Abgleich im Erfassungsgerät

Matthias Pocs, LL. M.

Projektgruppe verfassungsverträgliche Technikgestaltung (provet), Uni Kassel
matthias.pocs@uni-kassel.de

Zusammenfassung

Biometrische Fahndungstechnik kommt. Sie verspricht das Aufspüren potenzieller Terroristen, aber birgt auch neuartige Risiken. Sollten Innenminister und Polizeibehörden künftig mit biometrischen Fahndungssystemen experimentieren dürfen, ist die Gestaltung des biometrischen Systems maßgeblich für den Grundrechtsschutz. Insbesondere müssen sich Technikgestalter zwischen einem zentralisierten biometrischen Vergleich in einer externen Referenzdatenbank und einem Abgleich bereits im Erfassungsgerät entscheiden. Dieser Beitrag [DiDa10] untersucht, welche Gestaltungsoption das Grundrecht auf informationelle Selbstbestimmung vorschreibt.

Einleitung

An mehreren Stellen des Bahnhofs hängen Kameras, die optisch die Gesichter der Vorbeigehenden erfassen. An den Kameras geht eine Vielzahl von Personen vorbei. Wenn jemand als gesuchter Verdächtiger erkannt wird, meldet dies das System. Die Meldung wird erzeugt, indem die Gesichtsdaten automatisiert mit polizeilichen Fahndungsdateien abgeglichen werden. Eine solche Technik hat das Bundeskriminalamt bereits getestet [BKA-07]. Es ist das am meisten fortgeschrittene Stadium eines systematisch untersuchten biometrischen Systems, mit dem Störer und Verdächtige entdeckt werden sollen, kurz: eines Systems zur „Verdachtsgewinnung“ [BVGE04].

Nicht nur dieser Test zeigt die Entschiedenheit, mit der solche Technik entwickelt wird. Bereits 2001 wurde in Tampa ein Gesichtserkennungssystem für solche Zwecke eingesetzt [Gate10]. Nicht nur das Gesicht, sondern auch andere biometrische Modalitäten werden genutzt; z. B. die Iris an Flughäfen der Arabischen Emirate [DaMa04]. Außerdem werden große Summen aufgebracht, um solche Systeme zu erforschen. Es werden biometrische Techniken erforscht, mit denen Fingerspuren an Gepäckstücken [DiDa10] [Hil+11] und abweichendes Verhalten aus der Videoüberwachung [FPBM11] sowie Online-Videos [INDE11] erkannt werden.

Aufgrund dieser Entwicklungen ist es vorstellbar, dass künftig Gesetze erlassen werden, die z. B. den Einsatz von Gesichtserkennungssystemen an internationalen Flughäfen zum Entdecken und Anhalten potenzieller Terroristen erlauben. Eine solche vorsorgliche Datenerfassung - also vor Verursachung einer Gefahr oder Begehung einer Straftat - stellt das Recht vor neue Herausforderungen [DPS+11] [Pocs11d] [Pocs11a] [Hil+11] [HoDP10] [WP2909], insbesondere weil biometrische Charakteristika erfasst werden, ohne dass der Betroffene einen Anlass dafür geschaffen hat, und eine Vielzahl von Personen davon betroffen sind. Ein Aspekt des Einsatzes solcher biometrischer Systeme ist der Ort, an dem die biometrischen Daten über die Passanten mit den Daten über Verdächtige zur Verdachtsgewinnung verglichen wer-

P. Schartner · J. Taeger (Hrsg.) · DACH Security 2011 · syssec (2011) 349-360.

den.
Dieser Aufsatz untersucht, ob die Verfassung vorschreibt, dass des biometrische Vergleich statt in externen Referenzdatenbanksystemen im Erfassungsgerät durchgeführt wird, und wie die Technik gestaltet wird, um einem solchen Erfordernis zu genügen.

Grundlagen

Unverdächtige, die von der automatisierten Erfassung biometrischer Charakteristika betroffen sind, werden insbesondere bei einem zentralen biometrischen Vergleich im Gegensatz zu einem dezentralen Vergleich im Erfassungsgerät spezifischen Risiken ausgesetzt.

Technische Grundlagen

Biometrische Systeme, die bei der polizeilichen Fahndung zur Verdachtsgewinnung eingesetzt werden sollen, unterscheiden sich aus mehreren Gründen von herkömmlichen Systemen zur biometrischen Zugriffs-, Zugangs-, Zutritts- und Ausweiskontrolle. Zunächst kann das System nicht zur Verifikation, sondern nur zur Identifikation eingesetzt werden [ISO-09]. Dies liegt daran, dass die gesuchten Verdächtigen nicht daran interessiert sind, sich als solche auszugeben. Zudem werden die erfassten Daten über die Personen vor Ort (Proben) mit einer Fahndungsdatei oder sonstigen Referenzdatenbank verglichen (Eins-zu-N-Vergleich), in der die biometrischen Referenzen zentral gespeichert sind. Wenn Personen nicht erkannt werden, erleiden sie auch keinen Nachteil; dadurch entfallen bestimmte Risiken [Pocs11e] Überdies unterliegen biometrische Identifikationssysteme einer spezifischen Fehlerquoten [Pocs11e].

Außerdem stellt die Automatisierung der Erfassungen eine Besonderheit dar. Die Automatisierung ermöglicht eine Vervielfachung der Erfassungen biometrischer Charakteristika und Vergleiche mit biometrischen Referenzen, insbesondere weil die Daten in unkontrollierten Umgebungen erfasst werden, in welchen der Betroffene nicht mitwirken muss. Da die anderen Datenverarbeitungsvorgänge, insbesondere der Vergleich, meist bereits automatisiert sind (z. B. bei AFIS), liegt es an der Automatisierung der Erfassungen, dass Referenzdatenbanken für vorsorgliche Datenerfassungen zur Überprüfung einer Vielzahl von Betroffenen genutzt werden können.

Insbesondere werden Fahndungsdateien zentral verwaltet. In Deutschland verwaltet das BKA die deutschen und Schengener Fahndungsdateien und AFIS [BKAG09]. Dass man die Referenzen an einer Stelle zentral speichern muss, bedeutet nicht, dass man sie auch nur in der Zentrale für den Vergleich nutzen kann. Zwar ist ein Vergleich auf einer Chipkarte, unter der Kontrolle des Betroffenen, nicht möglich. Jedoch kann man den Abgleich mit einer Datenbank mehr oder weniger zentral durchführen: statt auf EU-Ebene nur in den Mitgliedstaaten, z. B. wird die Fahndungsdatei des SIS in die nationalen Systeme („N.SIS“) kopiert; statt bundesweit nur landesweit, statt landesweit nur in der Polizeidienststelle; und statt in einer Dienststelle nur in einem Erfassungsgerät, wie z. B. bei der Kfz-Kennzeichenerfassung [Hess07a] oder dem mobilen Fingerabdruckscanner „Fast ID“ [Crime11].

Wird die Durchführung im zentralen System gewählt, müssen die Proben aus mehreren Erfassungsgeräten an dieselbe Stelle, die Zentrale, fernübertragen werden; wird die Durchführung im Erfassungsgerät gewählt, müssen die Referenzen zumindest als Indexdaten aus dem zentralen System in die Erfassungsgeräte kopiert werden. In diesem Fall können die Erfassungsgeräte mit der Zentrale vernetzt werden, um die Referenzen automatisiert zu aktualisieren.

Die dezentrale Speicherung macht nur Sinn, wenn der Zugriff der Zentrale auf die Proben auch trotz der Vernetzung beschränkt ist; sonst wäre es zwar kein zentrales System in physischer, jedoch in logischer Hinsicht.

Risiken

Der Einsatz des biometrischen Systems birgt Risiken. Die Automatisierung steigert herkömmliche Risiken auf neuartige Weise. Das Bundesverfassungsgericht erkannte das Betroffensein einer Vielzahl von Personen, das aus vorsorglichen Datenerfassungen folgt, und berücksichtigte es mithilfe des Kriteriums der „Streubreite“ einer Datenverarbeitung [BVGE08] [BVGE01a]. Wie breit eine polizeiliche Maßnahme tatsächlich streut, ermöglicht daher auch das Gegenüberstellen unterschiedlicher Systemeinsätze [Pocs11d]. Die Vervielfachung der Erfassungen steigert das Risiko

- der Offenbarung sensibler Informationen aus Roh- und Template-Daten [WP2903],
- Verknüpfung mehrerer Datenbanken zu einem Persönlichkeitsprofil aufgrund der Einzigartigkeit, Universalität und lebenslangen Gültigkeit biometrischer Charakteristika [WP2903],
- Gewinnung von Informationen über Aufenthaltsort, Zeit und Richtung und
- des unbefugten oder zweckfremden Zugriffs auf personenbezogene Daten.

Insbesondere werden die Risiken durch den Einsatz einer Referenzdatenbank gesteigert. Gegenwärtig nutzen Polizeien die Lichtbild- und Fingerabdrucksammlungen nur bei einzelnen Personen, welche einen Anlass geschaffen oder Verdacht erregt haben. Werden biometrische Charakteristika automatisiert erfasst, dann werden die Referenzdatenbanken jedoch intensiv genutzt. Dafür wurden sie jedoch nicht gebaut [Pocs11a]. Ferner könnte die Nutzung der zentralen Datei zu einer Konzentration informationeller Macht führen, wenn auch der Abgleich in einem bundes- oder europaweiten Zentralsystem durchgeführt wird.

Aufgrund des Risikos der Zweckentfremdung können Betroffenen so wie ursprünglich verfolgte Schwerkriminelle Treffermeldungen und möglichen Folgemaßnahmen ausgesetzt werden. So hat sich z. B. herausgestellt, dass bei der automatisierten Kfz-Kennzeichenerfassung im Nachhinein andere Zwecke verfolgt wurden (2007: 67 % der Treffermeldungen über Verstöße gegen das Pflichtversicherungsgesetz) als ursprünglich geplant (Bekämpfung grenzüberschreitender Kriminalität, Verhinderung von Anschlusstaten wie Einbrüchen und Unterstützung der Sachfahndung) [Bode10].

Die einzig bekannte polizeiliche Maßnahme, bei der Daten mittels Musterkennung (Kfz-Kennzeichen) automatisiert erhoben und mit Referenzen (gesuchte Kennzeichen) verglichen werden, ist durch das Bundesverfassungsgericht überprüft worden [BVGE08]. Wie die biometrische Technik kann auch bei dieser Mustererkennungstechnik zentral oder dezentral abgeglichen werden [Roßn08]. Das Gericht erklärte die Maßnahme bereits aufgrund einer zu weiten Zweckbestimmung für unzulässig. Zudem bestimmte es eine Technikgestaltung, nach der Daten unverzüglich abgeglichen und sofort spurenlos gelöscht werden [BVGE08]. Es entschied nicht, ob ein zentraler oder dezentraler Abgleich rechtlich geboten ist. Auch in der Literatur ist eine rechtliche Bewertung einer solchen Entscheidung nicht ersichtlich.

Sollten in Zukunft biometrische Systeme zur Verdachtsgewinnung eingesetzt werden, ist zu befürchten, dass ein (in logischer Hinsicht) zentrales System eingesetzt wird. Die rechtlichen Folgen einer solchen Systemarchitektur sind zu klären, bevor sich Technikgestalter und

-hersteller sowie Innenminister und Polizeibehörden festgelegt haben. Daher ist zu untersuchen, ob es rechtlich erforderlich ist, dass der biometrische Vergleich nicht etwa in externen Referenzdatenbanksystemen, sondern im Erfassungsgerät selbst erfolgt, und wie das biometrische Fahndungssystem gestaltet wird, um einem solchen Erfordernis zu genügen.

Verfassungsmäßigkeit

Im Folgenden wird die Verfassungsmäßigkeit des Systemeinsatzes geprüft. Die Prüfung ermöglicht es, Kriterien für die Technikgestaltung aus den grundrechtlichen Anforderungen herzuleiten. Die Verfassungsmäßigkeit der automatisierten Erfassung biometrischer Charakteristika zur Verdachtsgewinnung ist bereits dargestellt worden [Pocs11e] [Pocs11d] [Pocs11a] [Hil+11] [HoDP10]. Im Folgenden werden daher nur die Kriterien untersucht, die spezifisch mit der Frage zusammenhängen, ob der Abgleich dezentral durchgeführt werden muss.

Normenbestimmtheit

Der Eingriff darf nur auf einem Gesetz beruhen, das Anlass, Zweck und Grenzen des Eingriffs so präzise und rechtsklar formuliert, dass der Systemeinsatz vorauszusehen ist [BVGE08]. Zum einen muss das Ziel bestimmt werden, z. B. Störer und Verdächtige am Einsatzort zu entdecken und anzuhalten. Aufgrund des hohen Eingriffsgewichts (siehe nächster Punkt) sind erhöhte Anforderungen an die Normenbestimmtheit zu stellen. Eine rein faktische „Regelung“ durch Technikgestaltung reicht nicht aus. So werden z. B. bei der automatisierten Kennzeichenerfassung die Kfz-Kennzeichen dezentral abgeglichen [Hess07a], ohne es in der Ermächtigungsgrundlage zu regeln [HSOG10]. Grundrechtlich zu beanstanden ist, dass diese Art der Bestimmung die Rechtssicherheit und Vorhersehbarkeit nicht bietet, die durch die Normenbestimmtheit verlangt wird.

Grundrecht auf informationelle Selbstbestimmung

Insbesondere wird in das Grundrecht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz (GG) [BBD+10] eingegriffen, nach dem der Einzelne befugt ist, selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden. Dies liegt daran, dass biometrische und Fahndungsdaten verarbeitet werden, die personenbezogen i. S. d. § 3 Bundesdatenschutzgesetz (BDSG) und Art. 2 Buchst. a i. V. m. EG 26 Datenschutzrichtlinie (DSRL) sind [DPS+11].

1.1.1 Eignung und Erforderlichkeit

Zunächst muss der Einsatz des biometrischen Systems für die Zielerreichung geeignet und erforderlich sein. Der Einsatz eines biometrischen Systems ist für die Zielerreichung nicht ungeeignet, da die Erfassungen biometrischer Charakteristika unabhängig von einer Zentralisierung des biometrischen Vergleichs im Einzelfall Erfolg haben können (als relevant eingestuft in [BVGE07] [BVGE01b]) Wird die Durchführung des Abgleichs im Erfassungsgerät gewählt, müssen die Referenzen zumindest als Indexdaten aus dem zentralen System in die Erfassungsgeräte kopiert werden.

Es könnte eingewendet werden, dass es zu aufwendig ist, die Referenzen in den Erfassungsgeräten zu aktualisieren. Jedoch zeigt das Beispiel der Kfz-Kennzeichenerfassung, dass die Aktualisierung der Referenzen als Indexdaten in den flüchtigen Speicher der Erfassungsgeräte nicht zu aufwendig ist [Hess07a]. Außerdem könnte notfalls die Eignung hergestellt werden,

wenn die Referenzen seltener aktualisiert werden. Auch Erwägungen bezüglich der Performanz des Systems beseitigen die Eignung nicht, da die Eingriffe im Einzelfall Erfolg haben können. Ferner könnte eingewendet werden, dass Daten bei dezentraler Speicherung unsicherer sind. Dies trifft jedoch nicht für die Proben, sondern nur für die Referenzen zu. Ein Zugriff auf Referenzen zur Überlistung des Systems beseitigt die Eignung auch nicht (in Anlehnung an [BVGE10]).

Der Eingriff ist erforderlich, wenn kein milderes und gleich wirksames Mittel verfügbar ist. Insbesondere ist der Einsatz biometrischer Systeme milder, wenn ein dezentraler Abgleich im Erfassungsgerät gewählt wird. Dies folgt aus mehreren Gründen; zunächst aus der Verhältnismäßigkeit (siehe nächster Punkt). Dies folgt überdies aus der Erkenntnis, dass eine zentrale Speicherung nicht erforderlich ist, bezüglich des Pass- und Ausweisrechts [Horn05], weil beide Systeme die allgemeine Verarbeitung von Daten über Unverdächtige betreffen.

Zudem folgt der Vorzug eines dezentralen Abgleichs aus der unionsrechtlichen Auslegung des Grundrechts bezüglich der Erforderlichkeit nach Art. 7 Buchst. e DSRL. Der EuGH beurteilte das deutsche Ausländerzentralregister, das für Zwecke der Verbrechensbekämpfung eingesetzt wird [EuGH08]. Wie beim Einsatz des biometrischen Systems zur Verdachtsgewinnung ist eine Verarbeitung auf einer Chipkarte nicht möglich. Somit kamen nur die Alternativen einer zentralen bundesweiten Speicherung und dezentralen lokalen Speicherung infrage, beide in Form einer Datenbank, die den Eins-zu-N-Vergleich ermöglicht. Das Gericht entschied, dass das Zentralsystem nur dann erforderlich ist, wenn sein zentralisierter Charakter eine effizientere Gesetzesanwendung erlaubt [EuGH08]; die dezentrale Speicherung ist also ein milderes Mittel.

1.1.2 Verhältnismäßigkeit im engeren Sinne

Das Gewicht des Eingriffs ins Grundrecht auf informationelle Selbstbestimmung darf nicht außer Verhältnis stehen zum Gewicht des Ziels, das mit dem Einsatz des biometrischen Systems verfolgt wird. Die Verhältnismäßigkeit i. e. S. der automatisierten Erfassung personenbezogener Daten wird anhand von mehreren Kriterien beurteilt. Dazu gehören Kriterien, die durch das Bundesverfassungsgericht bereits ausdrücklich für dieses Grundrecht anerkannt hat, sowie Kriterien aus Wertungen des EU-Richtliniengebers bezüglich des Datenschutzrechts, deutschen Verfassungsgebers bezüglich anderer Anforderungen sowie Wertungen des Gesetzgebers bezüglich analog anwendbaren Rechts. Die Kriterien der ersten Gruppe sind:

- Anlasslosigkeit und Verdachtslosigkeit,
- Streubreite [BVGE08] [BVEGE01a],
- Heimlichkeit und Transparenz [BVGE08] [BVGE06],
- Gefühl des Überwachtwerdens [BVGE08] [BVGE05],
- Anpassungsdruck,
- Ermittlung „ins Blaue hinein“,
- Datensparsamkeit [BVGE10] [DSDS95],
- Erklärungsdruck und Stigmatisierung,
- Verwendung einheitlicher Personenkennzeichen und Persönlichkeitsprofile [BVGE83],
- Zweckbindung und informationelle Gewaltenteilung sowie Datensicherheit.

Das Eingriffsgewicht der allgemeinen Datenerfassung, die die Anlasslosigkeit, Heimlichkeit u. a. dieser Kriterien verursacht, könnte erhöht werden, wenn statt des dezentralen Abgleichs im Erfassungsgerät die Durchführung im zentralen System gewählt wird.

Streubreite: Ein biometrischer Systemeinsatz, der im rechtlichen Sinne erforderlich ist, ermöglicht eine neuartige Reichweite polizeilicher Beobachtung, weil die Zahl möglicher Erfassungsvorgänge vervielfacht wird. Die Zahl der Erfassungsvorgänge läuft mit der Zahl der Betroffenen gleich. Daher haben solche biometrische Systeme immer eine hohe Streubreite. Der zentrale Abgleich erhöht diese Streubreite so, dass nicht nur die Zahl der Personen, die von der Erfassung eines einzigen Erfassungsgeräts betroffen sind, zu berücksichtigen ist. Stattdessen wird die Zahl der Betroffenen erhöht, weil die Daten aus mehreren Erfassungsgeräten und von mehreren deutschen oder gar europäischen Einsatzorten zusammengeführt werden.

Im Übrigen kann sich die Bezeichnung der Zentralisierung auch auf Risiken der Profilbildung bezüglich einer einzelnen Person beziehen. Im Sinne des Kriteriums der Streubreite bedeutet „zentral“ jedoch, dass eine Vielzahl von Personen betroffen sind. Die zwei Begriffe sind voneinander zu unterscheiden und die Unterscheidung ist z. B. bei Auslegung des Begriffs „dezentral“ i. S. d. Art. 2 Buchst. c DSRL zu beachten. Den Begriff der Zentralisierung, der die Streubreite berührt, meint die EU-Kommission in ihrem Überblick über das Informationsmanagement im sog. Bereich der Freiheit, Sicherheit und des Rechts [Komm10].

Transparenz: Beim zentralen Abgleich verlagert sich die konzentriert sich die Verarbeitung von Daten über eine Vielzahl von Personen bei der Zentrale. Wenn Betroffene Rechtsschutz begehren, verweist die örtliche Polizeidienststelle an die Zentrale. Die zuständige Datenschutzbehörde und das zuständige Gericht können jedoch nur einer begrenzten Zahl an Beschwerden nachgehen; dies kann den Rechtsschutz faktisch verhindern. Aufgrund der vertikalen Gewaltenteilung (s. u.) ist die jeweilige Landesdatenschutzbehörde zuständig; sie kann jedoch nur dann gemäß Art. 20 DSRL und § 4d Abs. 5 BDSG über den Systemeinsatz entscheiden, soweit Daten durch die Landespolizei verarbeitet werden.

Gefühl des Überwachtwerdens: Durch die hohe Streubreite, die bundes- oder europaweites Zentralsystem hat, können sich Betroffene eher überwacht fühlen, als durch den Einsatz einer Überwachungstechnik, bei der Betroffene Folgemaßnahmen höchstens im überwachten Raum fürchten müssen. Daher verstärkt der zentrale Abgleich das Gefühl des Überwachtwerdens.

Datensparsamkeit: Die Daten über Unverdächtige werden an ein anderes System i. S. d. § 3 Abs. 4 Nr. 3 BDSG und Art. 2 Buchst. b DSRL übermittelt oder sonst wie fernübertragen. Diese Fernübertragung kann vermieden werden, da das Erfassungsgerät auch selbst den Abgleich ausführen kann. Die Übermittlung ist für den festgelegten Zweck, Verdächtige am Einsatzort zu entdecken und anzuhalten, nicht erforderlich. Auch die Daten, die im entfernten System nach der Übermittlung gespeichert sind, sind für die Erreichung des verfolgten Ziels nicht erforderlich.

Einheitliche Personenkennzeichen: Zwar werden die biometrischen Charakteristika beim Einsatz des Systems zur Verdachtsgewinnung nicht für eine umfassende Registrierung verwendet - die biometrischen Daten werden nur mit dem Standort des biometrischen Erfassungsgeräts verknüpft. Trotzdem muss die Wertung, dass die Verwendung einheitlicher Personenkennzeichen für den Grundrechtsschutz riskant ist, im Rahmen der Verhältnismäßigkeit berücksichtigt werden.

Die Verwendung einheitlicher Personenkennzeichen wird bereits mit der Datenerfassung durch ein einziges Erfassungsgerät ermöglicht. Biometrische Charakteristika sind als solche eindeutige Kennzeichen [WP2903]. Die Verwendbarkeit als einheitliche Personenkennzei-

chen wird erhöht, weil biometrische Charakteristika nicht nur einzigartig, sondern auch universell (jeder hat sie) und lebenslang gültig sind.

Zusätzlich erhöht der zentrale Abgleich diese Möglichkeit. Risiken für den Grundrechtsschutz entstehen dadurch, dass vielfältige Nutzungen und Verknüpfungen personenbezogener Daten möglich sind, diese Daten technisch unbegrenzt speicherbar und in Sekundenschnelle abrufbar sind sowie zu Datensammlungen zusammengefügt werden können [BVGE08]. Insbesondere für biometrische Systeme wurde festgestellt, dass bei zentraler Verarbeitung biometrische Daten eher als „Zugangsschlüssel“ zu verschiedenen Datenbanken verwendet werden könnten [WP2905]. Es könnte dann auch nicht nur ein einziger Aufenthaltsort gespeichert werden, sondern es könnten potenziell die Ortsdaten aller überwachten Räume zu einem Bewegungsprofil vervollständigt werden.

1.1.3 Zweckbindung und informationelle Gewaltenteilung

Das Prinzip der Zweckbindung verbietet, dass Daten zweckwidrig verwendet werden [BVGE83]. Dieses wird durch das Prinzip der informationellen Gewaltenteilung konkretisiert [BVGE83]. Dieses Prinzip ist verfassungsrechtlich anerkannt [BVGE83] und in § 9 Satz 1 i. V. m. Nr. 8 der Anlage des BDSG ausgedrückt. Das Prinzip der informationellen Gewaltenteilung ist - innerhalb der Grenzen der Zweckbindung - eine Ausprägung des allgemeinen Prinzips der Gewaltenteilung. Neben der horizontalen Teilung zwischen Legislative, Exekutive und Judikative nach Art. 20 Abs. 2 Satz 2 GG schreibt dieses Prinzip die vertikale Teilung vor. Die vertikale Gewaltenteilung wird durch die Bundesstaatlichkeit nach Art. 20 Abs. 1 und Art. 30 GG und kommunale Selbstverwaltung nach Art. 28 Abs. 2 Satz 1 GG [LVEC85] ausgedrückt.

Allgemeiner drückt dies das Prinzip der Subsidiarität nach Art. 5 EUV i. V. m. dem Protokoll über das Subsidiaritätsprinzip [Proto07] aus, welches nach Art. 23 GG anerkannt ist. Entsprechend dem Subsidiaritätsprinzip werden Entscheidungen möglichst bürgernah getroffen [Präa07]. Je näher Entscheidungen am Bürger getroffen werden, desto größer ist der Raum für Selbstbestimmung, von welcher die informationelle Selbstbestimmung eine Ausprägung ist.

Entsprechend wird festgestellt, dass das Prinzip der informationellen Gewaltenteilung eine Dezentralisierung staatlicher Datensammlungen vorschreibt [Stube09]. Auch das Bundesverfassungsgericht hat dieses Prinzip so weiterentwickelt, dass es nicht nur der Transparenz dient. Zusätzlich hält es für grundrechtsfördernd, wenn Daten bei der Speicherung nicht zusammengeführt, sondern auf viele einzelne Unternehmen verteilt bleiben [BVGE10]. Es begründet diese Ansicht damit, dass die Daten dem Staat im Ergebnis nicht in ihrer Gesamtheit verfügbar sind [BVGE10]. Damit ist ausdrücklich für die informationelle Selbstbestimmung anerkannt, dass auch eine vertikale Datenteilung unter Vielen, also eine “informationelle Bürgernähe” oder “Datensubsidiarität”, geboten ist.

Insbesondere für biometrische Systeme wurde festgestellt, dass durch Schaffung einer zentralen Datenbank das Risiko der Zweckentfremdung erhöht wird [WP2905]. Das Risiko einer solchen Zweckentfremdung hängt zum einen davon ab, ob die Vorteile für Innenminister und Polizeibehörden aus der Einführung einer Rechtsgrundlage für Zweckänderungen die Nachteile überwiegen. Ein Gesetzgebungsverfahren für die Rechtsgrundlage einzuleiten und Forderungen bis zum Schluss zu verteidigen, ist mit Mühen verbunden. Diesen Nachteil überwiegt nur ein großer Fahndungserfolg. Mit der zentralen Verarbeitung wächst die informationelle Macht der Zentrale. Die Macht verschiebt sich im Gegensatz zur herkömmlichen poli-

zeilichen Arbeit - von der Dienststelle zur Zentrale. Dadurch konzentriert sich die informationelle Macht.

Gegenstand der vertikalen Gewaltenteilung sind die drei Gewalten: Legislative, Exekutive und Judikative. Zur Exekutive gehören die Regierungen und Verwaltungen, wie z. B. die Polizeien. Die unterste Ebene der Regierung ist die Landesregierung, welche Polizeigesetze vorschlägt. Ein Gesetz, das einen zentralen Abgleich durch das BKA regelt, darf sie nicht nur deshalb nicht vorschlagen, weil schon zweifelhaft ist, ob die Weisungen der 16 Landespolizeien wirksam sein und eine Auftragsverarbeitung angenommen werden können, sondern auch weil es dem Sinn und Zweck der vertikalen Gewaltenteilung - Polizeirecht ist Ländersache - widerspräche. Die unterste Ebene der Polizeibehörde ist die einzelne Polizeidienststelle. Bezüglich des zentralen biometrischen Abgleichs darf also höchstens die Polizeidienststelle die biometrischen Proben verarbeiten. Eine Übermittlung der biometrischen Proben aus dem Erfassungsgerät an eine andere Stelle, an welcher zentrale Abgleiche durchgeführt würden, verletzt das Prinzip der informationellen Gewaltenteilung und somit der Zweckbindung.

1.1.4 Datensicherheit

Es muss ein Standard an Datensicherheit gewährleistet werden, der die spezifische Eingriffstiefe berücksichtigt [BVGE10]. Die zentrale Verarbeitung hat den Vorteil, dass Aufwand an Zeit, Kosten und Arbeitskraft eingespart werden kann. Auf die biometrischen Referenzen könnte insbesondere unbefugt zugegriffen werden, um eine erfolgreiche Identifizierung von gesuchten Kriminellen zu verhindern. Vor einem solchen Zugriff schützt das Grundrecht auf informationelle Selbstbestimmung jedoch nicht. Das Grundrecht, konkretisiert durch das Datenschutzrecht, schützt nach § 1 Abs. 1 BDSG den Einzelnen davor, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Durch den Zugriff, mit dem er seine Bestrafung verhindert, wird der einzelne Kriminelle jedoch nicht beeinträchtigt.

Außerdem trifft das Argument der besseren Schutzmöglichkeiten zwar für Referenzen, nicht aber die Vielzahl von biometrischen Proben zu. Der Schutz der Referenzen dient dem Fahndungserfolg. An diesem Schutz sind Innenministerien und Polizeibehörden daher selbst interessiert. Außerdem ist zu berücksichtigen, dass im Gegensatz zur Vielzahl der unverdächtigen Betroffenen die Datenverarbeitung bezüglich der kleinen Zahl von potenziellen Terroristen nicht breit streut. Ferner müssen sie Einschränkungen ihres Grundrechts auf informationelle Selbstbestimmung hinnehmen.

Die Proben sind sicherer, wenn sie so früh wie möglich und ohne Übermittlung oder sonstiger Übertragung gelöscht werden. Außerdem gibt es bei dezentraler Verarbeitung kein Bedürfnis nach einem Schutzniveau, mit dem Angriffe auf zentrale Systeme abgewehrt werden. Im Gegenteil, so schreiben nämlich die Verfassung [BVGE10] sowie Art. 17 Abs. 1 Satz 2 DSRL und § 9 Satz 2 BDSG vor, dass die Maßnahmen für die Datensicherheit das spezifische Eingriffsgewicht berücksichtigen bzw. angemessen sein müssen. Die Angemessenheit hängt u. A. von der Größe der Datei ab [Geig06]. Für zentrale Verarbeitung müsste ein Standard an Datensicherheit gewährleistet werden, der berücksichtigt, dass nicht die Daten bezüglich eines einzigen überwachten Raums, sondern aller überwachten Räume verarbeitet werden. Insbesondere für biometrische Systeme wird festgestellt, dass ein Zentralsystem die Risiken der Zweckwidrigkeit im Sinne des unbefugten Zugriffs steigert [WP2905] [Cavo98].

Neben unbefugten Zugriffen, vor denen das Grundrecht nicht schützt, sind auch unbefugte Zugriffe denkbar, die die Persönlichkeit der gesuchten Störer und Verdächtigen beeinträchti-

gen. Daher sollte für die Referenzen nach dem Prinzip der Datensparsamkeit nur das Minimum an Personenbezug hergestellt werden. Diese Personen werden durch Nutzung von Indexdaten, mit denen die Referenzen pseudonymisiert werden, geschützt. Außerdem könnte zwar auch bei Verarbeitung im Erfassungsgerät ein Einzeltäter interessiert sein, unbefugt auf Daten zuzugreifen. Ihm könnte jedoch die technische Unfähigkeit den Datenzugriff verhindern. Die zentrale, bundes- oder europaweite Verarbeitung könnte jedoch darüber hinaus das Interesse von terroristischen und anderen kriminellen Organisationen oder das politische Interesse anderer Staaten wecken. Solche Organisationen können die Menge an Zeit, Geld und Expertise haben, die selbst die anspruchsvollsten Datensicherheitsmaßnahmen unwirksam machen. Der Aufwand an Zeit, Geld und Expertise, mit dem die Datensicherheit der biometrischen Proben sichergestellt wird, kann vermieden werden, wenn die Abgleiche in dezentralen Systemen durchgeführt werden. Sofern nicht ein Standard an Datensicherheit gewährleistet wird, der die spezifische Eingriffstiefe berücksichtigt, verletzt der zentrale Abgleich das Prinzip der Datensicherheit.

1.1.5 Unionsrechtskonforme Auslegung

Zudem folgt eine Anforderung aus der Datenschutzrichtlinie 95/46/EG: das Prinzip des Schutzes sensibler Daten. Der zentrale Abgleich verletzt das Prinzip des Schutzes sensibler Daten, da sensible Daten nach Art. 8 Abs. 1 DSRL (aus welchen z. B. die ethnische Herkunft hervorgeht, und Daten über Gesundheit) [WP2903]. Aufgrund des zentralen Abgleichs werden solche Daten jedoch zusätzlich übermittelt oder sonst wie übertragen und in einem anderen System gespeichert und genutzt. Somit verletzt der zentrale Abgleich das Prinzip des Schutzes sensibler Daten.

1.1.6 Gesetzliche Analogie

Überdies folgt eine Anforderung aus dem Pass- und Ausweisrecht: die Verbote zentraler Dateien. Die Verbote sind Wertungen des Gesetzgebers und im Rahmen der gesetzlichen Analogie zu berücksichtigen. Für die Pass- und Ausweisregister verbieten § 4 Abs. 3 Satz 3 Passgesetz und § 26 Abs. 4 Personalausweisgesetz die Errichtung einer bundesweiten Datenbank für biometrische Daten. Eine solche Errichtung, etwa zu Zwecken der inneren Sicherheit, wäre grundrechtlich unzulässig [RoHo05] [Horn07]. Die Verbote des Pass- und Ausweisrechts regeln die Verarbeitung von Daten über jeden, also solchen Personen, die durch ihr Verhalten keinen Anlass für die Verarbeitung geschaffen haben. Auch beim biometrischen Systemeinsatz ist jeder betroffen, ohne einen Anlass für die Verarbeitung geschaffen zu haben. Die beiden Sachverhalte sind somit vergleichbar und die analog anzuwenden.

Insgesamt ist festzustellen, dass der Eingriff in das Grundrecht auf informationelle Selbstbestimmung besonders schwer ist. Vor- und Nachteile von zentraler und dezentraler Datenspeicherung beziehen sich aus technischer Sicht hauptsächlich auf den Schutz der Referenzen und Performanz, welche grundrechtlich im Rahmen der Eignung berücksichtigt werden. Aus rechtlicher Sicht ist dagegen vor allem der Schutz der Proben bedeutsam. Insbesondere erhöht der zentrale Abgleich das Eingriffsgewicht. Die rechtliche Beurteilung gilt unabhängig vom spezifischen Einsatzzweck, da der zentrale Abgleich im Gegensatz zum dezentralen immer den Grundrechtseingriff vertieft. Der dezentrale Abgleich im Erfassungsgerät stellt daher ein milderes Mittel i. S. d. Erforderlichkeit dar. Dies folgt aus der Verhältnismäßigkeit i. e. S. Demzufolge ist ein zentraler Abgleich unzulässig.

Technikgestaltung

Aufgrund der oben genannten rechtlichen Anforderungen muss die Technikgestaltung rechtlich geregelt werden. Die Verfassung schreibt den Inhalt der Regelung nicht detailgenau vor. Im Ergebnis muss jedoch ein Standard gewährleistet werden, der die spezifische Eingriffstiefe berücksichtigt [BVGE10]. Erforderlich ist daher eine gesetzliche Regelung, die einen Abgleich im Erfassungsgerät eines dezentralen Systems in qualifizierter Weise jedenfalls dem Grunde nach normenklar und verbindlich vorgibt (in Anlehnung an [BVGE10]).

Die Festlegung von technischen Gestaltungskriterien folgt insbesondere aus dem Prinzip „Privacy by Design“ (eingebauter Datenschutz). An dieses Prinzip sind aufgrund des spezifischen Eingriffsgewichts erhöhte Anforderungen zu stellen. Dieses Prinzip verlangt, die Einhaltung der Datenschutzprinzipien durch technisch-organisatorische Maßnahmen des Technikgestalters zu gewährleisten [WP2909] [Pocs11d]. Wenn Polizeibehörden das biometrische System einsetzen, wird die Technik mittels öffentlicher Vergabe beschafft, in deren Bedingungen die Gestaltungskriterien aufgenommen werden sollten.

Die aus der rechtlichen Beurteilung abzuleitenden technischen Maßnahmen sind zu differenzieren, je nachdem, ob der Abgleich sofort erfolgt oder erst anlassbezogen, z. B. wenn das Flugzeug abstürzt [Hil+11]. Bei anlassbezogenen Erfassungen werden die Daten länger gespeichert. Daher sind für sie nicht nur die i. F. genannten, sondern weitergehende technische Maßnahmen notwendig, welche gesondert untersucht worden sind [HiPo12].

Das Risiko zweckwidriger Datenzugriffe kann nur dann ausreichend minimiert werden, wenn das biometrische Fahndungssystem so gestaltet wird, dass der biometrische Vergleich nicht etwa in externen Referenzdatenbanksystemen, sondern im Erfassungsgerät selbst erfolgt. Für die Durchführung im Erfassungsgerät müssen die Referenzen als Indexdaten aus dem zentralen System in die Erfassungsgeräte kopiert werden. Die Erfassungsgeräte können mit der Zentrale vernetzt werden, um die Referenzen automatisiert zu aktualisieren. Die Erfassungsgeräte müssen dann jedoch so geschützt werden, dass der Zugriff der Zentrale auf die Proben auch trotz der Vernetzung auf diese eine Richtung der Netzwerkkommunikation beschränkt ist. Also darf zwar der Download der Referenzen, nicht aber der Upload der Proben, der erfassten Daten über die Vielzahl der Unverdächtigen, möglich sein.

Wenn eine Aktualisierung der Referenzen zu aufwendig ist, kann sie notfalls weniger häufig durchgeführt werden, da dieser Spielraum bezüglich der grundrechtlichen Eignung aufgrund des hohen Eingriffsgewichts genutzt werden muss. Jedoch muss berücksichtigt werden, dass bei einzelnen Störern und Verdächtigen der Anlass bzw. Verdachtsgrund zwischenzeitlich entfallen sein kann. Polizeibeamte, die Treffer weiterverfolgen, müssen die Daten entsprechend interpretieren können. Daher müssen sie entsprechend geschult werden. Außerdem müssen die Daten unverzüglich abgeglichen und sofort spurenlos gelöscht werden [BVGE08]. Dazu ist notwendig, dass der Arbeitsspeicher des Erfassungsgeräts klein ist und nur eine begrenzte Zahl an Proben erfassen kann. Im Fall der automatisierten Kfz-Kennzeichenerfassung kann der flüchtige Speicher höchstens neun Kennzeichen gleichzeitig verarbeiten [Hess07b].

Fazit

Bevor die Polizei ermächtigt wird, biometrische Systeme zum Entdecken potenzieller Terroristen und Schwerkrimineller einzusetzen, muss die Entscheidung zwischen zentralem und dezentralem Abgleich getroffen werden. Die Umsetzung des technischen Gestaltungsvorschlags

ist ein wichtiger Aspekt, um die Verfassungsverträglichkeit des Systemeinsatzes herzustellen. Der Gestaltungsvorschlag könnte darüber hinaus auch künftige grundrechtliche Untersuchungen über die Systemarchitektur in anderen Systemen anstoßen, in denen der Verdacht wie bei biometrischen Systemen der Verhaltensmusteranalyse anhand von allgemeinem abweichendem Verhalten gewonnen wird.

Die Gesellschaft kann mit dem neuartigen Risiko der Zentralisierung von Körper- und Ortsdaten umgehen. Ein solcher verfassungsverträglicher Umgang ist auch notwendig, um beides zu erreichen: Schutz vor Gefahren und Straftaten sowie Schutz vor Folgen des Missbrauchs informationeller Macht. Wenn diese und andere Gestaltungsmöglichkeiten genutzt werden, kann das Fundament für eine Zukunft der Verbrechensbekämpfung gelegt werden, die sich die Gesellschaft wünscht.

Literatur

[BBD+10] Jüngst BVerfG, 2 BvR 1372/07, Abs. 18; seit BVerfGE 65, 1.

[BKA-07] Bundeskriminalamt, Bericht zur "Fotofahndung", http://www.bka.de/kriminalwissenschaften/fotofahndung/pdf/fotofahndung_abschlussbericht.pdf, 2/2007.

[BKAG09] §§ 2 Abs. 3 und 11 Abs. 1 BKA-G.

[Bode10] Bodenbenner, NVwZ 2010, 679.

[BVGE83] BVerfGE 65, 1 (53) und 27, 1 (6); 65, 1 (46); bzw. 65, 1 (69).

[BVGE01a] BVerfGE 115, 320 (354 f.); 107, 299 (328).

[BVGE01b] So z. B. BVerfGE 115, 320 (345); 100, 313 (373).

[BVGE04] So z. B. in BVerfGE 115, 320 (355) m. w. N. als Spezialfall der Fahndung.

[BVGE05] BVerfGE 113, 29 (46); 65, 1 (42).

[BVGE06] BVerfGE 118, 168 (197 f.); 113, 348 (383 f.).

[BVGE07] So z. B. in BVerfGE 120, 274.

[BVGE08] Sammlung Entscheidungen des Bundesverfassungsgerichts (BVerfGE) 120, 378.

[Cavo98] Cavoukian, Tagung Computers, Freedom and Privacy 98, Austin (Texas).

[Crime11] So z. B. von der australischen Behörde für polizeiliche Informationstechnik „CrimTrac", http://www.crimtrac.gov.au/systems_projects/Biometrics.html

[DaMa04] Daugman/Malhas, International Airport Review 2/2004.

[DiDa10] Diese Arbeit wurde durch das BMBF gefördert, FKZ: 13N10820 - "Digitale Fingerspuren" (Digi-Dak), http://omen.cs.uni-magdeburg.de/digi-dak/

[DPS+11] Desoi/Pocs/Stach in: Brömme/Busch, Proceedings BIOSIG 2011 (eingereicht).

[DSDS95] § 3a BDSG; Art. 6 Buchst. c/e DSRL; Art. 5 Buchst. c/e DSÜ SEV Nr. 108.

[EuGH08] EuGH, Huber ./. Deutschland, C-524/06 v. 16.12.2008, Abs. 66 bzw. 42.

[FPBM11] FP7-Projekte: ADABTS (RCN: 91158), SAMURAI (89343), SUBITO (89391); BMBF-Projekte: z. B. ADIS (FKZ: 13N10977-9); CamInSens (13N10814).

[Gate10] Gates, Culture Unbound 2/2010, S. 67.

[Geig06] Geiger in: Simitis, BDSG, 6. Aufl., Baden-Baden 2006, § 9 Rn 28.

[Hess07a] Hess. Staatskanzlei, 5/2007, http://www.daten-speicherung.de/data/Schriftsatz_Staatskanzlei_2007-06-01.pdf, S. 2; auch Roßnagel, NJW 2008, 2547 (2547).

[Hess07b] Hessische Staatskanzlei, 23.10.2007, http://www.daten-speicherung.de/data/Hessen_Antworten_2007-10-23.pdf, Frage 3.

[Hil+11] Hildebrandt u. A., in: Proceedings BioID 2011, LNCS 6583, Berlin (2011) 286.

[HiPo12] Hildebrandt/Pocs in: Gutwirth u. A.: Proceedings Computers, Privacy & Data Protection, Heidelberg 2012 (eingereicht).

[HoDP10] Hornung/Desoi/Pocs in: Brömme/Busch, Proceedings BIOSIG 2010, Bonn 2010, S. 83.

[Horn05] Hornung, Die digitale Identität, Baden-Baden 2005, Fn 1153.

[HSOG10] § 14a Abs. 2 HSOG.

[INDE11] INDECT, FP7 RCN: 89374, D7.2, D4.3; EU-Parlament fordert Aussetzung, Bericht des EP (A7–0160/2011), 15.4.2011, Abs. 27.

[ISO-09] Zur Terminologie, ISO SC37 Harmonized Biometric Vocabulary (SD 2 V12) in SC37 WG 1.

[Komm10] KOM(2010)385 endg., 20.7.2010, Nr. 3 („Decentralised structure“).

[LVEC85] So z. B. Art. 137 Abs. 1 Hess. Verfassung; Charta SEV Nr. 122, 15.10.1985.

[Pocs11a] Pocs, DuD 2011, 163.

[Pocs11d] Pocs in: Proceedings PATS Privacy and Accountability 2011 (i. E.).

[Pocs11e] Pocs, Kriminologisches Journal (KrimJ) 2011 (i. E.).

[Präa07] Präambel des EUV und Protokolls über das Subsidiaritätsprinzip.

[Proto07] Protokoll Nr. 2 zum Lissaboner Vertrag, ABl. 2007 EU C 306 S. 150.

[RoHo05] Roßnagel/Hornung, in: Reichl/Roßnagel/Müller 2005, 138; DuD 2005, 69, 72; Hornung, KJ 2004, 344, 357; DuD 2007, 181 (185).

[Roßn08] Roßnagel, NJW 2008, 2547 (2547).

[Stube09] Ausführlich Stubenrauch, Gemeinsame Verbunddateien von Polizei und Nachrichtendiensten, Baden-Baden 2009, S. 133 f.

[WP2903] Art.-29-DS-Gruppe: Biometrics (WP80), Nr. 3.7 bzw. 3.2.

[WP2905] Art.-29-DS-Gruppe: Biometric Passports (WP112), Nr. 2.3 a).

[WP2909] Art.-29-DS-Gruppe: The Future of Privacy (WP168), Abs. 107, 112 bzw. 46.