es zurzeit an geeigneten Methoden und Maßstäben für die Überprüfung der Geeignetheit des Einsatzes einzelner Beobachtungstechnologien fehlt, gilt dies erst recht für eine vergleichende Betrachtung verschiedener Handlungsalternativen zur Kriminalitätsbekämpfung. Damit die für die Geeignetheitsprüfung zu entwickelnden Methoden sowohl die Vergleichbarkeit zwischen verschiedenen Beobachtungspraktiken als auch zwischen technischen und nichttechnischen Handlungsansätzen ermöglichen können, müssten sie die jeweiligen Wirkungen und Folgen längerfristig erfassen bzw. abschätzen und einander gegenüberstellen können.

Spektrum der berücksichtigten Folgewirkungen erweitern

Der polizeiliche Einsatz von Beobachtungstechnologien wird in aktuellen Debatten vor allem im Hinblick auf mögliche Eingriffe in grundrechtlich geschützte Privatheitsgarantien problematisiert. Die Fokussierung auf Privatheitsfragen birgt aber unter Umständen die Gefahr, dass Beobachtungsmaßnahmen bereits dann als angemessen betrachtet werden, sobald daraus resultierenden Schutzbedarfen ausreichend Rechnung getragen wurde (z. B. durch Vorkehrungen zum Datenschutz). Allerdings kann der staatliche Einsatz von Beobachtungstechnologien je nach Anwendungsform und Einsatzkontext weitere Grundrechte berühren, etwa wenn potenzielle Einschüchterungseffekte die Bereitschaft zur freien Meinungsäußerung mindern oder der Einsatz von Beobachtungstechnologien mit automatisierter Datenauswertung mit Diskriminierungen für bestimmte Personengruppen einhergeht. Eine adäquate Verhältnismäßigkeitsprüfung sollte daher stets das gesamte Spektrum der möglichen Auswirkungen und (grundrechtsrelevanten) Folgen für die Betroffenen berücksichtigen. Dies unterstreicht die Notwendigkeit, den diesbezüglichen Wissensstand durch eine Stärkung der gesellschafts- und rechtswissenschaftlichen (Folgen-)Forschung weiter auszubauen.

Kontinuierliche Verhältnismäßigkeitsüberprüfungen

Die Bewertung der Verhältnismäßigkeit von polizeilichen Beobachtungspraktiken hängt von den jeweiligen technischen und sozialen Rahmenbedingungen ab, die allerdings einem kontinuierlichen Wandel unterliegen. Daher gilt es, bei der Verhältnismäßigkeitsüberprüfung nicht nur kurzfristige, sondern auch langfristig relevante Wirkungen und Folgen der jeweiligen Beobachtungsmaßnahme in den Blick zu nehmen. Langfristige Effekte können aber gerade vor dem Hintergrund der großen Dynamiken in der Technikentwicklung und -nutzung nur äußerst schwer antizipiert werden. So wurden beispielsweise die strafprozessualen Befugnisse zur Telekommunikationsüberwachung vor über 50 Jahren eingeführt (Kap. 2.5.2) und dazu zuletzt durchgeführte Evaluationen basieren auf empirischen Daten, die mittlerweile über 20 Jahre alt sind (Kap. 5.4). Angesichts des starken Wandels sowohl in technischer Hinsicht als auch in Bezug auf das Kommunikationsverhalten und -aufkommen kann stark bezweifelt werden, dass die damals vorgenommenen Wirkungs- und Folgenabschätzungen heute noch Bestand haben.

Vor diesem Hintergrund sollte der Gesetzgeber die Überprüfung der Verhältnismäßigkeit staatlicher Beobachtungspraktiken nicht nur als einmalige Verpflichtung während des Gesetzgebungsverfahrens, sondern vielmehr als eine fortwährende Aufgabe verstehen. Eine Möglichkeit dazu böten gesetzlich beauftragte, in regelmäßigen Zeitabständen (z. B. alle 10 Jahre) durchgeführte Evaluationen der Wirkungen und Folgen bestehender Beobachtungspraktiken, die das übergeordnete Ziel haben, ggf. vorhandene gesetzgeberische Anpassungsbedarfe

zu identifizieren. Im angesprochenen Beispiel der Telekommunikationsüberwachung könnte dies unter Umständen sogar die Notwendigkeit aufzeigen, den grundrechtlichen Schutz elektronischer Kommunikationsinhalte gänzlich neu zu konzipieren, indem nach technisch und sozial anschlussfähigeren Kriterien für die Sensibilität digitaler Inhalte gesucht wird (Kap. 6.1.2.1).

Überprüfung der Verhältnismäßigkeit im Gesamtkontext aller polizeilichen Beobachtungsmaßnahmen

Die Überprüfung der Verhältnismäßigkeit polizeilicher Beobachtungspraktiken erfolgt jeweils isoliert für einzelne Maßnahmen. Allerdings können Personen gleichzeitig von mehreren Beobachtungsmaßnahmen betroffen sein. Hierzu ein fiktives, aber realitätsnahes Beispiel: Ein Besucher eines Risikospiels im Fußball wird bei der An- und Abreise und im Stadion von zahlreichen Videokameras erfasst, seine Internetaktivitäten auf einschlägigen Fanseiten können Gegenstand von polizeilicher Internetbeobachtung sein und seine Mobilfunknummer wird, weil er sich zufällig in räumlicher Nähe zu gewalttätigen Ausschreitungen befand, ggf. im Rahmen einer Funkzellenabfrage erhoben und zur Bestimmung seiner Personalien verwendet. Aus der Verhältnismäßigkeit jeder einzelnen Beobachtungsmaßnahme kann jedoch nicht auf die Verhältnismäßigkeit der Summe der Einzelmaßnahmen geschlossen werden, da diese miteinander wechselwirken, wodurch sich ihre Wirkungen und Folgen in komplexer Weise verstärken oder abmildern können. Im gewählten Beispiel könnte die mehrfache Beobachtung zu unbegründeten Verdachtsmomenten gegen den Spielebesucher führen, ebenso aber auch ihn entlastende Informationen liefern.

Die äußert schwierige, aber notwendige Aufgabe besteht also darin, die Verhältnismäßigkeit polizeilicher Beobachtung jeweils unter Betrachtung des Gesamtkontextes aller Beobachtungsmaßnahmen zu überprüfen. Dies gilt umso mehr, als der künftig verstärkt zu erwartende Einsatz von immer leistungsfähigeren Verfahren der Datenerfassung und -auswertung die Möglichkeiten der Verknüpfung und Analyse von Daten aus unterschiedlichsten Quellen erheblich erweitert und in Kombination mit der stetig anwachsenden Fülle an Informationsquellen in der digitalen Gesellschaft eine neue Qualität an *potenzieller* Beobachtung schafft.

Die hier notwendig zu führenden Debatten sollten sich dabei auch nicht der Frage verschließen, ob in der Gesamtbetrachtung der Wirkungen und Folgen ggf. auf einzelne bereits bestehende polizeiliche Beobachtungsmaßnahmen künftig verzichtet werden könnte bzw. müsste.

8.3 Akteure der zivilen Sicherheit

Gestaltungsmöglichkeiten zur Förderung eines gesellschaftlich tragfähigen Umgangs mit Beobachtungstechnologien im Bereich der zivilen Sicherheit gibt es schließlich für die Akteure, die die Technologien im Rahmen ihrer jeweiligen Aufgaben und Befugnisse in der Praxis anwenden. Dazu zählen insbesondere Behörden und Organisationen mit Sicherheitsaufgaben und deren Einsatzkräfte, darüber hinaus aber auch beispielsweise Strafverfolgungsbehörden, Gerichte oder die jeweiligen Aufsichtsbehörden wie Innen- oder Justizministerien.

Evaluation bestehender Beobachtungspraktiken

Die zentrale Aufgabe, den Erkenntnisstand zu den Wirkungen und Folgen bestehender Beobachtungspraktiken im zivilen Sicherheitsbereich auszubauen, richtet sich nicht nur an die Forschung oder an den Gesetzgeber. Auch BOS und/oder die jeweiligen Aufsichtsbehörden auf Bundes- und Landesebene sollten – über ggf. vorhandene gesetzliche Evaluationspflichten hinaus – den Einsatz von Beobachtungstechnologien regelmäßig auf den Prüfstand stellen. Gerade hier bieten sich gute Voraussetzungen, um mögliche nichtintendierte Wirkungen der Technologieanwendung (z. B. nachteilige Effekte auf die internen Arbeitsprozesse) zu erkennen, den Ressourceneinsatz und damit die Wirtschaftlichkeit der Beobachtungsmaßnahmen zu bewerten und die Frage zu klären, ob die aufgewendeten Mittel im Verhältnis zu den erlangten Erkenntnissen stehen bzw. ob konventionelle Sicherheitsarbeit im Rahmen der vorhandenen Ressourcen bessere Wirkungen entfalten könnte. Hierfür wäre es wichtig, dass die zur Durchführung erfolgreicher Evaluationen notwendigen Rahmenbedingungen geschaffen werden. Insbesondere wäre dafür Sorge zu tragen, dass die erforderlichen empirischen Daten und Erfahrungen immer unter Wahrung des Datenschutzes gesammelt werden (können) und den mit der Evaluation beauftragten Instanzen möglichst vollumfänglich zur Verfügung stehen.[190]

Die Evaluationsergebnisse sollten anderen Sicherheitsakteuren, der Wissenschaft und – im Sinne der Transparenz – der allgemeinen Öffentlichkeit zugänglich gemacht werden.

Kompetenzaufbau bei Technologieanwendern und darüber hinaus

Angesichts einer steigenden Komplexität bei vielen Beobachtungstechnologien ist dafür Sorge zu tragen, dass die Aus- und Weiterbildung der Technologieanwender der Entwicklung nicht hinterherhinkt. Insbesondere der künftig zu

190 Beispielsweise wurde die Evaluation der Befugnisse des Bundeskriminalamts durch unabhängige Wissenschaftler durch den Umstand erheblich erschwert, dass die zu den Vorgängen gehörenden Akten und Datenbestände bereits gelöscht bzw. vernichtet worden waren oder der Zugang zu den Informationen gesperrt war (Kap. 5.4.2).

erwartende verstärkte Einsatz leistungsfähiger Algorithmen zur automatisierten Datenerfassung und -auswertung (z. B. im Bereich des Internetbeobachtung oder des Predictive Policing; Kap. 4) erfordert spezielle Fähigkeiten in den Bereichen Modellierungstheorie und -verständnis, Annahmenkritik und Rekontextualisierung, um eine sinnvolle Interpretationsarbeit an den Datenquellen und Analyseergebnissen zu leisten (Hempel/Rehak 2017, S. 149). Aber auch im Kontext (vermeintlich) einfach anwendbarer Beobachtungstechnologien sollte der Bedarf an Aus- und Fortbildung bzw. an Einsatztraining nicht unterschätzt werden. Zum Beispiel gehen die erforderlichen Kompetenzen eines Videobeobachters über die technische Bedienung der Kameras weit hinaus. Die Komplexität seiner Tätigkeit ergibt sich vielmehr aus der Notwendigkeit, die auf seinen Monitoren dargestellten Räume durch die erneute Anreicherung mit Informationen zu rekontextualisieren. Dazu ist Wissen über den beobachteten Raum notwendig, vor allem aber auch praktisches Erfahrungswissen, das durch intensives Training und den Austausch mit erfahrenen Videobeobachtern aufgebaut werden kann bzw. muss (Kap. 7.2.2).

Notwendig erscheint aber nicht nur ein entsprechender Kompetenzaufbau bei den unmittelbar mit der Technologieanwendung betrauten Personen. Um eine effektive Kommunikation über die entsprechenden Beobachtungsmaßnahmen und deren Ergebnisse zwischen den verschiedenen Dienstebenen, Behörden und Organisationen zu ermöglichen, sollte ein Mindestmaß an Systemverständnis bei allen Akteuren, deren berufliche Tätigkeit mit dem Technologieeinsatz im Zusammenhang steht, vorhanden sein. Beispielsweise können Maßnahmen der Quellen-TKÜ oder Onlinedurchsuchung aufgrund ihrer hohen Komplexität nur von speziell dafür geschulten Fachleuten durchgeführt werden (Kap. 5.2.3). Aber auch etwa Staatsanwälte und Richter, die solche Maßnahmen beantragen, anordnen und kontrollieren müssen, benötigen ein Systemverständnis, das zumindest so weit reicht, dass ein rechtskonformer Einsatz der Maßnahmen gewährleistet bleibt.

Zum Kompetenzaufbau gehört immer auch die Sensibilisierung der Technologieanwender für die Limitationen und Begrenzungen von Beobachtungstechnologien. Anderenfalls besteht ggf. die Gefahr, dass deren Funktions- und Leistungsfähigkeit überschätzt wird, unrealistische Nutzenerwartungen entstehen oder Beobachtungsdaten bzw. Analyseergebnisse, die Informationen aus anderen Quellen oder den eigenen Erfahrungen widersprechen, nicht mehr kritisch hinterfragt werden. Das Bewusstsein dafür, dass Beobachtungstechnologien den menschlichen Wahrnehmungs- und Beurteilungsprozess unterstützen, nicht aber ersetzen können, muss erhalten bleiben (vgl. Knobloch 2018, S. 39, zum Predictive Policing).

Umgang mit automatisierten Beobachtungstechnologien

Besondere Herausforderungen stellen sich im Kontext des (geplanten) Einsatzes von Beobachtungstechnologien mit automatisierter Datenauswertung (z. B. automatisierte Videobeobachtung; Kap. 3.3 u. 3.5, teilautomatisierte Social Media Intelligence; Kap. 4.2, Ansätze des Predictive Policing; Kap. 4.3). Hier stellen sich ähnliche Fragen wie in anderen Anwendungsfeldern der künstlichen Intelligenz, etwa im Zusammenhang mit der Robotik, autonomen Fahrzeugen oder autonomen Waffensystemen.

Ein zentrales Problem stellt die Frage der Verantwortungszuschreibung dar: Obschon als Systeme zur Entscheidungs*unterstützung* ausgelegt, sprechen verschiedene Gründe dafür, dass das Prinzip der menschlichen Letztverantwortung bei automatisierten Beobachtungstechnologien zunehmend untergraben werden könnte (Kap. 7.2.5). Wenn aber eine individuelle Verantwortungszuschreibung nicht mehr gegeben ist, kann niemand für unrechtmäßige oder unmoralische Handlungen zur Rechenschaft gezogen werden. Eine individuelle Verantwortungszuschreibung ist jedoch gerade im Sicherheitskontext von essentieller Bedeutung, da Sicherheitshandeln mitunter tiefgreifende Grundrechtseingriffe legitimieren kann. Wie in anderen Feldern auch bleibt hier die schwierige Frage zu diskutieren, wie eine geteilte Verantwortung zwischen Menschen und technischen Systemen genau aussehen könnte. Hierbei kann Verantwortung nicht (allein) den jeweiligen Technologieanwendern zugeschrieben werden, sondern es müssen neue Formen geteilter Verantwortung gefunden werden, die auch andere Akteure, wie etwa die beteiligten Unternehmen und Programmierer oder die jeweiligen Sicherheitsbehörden, mit einbeziehen.

Zusätzlich gilt es Wege und Lösungen zu finden, wie die Qualität der hier eingesetzten Softwareprodukte (weiter) verbessert bzw. garantiert werden kann, um unerwünschte Wirkungen durch ggf. unzuverlässig funktionierende oder fehlerhaft arbeitende Algorithmen möglichst zu vermeiden. Dies ist vor allem für Softwareprodukte aus dem maschinellen Lernen eine schwierige Aufgabe (Kap. 3.3.8). Ansätze und Vorschläge dafür sind etwa die Schaffung unabhängiger Instanzen zur Kontrolle der Systeme (Algorithmen-TÜV), die Etablierung einer Berufsethik für die Entwickler solcher Algorithmen oder die Entwicklung von besonderen Trainingsmaßnahmen für die Systemanwender (Zweig 2018, S. 29 ff.). Solche Ansätze sollten intensiv weiterverfolgt und -entwickelt werden. Bereits jetzt sollte als Mindestanforderung für im Sicherheitsbereich eingesetzte Softwaresysteme gelten, dass diese die Bedingungen, die für eine unabhängige Überprüfung notwendig sind, erfüllen. Eine solche Bedingung wäre beispielsweise, dass die Daten, die zum Training der Systeme benutzt wurden, für die Öffentlichkeit, für Forschende oder staatliche Akteure zugänglich sind, um sie auf Vollständigkeit, Diskriminierungsfreiheit und Korrektheit überprüfen zu können (Zweig 2018, S. 29 f.).

Ausgleich zwischen den Zielen der zivilen und IT-Sicherheit

Der Einsatz von informationstechnischen Beobachtungsverfahren für zivile Sicherheitsaufgaben steht häufig mit den Zielen der IT-Sicherheit in Konflikt: Während die IT-Sicherheit den Anspruch hat, Daten und informationstechnische Systeme durch Schutzkonzepte zu härten, erfordert es die zivile Sicherheit, die Schutzkonzepte ggf. auch umgehen zu können (Hempel/Rehak 2017, S. 137).

Ein aus Sicht der zivilen Sicherheit wesentliches Problemfeld ergibt sich beispielsweise aus dem Umstand, dass potenzielle Straftäter/innen ihre Kommunikation und/oder Daten zunehmend durch Verschlüsselung vor staatlichen Zugriffen wirksam schützen können. Dieser Herausforderung kann im Wesentlichen auf zwei verschiedene Arten begegnet werden. Eine Möglichkeit besteht in einer Schwächung existierender Verschlüsselungsstandards, z. B. durch ein Verbot starker Verschlüsselungsverfahren (Kap. 5.2.1.3). Dies würde jedoch die IT-Sicherheit insgesamt erheblich gefährden, sodass an der bisher von der Bundesregierung verfolgen Strategie, von jeglicher Schwächung der Verschlüsselung abzusehen, unbedingt festgehalten werden sollte.

Die andere Möglichkeit besteht in der Durchführung von Maßnahmen der Quellen-TKÜ oder Onlinedurchsuchung (Kap. 5.2.3). Durch die Notwendigkeit der heimlichen Installation einer Beobachtungssoftware auf dem Endgerät birgt dieser Ansatz Risiken für die IT-Sicherheit auch anderer informationstechnischer Systeme. In diesem Zusammenhang zu problematisieren ist insbesondere die Ausnutzung von Schwachstellen in der Software (Kap. 5.2.3.4). Durch eine umsichtige Vorgehensweise, die sich gleichermaßen an den Zielen der zivilen Sicherheit *und* jenen der IT-Sicherheit orientiert, lassen sich diese Risiken allerdings erheblich reduzieren. So könnte beispielsweise eine Verwendung von Schwachstellen mit hohem Gefährdungspotenzial für die IT-Sicherheit kategorisch ausgeschlossen werden, also insbesondere solche, die dem Softwarehersteller noch nicht bekannt sind (Zero-Day-Schwachstellen). Eine ausschließliche Nutzung öffentlich bekannter Schwachstellen mit geringem Gefährdungspotenzial für die IT-Sicherheit würde die Durchführung der Maßnahmen zwar erschweren, nicht aber verunmöglichen. Bislang fehlt es jedoch an einer tragfähigen Strategie für den staatlichen Umgang mit Schwachstellen in der Software. Diese Aufgabe sollte – nicht zuletzt auch angesichts der 2017 ausgeweiteten strafprozessualen Befugnisse für Maßnahmen der Quellen-TKÜ und Onlinedurchsuchung (Kap. 5.3) – dringend angegangen werden.

Vertrauensbildende und transparenzfördernde Maßnahmen

Obgleich der empirische Forschungsstand zu den psychischen und sozialen Wirkungen staatlicher Beobachtung (namentlich im Kontext von polizeilichen Beobachtungspraktiken) noch sehr lückenhaft ist (Kap. 7.1), lässt sich mit Blick auf die teils sehr kontrovers geführten öffentlichen Debatten zum Thema konsta-

tieren, dass staatliche Beobachtungspraktiken das Potenzial haben, bei Bürger/innen auch ein Gefühl der Verunsicherung auszulösen. Angesprochen sind hier in erster Linie polizeiliche Beobachtungsmaßnahmen und/ oder solche Formen der Beobachtung, bei denen davon (potenziell) betroffene Personen nicht nachvollziehen können, ob sie tatsächlich beobachtet werden (und ggf. durch wen). Bei der Videobeobachtung im öffentlich zugänglichen Raum beispielsweise markieren Kameras und Hinweisschilder zwar die Beobachtung, gleichwohl ist nicht klar, ob die Bilder zeitgleich durch einen Menschen (oder künftig ggf. durch einen Algorithmus) ausgewertet, lediglich gespeichert oder aber gar nicht aufgezeichnet (Kameraattrappe) werden. Andere Formen der Beobachtung, vor allem solche der Internet- oder informationstechnischen Beobachtung, finden häufig ohne Wissen der Betroffenen statt. Ob, wann und zu welchem Zweck jemand beobachtet wird, kann kaum überprüft werden – im Bewusstsein bleibt einzig die Möglichkeit, dass man beobachtet werden *könnte*. Gerade heimlich stattfindende Formen der Beobachtung können im Zusammenspiel mit unzureichendem Wissen über die jeweiligen Beobachtungstechnologien bzw. -verfahren, die rechtlichen Voraussetzungen und Grenzen ihres Einsatzes und den tatsächlichen Umfang der praktischen Anwendung bei Bürger/innen Sorgen auslösen, die zum Teil auf falschen Annahmen beruhen und somit unbegründet sind.

Zu unterstreichen ist die Bedeutung des gesellschaftspolitischen Diskurses um Sicherheit und den Einsatz entsprechender Sicherheitstechnologien: Verlangt Sicherheitshandeln das Vertrauen von Bürger/innen in die Sicherheitsbehörden, so umfasst dies selbstverständlich auch den behördlichen Einsatz von Beobachtungstechnologien. Dies gilt umso mehr, wenn Technologien zur Verarbeitung von Massendaten genutzt werden, die potenziell auch eine anlasslose Beobachtung erlauben. Das Vertrauen in Sicherheitsbehörden ist ein hohes Gut, das oftmals schwer erworben wird, aber auch (schnell) Schaden nehmen kann. Um es zu erhalten, müssen die Praktiken des Einsatzes gerade für diejenigen, zu deren Schutz sie eingesetzt werden, transparent und nachvollziehbar sein. Es muss von vornherein sichergestellt sein, dass sich die Rechtmäßigkeit des Einsatzes auch im Nachhinein noch feststellen lässt und auch ethische und gesellschaftliche Wertfragen berücksichtigt wurden.

Es sollte daher (grundsätzlich) nach Wegen gesucht werden, um einer in der Bevölkerung ggf. vorhandenen Verunsicherung entgegenzuwirken. Eine Möglichkeit dazu wären vertrauensbildende Maßnahmen, mit denen beispielsweise die Einführung neuer polizeilicher Beobachtungsmaßnahmen flankiert werden. Ziel wäre insbesondere die Informationsvermittlung, um aus Wissensdefiziten und falschen Vorstellungen ggf. resultierenden Unsicherheitsgefühlen vorzubeugen. Dies betrifft mindestens folgende Aspekte:

- technische Funktionsweisen,
- verfolgte Zwecke und Erforderlichkeit der Beobachtungsmaßnahme,
- handelnde Akteure und Umfang der geplanten Anwendung,

- unerwünschte Wirkungen und Folgen (z. B. Grundrechtseingriffe) sowie
- technische, organisatorische und rechtliche Vorkehrungen zur Abmilderung unerwünschter Wirkungen.

Eine weitere Möglichkeit wären transparenzfördernde Maßnahmen für bereits bestehende Einsatzformen. Die derzeit von Regierungen und Behörden auf Bundes- und Landesebene zumeist verfolgte Informationspolitik scheint nicht zwingend geeignet, Verunsicherungen zu mildern. So liegen zur polizeilichen Einsatzpraxis von Beobachtungstechnologien – sofern keine gesetzlichen Berichtspflichten bestehen – bislang kaum öffentlich zugängliche Informationen vor. Wenn überhaupt, finden sich solche Angaben in Parlamentsdokumenten, namentlich in Regierungsantworten auf entsprechende parlamentarische Anfragen, die allerdings auch nur fragmentarische Einblicke in die polizeiliche Einsatzpraxis erlauben: Zum einen erfolgt die Berichterstattung sehr uneinheitlich, zum anderen werden diesbezügliche Auskünfte teilweise als Verschlusssache einstuft. Eine (zu) defensive Informationspolitik und insbesondere das Vorenthalten von Informationen gegenüber der Öffentlichkeit tragen aber wenig zum Abbau von Verunsicherung bei. Es wäre also nach Wegen zu suchen, wie durch eine proaktivere Informationspolitik die Transparenz polizeilicher Beobachtungspraktiken erhöht werden könnte, ohne gleichzeitig durch die Preisgabe von zu vielen Informationen die operativen Fähigkeiten der Polizeibehörden zu schwächen. Ist vor diesem Hintergrund beispielsweise das Zurückhalten von konkreten Informationen zur technischen und taktischen Vorgehensweise bei Maßnahmen der Quellen-TKÜ und Onlinedurchsuchung gut nachvollziehbar, so trifft dies nicht vorbehaltlos auf die Nennung von bloßen Fallzahlen zu (Kap. 5.4.1.5 u. 5.4.2). Denn wenn potenziellen Straftäter/innen die Möglichkeiten und Fähigkeiten der Polizeibehörden klar vor Augen geführt werden, kann dies ggf. auch eine kriminalpräventive Wirkung entfalten, indem Täter/innen in ihren Kommunikationsmöglichkeiten eingeschränkt werden und so die Durchführung ihrer Taten erschwert oder im besten Fall sogar verhindert wird.

Nicht zuletzt könnten vertrauensbildende und transparenzfördernde Maßnahmen zu einer »Demystifizierung« (Knobloch 2018, S. 40) staatlicher Beobachtungspraktiken beitragen. Lässt sich dadurch wohl niemals Übereinstimmung bei allen gesellschaftlichen Gruppen herstellen, so sind Verständnis und Transparenz über die Funktionsweisen, das Ausmaß sowie die Wirkungen und Folgen technisierter Beobachtung notwendige und bedeutende Voraussetzungen für eine informierte gesellschaftliche Verständigung über einen zielführenden und zugleich gesellschaftlich akzeptablen Einsatz von Beobachtungstechnologien im Bereich der zivilen Sicherheit.

9 Literatur

9.1 In Auftrag gegebene Gutachten

Hempel, L. (2016): Beobachtungstechnologien im Bereich der zivilen Sicherheit. Möglichkeiten und Herausforderungen zwischen situational awareness (Lagebewusstsein) und situativem Handeln. Berlin

Fraunhofer INT (Fraunhofer-Institut für Naturwissenschaftlich-Technische Trendanalysen) (2016): Beobachtungstechnologien im Bereich der zivilen Sicherheit – Möglichkeiten und Herausforderungen: Forschungslandschaft. (Römer, S., mit Beiträgen von Müller, S.; Suwelack, K.-W.). Euskirchen

Hempel, L.; Rehak, R. (2017): Beobachtungstechnologien im Bereich der zivilen Sicherheit. Möglichkeiten und Herausforderungen von Verfahren informationstechnisch vernetzter Beobachtung. Berlin

IZEW (Internationales Zentrum für Ethik in den Wissenschaften) (2017): Soziale und psychologische Wirkungen technisierter Beobachtung (Ammicht Quinn, R.; Heesen, J.; Pawelec, M.; Hauschild, A.; unter Mitarbeit von Baur-Ahrens, A.; Booz, S.; Burkhardt, A.; Erben, S.; Gabel, F.; Grote, T.; Hagendorff, T.; Krüger, M.; Nadolski, S.; Spindler, M.; Tilling, A.; Zinsmaier, J.). Tübingen

Bäcker, M. (2019): Kommentargutachten zum TAB-Arbeitsbericht »Beobachtungstechnologien im Bereich der zivilen Sicherheit - Möglichkeiten und Herausforderungen«. Mainz

9.2 Weitere Literatur

Albers, M. (2015): Zukunftsszenarien polizeilicher Überwachung. In: Lichdi, J. (Hg.): Digitale Schwellen. Privatheit und Freiheit in der digitalen Welt. Weiterdenken – Heinrich-Böll-Stiftung Sachsen, S. 135-147

Albrecht, H.-J. (2010): Geheime Ermittlungsmaßnahmen im Strafprozess – Entwicklungen im Spannungsfeld von Sicherheit und Freiheitsrechten. Vortrag.

Albrecht, H.-J.; Brunst, P.; Busser, E.; Grundies, V.; Rinceanu, J.; Kenzel, B.; Nikolova, N.; Rotino, S.; Tauschwitz, M. (2011): Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten. Freiburg, www.mpg.de/5000721/vorratsdatenspeicherung.pdf (28.10.2019)

Albrecht, H.-J.; Dorsch, C.; Krüpe, C. (2003): Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen. Abschlussbericht. Freiburg

Albrecht, H.-J.; Grafe, A.; Kilchling, M. (2008): Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO. Forschungsbericht im Auftrag des Bundesministeriums der Justiz. Freiburg

Albrecht, H.-J.; Poscher (2017): Evaluationsbericht zu den §§ 4a, 20j, 20k des Bundeskriminalamtgesetzes. Unterrichtung durch die Bundesregierung. Deutscher Bundestag (Hg.), Drucksache 18/13031, Berlin

Alexandrie, G. (2017): Surveillance cameras and crime. A review of randomized and natural experiments. In: Journal of Scandinavian Studies in Criminology and Crime Prevention 18(2), S. 210–222

Ammicht Quinn, R. (Hg.) (2014): Sicherheitsethik. Wiesbaden

Ammicht Quinn, R.; Koch, H.; Held, C.; Matzner, T.; Krumm, J.; Flack, J.; Hälterlein, J.; Markel, P.; Möllers, N.; Wittmann, P. (2015): Intelligente Videoüberwachung: eine Handreichung. IZEW Materialien Band 11. Tübingen. https://publikationen.uni-tuebingen.de/xmlui/handle/10900/67099 (29.10.2019)

Amnesty International (2015): Global opposition to USA big brother mass surveillance, www.amnesty.org/en/latest/news/2015/03/global-opposition-to-usa-big-brother-mass-surveillance/ (16.05.2019)

Angerer, C. (2018): Neuronale Netze. Revolution für die Wissenschaft? In: Spektrum der Wissenschaft 2018(1), S. 12–21

Ariel, B.; Sutherland, A.; Henstock, D.; Young, J.; Drover, P.; Sykes, J.; Megicks, S.; Henderson, R. (2016): Wearing body cameras increases assaults against officers and does not reduce police use of force: Results from a global multi-site experiment. In: European Journal of Criminology 13(6), S. 744–755

Bäcker, M. (2015): Kriminalpräventionsrecht. Eine rechtsetzungsorientierte Studie zum Polizeirecht, zum Strafrecht und zum Strafverfahrensrecht. Jus Publicum 247, Tübingen

Bäcker, M.; Giesler, V.; Harms, M.; Hirsch, B.; Kaller, S.; Wolff, H. (2013): Bericht der Regierungskommission zur Überprüfung der Sicherheitsgesetzgebung in Deutschland vom 28. August 2013, www.bmjv.de/SharedDocs/Downloads/DE/Fachinformationen/Bericht_RegKom_Sicherheitsgesetzgebung.pdf (28.10.2019)

Bateson, M.; Nettle, D.; Roberts, G. (2006): Cues of being watched enhance cooperation in a real-world setting. In: Biology letters 2(3), S. 412–414

Bäuerle, M. (2008): Polizeirecht in Deutschland. In: APuZ 2008(48), S. 15–20

Bayerische Staatsregierung (2013): Videoüberwachung in Bayern. Antwort des Staatsministeriums des Innern vom 01.02.2013 auf die Schriftliche Anfrage der Abgeordneten Christine Kamm BÜNDNIS 90/DIE GRÜNEN vom 24.09.2012. Bayerischer Landtag, Drucksache 16/15571, München

Bayerische Staatsregierung (2017): Videoüberwachung in Bayern. Antwort des Staatsministeriums des Innern, für Bau und Verkehr vom 05.12.2016 auf die Schriftliche Anfrage der Abgeordneten Katharina Schulze, Verena Osgyan BÜNDNIS 90/DIE GRÜNEN vom 27.10.2016. Bayerischer Landtag, Drucksache 17/14658, München

Bayerl, P. S.; RüdigerT.-G. (2017): Die polizeiliche Nutzung sozialer Medien in Deutschland: Die Polizei im digitalen Neuland. In: Stierle, J.; Wehe, D.; Siller, H. (Hg.): Handbuch Polizeimanagement: Polizeipolitik – Polizeiwissenschaft – Polizeipraxis. Wiesbaden, S. 919–943

BBK (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe) (o.J. a): Die Analytische Task Force (ATF) des Bundes, www.bbk.bund.de/DE/AufgabenundAusstattung/CBRNSchutz/ATF/ATF_node.html (28.10.2019)

BBK (o.J. b): Mess- und Nachweistechnik, www.bbk.bund.de/DE/AufgabenundAusstattung/CBRNSchutz/Biologie/BMundNwtechn/bmundnwtechn_node.html (28.10.2019)

BBK (2016): Rahmenkonzeption für den CBRN-Schutz (ABC-Schutz) im Bevölkerungsschutz, www.bbk.bund.de/SharedDocs/Kurzmeldungen/BBK/DE/2016/Rahmenkonzeption_CBRN_Schutz_im_BevSchutz.html (28.10.2019)

BBK (2017): Rahmenempfehlungen für den Einsatz von Social Media im Bevölkerungsschutz, www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Broschueren_Flyer/Rahmenempf_Einsatz_Social_Media_BevS.html (31.10.2019)

BBK (2019a): Die Analytische Task Force. Informationen zu Leistungsspektrum und Anforderungen. www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/CBRN-Schutz/ATF_Informationen_zu_Leistungsspektrum_und_Anforderungswegen.pdf (28.10.2019)

BBK (2019b): Empfehlungen für Gemeinsame Regelungen zum Einsatz von Drohnen im Bevölkerungsschutz. https://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Broschueren_Flyer/Empfehlungen_Geme_Regelungen_Drohneneinsatz_BevS.pdf (21.5.2021)

BDK (Bund Deutscher Kriminalbeamter) (2018): Forschungsprogramm LiDaKrA. Internetartikel des Bundes Deutscher Kriminalbeamter vom 9.7.2015, zuletzt verändert am 15.5.2018, www.bdk.de/der-bdk/aktuelles/artikel/bdk-beteiligt-sich-im-forschungsprogramm-lidakra (28.10.2019)

Bedner, M. (2009): Rechtmäßigkeit der »Deep Packet Inspection«. Projektgruppe verfassungsverträgliche Technikgestaltung (provet). Universität Kassel, http://kobra.bibliothek.uni-kassel.de/bitstream/urn:nbn:de:hebis:34-2009113031192/5/BednerDeepPacketInspection.pdf (28.1.2020)

Bennett Moses, L.; Chan, J. (2018): Algorithmic prediction in policing: assumptions, evaluation, and accountability. In: Policing and Society 28(7), S. 806–822

Benöhr-Laqueur, S. (2018): 2018 – das Jahr, in dem die deutsche Polizei erstmals Drohnen gegen Gefährder einsetzte. In: TATuP 27(3), S. 14–19

Beuth, P. (2016): Apple versus FBI: Eine politische Niederlage für das FBI. In: Zeit Online 22.3.2016, www.zeit.de/digital/datenschutz/2016-03/apple-fbi-iphone-hacken-geht-doch (28.10.2019)

Beuth, P. (2017): Microsoft: Supreme Court entscheidet über die Zukunft der Cloud. In: Zeit Online 16.10.2017, www.zeit.de/digital/datenschutz/2017-10/microsoft-supreme-court-warrant-case-cloud (28.10.2019)

BfS (Bundesamt für Strahlenschutz) (2019): Strahlenschutzaspekte bei Ganzkörperscannern, www.bfs.de/DE/themen/emf/hff/quellen/ganzkoerperscanner/ganzkoerperscanner_node.html (28.10.2019)

BfV (Bundesamt für Verfassungsschutz) (o.J.): Gemeinsames Internetzentrum (GIZ), www.verfassungsschutz.de/de/arbeitsfelder/af-islamismus-und-islamistischer-terrorismus/gemeinsames-internetzentrum-giz (28.10.2019)

Bijker, W. (1995): Of Bicycles, Bakelites, and Bulbs: Toward a Theory of Sociotechnical Change. Cambridge

Bitkom (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.) (2018): Neun von zehn Internetnutzern verwenden Messenger. Pressemitteilung vom 2.5.2018, www.bitkom.org/Presse/Presseinformation/Neun-von-zehn-Internetnutzern-verwenden-Messenger.html (28.10.2019)

BKA (Bundeskriminalamt) (o.J.a): Politisch motivierte Kriminalität, www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/PMK/pmk_node.html (28.10.2019)

BKA (o.J.b): Koordinierte Internetauswertung (KIA), www.bka.de/DE/UnsereAufgaben/Kooperationen/KIA/kia_node.html (28.10.2019)

BKA (2007): Forschungsprojekt. Gesichtserkennung als Fahndungshilfsmittel. Foto-Fahndung. Abschlussbericht. Wiesbaden, www.bka.de/SharedDocs/Downloads/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Forschung/FotoFahndung/fotofahndungAbschlussbericht.pdf (28.10.2019)

BKA (2018): Mindestspeicherfristen und ihre Bedeutung für die Kriminalitätsbekämpfung. Aktuelle Meldung vom 11. Juni 2018, www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/180611_MINDESTSPEICHERFRISTEN.html (28.10.2019)

BMBF (Bundesministerium für Bildung und Forschung) (2012): Forschung für die zivile Sicherheit 2012 – 2017. Rahmenprogramm der Bundesregierung, www.bmbf.de/pub/rahmenprogramm_sicherheitsforschung_2012.pdf (28.10.2019)

BMI (Bundesministerium des Innern, für Bau und Heimat) (2016): Cyber-Sicherheitsstrategie für Deutschland. Berlin, www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (28.1.2020)

BMI (2017): Blick von oben öffnet neue Perspektiven für den Bevölkerungsschutz. Experten diskutieren Rahmenbedingungen für Unbemannte Luftfahrtsysteme als innovative Zukunftstechnologie im Bevölkerungsschutz. Meldung vom 27. Juni 2017, www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2017/06/uas-workshop.html (28.10.2019)

BMI (2018): Projekt zur Gesichtserkennung erfolgreich. Testergebnisse veröffentlicht – Systeme haben sich bewährt. Pressemittelung vom 11.10.2018, www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2018/10/gesichtserkennung-suedkreuz.html (28.10.2019)

Bogk, A. (2007): Antwort zum Fragenkatalog zur Verfassungsbeschwerde 1 BvR 370/07 und 1 BvR 95/07. Chaos Computer Club

BondGraham, D. (2015): Oakland Mayor Schaaf and Police Seek Unproven 'Predictive Policing' Software. In: East Bay Express 24.6.2015, www.eastbayexpress.com/oakland/oakland-mayor-schaaf-and-police-seek-unproven-predictive-policing-software/Content?oid=4362343 (28.10.2019)

Bornewasser, M.; Schulz, F. (2008): Videoüberwachung öffentlicher Straßen und Plätze: Ergebnisse eines Pilotprojekts im Land Brandenburg. Frankfurt am Main

Bossong, R.; Hegemann, H. (2017): Die Politik der zivilen Sicherheit: Bedeutungen und Wirkungen eines aufstrebenden Begriffs. In: Zeitschrift für Außen- und Sicherheitspolitik 10(1), S. 39–65

Brühl, J. (2018): Gotham am Main. In: Süddeutsche Zeitung, 18.10.2018, www.sueddeutsche.de/wirtschaft/innere-sicherheit-gotham-am-main-1.4175521 (28.10.2019)

Bruker Optik GmbH (2017): SIGIS 2. Long Distance Identification, Visualization and Quantification of Gases, www.bruker.com/fileadmin/user_upload/8-PDF-Docs/OpticalSpectrospcopy/RemoteSensing/SIGIS2/Brochures/SIGIS2_Brochure_EN.pdf (28.10.2019)

BSI (Bundesamt für Sicherheit in der Informationstechnik) (o.J.): Gesichtserkennung. www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Gesichtserkennung_pdf.pdf (28.10.2019)

BSI (2017): Die Lage der IT-Sicherheit in Deutschland 2017. www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf (28.10.2019)

BSI (2018): Lebenszyklus einer Schwachstelle. www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_027.pdf (28.10.2019)

BSI; ConSecur GmbH (2002): Leitfaden zur Einführung von Intrusion-Detection-Systemen. Grundlagen. www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/IDS/Grundlagenv10_pdf.html (28.1.2020)

Buchenau, S.; Rüffer, M. (2019): Feuerwehr Drohne im Einsatz: Fakten und Hinweise. In: Feuerwehr-Magazin 29.8.2019. www.feuerwehrmagazin.de/wissen/feuerwehr-drohnen-im-einsatz-53634 (28.10.2019)

Buermeyer, U. (2017a): Gutachterliche Stellungnahme zur Öffentlichen Anhörung des Gesetzentwurfs der Fraktionen der CDU/CSU und der SPD zur Neustrukturierung des Bundeskriminalamtgesetzes. BT-Drucksache 18/11163 im Innenausschuss des Deutschen Bundestages am 20. März 2017. www.bundestag.de/blob/498672/bb3800be0e6419eee6fe18abc37dd626/18-4-806-e-data.pdf (28.10.2019)

Buermeyer, U. (2017b): Gutachterliche Stellungnahme zur Öffentlichen Anhörung zur »Formulierungshilfe« des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess. Ausschuss-Drucksache 18(6)334 im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages am 31. Mai 2017, www.bundestag.de/resource/blob/508848/bdf7512e32578b699819a5aa33dde93c/buermeyer-data.pdf (28.10.2019)

Bundesnetzagentur (2017): Digitale Transformation in den Netzsektoren. Aktuelle Entwicklungen und regulatorische Herausforderungen. www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Bundesnetzagentur/Publikationen/Berichte/2017/Digitalisierung.pdf (28.10.2019)

Bundesnetzagentur (2018): Jahresbericht 2017. Netze für die Zukunft. www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Bundesnetzagentur/Publikationen/Berichte/2018/JB2017.pdf (28.10.2019)

Bundesnetzagentur (2019): Jahresbericht 2018. 20 Jahre Verantwortung für Netze. www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Bundesnetzagentur/Publikationen/Berichte/2019/JB2018.pdf (28.10.2019)

Bundesnetzagentur (2021): Jahresbericht 2020. Märkte im digitalen Wandel. https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Jahresberichte/JB2020.pdf (24.2.2022)

Bundespolizeipräsidium (2018): Teilprojekt 1 »Biometrische Gesichtserkennung« des Bundespolizeipräsidiums im Rahmen der Erprobung von Systemen zur intelligenten Videoanalyse durch das Bundesministerium des Innern, für Bau und Heimat, das Bundespolizeipräsidium, das Bundeskriminalamt und die Deutsche Bahn AG am Bahnhof Berlin Südkreuz im Zeitraum vom 01.08.2017 – 31.07.2018. www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung_down.pdf (28.10.2019)

Bundesregierung (2001): Bericht der Bundesregierung zu den Auswirkungen der Nutzung kryptografischer Verfahren auf die Arbeit der Strafverfolgungs- und Sicherheitsbehörden (Ziffer 4 der Eckpunkte der deutschen Kryptopolitik vom 2. Juni 1999) »Verschlüsselungsbericht«. www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/2002-06-06/anlage-15.pdf (28.10.2019)

Bundesregierung (2010): Ausmaß von staatlicher und privater Videoüberwachung. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte, Ulla Jelpke, Jens Petermann, Halina Wawzyniak und der Fraktion DIE LINKE. – Drucksache 17/2349 –. Deutscher Bundestag, Drucksache 17/2750, Berlin

Bundesregierung (2011): Auskunft über Einsatz staatlicher Schadprogramme zur Computerspionage (»Staatstrojaner«). Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte, Andrej Hunko, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 17/7104 –. Deutscher Bundestag, Drucksache 17/7760, Berlin

Bundesregierung (2012): Computergestützte Kriminaltechnik bei Polizeibehörden. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan Korte, Herbert Behrens, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 17/8257 –. Deutscher Bundestag, Drucksache 17/8544 (neu), Berlin.

Bundesregierung (2013a): Kooperation von Behörden im Bereich der Inneren Sicherheit. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Sevim Dagdelen, Heidrun Dittrich, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 17/14766 –. Deutscher Bundestag, Drucksache 17/14830, Berlin

Bundesregierung (2013b): Neuere Formen der Überwachung der Telekommunikation durch Polizei und Geheimdienste. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan Korte, Wolfgang Gehrcke, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 17/14515 –. Deutscher Bundestag, Drucksache 17/14714, Berlin

Bundesregierung (2013c): Antwort des Staatssekretärs Klaus-Dieter Fritsche vom 5. April 2013 auf die schriftliche Frage des Abgeordneten Jan Korte (DIE LINKE.). Schriftliche Fragen mit den in der Woche vom 8. April 2013 eingegangenen Antworten der Bundesregierung. Deutscher Bundestag, Drucksache 17/13046, Berlin

Bundesregierung (2014a): Einsätze von sogenannten stillen SMS, WLAN-Catchern, IMSI-Catchern, Funkzellenabfragen sowie Software zur Bildersuche im ersten Halbjahr 2014. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan Korte, Herbert Behrens, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 18/1991 –. Deutscher Bundestag, Drucksache 18/2257, Berlin

Bundesregierung (2014b): Rechtmäßigkeit des Versandes von »Stillen SMS«. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan Korte, Jan van Aken, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 18/2504 –. Deutscher Bundestag, Drucksache 18/2695, Berlin.

Bundesregierung (2015a): Anstrengungen von Europol, INTERPOL und der Europäischen Kommission zum Aushebeln von Verschlüsselungstechniken. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Wolfgang Gehrcke, Jan van Aken, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 18/5013 –. Deutscher Bundestag, Drucksache 18/5144, Berlin.

Bundesregierung (2015b): Einsätze von sogenannten stillen SMS, WLAN-Catchern, IMSI-Catchern, Funkzellenabfragen sowie Software zur Bildersuche im ersten Halbjahr 2015. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan Korte, Jan van Aken, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 18/5509 –. Deutscher Bundestag, Drucksache 18/5645, Berlin

Bundesregierung (2015c): Einsätze von sogenannten stillen SMS, WLAN-Catchern, IMSI-Catchern, Funkzellenabfragen sowie Software zur Bildersuche im zweiten Halbjahr 2014. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan Korte, Wolfgang Gehrcke, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 18/3905 –. Deutscher Bundestag, Drucksache 18/4130, Berlin

Bundesregierung (2016a): Einsätze von sogenannten stillen SMS, WLAN-Catchern, IMSI-Catchern, Funkzellenabfragen sowie Software zur Bildersuche im ersten Halbjahr 2016. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeor-

dneten Andrej Hunko, Jan Korte, Frank Tempel, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 18/9258 –. Deutscher Bundestag, Drucksache 18/9366, Berlin

Bundesregierung (2016b): Beobachtungsansätze der Sicherheitsbehörden in sozialen Netzwerken und im sogenannten »Darknet«. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Martina Renner, Frank Tempel, Dr. André Hahn, Ulla Jelpke und der Fraktion DIE LINKE. – Drucksache 18/9386 –. Deutscher Bundestag, Drucksache 18/9487, Berlin

Bundesregierung (2016c): Die Strategie der Bundesregierung zur Bekämpfung der Internetkriminalität – Gemeinsames Internetzentrum. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Petra Pau, Jan Korte, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 17/5557 –. Deutscher Bundestag, Drucksache 17/5695, Berlin

Bundesregierung (2016d): Einsätze von sogenannten stillen SMS, WLAN-Catchern, IMSI-Catchern, Funkzellenabfragen sowie Software zur Bildersuche im zweiten Halbjahr 2015. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Frank Tempel, Jan van Aken, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 18/7166 –. Deutscher Bundestag, Drucksache 18/7285, Berlin

Bundesregierung (2016e): EU-Maßnahmen für den Zugang von Strafverfolgungsbehörden zu verschlüsselter Kommunikation. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan Korte, Christine Buchholz, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 18/9919 –. Deutscher Bundestag, Drucksache 18/10148, Berlin

Bundesregierung (2016f): Weitere europäische Anstrengungen zur möglichen Aushebelung verschlüsselter Telekommunikation. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Frank Tempel, Annette Groth, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 18/8686 –. Deutscher Bundestag, Drucksache 18/8929, Berlin.

Bundesregierung (2017a): Betrieb von Körperscannern auf deutschen Flughäfen. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Jan Korte, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 19/66 –. Deutscher Bundestag, Drucksache 19/153, Berlin

Bundesregierung (2017b): Die Copernicus Strategie der Bundesregierung. Copernicus für Deutschland und Europa – Strategie und Handlungsfelder der Bundesregierung für eine erfolgreiche Umsetzung des europäischen Erdbeobachtungsprogramms. www.bmvi.de/SharedDocs/DE/Anlage/DG/Digitales/copernicus-strategie-bundesregierung.pdf (28.10.2019)

Bundesregierung (2017c): Einsatz und Verwendung von Accounts in Kommunikationsnetzwerken durch Bundesbehörden der Polizei und den Zoll. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Martina Renner, Dr. André Hahn, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 19/35 –. Deutscher Bundestag, Drucksache 19/116, Berlin

Bundesregierung (2017d): Einsätze von sogenannten »Stillen SMS«, WLAN-Catchern, IMSI-Catchern, Funkzellenabfragen sowie Software zur Bildersuche im zweiten Halbjahr 2016. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan Korte, Jan van Aken, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 18/10824 –. Deutscher Bundestag, Drucksache 18/11041, Berlin

Bundesregierung (2017e): Einsätze von sogenannten Stillen SMS, WLAN-Catchern, IMSI-Catchern, Funkzellenabfragen sowie Software zur Bildersuche im ersten Halbjahr 2017. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan Korte, Annette Groth, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 18/13036 –. Deutscher Bundestag, Drucksache 18/13205, Berlin

Bundesregierung (2017f): Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes – Erhöhung der Sicherheit in öffentlich zugänglichen großflächigen Anlagen und im öffentlichen Personenverkehr durch optisch-elektronische Einrichtungen (Videoüberwachungsverbesserungsgesetz). Gesetzentwurf der Bundesregierung. Deutscher Bundestag, Drucksache 18/10941, Berlin

Bundesregierung (2017g): Internationale Herausgabe sogenannter elektronischer Beweismittel. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan van Aken, Eva Bulling-Schröter, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 18/10763 –. Deutscher Bundestag, Drucksache 18/10948, Berlin

Bundesregierung (2017h): Techniken zur Internetermittlung bei der Polizeiagentur Europol. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Annette Groth, Inge Höger, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 18/13194 –. Deutscher Bundestag, Drucksache 18/13310, Berlin.

Bundesregierung (2018a): Biometrie und Datenschutz nach der EU-Datenschutz-Grundverordnung. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Niema Movassat, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 19/3726 –. Deutscher Bundestag, Drucksache 19/3931, Berlin

Bundesregierung (2018b): Einsatz von Spähsoftware bei der Strafverfolgung (Quellen-Telekommunikationsüberwachung und Online-Durchsuchung). Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Katja Keul, Dr. Konstantin von Notz, Luise Amtsberg, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache 19/1810 –. Deutscher Bundestag, Drucksache 19/2306, Berlin

Bundesregierung (2018c): Einsätze von sogenannten Stillen SMS, WLAN-Catchern, IMSI-Catchern, Funkzellenabfragen sowie Software zur Bildersuche im ersten Halbjahr 2018. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Anke Domscheit-Berg, Heike Hänsel, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 19/3221 –. Deutscher Bundestag, Drucksache 19/3678, Berlin

Bundesregierung (2018d): Einsätze von sogenannten stillen SMS, WLAN-Catchern, IMSI-Catchern, Funkzellenabfragen sowie Software zur Bildersuche im zweiten Halbjahr 2017. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Martina Renner, Dr. André Hahn, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 19/316 –. Deutscher Bundestag, Drucksache 19/505, Berlin

Bundesregierung (2018e): Informationsaustausch im Gemeinsamen Terrorismusabwehrzentrum (GTAZ) von Bund und Ländern und seine rechtlichen Grundlagen. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Benjamin Strasser, Stephan Thomae, Grigorios Aggelidis, weiterer Abgeordneter und der

Fraktion der FDP – Drucksache 19/3273 –. Deutscher Bundestag, Drucksache 19/3530, Berlin

Bundesregierung (2018f): Informationstechnische Überwachung durch Bundeskriminalamt und Zoll. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Martina Renner, Ulla Jelpke, Jan Korte, Niema Movassat und der Fraktion DIE LINKE. – Drucksache 19/314 –. Deutscher Bundestag, Drucksache 19/522, Berlin

Bundesregierung (2018g): Linksextreme Internetseiten. Antwort der Bundesregierung auf die Kleine Anfrage des Abgeordneten Enrico Komning und der Fraktion der AfD – Drucksache 19/3788 –. Deutscher Bundestag, Drucksache 19/4025, Berlin

Bundesregierung (2018h): Nicht vollstreckte Haftbefehle als Gefahr für die innere Sicherheit 2018. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Irene Mihalic, Luise Amtsberg, Canan Bayram, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache 19/2576 –. Deutscher Bundestag, Drucksache 19/2914, Berlin.

Bundesregierung (2018i): Personenpotentiale islamistischer »Gefährder«. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 19/5202 –. Deutscher Bundestag, Drucksache 19/5648, Berlin

Bundesregierung (2018j): Predictive Policing in Deutschland. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Benjamin Strasser, Manuel Höferlin, Konstantin Kuhle, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/1234 –. Deutscher Bundestag, Drucksache 19/1513, Berlin

Bundesregierung (2018k): Rahmenprogramm der Bundesregierung »Forschung für die zivile Sicherheit 2018 – 2023«. Unterrichtung durch die Bundesregierung. Deutscher Bundestag, Drucksache 19/2910, Berlin

Bundesregierung (2018l): Rechtsgrundlagen und Einsatz der Quellen-Telekommunikationsüberwachung. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Konstantin Kuhle, Jimmy Schulz, Manuel Höferlin, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/1020 –. Deutscher Bundestag, Drucksache 19/1505, Berlin

Bundesregierung (2018m): Satellitenüberwachung beim G20-Gipfel. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Ulla Jelpke, Michel Brandt, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 19/1142 –. Deutscher Bundestag, Drucksache 19/1437, Berlin

Bundesregierung (2018n): Antwort des Staatssekretärs Dr. Helmut Teichmann vom 25. Juli 2018 auf die Frage des Abgeordneten Alexander Ulrich (DIE LINKE.). Schriftliche Fragen mit den in der Woche vom 23. Juli 2018 eingegangenen Antworten der Bundesregierung. Deutscher Bundestag, Drucksache 19/3592, Berlin

Bundesregierung (2018o): Staatliches Hacking von Internetkommunikation – Transparenz rechtlicher und tatsächlicher Voraussetzungen. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Konstantin von Notz, Luise Amtsberg, Canan Bayram, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache 19/982 –. Deutscher Bundestag, Drucksache 19/1434, Berlin

Bundesregierung (2018p): Umfang des parlamentarischen Fragerechts zu Rechtsgrundlagen und Einsatz der Quellen-Telekommunikationsüberwachung (Nachfrage zur Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 19/1505). Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten

Konstantin Kuhle, Manuel Höferlin, Jimmy Schulz, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/2247 –. Deutscher Bundestag, Drucksache 19/2907, Berlin

Bundesregierung (2018q): Verdeckte Fahndungen mithilfe des Schengener Informationssystems. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Dr. Diether Dehm, Anke Domscheit-Berg, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 19/994 –. Deutscher Bundestag, Drucksache 19/1261, Berlin

Bundesregierung (2019a): Antwort des Staatssekretärs Hans-Georg Engelke vom 4. März 2019 auf die schriftliche Frage des Abgeordneten Martin Hess (AfD). Schriftliche Fragen mit den in der Woche vom 4. März 2019 eingegangenen Antworten der Bundesregierung. Deutscher Bundestag, Drucksache 19/8180, Berlin

Bundesregierung (2019b): Einsatz und Verwendung von Accounts in Kommunikationsnetzwerken durch Bundesbehörden. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Martina Renner, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 19/6596 –. Deutscher Bundestag, Drucksache 19/7163, Berlin

Bundesregierung (2019c): Einsätze von sogenannten Stillen SMS, WLAN-Catchern, IMSI-Catchern, Funkzellenabfragen sowie Software zur Bildersuche im zweiten Halbjahr 2018. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Martina Renner, Heike Hänsel, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 19/7104 –. Deutscher Bundestag, Drucksache 19/7847, Berlin

Bundesregierung (2019d): Nutzung von Kfz-Kennzeichenerfassungssystemen durch deutsche Sicherheitsbehörden. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Konstantin von Notz, Dr. Irene Mihalic, Stefan Gelbhaar, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache 19/9313 –. Deutscher Bundestag, Drucksache 19/9705, Berlin

Bundesregierung (2019e): Antwort des Parlamentarischen Staatssekretärs Dr. Günter Krings vom 9. April 2019 auf die Frage der Abgeordneten Martina Renner (DIE LINKE.). Schriftliche Fragen mit den in der Woche vom 23. April 2019 eingegangenen Antworten der Bundesregierung. Deutscher Bundestag, Drucksache 19/9692, Berlin

Bundesregierung (2019f): Antwort des Staatssekretärs Klaus Vitt vom 23. Mai 2019 auf die Frage des Abgeordneten Dr. Diether Dehm (DIE LINKE.). Schriftliche Fragen mit den in der Woche vom 27. Mai 2019 eingegangenen Antworten der Bundesregierung. Deutscher Bundestag, Drucksache 19/10535, Berlin

Bundesregierung (2019g): Global vernetzter Online-Rechtsextremismus – Sicherheitsarchitektur und Prävention. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Petra Pau, Dr. André Hahn,Doris Achelwilm, weiterer Abgeordneter und der Fraktion DIE LINKE.– Drucksache 19/15214 –. Deutscher Bundestag, Drucksache 19/16170, Berlin

Bundesregierung (2019h): Bericht über die Anwendung verdeckter Überwachungsmaßnahmen im Rahmen der Gefahrenabwehr. Unterrichtung durch die Bundesregierung. Deutscher Bundestag, Drucksache 19/15570, Berlin

Bundesregierung (2019i): Erfahrungen mit dem Einsatz von Bodycams bei der Bundespolizei. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn,Gökay Akbulut, weiterer Abgeordneter und der

Fraktion DIE LINKE.– Drucksache 19/13972 –. Deutscher Bundestag, Drucksache 19/14620, Berlin

Bundesregierung (2019j): Einsätze von sogenannten Stillen SMS, WLAN-Catchern, IMSI-Catchern und Funkzellenabfragen im ersten Halbjahr 2019. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Martina Renner, Heike Hänsel, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 19/11706 –. Deutscher Bundestag, Drucksache 19/12465, Berlin

Bundesregierung (2020a): Zahlen zu Speicherungen in polizeilichen EU-Datenbanken (2019) (Nachfrage zur Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 19/16723). Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Ulla Jelpke,Niema Movassat, weiterer Abgeordneter und der Fraktion DIE LINKE.– Drucksache 19/17989 –. Deutscher Bundestag, Drucksache 19/18872, Berlin

Bundesregierung (2020b): Einsätze von sogenannten Stillen SMS, WLAN-Catchern, IMSI-Catchern, Funkzellenabfragen im zweiten Halbjahr 2019. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Martina Renner, Heike Hänsel, weiterer Abgeordneter und der Fraktion DIE LINKE.– Drucksache 19/16427 –. Deutscher Bundestag, Drucksache 19/17055, Berlin

Bundesregierung (2021a): Bericht über die Anwendung verdeckter Überwachungsmaßnahmen im Rahmen der Gefahrenabwehr. Unterrichtung durch die Bundesregierung. Deutscher Bundestag, Drucksache 20/43, Berlin

Bundesregierung (2021b): Einsätze von sogenannten Stillen SMS, WLAN-Catchern, IMSI-Catchern, Funkzellenabfragen (2020). Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Martina Renner, Dr. André Hahn, weiterer Abgeordneter und der Fraktion DIE LINKE.– Drucksache 19/25576 –. Deutscher Bundestag, Drucksache 19/26424, Berlin

Bundesverwaltungsgericht (2019): EuGH soll Vereinbarkeit der deutschen Regelung zur Vorratsdatenspeicherung mit dem Unionsrecht klären. Pressemitteilung Nr. 66/2019 vom 25.09.2019. https://www.bverwg.de/de/pm/2019/66 (8.6.2021)

Buolamwini, J.; Gebru, T. (2018): Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. In: Proceedings of the 1st Conference on Fairness, Accountability and Transparency. Proceedings of Machine Learning Research (81), S. 77–91

BVG (Berliner Verkehrsbetriebe - AöR -) (2017): Sicherheitsbericht der Berliner Verkehrsbetriebe 2016. Berlin

BVG (2018): Sicherheitsbericht der Berliner Verkehrsbetriebe 2017. Berlin

Cameron, A.; Kolodinski, E.; May, H.; Williams, N. (2008): Measuring the Effects of Video Surveillance on Crime in Los Angeles. Prepared for the California Research Bureau. School of Policy, Planning and Development. University of Southern California. Los Angeles. www.library.ca.gov/Content/pdf/crb/reports/08-007.pdf (28.10.2019)

Castro, D.; McQuinn, A. (2016): Unlocking Encryption: Information Security and the Rule of Law. Report. Information Technology and Innovation Foundation (ITIF). www2.itif.org/2016-unlocking-encryption.pdf (28.10.2019)

CDU/CSU-Fraktion; SPD-Fraktion (2017): Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes. Gesetzentwurf der Fraktionen der CDU/CSU und SPD. Deutscher Bundestag, Drucksache 18/11163, Berlin

CCC (Chaos Computer Club) (2011): Chaos Computer Club analysiert Staatstrojaner. Pressemittelung vom 8.10.2011. www.ccc.de/de/updates/2011/staatstrojaner (28.10.2019)

CCC (2018): Biometrische Videoüberwachung: Der Südkreuz-Versuch war kein Erfolg. Pressemittelung vom 13.10.2018. www.ccc.de/de/updates/2018/debakel-am-suedkreuz (28.10.2019)

Chen, L. (2017): Shanghai police turn to facial recognition software to catch misbehaving cyclists. City plans to expand use of »electronic police« after pilot scheme snares more than 30 bike lane offenders in less than a month. In: South China Morning Post 20.09.2017. www.scmp.com/news/china/society/article/2112006/shanghai-police-turn-facial-recognition-software-catch (28.10.2019)

Cho, Y.; Yoon, K. (2016): Improving Person Re-identification via Pose-Aware Multi-shot Matching. 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, S. 1354-1362

City of Chicago (2017): Police Department announces expansion of predictive technology in Chatham and Auburn Gresham. Offive of the Mayor, Pressemitteilung vom 25.7.2017. www.chicago.gov/content/dam/city/depts/mayor/Press%20Room/Press%20Releases/2017/July/072517_PolicePredictiveTechnology.pdf (28.10.2019)

Crocco, M.; Cristani, M.; Trucco, A.; Murino, V. (2016): Audio Surveillance. A Systematic Review. In: ACM Computing Surveys 48(4), Article 52, S. 1–46

Daase, C.; Deitelhoff, N. (2013): Privatisierung der Sicherheit. Eine sozialwissenschaftliche Expertise. Schriftenreihe Sicherheit Nr. 11. Forschungsforum Öffentliche Sicherheit. Berlin. http://refubium.fu-berlin.de/bitstream/handle/fub188/18278/sr_11.pdf (28.10.2019)

Davies, B.; Innes, M.; Dawson, A. (2018): An Evaluation of South Wales Police's Use of Automated Facial Recognition. Universities' Police Science Institute, Crime & Security Research Institute, Cardiff University. http://afr.south-wales.police.uk/cms-assets/resources/uploads/AFR-EVALUATION-REPORT-FINAL-SEPTEMBER-2018.pdf (28.10.2019)

DB AG (Deutsche Bahn AG) (2017): 190 neue Videokameras für mehr Sicherheit an Hamburgs Hauptbahnhof. Pressemitteilung vom 13.12.2017. www.deutschebahn.com/resource/blob/1310622/5ccc2055732b1d76886b25d463573b75/20171213-Videokameras-HH-Hbf-data.pdf (28.10.2019)

DB AG (2019): Innovative Technik für mehr Zuverlässigkeit und Qualität. DB testet Videoanalyse-Systeme für bessere Abläufe im Bahnhof. Pressemittelung vom 7.6.2019. www.deutschebahn.com/de/presse/pressestart_zentrales_uebersicht/Innovative-Technik-fuer-mehr-Zuverlaessigkeit-und-Qualitaet--4183854 (28.10.2019)

Der Senat von Berlin (2016): Henkels letzter großer Traum – Ausweitung der Videoüberwachung im Land Berlin. Schriftliche Anfrage des Abgeordneten Christopher Lauer (PIRATEN) vom 11. Januar 2016 (Eingang beim Abgeordnetenhaus am 14. Januar 2014) und Antwort. Abgeordnetenhaus Berlin, Drucksache 17/17723, Berlin

Der Senat von Berlin (2017a): Einsatz des Predictive Policing bei der Berliner Polizei. Schriftliche Anfrage des Abgeordneten Hanno Bachmann (AfD) vom 16. März 2017 (Eingang beim Abgeordnetenhaus am 16. März 2017) und Antwort. Abgeordnetenhaus Berlin, Drucksache 18/10732, Berlin

Der Senat von Berlin (2017b): Mitteilung – zur Kenntnisnahme – Einführung einer Erhebungsmatrix für Funkzellenabfragen – Bessere statistische Erfassung von Daten für echte parlamentarische Kontrolle Drucksachen 17/1700 und 17/1975. Abgeordnetenhaus Berlin, Drucksache 18/0366, Berlin

Dialog Consult; VATM (Verband der Anbieter für Telekommunikation und Mediendienste) (2015): 17. TK-Marktanalyse Deutschland 2015. www.vatm.de/wp-content/uploads/2018/07/2015-Marktstudie.pdf (28.10.2019)

Dialog Consult; VATM (2018): 20. TK-Marktanalyse Deutschland 2018, www.vatm.de/wp-content/uploads/2018/12/VATM_TK-Marktstudie-2018_091018_f.pdf (28.10.2019)

Die Johanniter (2018): Drohnen im Bevölkerungsschutz. Johanniter-Unfall-Hilfe (JUH) sammelt erste Erfahrungen im Einsatz von unbemannten Luftfahrtsystemen. In: Bevölkerungsschutz 2, S. 45–46

Die rbb Reporter (2018): Unter Beobachtung, https://web.archive.org/web/20180825094634/www.rbb-online.de/doku/die_rbb_reporter/beitraege/unter-beobachtung.html (25.5.2021)

Ditton, J. (2000): Crime and the City. In: British Journal of Criminology 40(4), S. 692–709

DIVSI (Deutsches Institut für Vertrauen und Sicherheit im Internet) (2013): Überwachung elektronischer Daten und ihr Einfluss auf das Nutzungsverhalten im Internet. www.divsi.de/wp-content/uploads/2013/07/2013-07-03-DIVSI-PRISM-Blitzumfrage-PK.pdf (29.10.2019)

DIVSI; dimap GmbH (2014): Untersuchung zur Wahrnehmung des »Snowden/NSA-Skandals« in Deutschland, www.divsi.de/wp-content/uploads/2014/05/dimap-Bericht-DIVSI.pdf (29.10.2019)

DLR (Deutsches Zentrum für Luft- und Raumfahrt e.V.) (2017): ZKI-DE. Service für Bundesbehörden. Jahresbericht 2016, www.dlr.de/eoc/Portaldata/60/Resources/dokumente/zki/zki_0_jahresb/ZKI-DE_Jahresbericht_2016.pdf (29.10.2019)

DLR (2018): ZKI-DE. Service für Bundesbehörden. Jahresbericht 2017, www.dlr.de/eoc/Portaldata/60/Resources/dokumente/zki/zki_0_jahresb/ZKI-DE_Jahresbericht_2017.pdf (29.10.2019)

Donato, P. de; Barres, O.; Sausse, J.; Martin, D. (2018): Near Real-Time Ground-to-Ground Infrared Remote-Sensing Combination and Inexpensive Visible Camera Observations Applied to Tomographic Stack Emission Measurements. In: Remote Sensing 10(5), S. 1-15

DSK (Datenschutzkonferenz) (2015): Big Data zur Gefahrenabwehr und Strafverfolgung: Risiken und Nebenwirkungen beachten. Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19. März 2015 in Wiesbaden. www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/89DSK-BigData.pdf (29.10.2019)

DSK (2016): »Videoüberwachungsverbesserungsgesetz« zurückziehen! Entschließung der 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder. www.lfd.niedersachsen.de/download/112520 (29.10.2019)

DSK (2018a): Der Vorschlag der EU-Kommission für eine E-Evidence-Verordnung führt zum Verlust von Betroffenenrechten und verschärft die Problematik der sog. Vorratsdatenspeicherung. Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – Münster, 7. November 2018. www.datenschutz-bayern.de/dsbk-ent/DSK_96-E-Evidence.pdf (29.10.2019)

DSK (2018b): Videoüberwachung nach der Datenschutz-Grundverordnung. Kurzpapier Nr. 15. www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_15.pdf (27.09.2018)

Düsseldorfer Kreis (2015): Orientierungshilfe »Videoüberwachung in öffentlichen Verkehrsmitteln«. Datenschutzgerechter Einsatz von optisch-elektronischen Einrich-

tungen in Verkehrsmitteln des öffentlichen Personennahverkehrs und des länderübergreifenden schienengebundenen Regionalverkehrs. www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2015/10/OH-VUE-OEPNV.pdf (29.10.2019)

Eckhardt, A.; Börner, A.; Lehmann, F. (2009): The Bright Future of High Resolution Satellite Remote Sensing – Will Aerial Photogrammetry Become Obsolete? Presentation at Photogrammetric Week 2009. http://phowo.ifp.uni-stuttgart.de/2009/presentations/150Eckhardt.pdf (29.10.2019)

Egbert, S. (2018): Predictive Policing und die soziotechnische Konstruktion ethnisch codierter Verdächtigkeit. In: Pfadenhauer, M.; Poferl, A. (Hg.): Wissensrelationen. Beiträge und Debatten zum 2. Sektionskongress der Wissenssoziologie. Weinheim/Basel, S. 241–265

Elbing, B. R.; Petrin, C.; van den Broeke, M. S. (2018): Monitoring infrasound from a Tornado in Oklahoma. In: The Journal of the Acoustical Society of America 143(3), S. 1808

Epple, G.; Ludewig, F. (2019): »Sicherheit im Einsatz durch Open Source Intelligence in Einsatzleitstellen« (SENTINEL). In: Polizeispiegel (1/2), S. 20–22

Epple, G.; Ludewig, F. (2020): Open Source Intelligence in Einsatzleitstellen der Polizei: Eine empirische Untersuchung zu neuen Möglichkeiten der Informationsgewinnung. Schriftenreihe der Deutschen Hochschule der Polizei 11, Münster

Ethik-Kommission (2017): Automatisiertes und vernetztes Fahren. Eingesetzt durch den Bundesminister für Verkehr und digitale Infrastruktur, www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf (29.10.2019)

EK (Europäische Kommission) (o.J.): Emergency Management Service. Service Overview. https://emergency.copernicus.eu/mapping/sites/default/files/files/Copernicus EMS-Service_Overview_Brochure.pdf (29.10.2019)

EK (2018): Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen. COM(2018) 225 final, Straßburg

EK (2019): Empfehlung für einen Beschluss des Rates über die Ermächtigung zur Aufnahme von Verhandlungen über ein Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln für die justizielle Zusammenarbeit in Strafsachen. COM(2019) 70 final, Straßburg

Faßnacht, U. (2012): Rechtsfragen bei der Verwendung von Ortungstechnologien und einsatzunterstützender Systeme durch Feuerwehr und THW. Rechtlicher Rahmen und Haftungsfragen. Zivile Sicherheit. Berlin

Feltes, T.; Ruch, A. (2017): Stellungnahme zur öffentlichen Anhörung am Montag, 06.03.2017 im Innenausschuss des Deutschen Bundestages »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) und »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)«, Innenausschuss, Deutscher Bundestag, Ausschussdruckdache 18(4)785 C, Berlin

Forsa (2016): Ergebnisbericht »Fahrgastbefragung Videoaufzeichnung 2016«. Berlin, www.bahnaktuell.net/BA2/wordpress/wp-content/uploads/2016/07/2016-07-01-APS-Ergebnisbericht_Fahrgastbefragung_Videoaufzeichung_2016.pdf (29.10.2019)

Forsa (2018): Sicherheit in der Stadt. Ergebnisse einer repräsentativen Bevölkerungsbefragung. Berlin. www.lebendige-stadt.de/pdf/Forsa-Umfrage.pdf (29.10.2019)

Fox, D. (2007): Stellungnahme zur »Online-Durchsuchung« Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07. www.secorvo.de/publikationen/stellungnahme-secorvo-bverfg-online-durchsuchung.pdf (29.10.2019)

Fraunhofer FHR (Fraunhofer-Institut für Hochfrequenzphysik und Radartechnik) (2018): Frühwarnsystem RAWIS in Katastrophenübung mit THW final getestet. Pressemittelung vom 23. Mai 2018, www.fhr.fraunhofer.de/content/dam/fhr/de/images/D_Pressemedien/2018/20180523_PI_Fraunhofer_FHR_RAWIS_Projekt abschluss_de.pdf (29.10.2019)

Fraunhofer IOSB (Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung) (o.J.): Intelligente Videoüberwachung für mehr Sicherheit und Datenschutz. Start für Pilotprojekt in Mannheim. www.iosb.fraunhofer.de/servlet/is/93474/ (29.10.2019)

Freiling, F. (2007): Schriftliche Stellungnahme zum Fragenkatalog Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07. Mannheim

Frommberg, L. (2019): 40 Sekunden, um die Katastrophe zu verhindern. In: aeroTELEGRAPH, 26.03.2019. www.aerotelegraph.com/40-sekunden-um-die-katastrophe-zu-verhindern-boeing-737-max-simulator (29.10.2019)

Funk, E.; Börner, A.; Ernst, I.; Grießbach, D.; Baumbach, D. (2016): IPS – ein System für eine mobile Datenerfassung in Innenräumen. http://elib.dlr.de/110834/1/paper_eva3.pdf (29.10.2019)

Geier, W. (2017): Strukturen, Zuständigkeiten, Aufgaben und Akteure. In: Karutz, H.; Geier, W.; Mitschke, T. (Hg.): Bevölkerungsschutz. Heidelberg, S. 93–128

GeoSN (Staatsbetrieb Geobasisinformation und Vermessung Sachsen) (2017): Überprüfen Sie die Genauigkeit Ihres Navigationsgerätes oder Smartphones. Referenzpunkte in Sachsen. www.landesvermessung.sachsen.de/info_refenz/FB_Referenz_sn.pdf (29.10.2019)

Gerstner, D. (2017): Predictive Policing als Instrument zur Prävention von Wohnungseinbruchdiebstahl. Evaluationsergebnisse zum Baden-Württembergischen Pilotprojekt P4. Freiburg

Gesellschaft für Informatik (2015): Informatiker fordern uneingeschränkte, starke Verschlüsselung für Jedermann. Meldung vom 6.2.2015. www.gi.de/aktuelles/meldungen/detailansicht/article/informatiker-fordern-uneingeschraenkte-starke-verschluesselung-fuer-jedermann.html (29.10.2019)

GGF (Gesellschaft für Freiheitsrechte) (2019): Polizeigesetz und Verfassungsschutzgesetz Hessen. https://freiheitsrechte.org/polizeigesetz-hessen (4.6.2021)

Giemulla, E. (2019): Nach Boeing-Absturz in Äthiopien. »Viele Piloten verstehen sich nur als Knöpfchendrücker«. www.deutschlandfunk.de/nach-boeing-absturz-in-aethiopien-viele-piloten-verstehen.694.de.html?dram:article_id=443328 (29.10.2019)

Glaubitz, C.; Kudlacek, D.; Neumann, M.; Fleischer, S.; Bliesener, T. (2018): Ergebnisse der Evaluation der polizeilichen Videobeobachtung in Nordrhein-Westfalen gemäß § 15a PolG NRW. Kriminologisches Forschungsinstitut Niedersachsen e.V.,

Forschungsbericht Nr. 143, Hannover, http://kfn.de/wp-content/uploads/Forschungsberichte/FB_143.pdf (29.10.2019)
Gödde, F.; Wessels, M. (2012): SensProCloth. Systemintegrierte sensorische Schutzkleidung für Feuerwehr und Katastrophenschutz. Teilprojekt: Erfassung und Weitermeldung von physiologischen Zustandsparametern und Umgebungsbedingungen mit Ortung zur Einleitung von Hilfsmaßnahmen. Landeshauptstadt Stuttgart, http://edok01.tib.uni-hannover.de/edoks/e01fb12/729004171.pdf (29.10.2019)
Google (o.J.): Häufig gestellte Fragen zu Google Trends-Daten. https://support.google.com/trends/answer/4365533?hl=de (10.6.2021)
Greven, M. (2017): Stellungnahmen zum Gesetzentwurf zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze. Öffentliche Anhörung im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages am 31.05.2017. www.bundestag.de/blob/508850/76fc6296143a5eba18aff59fce987bb8/greven_drb-data.pdf (29.10.2019)
Groß, H. (2008): Deutsche Länderpolizeien. In: APuZ 2008(48), S. 20–26
Groß, H. (2019): Polizei(en) und innere Sicherheit in Deutschland. Strukturen, Aufgaben und aktuelle Herausforderungen. In: APuZ 2019(21–23), S. 4–10
Grünwald, A.; Nüßing, C. (2016): Kommunikation over the Top. Regulierung für Skype, WhatsApp oder Gmail? In: Multimedia und Recht 2, S. 91–97
Gusy, C. (2017): Ziele, Aufträge und Maßstäbe der Sicherheitsgewährleistung. In: Gusy, C.; Kugelmann, D.; Würtenberger, T. (Hg.): Rechtshandbuch Zivile Sicherheit. Berlin/Heidelberg, S. 55–86
Gusy, C.; Kapitza, A. (2015): Evaluation von Sicherheitsgesetzen. In: Gusy, C. (Hg.): Evaluation von Sicherheitsgesetzen. Wiesbaden, S. 9–36
Häcker, E. (2018): Videoüberwachung und DSGVO. Praxistipps Datenschutz 3/2018, http://team-datenschutz.de/PDF/3-18.pdf (29.10.2019)
Hagendorff, T. (2017): Das Ende der Informationskontrolle. Zur Nutzung digitaler Medien jenseits von Privatheit und Datenschutz. Bielefeld
Hamburger Hochbahnen AG (2018): In Fahrzeugen. Die beste Methode: wenn viele bewährte Methoden zusammenwirken. www.hochbahn.de/hochbahn/hamburg/de/Home/Fahren/Mit_Sicherheit_ans_Ziel/In_Fahrzeugen (29.10.2019)
Hansen, M.; Pfitzmann, A. (2007): Technische Grundlagen von Online-Durchsuchung und -Beschlagnahme. In: Deutsche Richterzeitung August 2007, S. 225–228
Harnisch, S.; Pohlmann, M. (2009): Strafprozessuale Maßnahmen bei Mobilfunkendgeräten. Die Befugnis zum Einsatz des sog. IMSI-Catchers. In: HRRS. Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht 5, S. 202–217
Heesen, J. (2012): Preisgabe von Information und Konstituierung persönlicher Identität. In: Bartram, C.; Bobbert, M.; Dölling, D.; Fuchs, T.; Schwarzkopf, G.; Tanner, K. (Hg.): Der (un)durchsichtige Mensch. Wie weit reicht der Blick in die Person? Heidelberg, S. 237–254
Heesen, J. (2016): Prävention, Freiheit und Demokratie. In: Ammicht Quinn, R. (Hg.): Prävention und Freiheit. Zur Notwendigkeit eines Ethik-Diskurses. Gutachten für den 21. Deutschen Präventionstag am 6./7. Juni 2016 in Magdeburg. Tübingen, S. 49–62
Heinz, E.; May, T.; Born, D.; Zieger, G.; Anders, S.; Zakosarenko, V.; Meyer, H.-G.; Schäffel, C. (2015): Passive 350 GHz Video Imaging Systems for Security Applications. In: Journal of Infrared, Millimeter, and Terahertz Waves 36(10), S. 879–895

Hempel, L.; Töpfer, E. (2009): The Surveillance Consensus. Reviewing the Politics of CCTV in Three European Countries. In: European Journal of Criminology 6(2), S. 157–177

Hempel, L.; Rau, H.; Markwart, T. (2014): Subjektive Sicherheit. Berlin, www.fonds-soziale-sicherung.de/data/user/Downloaddateien/Projekt-Security/Projekt_Security_-_Subjektive_Sicherheit_-_Grundlagen.pdf (29.10.2019)

Hempel, L.; Wittich, R.; Protschky, A. (2019): Integrierte Technikentwicklung durch Konfliktnetzwerke. In: Draude, C.; Lange, M.; Sick, B. (Hg.): INFORMATIK 2019: 50 Jahre Gesellschaft für Informatik – Informatik für Gesellschaft. Bonn, S. 445–446

Henzler, P. (2017): Anhörung des Vizepräsidenten des Bundeskriminalamtes Peter Henzler im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages am 31. Mai 2017 zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze. Hier: zum Thema Quellen-TKÜ und Online-Durchsuchung in der StPO gem. Formulierungshilfe der BReg. www.bundestag.de/blob/509190/ce315ac513c903afc986b8110078ddea/henzler-data.pdf (29.10.2019)

Herpig, S. (2018): Schwachstellen-Management für mehr Sicherheit. Wie der Staat den Umgang mit Zero-Day-Schwachstellen regeln sollte. Stiftung Neue Verantwortung, www.stiftung-nv.de/sites/default/files/vorschlag.schwachstellenmanagement.pdf (29.10.2019)

Hessische Landesregierung (2016): Innenminister Peter Beuth stellt Prognose-Software »KLB-operativ« vor. Pressemitteilung vom 20.07.2016, www.hessen.de/pressearchiv/pressemitteilung/innenminister-peter-beuth-stellt-prognose-software-klb-operativ-vor (29.10.2019)

Hessisches Ministerium für Justiz (2017): Fünf Jahre Gemeinsame elektronische Überwachungsstelle der Länder (GÜL). Pressemittelung vom 02.01.2017, http://justizministerium.hessen.de/pressearchiv/pressemitteilung/fuenf-jahre-gemeinsame-elektronische-ueberwachungsstelle-der-laender-guel (29.10.2019)

Hiéramente, M. (2016): Surfen im Internet doch Telekommunikation im Sinne des § 100a StPO? Anmerkung zum Beschluss des Bundesverfassungsgerichts vom 6. Juli 2016, 2 BvR 1454/13 (BVerfG HRRS 2016 Nr. 860). In: HRRS. Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht 17(10), S. 448–452

HmbBfDI (Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit) (2018): Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg. http://datenschutz-hamburg.de/assets/pdf/Pruefbericht_Gesichtserkennungssoftware.pdf (29.10.2019)

Hoffknecht, A.; Holtmannspötter, D.; Zweck, A. (2006): Die Terahertz-Technologie und ihre möglichen Anwendungen. VDI Technologiezentrum GmbH, Düsseldorf, www.vditz.de/fileadmin/media/publications/pdf/Band64_Terahertz.pdf (29.10.2019)

Honeywell International Inc. (2018): MultiRAE Pro. Wireless Portable Multi-Threat Radiation and Chemical Detector. www.raesystems.com/sites/default/files/content/resources/Datasheet_MultiRAE%20Pro_DS-1068-11_US-EN_LR.pdf (29.10.2019)

Hornung, G.; Schindler, S. (2017): Das biometrische Auge der Polizei. Rechtsfragen des Einsatzes von Videoüberwachung mit biometrischer Gesichtserkennung. In: Zeitschrift für Datenschutz 5, S. 203–209

Huerta, I.; Fernández, C.; Segura, C.; Hernando, J.; Prati, A. (2015): A deep analysis on age estimation. In: Pattern Recognition Letters 68, S. 239–249

Hufschmidt, G.; Schrott, L.; Simmer, C.; Krahe, P.; Reicherter, K.; Rechenbach, P.; Plattner, H. P.; Helmerichs, J.; Karutz, H.; Geier, W.; Genzwürker, H.; Geenen, E.; May, A.; Sass, H.-M. (2017): Bewältigung. In: Karutz, H.; Geier, W.; Mitschke, T. (Hg.): Bevölkerungsschutz: Notfallvorsorge und Krisenmanagement in Theorie und Praxis. Berlin/Heidelberg, S. 225–322

Hunt, P.; Saunders, J.; Hollywood, J. (2014): Evaluation of the Shreveport Predictive Policing Experiment. RAND Corporation. Santa Monica, www.rand.org/content/dam/rand/pubs/research_reports/RR500/RR531/RAND_RR531.pdf (29.10.2019)

InfoTip Service GmbH (o.J.): Das InfoTip-Kompendium. Informationstechnik. http://kompendium.infotip.de/informationstechnik.html (29.10.2019)

Integrierte Leitstelle Freiburg (2018): Standortdaten beim Notruf 112. www.ils-freiburg.de/standortdaten.php (29.10.2019)

Jing, M. (2018): From travel and retail to banking, China's facial-recognition systems are becoming part of daily life. The growing number of public and commercial applications for facial recognition in China may bolster the nation's wider push to lead the world in artificial intelligence. South China Morning Post, 8.2.2018, www.scmp.com/tech/social-gadgets/article/2132465/travel-and-retail-banking-chinas-facial-recognition-systems-are (29.10.2019)

Jüttner, J. (2016): Lebenslange Haft für Supermarkträuber »Mit eiskalter Ruhe«. Spiegel Online, 17.2.2016, www.spiegel.de/panorama/justiz/hannover-supermarktraeuber-zu-lebenslanger-haft-verurteilt-worden-a-1077895.html (29.10.2019)

Kammerer, D. (2010): Die Anfänge von Videoüberwachung in Deutschland. In: Zeitgeschichte-online, Dezember 2010. https://zeitgeschichte-online.de/kommentar/die-anfaenge-von-videoueberwachung-deutschland (29.10.2019)

Kammerer, D. (2008): Bilder der Überwachung. Dissertation, Frankfurt a.M.

Karamalis, A.; Evers, C. (2015): Automatische Erkennung von Objekten in 3D Millimeterwellen Bilddaten für den QPS Sicherheitsscanner. www.ndt.net/article/dgzfp-thz-2015/papers/3.pdf (29.10.2019)

Kees, B. (2015): Algorithmisches Pantopicon – Identifikation gesellschaftlicher Probleme automatisierter Videoüberwachung. Münster

Kersting, S.; Naplava, T.; Reutemann, M.; Heil, M.; Scheer-Vesper, C. (2019): Die deeskalierende Wirkung von Bodycams im Wachdienst der Polizei Nordrhein-Westfalen. Abschlussbericht, Institut für Polizei- und Kriminalwissenschaft der Fachhochschule für öffentliche Verwaltung NRW, Gelsenkirchen

Kersting, S.; Naplava, T.; Reutemann, M.; Scheer-Vesper, C. (2017): Die deeskalierende Wirkung von Bodycams im Wachdienst der Polizei Nordrhein-Westfalen. Zwischenbericht, Institut für Polizei- und Kriminalwissenschaft der Fachhochschule für öffentliche Verwaltung NRW, Gelsenkirchen

King, J.; Mulligan, D. K.; Raphael, S. (2008): CITRIS Report: The San Francisco Community Safety Camera Program – An Evaluation of the Effectiveness of San Francisco's Community Safety Cameras. University of California, Berkeley, www.wired.com/images_blogs/threatlevel/files/sfsurveillancestudy.pdf (29.10.2019)

Kingreen, Th. (2018): Antrag auf abstrakte Normenkontrolle (Art. 93 Abs. 1 Nr. 2 GG) von Vorschriften des Bayerischen Polizeiaufgabengesetzes (PAG). Namens und im Auftrag der Abgeordneten des 19. Deutschen Bundestages. Doris Achelwilm, Grigorios Aggefidis, Gökay Akbufut, Renata Alt, Luise Amtsberg, Kerstin Andreae,

Christine Aschenberg-Dugnus, Lisa Badum, Annalena Baerbock, Simone Barrientos und weiterer Abgeordneter. Regensburg, https://www.fdpbt.de/sites/default/files/2018-09/Normenkontrollantrag%20Bayr.%20PAG%20Endfassung%206.9.18.pdf (13.2.2020)

Kiss, P. (2019): Neue Notruftechnik. Schnellere Hilfe im Notfall. Tagesschau.de, 10.10.2019, www.tagesschau.de/inland/notruf-standort-technik-101.html (29.10.2019)

Klare, B. F.; Burge, M. J.; Klontz, J. C.; Bruegge, R. W. V.; Jain, A. K. (2012): Face Recognition Performance: Role of Demographic Information. In: IEEE Transactions on Information Forensic and Security 7(6), S. 1789–1801

Knobloch, T. (2018): Vor die Lage kommen: Predictive Policing in Deutschland. Policy Brief. Stiftung Neue Verantwortung und Bertelsmannstiftung, Berlin/Gütersloh, www.stiftung-nv.de/sites/default/files/predictive.policing.pdf (29.10.2019)

Ko, B. C. (2018): A Brief Review of Facial Emotion Recognition Based on Visual Information. In: Sensors (Basel) 18(2), S. 401

Kochheim, D. (2015): Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik. München

Kraft, T.; Bayer, S.; Hein, D.; Stebner, Karsten, Lesmeister, Daniela; Berger, R. (2018): Echtzeit-Lagekarten für die Katastrophenhilfe. In: DVW e.V. (Hg.): UAV 2018 – Vermessung mit unbemannten Flugsystemen. DVW-Schriftenreihe 89, Augsburg, S. 123–135

Krauß, M. (2015): Quellen-Telekommunikationsüberwachung. In: Bundesministerium der Justiz und für Verbraucherschutz (Hg.): Bericht der Expertenkommission zur effektiveren und praxistauglicheren Ausgestaltung des allgemeinen Strafverfahrens und des jugendgerichtlichen Verfahrens. Anlagenband I – Gutachten, S. 117–135, www.bmjv.de/SharedDocs/Downloads/DE/PDF/Anlage_1_StPO_Kommission.pdf (29.10.2019)

Krauß, M. (2017): Stellungnahme zum Gesetzentwurf zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze. Öffentliche Anhörung im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages am 31.05.2017. www.bundestag.de/resource/blob/509046/5aa0ea61c4f3df0429208b5fda260a0a/krauss-data.pdf (29.10.2019)

Kriminologisches Forschungsinstitut Niedersachsen (2016): Schriftliche Stellungnahme zum Innenausschuss des Landtages Nordrhein-Westfalen. Maßnahmenpaket zur Bekämpfung des Wohnungseinbruchsdiebstahls (Antrag der Fraktion der CDU, Drucksache 16/12344). www.landtag.nrw.de/Dokumentenservice/portal/WWW/dokumentenarchiv/Dokument/MMST16-4315.pdf (23.05.2019)

Krizhevsky, A.; Sutskever, I.; Hinton, G. E. (2012): ImageNet Classification with Deep Convolutional Neural Networks. In: Pereira, F.; Burges, C.; Bottou, L.; Weinberger, K. (Hg.): Advances in Neural Information Processing Systems 25. S. 1097–1105

Krüger, C. (2012): Die sogenannte »stille SMS« im strafprozessualen Ermittlungsverfahren Erkenntnisse zum Einsatz in der Praxis und Betrachtung der rechtlichen Anwendungsvoraussetzungen. In: Zeitschrift für das Juristische Studium 2012(5), S. 606–613

Kudlacek, D. (2015): Akzeptanz von Videoüberwachung. Eine sozialwissenschaftliche Untersuchung technischer Sicherheitsmaßnahmen. Wiesbaden

Kühling, J. (2017): Neues Bundesdatenschutzgesetz – Anpassungsbedarf bei Unternehmen. In: Neue Juristische Wochenschrift 28, S. 1985–1991

Kühling, J.; Martini, M.; Heberlein, J.; Kühl, B.; Nink, D.; Weinzierl, Quirin, Wenzel, Michael (2016): Die Datenschutz-Grundverordnung und das nationale Recht. Erste Überlegungen zum innerstaatlichen Regelungsbedarf. Münster

Kurz, C.; Neumann, L.; Rieger, F. (2016): Stellungnahme zur »Quellen-TKÜ« nach dem Urteil des Bundesverfassungsgerichts vom 20. April 2016 1 BvR 966/09. http://ccc.de/system/uploads/216/original/quellen-tkue-CCC.pdf (30.01.2018)

La Vigne, N.; Lowry, S.; Markman, J.; Dwyer, A. (2011): Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention. Urban Institute, Washington, www.urban.org/sites/default/files/publication/27556/412403-evaluating-the-use-of-public-surveillance-cameras-for-crime-control-and-prevention_0.pdf (29.10.2019)

Landesbetrieb Forst Brandenburg (2019): Waldbrandgefahr in Brandenburg. Waldbrand-Früherkennung mit »Fire Watch«. https://forst.brandenburg.de/lfb/de/themen/wald-schuetzen/waldbrandgefahr-in-brandenburg/ (29.10.2019)

Landesregierung Brandenburg (2018): Stand der Umsetzung von Precobs. Antwort der Landesregierung auf die Kleine Anfrage Nr. 3193 der Abgeordneten Björn Lakenmacher (CDU-Fraktion) und Sven Petke (CDU-Fraktion) Drucksache 6/7837. Landtag Brandenburg, Drucksache 6/7985, Potsdam

LDI (Landesbeauftragte für Datenschutz und Informationsfreiheit) NRW (2016): Videoüberwachung durch öffentliche Stellen des Landes Nordrhein-Westfalen – Allheilmittel oder Teufelszeug? www.ldi.nrw.de/mainmenu_Service/submenu_Newsarchiv/Inhalt/Video__berwachung_durch___ffentliche_Stellen_des_Landes_Nordrhein-Westfalen/Video__berwachung_durch___ffentliche_Stellen_des_Landes_NRW_Juli_2016.pdf (29.10.2019)

LeCun, Y.; Bengio, Y.; Hinton, G. (2015): Deep learning. In: Nature 521, S. 436–444

Legnaro, A.; Kretschmann, A. (2015): Das Polizieren der Zukunft. In: Kriminologisches Journal 2, S. 94–111

Lin, C.-Y. (2006): Öffentliche Videoüberwachung in den USA, Großbritannien und Deutschland. Ein Drei-Länder-Vergleich. Dissertation, Göttingen, http://ediss.uni-goettingen.de/bitstream/handle/11858/00-1735-0000-0006-B3C4-7/lin.pdf (29.10.2019)

Lipp, S.; Hoppenstedt, M. (2016a): 3,5 Gründe, warum der BKA-Hack gegen Telegram illegal ist. Motherboard, 8.12.2016, http://motherboard.vice.com/de/article/aek5xa/3-5-gruende-warum-der-bka-hack-gegen-telegram-illegal-ist (29.10.2019)

Lipp, S.; Hoppenstedt, M. (2016b): Exklusiv: BKA-Mitarbeiter verrät, wie Staatshacker illegal Telegramm knacken. Motherboard, 8.12.2016, http://motherboard.vice.com/de/article/53dnv8/bka-telegram-hack-mitarbeiter-gericht-muenchen (29.10.2019)

Lischka, K.; Klingel, A. (2017): Wenn Maschinen Menschen bewerten. Internationale Fallbeispiele für Prozesse algorithmischer Entscheidungsfindung – Arbeitspapier. Bertelsmann Stiftung, Gütersloh, www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/ADM_Fallstudien.pdf (29.10.2019)

LKA (Landeskriminalamt) Hessen (2017): Handlungsempfehlung für die Errichtung und den Betrieb von Videoüberwachungsanlagen im öffentlichen Raum. Wiesbaden. www.polizei.hessen.de/File/2017-handlungsempfehlung-video-www_2.pdf (29.10.2019)

LKA NRW (2018): Kooperative Evaluation des Projekts »SKALA«. Abschlussbericht der Zentralstelle Evaluation beim LKA NRW (ZEVA) und der Gesellschaft für innovative Sozialforschung und Sozialplanung e.V. Bremen (GISS). Düsseldorf,

http://lka.polizei.nrw/sites/default/files/2018-06/160430_Evaluationsbericht_SKALA.pdf (29.10.2019)
Löw, F.; Judex, M.; Wania, A.; Salamon, P. (2018): »Mit Fernerkundung vor die Lage kommen«. Was nach Zukunftsmusik klingt, soll bei Copernicus Realität werden. In: Bevölkerungsschutz 2018(1), S. 23–24
Lüdemann, C.; Schlepper C. (2011): Der überwachte Bürger zwischen Apathie und Protest: Eine empirische Studie zum Widerstand gegen staatliche Kontrolle. In: Zurawski, N. (Hg.): Überwachungspraxen – Praktiken der Überwachung: Analysen zum Verhältnis von Alltag, Technik und Kontrolle, Opladen, S. 119–138
Maguire, M. (2000): Policing by risks and targets: Some dimensions and implications of intelligence-led crime control. In: Policing and Society 9(4), S. 315–336
Marthews, A.; Tucker. C. (2017): Government Surveillance and Internet Search Behavior. SSRN Journal, 17.2.2017, https://ssrn.com/abstract=2412564 (29.10.2019)
Matz, G.; Fischer, H.; Frank, J. (2012): Detektoren Array mit Gaschromatograph zur Identifikation toxischer Substanzen (DACHS). TU Hamburg-Harburg, http://edok01.tib.uni-hannover.de/edoks/e01fb12/731594746.pdf (29.10.2019)
Matzner, T. (2016): Videoüberwachung als Instrument der Prävention? In: Ammicht Quinn, R. (Hg.): Prävention und Freiheit. Zur Notwendigkeit eines Ethik-Diskurses. Tübingen, S. 63–75
McDuff, D.; Cheng, R.; Kapoor, A. (2018): Identifying Bias in AI using Simulation. http://arxiv.org/pdf/1810.00471 (29.10.2019)
Menevidis, Z.; Ajami, M. (2013): Verbundprojekt: ADIS. Automatisierte Detektion interventionsbedürftiger Situationen durch Klassifizierung visueller Muster. Teilvorhaben BAMDIS. Bewegungsanalysemethoden zur Detektion interventionsbedürftiger Situationen. Schlussbericht. Fraunhofer-Institut für Produktionsanlagen und Konstruktionstechnik. Berlin, http://edok01.tib.uni-hannover.de/edoks/e01fb15/815812493.pdf (29.10.2019)
Merz, C. (2016): Predictive Policing – Polizeiliche Strafverfolgung in Zeiten von Big Data. Karlsruher Institut für Technologie, ABIDA-Dossier Januar 2016, www.abida.de/sites/default/files/Dossier_Predictive_Policing.pdf (29.10.2019)
Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg (2018): Startschuss für die algorithmenbasierte Videoüberwachung beim Polizeipräsidium Mannheim. Pressemitteilung vom 3.12.2018, http://im.baden-wuerttemberg.de/de/service/presse-und-oeffentlichkeitsarbeit/pressemitteilung/pid/startschuss-fuer-die-algorithmenbasierte-videoueberwachung-beim-polizeipraesidium-mannheim/ (29.10.2019)
Mo, H. (2018): Facial recognition used to catch suspect in crowd of 60,000 concertgoers. China Daily, 12.4.2018, www.ecns.cn/2018/04-12/298889.shtml (29.10.2019)
Monopolkommission (2015): Telekommunikation 2015: Märkte im Wandel. Sondergutachten 73. www.monopolkommission.de/images/PDF/SG/s73_volltext.pdf (29.10.2019)
Monroy, M. (2018): Bundesbehörden spähen immer öfter Mobiltelefone aus. netzpolitik.org, 24.1.2018, http://netzpolitik.org/2018/bundesbehoerden-spaehen-immer-oefter-mobiltelefone-aus/ (29.10.2019)
Nagenborg, M. (2014): Überwachungsdiskurse: Drei Beispiele und ihre Implikationen für die (Sicherheits-)Ethik. In: Ammicht Quinn, R. (Hg.): Sicherheitsethik. Wiesbaden, S. 211–223
Neumann, L.; Kurz, C.; Rieger, F. (2017): Risiken für die innere Sicherheit beim Einsatz von Schadsoftware in der Strafverfolgung. Sachverständigenauskunft zum

Änderungsantrag der Fraktionen CDU/CSU und SPD zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze (Ausschussdrucksache 18/11272). www.bundestag.de/resource/blob/509192/77ee7be3c9401ef4619fa0411758b045/neumann-data.pdf (29.10.2019)

Niedersächsisches Ministerium für Inneres und Sport (2017): Kleine Anfrage zur schriftlichen Beantwortung mit Antwort der Landesregierung – Drucksache 17/7855 – Nicht individualisierte Funkzellenabfragen. Anfrage der Abgeordneten Jan-Christoph Oetjen und Christian Grascha (FDP) an die Landesregierung. Niedersächsischer Landtag, Drucksache 17/8036, Hannover

Niedersächsisches Ministerium für Inneres und Sport (2018): Zweite Pilotphase startet: Einsatz der Prognosesoftware PreMAP wird zum 1. November weiter intensiviert. Pressemitteilung vom 2018, www.mi.niedersachsen.de/aktuelles/presse_informationen/zweite-pilotphase-startet-einsatz-der-prognosesoftware-premap-wird-zum-1-november-weiter-intensiviert-170622.html (29.10.2019)

NIST (National Institute of Standards and Technology) (2014): Face Recognition Vendor Test (FRVT). Performance of Face Identification Algorithms. NIST Interagency Report 8009, https://doi.org/10.6028/NIST.IR.8009 (29.10.2019)

NIST (2017a): Face In Video Evaluation (FIVE). Face Recognition of Non-Cooperative Subjects. NIST Interagency Report 8173, https://doi.org/10.6028/NIST.IR.8173 (29.10.2019)

NIST (2017b): The 2017 IARPA Face Recognition Prize Challenge (FRPC). NIST Interagency Report 8197, https://doi.org/10.6028/NIST.IR.8197 (29.10.2019)

Northover, S. B.; Pedersen, W. C.; Cohen, A. B.; Andrews, P. W. (2017): Artificial surveillance cues do not increase generosity: two meta-analyses. In: Evolution and Human Behavior 38(1), S. 144–153

Oberverwaltungsgericht für das Land Nordrhein-Westfalen (2017): Vorratsdatenspeicherung unionsrechtswidrig. Pressemitteilung vom 22.6.2017, www.ovg.nrw.de/behoerde/presse/pressemitteilungen/01_archiv/2017/36_170622/index.php (29.10.2019)

Ohlberg, M.; Ahmed, S.; Lang, B. (2018): Zentrale Planung, lokale Experimente. Die komplexe Umsetzung von Chinas gesellschaftlichem Bonitätssystem. Mercator Institute for China Studies, www.merics.org/sites/default/files/2018-04/180404_China_Monitor_43_Umsetzung_des_Gesellschaftlichen_Bonit%C3%A4tssystems.pdf (29.10.2019)

Omand, D.; Bartlett, J.; Miller, C. (2012): Introducing Social Media Intelligence (SOCMINT). In: Intelligence and National Security 27(6), S. 801–823

Parlamentarisches Kontrollgremium (2017): Bericht zu den Maßnahmen nach dem Terrorismusbekämpfungsgesetz für das Jahr 2015. Unterrichtung durch das Parlamentarische Kontrollgremium. Deutscher Bundestag, Drucksache 18/11228, Berlin

PEN America (2015): GLOBAL CHILLING. The Impact of Mass Surveillance on International Writers. Results from PEN's International Survey of Writers. http://pen.org/sites/default/files/globalchilling_2015.pdf (24.05.2019)

Penney, J. (2016): Chilling Effects: Online Surveillance and Wikipedia Use. In: Berkeley Technology Law Journal 31(1), S. 117–182

Penney, J. (2017): Internet surveillance, regulation, and chilling effects online: a comparative case study. In: Internet Policy Review 6(2), S. 1–39

Perry, W.; McInnis, B.; Price, C.; Smith, S.; Hollywood, J. (2013): Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations. RAND Corpo-

ration, Santa Monica, www.rand.org/pubs/research_reports/RR233.html (29.10.2019)
Petri, T. (2012): Der Bayerische Landesbeauftragte für den Datenschutz. Prüfbericht Quellen-TKÜ. München, www.datenschutz-bayern.de/0/bericht-qtkue.pdf (29.10.2019)
Pfitzmann, A. (2008): Contra Online-Durchsuchung. Möglichkeiten und Grenzen der Nutzungsüberwachung von Informations- und Kommunikationssystemen in einer freiheitlichen demokratischen Gesellschaft. In: Informatik Spektrum 31(1), S. 65–69
Pöhlmann, C.; Elßner, T. (2015): Sicheres Erkennen biologischer Gefahren vor Ort (GFEREASE). Schlussbericht zum Verbundprojekt. Leipzig, www.tib.eu/suchen/id/TIBKAT:870186922/ (29.10.2019)
Polizei Bremen (2017): Abschlussbericht Projekt Bodycam. Berichtszeitraum: 4. November 2016 – 31. Oktober 2017. Bremen, www.inneres.bremen.de/sixcms/media.php/13/TOP%2009%20staatlich_Anlage%201.20027.pdf (29.10.2019)
Rainie, L.; Madden, M. (2015): Americans' Privacy Strategies Post-Snowden. Pew Research Center, Washington, www.pewresearch.org/wp-content/uploads/sites/9/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf (29.10.2019)
Raji, I.; Buolamwini, J. (2019): Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products. In: AIES '19 Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society, S. 429–435
Rammert, W. (2000): Vom Nutzen der Technikgeneseforschung für die Technikfolgenabschätzung. In: Rammert, W. (Hg.): Technik aus soziologischer Perspektive 2. Kultur – Innovation – Virtualität. Wiesbaden, S. 203–215
Rat der Europäischen Union (2017): Abschlussbericht über die siebte Runde der gegenseitigen Begutachtung »Praktische Umsetzung und Durchführung europäischer Strategien zur Verhütung und Bekämpfung von Cyberkriminalität« – Informationen für den Rat. 12711/17. Brüssel, http://data.consilium.europa.eu/doc/document/ST-12711-2017-INIT/de/pdf (29.10.2019)
Ratcliffe, J. (2005): The Effectiveness of Police Intelligence Management: A New Zealand Case Study. In: Police Practice and Research 6(5), S. 435–451
Ren, S.; He, K.; Girshick, R.; Sun, J. (2017): Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks. In: IEEE Transactions on Pattern Analysis and Machine Intelligence 39(6), S. 1137–1149
Rolfes, M. (2017): Predictive Policing: Beobachtungen und Reflexionen zur Einführung und Etablierung einer vorhersagenden Polizeiarbeit. In: Fachgruppe Geoinformatik des Instituts für Geographie (Hg.): Geoinformation & Visualisierung. Pionier und Wegbereiter eines neuen Verständnisses von Kartographie und Geoinformatik: Festschrift anlässlich der Emeritierung von Herrn Prof. Dr. Hartmut Asche im März 2017. Potsdam, S. 51–76
Roßnagel, A.; Desoi, M.; Hornung, G. (2011): Gestufte Kontrolle bei Videoüberwachungsanlagen. In: Datenschutz und Datensicherheit 35(10), S. 694
Roßnagel, A.; Hammer, V.; Pordesch, U. (1993): KORA – Eine Methode zur Konkretisierung rechtlicher Anforderungen zu technischen Gestaltungsvorschlägen für Informations- und Kommunikationssysteme. In: InfoTech 5(1), S. 21–24
Roßnagel, A.; Jandt, S.; Skistims, H.; Zirfas, J. (2012): Zulässigkeit von Feuerwehr-Schutzanzügen mit Sensoren und Anforderungen an den Umgang mit personen-

bezogenen Daten. Dortmund/Berlin/Dresden. www.baua.de/DE/Angebote/Publikationen/Berichte/F2278.pdf (29.10.2019)
Rothmann, R. (2010): Sicherheitsgefühl durch Videoüberwachung? Argumentative Paradoxien und empirische Widersprüche in der Verbreitung einer sicherheitspolitischen Maßnahme. In: Neue Kriminalpolitik 22, S. 103–107
Rüffer, M. (2016): Überblick aus der Luft. In: Feuerwehr-Magazin: Drohnen bei der Feuerwehr Teil 1–3, Themen-Special, S. 8–14
Sächsischen Staatsministerium des Innern (2018): Stationäre Videoüberwachung an öffentlichen Orten in Sachsen 2018. Antwort der Sächsischen Staatsregierung auf die Kleine Anfrage des Abgeordneten Enrico Stange, Fraktion DIE LINKE, Drucksache 6/11668. Sächsisches Staatsministerium des Innern, Dresden, http://ws.landtag.sachsen.de/images/6_Drs_11668_1_1_1_.pdf (30.10.2019)
Saunders, J.; Hunt, P.; Hollywood, J. S. (2016): Predictions put into practice: a quasi-experimental evaluation of Chicago's predictive policing pilot. In: Journal of Experimental Criminology 12(3), S. 347–371
Schroff, F.; Kalenichenko, D.; Philbin, J. (2015): FaceNet. A unified embedding for face recognition and clustering. In: IEEE: Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR), S. 815–823
Schulcz, F.; Guerin, M.; Monteuil, P.; Kölln, I.; Engelhard, C.; Bär, T. (2015): UAV-Assisted Ad Hoc Networks for Crisis Management and Hostile Environment Sensing, Teilvorhaben: Entwicklung eines neuartigen, hochintegrierten und energieeffizienten miniaturisierten RN-Sensor Arrays und ergonomisches Nutzerinterface. Hamburg, http://doi.org/10.2314/GBV:863040225 (30.10.2019)
Schulze, M. (2017): Going Dark? Dilemma zwischen sicherer, privater Kommunikation und den Sicherheitsinteressen von Staaten. In: APuZ 67(46–47), S. 23–28
Schulzki-Haddouti, C. (2017): Die Funkzellenabfrage auf dem Weg zum Standard-Ermittlungsinstrument. Übersicht der Nutzung der nicht-individualisierten Funkzellenabfrage in den Bundesländern. Cives Redaktionsbüro GmbH, 11.5.2017, http://cives.de/die-funkzellenabfrage-auf-dem-weg-zum-standardermittlungsinstrument-5028 (30.10.2019)
Schweer, T. (2015): »Vor dem Täter am Tatort« – Musterbasierte Tatortvorhersagen am Beispiel des Wohnungseinbruchs. In: Die Kriminalpolizei 1, S. 13–16
Shanghai Municipal People's Government (2017): Smart cameras catch not so smart drivers. City News, 23.3.2017. www.shanghai.gov.cn/shanghai/node27118/node27818/u22ai85767.html (30.20.2019)
Sharan, R.V.; Moir, T.J. (2015): Noise robust audio surveillance using reduced spectrogram image feature and one-against-all SVM. In: Neurocomputing 158, S. 90–99
Sharif, M.; Bhagavatula, S.; Bauer, L.; Reiter, M. (2016): Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition. In: CCS '16 Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, S. 1528–1540
ShotSpotter (2018): ShotSpotter Frequently Asked Questions. www.shotspotter.com/system/content-uploads/SST_FAQ_January_2018.pdf (30.10.2019)
Singelnstein, T. (2018): Predictive Policing: Algorithmenbasierte Straftatprognosen zur vorausschauenden Kriminalintervention. In: NStZ 1, S. 1–9
Sparks, A.; Barclay, P. (2013): Eye images increase generosity, but not for long: the limited effect of a false cue. In: Evolution and Human Behavior 34(5), S. 317–322
Staben, J. (2016): Der Abschreckungseffekt auf die Grundrechtsausübung. Dissertation, Tübingen

Stadt Köln (2015): Beantwortung der Anfrage der Piratengruppe im Rat der Stadt Köln »Videoüberwachung der KVB AG«, AN/0205/2015, aus der Sitzung am 09.03.2015. Vorlagen-Nummer 1206/2015. https://ratsinformation.stadt-koeln.de/getfile.asp?id=499298&type=do (16.8.2021)

Statista (2018): Anzahl täglicher Besucher auf den größten Bahnhöfen in Deutschland im Jahr 2016. http://de.statista.com/statistik/daten/studie/739405/umfrage/groesste-bahnhoefe-in-deutschland-nach-anzahl-taeglicher-besucher/ (20.11.2018)

Statista (2020): Anzahl der Personenbahnhöfe im Besitz der Deutsche Bahn AG in den Jahren 2007 bis 2019. https://de.statista.com/statistik/daten/studie/13357/umfrage/anzahl-der-bahnhoefe-im-besitz-der-db-ag (6.8.2020)

Statistisches Bundesamt (2018): Statistisches Jahrbuch 2018. Deutschland und Internationales, https://www.destatis.de/DE/Themen/Querschnitt/Jahrbuch/statistisches-jahrbuch-2018-dl.pdf (25.5.2021)

Stockdale, K. (2019): Saskatchewan Police Predictive Analytics Lab Missing Persons Project: Year One. Defence Research and Development Canada, Saskatoon, https://cradpdf.drdc-rddc.gc.ca/PDFS/unc336/p809812_A1b.pdf (11.6.2021)

Stoycheff, E. (2016): Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring. In: Journalism & Mass Communication Quarterly 93(2), S. 296–311

Strack, F.; Markel, P. (2013): Verbundprojekt: MuViT. Mustererkennung und Video Tracking: sozialpsychologische, soziologische, ethische und rechtswissenschaftliche Analysen. Teilprojekt: MuViT – SozPsy. Exposition und Akzepanz – Sozialpsychologische Studien in Reaktion auf Mustererkennung und Video Tracking. Würzburg, https://doi.org/10.2314/GBV:79060146X (30.10.2019)

Strohschneider, S. (2010): Technisierungsstrategien und der Human Factor. In: Zoche, P.; Kaufmann, S.; Haverkamp, R. (Hg.): Zivile Sicherheit. S. 161–178

TAB (Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag) (2002): Biometrische Identifikationssysteme. (Autoren: Petermann, Th.; Sauter, A.) TAB-Arbeitsbericht Nr. 76, Berlin

TAB (2010): Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen Ausfalls der Stromversorgung. (Autoren: Petermann, Th.; Bradke, H.; Lüllmann, A.; Poetzsch, M.; Riehm, U.) TAB-Arbeitsbericht Nr. 141, Berlin

TAB (2012): Fernerkundung: Anwendungspotenziale in Afrika (Autorin: Gerlinger, K.) TAB-Arbeitsbericht Nr. 154, Berlin

TAB (2016a): Predictive Policing (Autor/in: Richter, S.; Kind, S.). Themenkurzprofil Nr. 9, Berlin

TAB (2016b): Technologien und Visionen der Mensch-Maschine-Entgrenzung. (Autoren: Kehl, C.; Coenen, C.) TAB-Arbeitsbericht Nr. 167, Berlin

TAB (2020): Autonome Waffensysteme. (Autoren: Grünwald, R.; Kehl, C.) TAB-Arbeitsbericht Nr. 187, Berlin

Thomsen, J. (2018): Videoüberwachung in Berlin. Vor allem Frauen und Ältere finden Kameras gut. Berliner Zeitung, 31.3.2018. www.berliner-zeitung.de/berlin/video ueberwachung-in-berlin-vor-allem-frauen-und-aeltere-finden-kameras-gut-29948236 (30.10.2019)

THW (Bundesanstalt Technisches Hilfswerk) (2017): Unbemanntes Fliegen im Technischen Hilfswerk (THW). Pressemitteilung vom 7.4.2017, www.thw.de/SharedDocs/Meldungen/DE/Pressemitteilungen/national/2017/04/pressemitteilung_001_ulfs_im_thw.html (30.10.2019)

TLfDI (Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit) (2016): 2. Tätigkeitsbericht zum Datenschutz: Nicht-öffentlicher Bereich. Erfurt, https://www.tlfdi.de/mam/tlfdi/datenschutz/taetigkeitsbericht/2_taetigkeitsbericht.pdf (30.10.2019)

Trottier, D. (2012): Policing Social Media. In: Canadian Review of Sociology/Revue canadienne de sociologie 49(4), S. 411–425

Trute, H.-H. (2009): Grenzen des präventionsorientierten Polizeirechts in der Rechtsprechung des Bundesverfassungsgerichts. In: Die Verwaltung 42(1), S. 85–104

Turow, J.; Hennessy, M.; Draper, N. (2015): The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation. A reprot from the Annenberg School for Communication. Philadelphia, www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf (30.10.2019)

Ulbrich, C. (2019): Die Überwachung lokaler Funknetzwerke (»WLAN-Catching«): Informationstechnologische und strafprozessuale Aspekte unter besonderer Berücksichtigung allgemeiner Fragen der Internetüberwachung und Verschlüsselung. Berlin

Verwaltungsgericht Köln (2018): Keine Pflicht für Telekommunikationsunternehmen zur Vorratsdatenspeicherung. Pressemitteilung vom 20.4.2018, www.vg-koeln.nrw.de/behoerde/presse/Pressemitteilungen/Archiv/2018/01_180420/index.php (30.10.2019)

Visser, W.; Schwaninger, A.; Hardmeier, D.; Flisch, A.; Costin, M.; Vienne, C.; Sukowski, F.; Hassler, U.; Dorion, I.; Marciano, A.; Koomen, G. et al. (2016): Automated comparison of X-ray images for cargo scanning. In: IEEE: International Carnahan Conference on Security Technology (ICCST), S. 1–8

Voßhoff, A. (2017): Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze, BT-Drs. 18/11272, und der Formulierungshilfe mit Änderungsantrag zur Einführung einer Quellen-Telekommunikationsüberwachung und einer Online-Durchsuchung in der Strafprozessordnung, A-Drs. 18(6)334. Bonn, http://cdn.netzpolitik.org/wp-upload/2017/05/186346_Stellungnahme_BfDI_zu_18-11272_und_186334.pdf (30.10.2019)

Waidner, M. (2014): Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 26.6.2014. www.bundestag.de/blob/285122/2f815a7598a9a7e9b4162d70173ecedb/mat_a_sv-1-2-pdf-data.pdf (30.10.2019)

Wang, Y.; Kosinski, M. (2018): Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. In: Journal of Personality and Social Psychology 114(2), S. 246–257

WAR (Wissenschaftlicher Arbeitskreis für Regulierungsfragen bei der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen) (2016): Fragen der Regulierung von OTT-Kommunikationsdiensten. Stellungnahme, www.bundesnetzagentur.de/DE/Allgemeines/DieBundesnetzagentur/WAR/Stellungnahmen/Stellungnahme_OTT.pdf (30.10.2019)

Weichert, T. (2005): Datenschutzrechtliche Kontrollen von Funkzellenabfragen. Bezug: Sitzung des Innen- und Rechtsausschusses vom 16. November 2005. Schleswig-Holsteinischer Landtag, Umdruck 16/490, Kiel, www.landtag.ltsh.de/infothek/wahl16/umdrucke/0400/umdruck-16-0490.pdf (30.10.2019)

Welsh, B.C.; Farrington. D. P. (2009): Public Area CCTV and Crime Prevention. An Updated Systematic Review and Meta-Analysis. In: Justice Quarterly 26(4), S. 716–745

Welsh, B.C.; Farrington, D.P. (2002): Crime prevention effects of closed circuit television. A systematic review. Home Office Research Study 252, London

Welt (2017): Fast drei Jahre Haft für Berliner U-Bahn-Treter. Welt, 6.7.2017, www.welt.de/vermischtes/article166357942/Fast-drei-Jahre-Haft-fuer-Berliner-U-Bahn-Treter.html (30.10.2019)

Wienbracke, M. (2013): Der Verhältnismäßigkeitsgrundsatz. In: Zeitschrift für das Juristische Studium 2, S. 148–155

Wienecke, F. (2013): Nutzung von Wärmebildkameras zur Personensuche und Lageerkundung im Feuerwehreinsatz über größere Entfernungen. Brandschutzforschung der Bundesländer. Bericht Nr. 172, Ständige Konferenz der Innenminister und -senatoren der Länder, Arbeitskreis V, Ausschuss für Feuerwehrangelegenheiten, Katastrophenschutz und zivile Verteidigung (Hg.), Heyrothsberge

Williams, D.; Ahmed, J. (2009): The relationship between antisocial stereotypes and public CCTV systems: exploring fear of crime in the modern surveillance society. In: Psychology, Crime & Law 15(8), S. 743–758

WD (Wissenschaftliche Dienste) (2015): Maßnahmen des Bundes zur Terrorismusbekämpfung seit 2001. Gesetzgebung und Evaluierung (Aktualisierung der Ausarbeitung WD 3 - 3000 - 044/15 vom 6. März 2015) Ausarbeitung. WD 3 - 3000 - 037/17, Deutscher Bundestag, Berlin

WD (2016a): Rechtsgrundlage für den Einsatz sog. intelligenter Videoüberwachung durch die Bundespolizei. Sachstand. WD - 3000 - 202/16, Deutscher Bundestag, Berlin

WD (2016b): Regulierung von Messengerdiensten. Datenportabilität und Interoperabilität. Sachstand. Deutscher Bundestag, Berlin

WD (2016c): Videoüberwachung im öffentlichen Raum. WD 3 - 2000 - 133/16. Deutscher Bundestag, Berlin

WD (2017a): Rechtsgrundlagen der Videoüberwachung in den Bundesländern. WD 3 - 3000 - 045/17. Deutscher Bundestag, Berlin

WD (2017b): Vergleich ausgewählter präventivpolizeilicher Standardmaßnahmen im Recht des Bundes und der Länder. WD 3 - 3000 - 020/17. Deutscher Bundestag, Berlin

WD (2017c): Zivilschutz in Deutschland. Sachstand. WD 3 - 3000 - 203/17. Deutscher Bundestag, Berlin

WD (2017d): Zusammenhang von Videoüberwachung und Straftaten in ÖPNV. Sachstand. WD - 3000 - 250/17, Deutscher Bundestag, Berlin

WD (2018a): Ortung und Verfolgung durch Peilsender oder Mobiltelefone zur Vollstreckung eines Europäischen Haftbefehls. WD 7 - 3000 - 079/18, Deutscher Bundestag, Berlin

WD (2018b): Polizeiliche Videoüberwachung im öffentlichen Raum. Aktualisierung des Sachstands WD 3 - 3000 - 065/17. WD 3 - 3000 - 171/18. Deutscher Bundestag, Berlin

Woodward, J.; Horn, C.; Gatune, J.; Aryn, T. (2003): Biometrics. A Look at Facial Recognition. Documented Briefing. Prepared for the Virginia State Crime Commission. RAND Public Safety and Justice. Santa Monica, http://apps.dtic.mil/dtic/tr/fulltext/u2/a414520.pdf (30.10.2019)

Zweig, K. (2018): Wo Maschinen irren können. Fehlerquellen und Verantwortlichkeiten in Prozessen algorithmischer Entscheidungsfindung. Bertelsmann Stiftung, Gütersloh. www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/WoMaschinenIrrenKoennen.pdf (30.10.2019)

10 Anhang

10.1 Abbildungen

10.2 Tabellen

10.3 Kästen

BÜRO FÜR TECHNIKFOLGEN-ABSCHÄTZUNG BEIM DEUTSCHEN BUNDESTAG

Karlsruher Institut für Technologie

Neue Schönhauser Straße 10
10178 Berlin

Telefon: +49 30 28491-0
E-Mail: buero@tab-beim-bundestag.de
Web: www.tab-beim-bundestag.de
Twitter: @TABundestag