Vier Augen, zwei Behörden und eine Technik für künftige Biometrie-basierte Kriminalitätsbekämpfung

Matthias Pocs, LL. M.
Projektgruppe verfassungsverträgliche Technikgestaltung
Universität Kassel
Wilhelmshöher Allee 64-66, 34109 Kassel
matthias.pocs@uni-kassel.de

Abstract: Biometrische Fahndungstechnik wird gegenwärtig erforscht. Sie verspricht, potenzielle Terroristen und andere Kriminelle aufzuspüren, aber birgt auch neuartige Risiken. Ein Szenario ist die vorsorgliche biometrische Datenerfassung, mit der Flugzeugabstürze u. Ä. aufgeklärt werden könnten. Um den Schutz des Grundrechts auf informationelle Selbstbestimmung sicherzustellen, schlägt dieser Beitrag eine Technikgestaltung für die Pseudonymisierung vor. Die Technikgestaltung soll eine sichere, offene, „smarte“ und vernetzte Verwaltungskultur fördern.

1 Einleitung

Polizeibehörden setzen schon gegenwärtig biometrische Technik ein. So hat z. B. das Bundeskriminalamt die Gesichtserkennung getestet [BKA07], 2001 wurde in Tampa (Florida) ein Gesichtserkennungssystem eingesetzt [Ga10] und Iriserkennung wird routinemäßig beim Grenzübergang in die Vereinigten Arabischen Emirate genutzt [DM04]. Entsprechende Forschung wird gefördert, z. B. Fingerspurenscanning an Gepäckstücken [Hi11], Gangerkennung [Bo11] und Verhaltensanalyse aus der Videoüberwachung [FP09].

Aufgrund dieser Entwicklungen ist es vorstellbar, dass künftig Gesetze erlassen werden, die eine vorsorgliche Datenerfassung - also vor Verursachung einer Gefahr oder Begehung einer Straftat - erlauben. Ein mögliches künftiges Szenario, in dem biometrische Daten von Bedeutung sind, könnte wie folgt aussehen: Am Flughafen könnten Gesichtsaufnahmen von Videoüberwachungskameras automatisiert erfasst werden. Sollte dann der Absturz des Flugzeugs herbeigeführt oder das Flugzeug entführt werden, könnten die vorsorglich erfassten Daten auf bereits bekannte Daten aus einer Datenbank (von Kontaktpersonen, Kriminellen o. ä.) durchsucht werden.

Solche vorsorglichen Datenerfassungen stellt das Recht vor neue Herausforderungen [DPS11] [Po12] [Po11a] [Hi11] [HDP10], insbesondere weil biometrische Charakteristika (und damit personenbezogene Daten) erfasst werden, ohne dass der Betroffene einen Anlass dafür geschaffen hat, sowie eine Vielzahl von Personen davon betroffen ist. Dieser Beitrag untersucht daher, ob die Verfassung eine Regelung zur Pseudonymisierung vorschreibt und wie die Technikgestaltung konkret geregelt werden sollte. Er untersucht nicht das allgemeine Verhältnis zwischen den Zielen der Kriminalitätsbekämpfung und dem Eingriff in Grundrechte, sondern greift einen Vorschlag für die Technikgestaltung heraus. Die wissenschaftliche Leistung dieses Beitrags ist die Konkretisierung rechtlicher Anforderungen für eine verfassungsverträgliche Technikgestaltung anhand der spezifischen Technik der Pseudonymisierung.

Die untersuchte Pseudonymisierung beruht darauf, dass die Daten in sog. „Pseudoidentitäten“ und „Hilfsdaten“ zerlegt werden (mittels „Biometric Template Protection“) und nur die Datenschutzbehörde die Hilfsdaten aufbewahrt. Dadurch soll eine sichere, offene, ‚smarte‘ und vernetzte Verwaltungskultur gefördert werden: die „informationelle Gewaltenteilung“ schafft Transparenz und Kontrolle, Biometric Template Protection ist sicher und ‚smart‘ und für die Übermittlung der Hilfsdaten muss die Datenschutzbehörde mit der Polizei (monodirektional) eine vernetzte Architektur und organisationsübergreifende Prozesskette verfügbar sein.

Nach dieser Einleitung werden im zweiten Abschnitt die technischen Besonderheiten künftiger biometrischer Systeme und ein Szenario für den Systemeinsatz beschrieben. Im dritten Abschnitt wird untersucht, wie die besondere Technik der Pseudonymisierung rechtliche Ziele der Verfassung fördert. Im vierten Abschnitt werden Gestaltungsvorschläge für die Technik entwickelt, die für das spezifische Szenario der Kriminalitätsbekämpfung bestimmt ist. Im fünften Abschnitt schließt dieser Beitrag mit einem kurzen Fazit.

2 Künftige Biometrie und ihre Chancen und Risiken

Biometrische Anwendungen für die Kriminalitätsbekämpfung: Der Einsatz künftiger biometrischer Systeme für die Kriminalitätsbekämpfung stellt das Recht vor neue Herausforderungen, weil er sich vom Einsatz herkömmlicher Systeme zur biometrischen Zugriffs-, Zugangs-, Zutritts- und Ausweiskontrolle unterscheidet. Die künftigen Anwendungen zeichnet insbesondere aus, dass die biometrischen Charakteristika in unkontrollierten Umgebungen, in welchen der Betroffene nicht mitwirken muss, automatisiert erfasst werden.

Zunächst ist zwischen Mustererkennung einerseits und andererseits Biometrie im engeren Sinne zu unterscheiden. Bei Technologien der Mustererkennung (Optik, Photonik, Signalverarbeitung usw.) werden nur die rohen biometrischen Daten in Form von Bildern erfasst. Dazu gehören z. B. Forschungsprojekte wie “Digi-Dak” [Hi11], bei denen die Spuren von Fingerabdrücken, die bei der Gepäckabfertigung an Koffern hinterlassen werden, gescannt werden. Hier ist ein automatischer Abgleich jedoch technisch nicht möglich. Bei Technologien der Biometrie im

engeren Sinne hingegen werden nicht nur Bilder erhoben, sondern auch Merkmale aus den Rohdaten extrahiert. Dadurch können erfasste Daten automatisiert mit biometrischen Referenzen abgeglichen werden. Der Ansatz der Biometric Template Protection damit der Technikgestaltung, die in diesem Beitrag vorgeschlagen wird, funktioniert nur bei Technologien der Biometrie im engeren Sinne.

Das für diesen Beitrag konkret zu realisierende Szenario kann dabei aus technischer Sicht, wie folgt beschrieben werden: Aufnahmen von Videoüberwachungskameras werden automatisiert auf Gesichter untersucht und vorsorglich erfasst. Dabei werden die Gesichter in Pseudoidentitäten (PI) (nach [BB08]) überführt. Die Hilfsdaten („Auxiliary Data“; nach [BB08]), also im simpelsten Fall die Systemparameter, unter denen die PI berechnet wurden oder ein kryptografischer Schlüssel o. Ä., werden ebenfalls gespeichert.

Anschließend werden die Hilfsdaten zu allen erstellten PI an einen Treuhänder, in diesem Fall eine Datenschutzbehörde, gesendet und für die Dauer eines Fluges verwahrt. Die PI werden für dieselbe Dauer bei der Polizeidienststelle hinterlegt. Sollte nun während des Fluges ein gesetzlich bestimmter Vorfall eintreten (herbeigeführter Absturz, Entführung, Reise von Mitgliedern der organisierten Kriminalität o. Ä.), sollen die vorsorglich gespeicherten PI die Identifikation beteiligter, bekannter Krimineller ermöglichen. Dafür greift die Polizeidienststelle auf die biometrische Referenzdatenbank zu und erlangt Zugriff auf die zu den PI gehörigen Hilfsdaten von der Datenschutzbehörde. Nun erzeugt die Polizeidienststelle zu den Referenzdaten mittels der Hilfsdaten ebenfalls PI, welche dann mit den am Flughafen erfassten PI verglichen werden.

Die vorsorgliche biometrische Datenerfassung erweitert das bisherige polizeiliche Instrumentarium, da ihretwegen Daten zur Kriminalitätsaufklärung verfügbar werden. Ziel ist es, Hinweise zum Aufdecken von kriminellen Netzwerken zu gewinnen. Die Referenzen, mit denen die am Flughafen erfassten Daten verglichen werden, stammen aus einer früheren Sicherung von Gesichtsbildern an überwachten Orten und Erstellung von Lichtbildern von Kriminellen. Über die Orte und Kriminellen werden häufig kriminologische Profile erstellt. Im Fall der terroristischen und organisierten Kriminalität können solche Profile offenlegen, mit wem der Fluggast in Kontakt stand. Außerdem können können sich Fluggäste in der Eingangshalle des Flughafens mit anderen Mitgliedern des kriminellen Netzwerks getroffen haben; dies legt auch offen, mit wem der Fluggast in Kontakt stand. Der Vorfall auf dem Flugzeug kann somit mit anderen Gesichtsbildern oder bekannten Kriminellen zusammenhängen.

Bisher sind rechtliche Regelungen zum Schutz von Personen, die von biometrischen Systemen betroffen sind, nur für die Verifikation (z. B. für die Zutrittskontrolle), jedoch nicht für die Identifikation auf vorsorglich erfassten Daten für die Kriminalitätsaufklärung entwickelt worden. Dieser Beitrag untersucht einen bestimmten Schutzmechanismus und szenarienspezifische Maßnahmen. Durch die institutionelle Trennung zwischen Datenschutzbehörde und Polizei wird nicht nur das Schlüsselmanagement anspruchsvoll, sondern es muss auch die Systemadministration auf dieser Ebene diskutiert werden muss, damit die Polizei nicht etwa das Verschlüsselungsprogramm einseitig ändern kann. Die

szenarienspezifischen Maßnahmen beinhalten u. A. eine automatisierte Löschung nach Landung des Flugzeugs.

Rechtliche Chancen und Risiken: Der Einsatz von Systemen zur automatisierten Erfassung biometrischer Charakteristika zwecks Fahndungsabgleich bietet Chancen und birgt Risiken. Einerseits können mit dem Einsatz die Begehung von Straftaten und Verursachung von Gefahren verhindert werden. Andererseits birgt der Systemeinsatz spezifische Risiken [DPS11] [Po12] [Po11a] [Po11b] [Hi11] [HDP10]:

- Offenbarung sensibler Informationen aus Roh- und Template-Daten ([WP03], Nr. 3.7),
- Verknüpfung mehrerer Datenbanken zu einem Persönlichkeitsprofil aufgrund der Einzigartigkeit,
- … Universalität (jeder hat biometrische Charakteristika) und
- … lebenslangen Gültigkeit biometrischer Charakteristika ([WP03], Nr. 3.2),
- Gewinnung von Informationen über Aufenthaltsort, Zeit und Zielort,
- Falschtreffer (es sei denn, der Abgleich ist i. G. z. Erfassung anlassbezogen),
- heimliche Datenerfassung (Fingerabdrücke und Gesichter hinterlassen Spuren ([WP03], Nr. 3.2)),
- unbefugter Datenzugriff („Identitätsdiebstahl“),
- zweckfremder Datenzugriff (z. B. Ahndung von Ordnungswidrigkeiten oder Bildung von Profilen über Kontaktpersonen (ausführlich [Po11a]),
- Folgemaßnahmen durch die Polizei am Einsatzort sowie
- Sicherheitsparadox bei konkurrierenden Kontrollen.

Insbesondere ist zu befürchten, dass eine Vielzahl von Personen identifizierbar wird, ohne einen Anlass für die Datenerfassung geschaffen zu haben. Daher ist zu untersuchen, inwieweit das Grundrecht auf informationelle Selbstbestimmung Regelungen zur Pseudonymisierung von vorsorglich erfassten biometrischen Daten vorschreibt.

Verfassungsverträgliche Technikgestaltung: Wissenschaft und Technik können insbesondere durch Regelung der Technikgestaltung geleitet werden. Die Konkretisierung rechtlicher Anforderungen für eine verfassungsverträgliche Technikgestaltung (KORA) ist eine rechtswissenschaftliche Methode, um Vorschläge für die Technikgestaltung zu entwickeln. Dies zielt darauf ab, vorhersagbare Risiken der Technikanwendungen zu vermeiden und zusätzliche Chancen zu nutzen. Dazu werden konkrete Anforderungen für Techniksysteme von rechtlichen Vorgaben in einem bestimmten mehrstufigen Prozess abgeleitet.

Diese Stufen beinhalten die Ableitung (1.) rechtlicher Anforderungen aus rechtlichen Vorgaben, (2.) rechtlicher Kriterien aus diesen Anforderungen, (3.) technischer Ziele aus diesen Kriterien

und (4.) technischer Gestaltungsvorschläge aus diesen Zielen. Während die ersten beiden Stufen in der Sprache des Rechts geprüft werden, werden die beiden letzten Stufen in der Sprache der Technik geprüft [Ha93] [Pr11]. Daher müssen erst rechtliche Kriterien erforscht werden, um Gestaltungsvorschläge aus der Verfassung abzuleiten. Um den Rahmen dieses Beitrags nicht zu sprengen, werden die ersten beiden Stufen mit der rechtlichen Analyse (Abschnitt 3) zusammengelegt.

Die Kriterien sind allgemeingültig, weil sie aus der Verfassung - der höchsten deutschen Rechtsquelle - abgeleitet werden. Verträglichkeit technischer Systeme mit der Verfassung wird verbessert, wenn sie die Ziele der Verfassung fördern. Die Methode legt das Zusammenwirken von sozialen, technischen und rechtlichen Systemen zugrunde und zeigt Möglichkeiten, eine verfassungsverträgliche Technikgestaltung zu verwirklichen, in Zusammenarbeit mit Technikentwicklern, -betreibern und -nutzern [Pr11].

Die verfassungsrechtlichen Kriterien (Abschnitt 3) bilden den Stand der Rechtswissenschaft und folgen aus den Entscheidungen des Bundesverfassungsgerichts zum Grundrecht auf informationelle Selbstbestimmung und dem Datenschutzrecht, welches das Grundrecht näher bestimmt. Die Kriterien sind im Wesentlichen gleichrangig. Allerdings bietet die Rechtswissenschaft noch keine detailliertere Gewichtung der Kriterien; ein solches Verdienst war gerade der Grund für die Einführung der Methode KORA. Die wissenschaftliche Leistung dieses Beitrags ist die Konkretisierung rechtlicher Anforderungen. Anforderungen werden in diesem Beitrag für die spezifische Technik der Pseudonymisierung konkretisiert.

3 Verfassungsmäßigkeit der künftigen Biometrie

Die Rechtmäßigkeit künftiger biometrischer Systeme setzt voraus, dass die verfassungsmäßigen Anforderungen des Grundgesetzes erfüllt werden. Im Folgenden wird die Verfassungsmäßigkeit des Systemeinsatzes bezüglich der Zerlegung in PI und Hilfsdaten geprüft, um zu ermitteln, ob und welche Regelungen grundrechtlich gefordert sind und wie sie die Ziele der Verfassung fördert.

Im Folgenden wird untersucht, wie die spezifische Technik der Pseudonymisierung die Ziele der Verfassung fördert. Dazu wurde eine Fokussierung vorgenommen. Die Verfassungsmäßigkeit wird zwar in den rechtswissenschaftlich üblichen Schritten geprüft (Eingriff, Normenbestimmtheit, Erforderlichkeit, Verhältnismäßigkeit bezüglich des Gefühls des Überwachtwerdens usw.), aber nicht um allgemeine Fragen des Verhältnisses von (künftiger biometrischer) Überwachungstechnik zu Eingriffen in Persönlichkeitsrechte zu beantworten - dafür reicht der Rahmen dieses Beitrags nicht aus (einen Überblick geben [DPS11] [Po12] [Po11a] [Hi11] [HDP10]). Vielmehr greift dieser Beitrag einen einzelnen Aspekt der Technikgestaltung heraus und betrachtet nur diejenigen Kriterien, die mit der spezifischen Technik der Pseudonymisierung in Zusammenhang stehen.

Personenbezug: Ein künftiger Systemeinsatz und das ihn erlaubende Gesetz greifen in das Grundrecht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz ein, weil personenbezogene Daten (biometrische und Fahndungsdaten) i. S. v. § 3 Bundesdatenschutzgesetz und Art. 2 Buchst. a i. V. m. EG 26 EU-Datenschutzrichtlinie verarbeitet werden. Für die Umkehrung der Pseudonymisierung ohne zweckgemäße Mitarbeit der Datenschutzbehörde dürfen insbesondere keine Mittel verfügbar sein, die vernünftigerweise entweder von der verantwortlichen Stelle oder von einem Dritten eingesetzt werden könnten, bzw. muss der Aufwand an Zeit, Kosten und Arbeitskraft unverhältnismäßig groß sein. Ein Kriterium des Personenbezugs ist das Zusatzwissen (etwa über Gesichter und Fingerabdrücke in Fahndungs- und erkennungsdienstlichen Dateien).

Aufgrund der spezifischen Risiken des biometrischen Fahndungssystems ist die Pseudonymisierung auf hoher organisatorischer Ebene durchzusetzen, da die Stelle das Zusatzwissen nicht besitzen und auch nicht mit vertretbarem Aufwand erlangen darf. Eine rein innerbehördliche Lösung stellt eine Pseudonymisierung nicht sicher. Für die Stelle, die die PI speichert, wäre die Kooperation mit der Stelle, die die das Zusatzwissen hat, und andersherum dann nämlich nicht unverhältnismäßig aufwendig. Zudem sind die Daten bei einer rein innerbehördlichen Lösung für die Leitung der Behörde, deren Teil die verantwortliche Stelle ist, oder übergeordnete Behörden nicht pseudonym, weil beide Stellen von den Weisungen des Behördenleiters nicht völlig unabhängig sind.

Daher wird gefordert, die Datenteile in getrennten Dateien in unabhängigen öffentlichen Einrichtungen zu speichern (für dienst- und anschlussbezogene Daten der Vorratsdatenspeicherung [Zi09]). Idealerweise ist eine der Einrichtungen die Datenschutzbehörde, da sie im Lichte von Art. 28 EU-Datenschutzrichtlinie nicht nur von der Polizei unabhängig, sondern völlig unabhängig ist [Eu10]. Im Übrigen gilt das Prinzip der Datenvermeidung auch für die Datenschutzbehörde oder andere „Treuhänder“. Bei der Zerlegung in PI und Hilfsdaten verarbeiten - im Gegensatz zur TK-Vorratsdatenspeicherung - weder die Polizei noch die Datenschutzbehörde personenbezogene Daten.

Normenbestimmtheit: Zudem muss das Gesetz Anlass, Zwecke und Grenzen des Zugriffs auf die vorsorglich erfassten biometrischen Daten festlegen [BV08(1)]. Zudem muss das Gesetz festlegen, dass die erfassten biometrischen Daten in PI und Hilfsdaten zerlegt und die Hilfsdaten der Datenschutzbehörde mittels Vernetzung zur exklusiven Aufbewahrung übermittelt werden.

Außerdem werden die biometrischen Roh- und Templatedaten gelöscht. Auch ohne solche Daten können kriminelle Netzwerke aufgedeckt werden. Zwar wären solche Daten für die Beweissicherung notwendig, aber der Systemeinsatz dient nicht dazu, revisionsfeste Beweise für Strafverfahren zu gewinnen, sondern wird nur durchgeführt, um Hinweise zu erlangen, mit denen kriminelle Netzwerke aufgedeckt werden können. Die Technikgestaltung wird so gewählt, dass so wenig Daten gespeichert werden, wie es die Zweckbestimmung erlaubt. Im Umkehrschluss muss das Gesetz auch festlegen, dass biometrische Treffer nicht als Beweis

oder Indiz für Strafverfahren, sondern nur als Anhaltspunkt verwertet werden, der die Eröffnung eines polizeilichen Ermittlungsverfahrens begründet.

Verhältnismäßigkeit: Die verfolgten Zwecke sind legitim, weil sie der Strafverfolgung und Gefahrenabwehr dienen. Der Einsatz ist zumindest nicht offensichtlich ungeeignet, wenn die Eingriffe im Einzelfall Erfolg haben können [BV09]. Wie die Kfz-Kennzeichenerfassung zeigt, ist die Übermittlung von Referenzen aus dem Zentralsystem in die Erfassungsgeräte nicht zu aufwendig [He07]; nichts Anderes kann für die Übermittlung der Hilfsdaten gelten. Auch etwa eine unzuverlässige Übermittlung der Hilfsdaten beseitigt die Eignung nicht, da die Eingriffe im Einzelfall Erfolg haben können. Im Gegenteil, die Tatsache, dass durch Zerlegung in PI und Hilfsdaten die technische Performanz gesteigert wird, spricht für die Eignung. Der Systemeinsatz kann erforderlich sein [BV08(2)]. Nur in solchen Fällen ist der Systemeinsatz zulässig. Die Frage kann offenbleiben, da jedenfalls die Pseudonymisierung die Erforderlichkeit nicht beseitigt.

Schließlich müssen der Grundrechtseingriff und die Zwecke, die mit dem Systemeinsatz erreicht werden sollen, miteinander abgewägt werden. In seiner Gesamtheit hat der Systemeinsatz ein hohes Eingriffsgewicht. Wie erwähnt wird i. F. nur geprüft, ob die Pseudonymisierung das Eingriffsgewicht verringert. Dafür werden die Kriterien, die das Bundesverfassungsgericht (für Überwachungstechniken) ausdrücklich anerkannt hat, betrachtet.

Streubreite: Ein Systemeinsatz hat eine hohe Streubreite (Vielzahl von Betroffenen, die keinen Anlass für die Datenverarbeitung geschaffen haben) [BV08(3)]. Die Streubreite wird auf ein Minimum verringert, wenn sich die Datenschutzbehörde erst beteiligen muss, bevor der Personenbezug hergestellt werden kann. Nicht die Gesamtheit aller Flüge in einem unbegrenzten Zeitraum ist betroffen, sondern nur ein einziger Flug.

Transparenz: Das System muss transparent und kontrollfähig sein. Eine solche Systemtransparenz kann unterschiedlich fortgeschritten gestaltet werden. Die erste Stufe der Systemtransparenz wird durch die Beteiligung von Datenschutzbehörden erreicht. Daher wird die Datenschutzbehörde in der EU-Datenschutzrichtlinie über Art. 18, 20, 22 und 28 Abs. 3 beteiligt. Für Fahndungsmaßnahmen ist typisch, dass Transparenz gegenüber den Betroffenen und die Betroffenenrechte beschränkt werden müssen; daher ist die unabhängige Kontrolle durch die Datenschutzbehörden umso wichtiger [BV01].

Eine zweite Stufe ist die Beteiligung eines unabhängigen „Treuhänders“, nach der eine Datenverwendung nur unter Mitwirkung dieser Stelle möglich ist. So ist z. B. bei der TK-Vorratsdatenspeicherung verfassungsrechtlich anerkannt, dass die Trennung der Speicherung durch private TK-Unternehmen und des Abrufs durch Polizeibehörden Transparenz und Kontrolle der Datenverwendung fördert [BV10(1)]. Vereinzelt wird auch für die Fingerabdruckidentifizierung vorgeschlagen, dass das AFIS statt bei der Polizei bei einer „informationellen Verrechnungsstelle“ verwaltet wird und der Polizei nur im Trefferverfahren

die Entscheidung über die Übereinstimmung einer Fingerabdruckspur und Referenz mitgeteilt wird [Wo03]. Dies erinnert an die Praxis von Eurodac, nach der die Meldebehörden nur im Trefferfall Asylbewerber identifizieren kann.

Eine dritte Stufe der Beteiligung ist, wenn weder der Datenverwender noch der „Treuhänder" personenbezogene Daten speichert. Dies folgt insbesondere aus dem Systemdatenschutz. Danach wird die das System kontrollierende Stelle von der es anwendenden Stelle institutionell getrennt. Die kontrollierende Stelle trägt die technische Verantwortung, indem sie das System zugriffsbereit hält und die Einhaltung der Systemvorschriften sicherstellt. Sie kann auf die personenbezogenen Daten jedoch nicht zugreifen. Die das System anwendende Stelle trägt die fachliche Verantwortung und verarbeitet die personenbezogenen Daten. Um Berechtigungen des Zugriffs auf bestimmte Daten zu erhalten, müssen sie erst bei der unabhängigen Einrichtung, die die technische Verantwortung über das System trägt, beantragt werden [Po76].

Die Pseudonymisierung mittels exklusiver Aufbewahrung der Hilfsdaten bei der Datenschutzbehörde schafft die fortgeschrittenste Stufe der Systemtransparenz und hebt somit das Prinzip der Transparenz auf ein besonders hohes Niveau. Die Technikgestaltung bietet damit die beste Gewähr, dass offengelegt wird, in welchen Fällen der Personenbezug hergestellt wird und somit einzelne Personen polizeilichen Maßnahmen ausgesetzt werden können.

Gefühl des Überwachtwerdens: Der Systemeinsatz könnte auch ein Gefühl des Überwachtwerdens hervorrufen. Ein solches Gefühl kann durch eine hohe Streubreite geschaffen werden [BV08(4)]. Im Umkehrschluss bedeutet dies, dass mit der spezifischen Technik der Pseudonymisierung nicht nur eine hohe Streubreite vermieden wird, sondern auch - begünstigt durch eine vertrauenswürdige Datentrennung auf hoher institutioneller Ebene - die Möglichkeit des Gefühls des Überwachtwerdens verringert wird.

Verhaltensanpassung: Darüber hinaus könnte der Grundrechtseingriff aufgrund des Systemeinsatzes dazu führen, dass Betroffene ihr Verhalten anpassen. Ein solcher Eingriff entspricht funktional Eingriffen in andere Grundrechte [BV08(5)]. Mit der spezifischen Technik der Pseudonymisierung können Betroffene darauf vertrauen, dass sie personenbezogenen Maßnahmen durch die Polizei oder personenbezogenen Nachteilen aufgrund von „Identitätsdiebstahl" nicht ausgesetzt werden. Daher werden die Möglichkeit von Eingriffen in andere Grundrechte und eine Verhaltensanpassung verringert.

Datensparsamkeit: Jede Gestaltung einer Technik, die zur Zweckerreichung geeignet ist, kann am Ziel [BV10(2)] ausgerichtet werden, keine personenbezogenen, sondern nur pseudonymisierte Daten zu verarbeiten und die Datenteile auf (völlig) unabhängige Einrichtungen zu verteilen. Auch der Treuhänder, die Datenschutzbehörde, erhält und verarbeitet keine personenbezogenen Daten.

Zweckbindung: Das Prinzip der Zweckbindung wird durch das Prinzip der informationellen Gewaltenteilung konkretisiert [BV83]. Dieses Prinzip ist verfassungsrechtlich anerkannt [BV83] [De85] [Si84] [He90] [Po83] [Di00] und in § 9 Satz 1 i. V. m. Nr. 8 der Anlage des BDSG ausgedrückt. Das Prinzip der informationellen Gewaltenteilung verlangt insbesondere von der Behörde oder dem Behördenteil, ihren bzw. seinen Aufgabenbereich mit dem jeweiligen Datenbestand von dem Aufgabenbereich anderer Behördenteile zu trennen. Das Prinzip folgt aus dem Systemdatenschutz. Ursprünglich meinte das Prinzip der informationellen Gewaltenteilung die Trennung der das System kontrollierenden Stelle von der es anwendenden Stelle (s. o.).

Dieser ursprüngliche Begriff der informationellen Gewaltenteilung gilt insbesondere für vorsorglich erfasste Daten. Solche Daten zeichnet aus, dass sie nur ausnahmsweise für die Zweckerfüllung benötigt werden. Daher ist bezüglich des Großteils der Daten festzustellen, dass die Datentrennung den Personenbezug verhindert. Die Behörden können nicht ohne Mitarbeit der jeweils anderen Behörde personenbezogene Daten verarbeiten. Dies fördert das Prinzip der informationellen Gewaltenteilung und Zweckbindung.

Datensicherheit: Neben unbefugten Zugriffen auf die Datenbank bei der Polizei sind auch unbefugte Zugriffe auf die Datenbank der Datenschutzbehörde denkbar, die durch die Zerlegung der Daten in PI und Hilfsdaten ausgeschlossen wird. Die Zerlegung der Daten in PI und Hilfsdaten erfüllt die Vorgabe des Vier-Augen-Prinzips, der asymmetrischen Verschlüsselung und des Need-To-Know-Prinzips und ermöglicht eine revisionssichere Protokollierung [BV10(3)]. Insbesondere das Vier-Augen-Prinzip wird erfüllt, nach dem zwei Personen nur gemeinsam berechtigt sein sollen, auf riskante Daten zuzugreifen, und einander somit kontrollieren können.

Jeder Datensatz wird mit einem eigenen Schlüssel erzeugt. Daher bietet die Pseudonymisierung gegenüber dem allgemeinen Zugriffsschutz den Vorteil, dass ein erfolgreicher Angriff auf einen Schlüssel nicht den Zugriff auf alle Datensätze ermöglicht, sondern nur auf einen Datensatz. Der Aufwand, um auf die Vielzahl der Datensätze zuzugreifen, wird entsprechend vergrößert.

4 Technikgestaltung: Template Protection für die künftige Biometrie

Wie bereits zuvor erwähnt, soll in diesem Beitrag ein Konzept vorgeschlagen werden, dass mithilfe der „Biometric Template Protection“ und vorsorglicher biometrischer Datenerfassung eine Identifikation (im Gegensatz zur Verifikation) erlaubt. Wie ein solches biometrie- und kryptoprotokollbasiertes Konzept grundsätzlich arbeiten kann und welche speziellen Herausforderungen bei der konkreten Implementation der entsprechenden Algorithmen zu bewältigen sind, kann in [UU04] nachgelesen werden. Die hier vorgestellte technische Betrachtungsweise bezieht sich dabei eher auf die Anforderungen eines komplexen Systems in einem bestimmten Szenario (s. o., Abschnitt 2), das ein solches Konzept als Basis verwendet. Die korrekte und sichere Funktionsweise des ausgewählten Ansatzes zur „Biometric Template Protection“ wird als vorausgesetzt angesehen.

Gesichtserfassung: Erster Schritt für die Erzeugung sämtlicher gewünschter PI ist die Erfassung der Gesichtsdaten aus den Aufnahmen der Videoüberwachungskameras. Außerdem sollte die Gesichtserfassung nicht direkt durch eine Stelle übernommen werden, die gleichzeitig auch direkten Zugriff auf die biometrische Referenzdatenbank besitzt. Das bedeutet, selbst wenn die Gesichtserfassung durch eine Polizeistelle durchgeführt wird, darf ihr nicht gleichzeitig auch ein Zugriffsrecht auf die bei der Polizei gespeicherten biometrischen Daten eingeräumt werden. Erst die Stelle, die die PI zugesandt bekommt, hat dann auch Zugriffsrecht auf die entsprechende Referenzdatenbank, darf allerdings im Gegensatz zu der Daten erfassenden Stelle wiederum keinen Zugriff auf die (nicht dauerhaft) gesicherten Rohdaten erlangen.

Sind die biometrischen Daten erfasst, muss daraufhin eine Merkmalsextraktion durch das System durchgeführt werden, um aus den so erlangten Merkmalsvektoren die eigentlichen PI erzeugen zu können. Für das dafür spezifisch genutzte Verfahren gibt es unterschiedliche Ansätze. Grundsätzlich entsprechen die „Biometric Template Protection“ Systeme aber immer den in [BB08] definierten Architekturen. Dabei wird üblicherweise eine biometrische Authentifizierung ermöglicht, ohne dabei aber tatsächliche biometrische Rohdaten, d. h. Daten, die direkt Auskunft über die Eigenschaften des zugrunde liegenden biometrischen Charakteristikums geben, in irgendeiner Form abspeichern zu müssen. Dabei wird ein im Enrolment aufgenommener Merkmalsvektor eines biometrischen Charakteristikums mithilfe von bestimmten Hilfsdaten in eine pseudonymisierte, digitale Repräsentation übertragen. Die Hilfsdaten selbst können dabei, abhängig von der Implementation, unterschiedlichster Art sein. So sind diese Hilfsdaten im einfachsten Fall, wie in [GK06], schlicht die Systemparameter, unter denen das System die PI berechnet hat oder aber auch echte kryptografische Schlüssel, wie zum Beispiel in [BSW07]. Zusätzlich dazu könnte bei einem System, in dem der zur Berechnung der PI verwendete Algorithmus austauschbar ist, noch zusätzlich ein Identifikator für diesen mit in die Hilfsdaten eingefügt werden.

An dieser Stelle ist es wichtig zu erwähnen, dass aus der PI keinerlei Informationen über das tatsächliche, zugrunde liegende biometrische Charakteristikum ableitbar sind. In einem System zur Verifikation würden dann die PI und die dazugehörigen Hilfsdaten auf einem geeigneten Medium zusammen abgespeichert werden. Die Merkmalsvektoren der erfassten biometrischen Merkmale werden dann sicher gelöscht (auch der Arbeitsspeicher sollte ausreichend klein sein).

Dieser Teil des grundsätzlichen Ablaufs der „Biometric Template Protection“ entspricht für das hier vorgeschlagene System auch größtenteils der allgemeinen Architektur nach [BB08]. Der einzig gravierende Unterschied für die vorsorgliche biometrische Datenerfassung besteht darin, dass die erzeugten PI und die dazugehörigen Hilfsdaten nicht zusammen abgespeichert werden. Die PI gehen dabei sicher digital signiert und verschlüsselt an die Polizei, wohingegen die

dazugehörigen Hilfsdaten ebenso digital signiert und verschlüsselt an die Datenschutzbehörde übertragen werden.

Die PI und Hilfsdaten bleiben nun für eine feste Zeitspanne bei den entsprechenden Instanzen abgespeichert, bis sie automatisiert gelöscht werden sollten. Die Zeitspanne sollte die tatsächliche Flugdauer und einen weiteren Tag umfassen, damit die Polizei etwaige Maßnahmen zur Sicherung der Fluggäste oder anderen Betroffenen und danach der Informationssicherung ergreifen können. Hinzu kommt die Dauer für den Aufenthalt im überwachten Raum, bevor Fluggäste einchecken und an Bord gehen. Aus Gründen der Effektivität des Rechtsschutzes sollte nicht eine von anderen Variablen abhängige (tatsächliche Flugdauer), sondern eine einheitliche Zeitspanne (z. B. fünf Tage) gewählt werden.

Identifikation: Sollte es nun notwendig werden, die vorsorglich erfassten Gesichter auf mögliche Übereinstimmungen mit biometrischen Referenzdaten zu untersuchen, müssen dafür die zuvor separierten PI und die dazugehörigen Hilfsdaten wieder zusammengeführt werden. Zu diesem Zweck müssen die bei der Datenschutzbehörde gespeicherten Hilfsdaten an die untersuchende Polizeistelle übersendet werden. Diese wäre dann in der Lage, mithilfe der Hilfsdaten PI zu den biometrischen Referenzdaten zu berechnen. Kann eine solche neu berechnete PI auch in dem von Flughafen erzeugten Datensatz ausfindig gemacht werden (Zuordnung), ist die Wahrscheinlichkeit hoch, dass der jeweilige Verdächtige zum betrachteten Zeitpunkt von der Kamera augenommen worden ist.

Nur diejenigen PI und Hilfsdaten dürfen zusammengeführt werden, die mit dem gesetzlich bestimmten Vorfalls während eines Flugs im Zusammenhang stehen. Um dies feststellen zu können, müssen daher Metadaten über die Kamera, die Zeit und ggf. den Flug mit den PI und Hilfsdaten in einem Datensatz/-format erhoben und gespeichert werden. Aufgrund der unterschiedlich hohen Streubreite sollte auch festgehalten werden, ob sich die Kamera am jeweiligen Gate (welcher gezielt mit dem Flug im Zusammenhang steht) oder in der Eingangshalle des Flughafens befindet.

Nachdem die PI zu den Referenzdaten erfolgreich berechnet worden sind, sind die Hilfsdaten frühstmöglich zu löschen. Die Hilfsdaten ermöglichen es der Polizeistelle, in Zukunft erhobene biometrische Daten mit gespeicherten Daten abzugleichen mit der Folge, dass dem Betroffenen zusätzliche Informationen (Flugzeit und -ziel bzw. Kriminalhistorie und Fahndungsausschreibung) zugeordnet werden können. Dies ist nicht von der gesetzlichen Zweckbestimmung gedeckt. Daher müssen die Hilfsdaten gelöscht werden, sobald die Datensätze erfolgreich abgeglichen worden sind, oder gar nicht erst offenbart werden. Dies könnte z. B. mittels eines geschützten „Match-On-Card“-Systems realisiert werden, das die Hilfsdaten geheim hält, den Abgleich durchführt und dem Systembediener nur die Zuordnung mitteilt.

Infrastrukturbetrachtungen: Um das vorgeschlagene System und vor allem die im nächsten Unterabschnitt vorgeschlagenen Sicherheitsmechanismen auch realisieren zu können, sind grundsätzlich auch einige infrastrukturelle Gegebenheiten notwendig. So ist für die Sicherung

der digitalen Kommunikation inklusive des sicheren Schlüsselaustauschs und der digitalen Signatur grundsätzlich eine „Public-Key-Infrastructure“ (PKI) empfehlenswert, mithilfe deren eine Zertifizierung der zur Kommunikation verwendeten Schlüssel überhaupt erst möglich wird.

Da zu erwarten ist, dass die zur Berechnung der PI genutzte Applikation über die Zeit gesehen häufiger einer Versionsaktualisierung unterzogen wird, muss auch grundsätzlich eine zentrale Versionsprotokollierung und -verwaltung durchgeführt werden. Diese dient dem Zweck der vollständigen Nachvollziehbarkeit aller Programmänderungen und der Archivierung von nicht aktuellen Versionen, die notwendig sein könnten, um Datensätze älterer Versionen korrekt verarbeiten zu können. Da die Daten erfassenden und verarbeitenden Instanzen - aus offensichtlichen Gründen - keine Möglichkeit zur Abänderung oder Vervielfältigung der verwendeten Anwendungen besitzen sollten, müsste diese Aufgabe durch eine zusätzliche Instanz ohne Zugriffsrecht auf personenbezogene Daten ausgeübt werden, deren Abänderungen aber trotzdem systemglobal verifiziert werden sollten.

Um alle Vorgänge im System auch zeitlich erfassen zu können, muss in jedem Fall auch ein zentraler vertrauenswürdiger Zeitgeber/-dienst verfügbar sein, der für alle Instanzen eine systemglobale Zeitmessung ermöglicht. Außerdem wird dieser Zeitgeber ebenfalls benötigt, um die Einhaltung der Speicherfristen für alle Instanzen überprüfbar und ausführbar zu realisieren. Für die notwendigen vertrauenswürdigen Zeitstempel das die Daten zu einem konkreten Zeitpunkt vorlag kann das Time-Stamp Protocol (RFC 3161) verwendet werden, das garantiert das Daten vor einem bestimmten Zeitpunkt vorlagen und nicht erst später hinzugekommen sind.

Sicherheitsmechanismen: Im Rahmen des vorgestellten Systems ist es notwendig, verschiedenste Sicherheitsmechanismen zu realisieren, die die sichere Kommunikation und Speicherung gewährleisten.

Der erste Teil in diesem System, der unter allen Umständen durch verschiedene Sicherheitsmechanismen geschützt werden muss, ist die Erfassung der biometrischen Gesichtsdaten vor der Verarbeitung zu den entsprechenden PI. An dieser Stelle ist es essenziell, dass die aus einem Gesichtsdatensatz extrahierten Merkmalsdaten unmittelbar nach der Erzeugung der entsprechenden PI vollständig und forensisch sicher gelöscht werden, um sicherzustellen, dass zu einem späteren Zeitpunkt eine Rekonstruktion des biometrischen Charakteristikums oder Teilen davon ausgeschlossen werden kann.

Da die erzeugten PI und die dazugehörigen Hilfsdaten zwischen den Instanzen kommuniziert werden, sind natürlich grundsätzliche integritäts- und authentizitätssichernde Maßnahmen zu ergreifen. Das bedeutet, die PI und Hilfsdaten werden grundsätzlich nur digital signiert zwischen den Instanzen kommuniziert. Prinzipiell enthalten die Daten für einen potenziellen Angreifer ohne Zugriff auf die Referenzdaten zwar keinen wirklichen Informationsgehalt, bei einer Anwendung mit dieser datenschutztechnischen Relevanz sollten die Daten jedoch nur verschlüsselt kommuniziert werden.

Die Speicherung der Daten bei der entsprechenden Instanz sollte dann ebenfalls nur in verschlüsselter Form erfolgen, um mehrere verschiedene Sicherheitsaspekte abzusichern. Zum einen ist das Schutzziel der Verschlüsselung an dieser Stelle natürlich die Vertraulichkeit. Wie zwar bereits erwähnt bieten die PI sowie die Hilfsdaten allein keinen wirklichen sensiblen Informationsgehalt, sollten aber trotzdem geschützt werden. Innentäter könnten nämlich die PI und Hilfsdaten wieder zusammenführen. In diesem Sinne ist es zudem notwendig, dass PI und Hilfsdaten mit unterschiedlichen Schlüsseln verschlüsselt werden. Rein aus Gründen der Performanz wäre es an dieser Stelle sinnvoll, einen symmetrischen Verschlüsselungsalgorithmus für die Sicherung der gespeicherten Daten zu nutzen. Das zweite Schutzziel, das die Verwendung von kryptografischen Protokollen an dieser Stelle verfolgt, ist die Absicherung gegen unberechtigte Veränderung, also die Integrität der gespeicherten Daten. Dafür kann implizit die Verschlüsselung genutzt werden, da nach einer Modifikation der (verschlüsselten) Daten, die Entschlüsselung ungültige Werte bzw. Datenstrukturen zurückgibt. Dies setzt jedoch die Verwendung von Datenformaten voraus bei denen derartige Fehler erkannt werden können. Besser wäre eine digitale Signatur, mit der in jedem Fall Veränderungen erkannt werden können. Aus beiden Gründen muss die Zugriffskontrolle auch die Authentizität natürlicher Personen kontrollieren (z. B. passwortbasierte personengebundene Zugriffsrechte).

Die beiden Verschlüsselungsschritte - zum einen für die Kommunikation und zum anderen für die Speicherung - sollten zusammengefasst werden, damit die Daten zu keinem Zeitpunkt im Klartext vorliegen. Dem kann entgegengewirkt werden, indem die Daten vor der Kommunikation verschlüsselt werden, wodurch eine dann zusätzliche Verschlüsselung auf Transport- oder Anwendungsschicht nicht mehr notwendig ist und diese verschlüsselten Daten dann so wie sie sind gespeichert werden. Zudem spart dies einen Verschlüsselungsdurchgang.

Bezüglich der digitalen Signaturen ist zu beachten, dass für jede Signatur eine zeitaufwendige asymmetrische Verschlüsselung notwendig ist, sowie je eine Kommunikation mit dem Zeitdienst für den Zeitstempel. Bei einer sehr großen Anzahl an Daten kann dies reduziert werden, in dem die Daten in Gruppen eingeteilt und über diese Gruppen, evtl. mit Hilfe von Hashbäumen, die Signatur berechnet wird (RFC 4998).

Ein weiterer Mechanismus, der um das gesamte System gespannt werden sollte, ist eine lückenlose Protokollierung sämtlicher im System ablaufender Vorgänge. Dies umfasst natürlich die ausreichend detaillierte Beschreibung dieser Vorgänge sowie ihre Chronologie. Dabei wäre es denkbar, die Kommunikation zwischen den Instanzen durch unabhängige, automatische, nicht abschaltbare, lokale Protokollierung bei jeder Instanz zu dokumentieren. Sollte es dann notwendig werden, diese Protokolle auszuwerten, kann über eine Konsistenzprüfung aller lokalen Protokolle, also einem Vergleich aller Protokolle miteinander, ihre globale Richtigkeit überprüft werden. Außerdem könnten die Protokolldaten direkt in einem Datensatz mit den signierten biometrischen Daten gespeichert werden.

Um die Gesichtserfassung an sich protokollieren zu können, bleibt ebenfalls nur die Möglichkeit einer fest implementierten, nicht abschaltbaren, automatischen Protokollierung nach der Erfassung jedes Gesichts. Das Gleiche gilt für die Abänderung und Aktualisierung der verwendeten Applikationen.

Die Sicherheit sämtlicher digitaler Signaturen und Verschlüsselungen setzen die Sicherheit des verwendeten spezifischen Algorithmus sowie den sicheren Austausch alle verwendeten Schlüssel voraus. Aus dieser Sicht ist es also angebracht, Algorithmen und Protokolle zu verwenden, von denen ein hoher sicherheitstechnischer Standard angenommen wird und die für die Verwendung in Hochsicherheitsbereichen (durch das BSI [BS08]) ausdrücklich empfohlen werden.

5 Fazit

Die Erfassung biometrischer Daten zur Vorsorge für die Kriminalitätsaufklärung ist nur in engen Grenzen zulässig. Wenn sie jedoch in einem konkreten Fall geeignet und erforderlich ist, ist die Technikgestaltung zu regeln. Dieser Beitrag zeigt, dass die Technik gestaltbar ist und insbesondere eine effektive Pseudonymisierung von vorsorglich erfassten biometrischen Daten ermöglicht.

Nur nach Umsetzung der technischen und rechtlichen Gestaltungsvorschläge ist ausreichend sicher, dass Betroffene nicht befürchten müssen, personenbezogenen Maßnahmen der Polizei ausgesetzt zu werden. Dies ist ein wichtiger Aspekt, um die Verfassungsverträglichkeit des Systemeinsatzes herzustellen. Dies liegt insbesondere daran, dass die zwei Hindernisse für die Biometrie - Einzigartigkeit biometrischer Charakteristika und Gewinnbarkeit von Gesundheitsdaten/ethnischen Daten - überwunden werden.

Die Gesellschaft kann mit dem neuartigen Risiko künftiger biometrischer Systeme zur Kriminalitätsbekämpfung umgehen. Ein solcher verfassungsverträglicher Umgang ist auch notwendig, denn der vernünftige Bürger ist an beidem interessiert: Schutz vor Gefahren und Straftaten sowie Schutz vor Folgen des Missbrauchs informationeller Macht und nachlässigen Umgangs mit Technik. Wenn diese und andere Gestaltungsmöglichkeiten genutzt werden, kann das Fundament für eine Zukunft der Terroristen- und Kriminalitätsbekämpfung gelegt werden, die sich die Gesellschaft wünscht.

Danksagung: Anregungen zu technischen Aspekten von Maik Schott (Arbeitsgruppe Multimedia and Security, Otto von Guericke Universität Magdeburg).

Literaturverzeichnis

[BB08] Breebaart, Busch, Grave und Kindt: *A Reference Architecture for Biometric Template Protection based on Pseudo Identities*. In Arslan Brömme, Christoph Busch, Detlef Hühnlein (Hrsg.): *BIOSIG 2008*, 2008, S. 25-37, Lecture Notes in Informatics 137, Gesellschaft für Informatik

[BKA07] Bericht des BKA zur "Fotofahndung", 2/2007.

[Bo11] Bouchrika u. A., Journal of Forensic Sciences 2011, 882.

[BS08] BSI Technische Richtlinie: *Kryptographische Verfahren: Empfehlungen und Schlüssellängen*. BSI TR-02102, Version 1.0, 20.06.2008.

[BSW07] Boult, Scheirer und Woodworth: *Revocable fingerprint biotokens: accuracy and security analysis*. In *Proc. IEEE Inter. Conf. on Comput. Vis. & Patt. Recog*, USA, 2007.

[BV83] So z. B. in BVerfGE 65, 1 (69).

[BV01] BVerfGE 100, 313 (361 f.); 65, 1 (46 f.).

[BV08] (1) So z. B. BVerfGE 120, 378 (424); (2): BVerfGE 120, 378 (428); (3): BVerfGE 120, 378 (402); 115, 320 (354 f.); 107, 299 (328); (4): BVerfGE 120, 378 (403); 113, 29 (46); 65, 1 (42); (5): BVerfGE 120, 378 (406); 116, 202 (222); 113, 63 (76).

[BV09] So z. B. BVerfGE 120, 274.

[BV10] (1): BVerfGE 125, 260 (Abs. 214); (2): BVerfGE 125, 260 (Abs. 270); (3): BVerfGE 125, 260, Abs. 223; Fox, DuD 2008, 375.

[De85] Denninger, KJ 1985, 215 (239 ff.).

[Di00] Di Fabio, in: Maunz/Dürig, GG, Art. 2 Abs. 1, Rn 184.

[DM04] Daugman/Malhas, International Airport Review 2/2004.

[DPS11] Desoi, Pocs und Stach: *Biometric Systems in Future Crime Prevention Scenarios – How to Reduce Identifiability of Personal Data*. In: Brömme, A./Busch, C. (Hrsg.): BIOSIG 2011. Proceedings - International Conference of the Biometrics Special Interest Group, Bonn 2011, S. 259-266.

[Eu10] EuGH, Urteil v. 9.3.2010, C-518/07.

[FP09] FP7-Projekte: ADABTS (RCN: 91158), SAMURAI (89343), SUBITO (89391); BMBF-Projekte: ADIS (FKZ: 13N10977-9); CamInSens (13N10814); APFEL (13N10795-801).

[Ga10] Gates, Culture Unbound 2/2010, S. 67; in Newham bereits 1998, Thomas, The Observer, 11.10.1998, S. 5.

[GK06] GenKey: *System, portable device and method for digital authenticating, crypting and signing by generating short-lived cryptokeys*. *US Patent 2006/0198514A1*.

[Ha93] Hammer, V.; Pordesch, U.; and Roßnagel, A.: Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet. Heidelberg, New York, 1993.

[HDP10] Hornung, Desoi und Pocs: *Biometric Systems in future preventive Scenarios – Legal Issues and Challenges*. In: Brömme/Busch: BIOSIG 2010, Bonn 2010, S. 83-94.

[He90] Heußner in: FS Simon, S. 233 ff.; BB 1990, 1281 (1283).

[He07] Hessische Staatskanzlei, 31.5.2007, http://www.daten-speicherung.de/data/Schriftsatz_ Staatskanzlei_2007-06-01.pdf, S. 2.

[Hi11] Hildebrandt, Pocs, Dittmann, Ulrich, Merkel und Fries: *Privacy preserving challenges: New Design Aspects for Latent Fingerprint Detection Systems with contact-less Sensors for Future Preventive Applications in Airport Luggage Handling*. In: Proceedings of BioID 2011, Springer Lecture Notes on Computer Sciences (LNCS) Vol. 6583, Berlin 2011, S. 286.

[Po76] Podlech in: Steinmüller, Informationsrecht und Informationspolitik, München 1976, S. 211.
[Po83] Podlech, Alternativkommentar zum Grundgesetz, Art. 2 Abs. 1, Rn 80.
[Po11a] Pocs: *Gestaltung von Fahndungsdateien - Verfassungsverträglichkeit biometrischer Systeme*. Datenschutz und Datensicherheit (DuD) 2011, S. 163-168.
[Po11b] Pocs: *Abgleich im Erfassungsgerät*. In: Schartner, P./Taeger, J. (Hrsg.): Tagungsband D-A-CH Security 2011, syssec 2011, 346-360.
[Po12] Pocs: *Constitutionally Compatible Design of Future Biometric Systems for Crime Prevention*. In: Friedewald, M./Pohoryles, R. und Sharan, Y. (Hrsg.): Innovation - European Journal of Social Science Research, Spezialausgabe „Privacy and Technology“, Routledge, Juni 2012 (i. E.).
[Pr11] provet (Projektgruppe verfassungsverträgliche Technikgestaltung) unter der Leitung von Prof. Dr. Alexander Roßnagel. http://provet.uni-kassel.de
[Si84] Simitis, NJW 1984, 398 (402 f.), NJW 1997, 1902 (1902 f.).
[UU04] Uludag, Pankanti, Prabhakar und Jain: *Biometric Cryptosystems: Issues and Challenges*. Proceedings of the IEEE 92(6): 948-960 (2004).
[Wo03] Woodward in: Woodward/Orlans/Higgins: Biometrics. Identity Assurance in the Information Age, New York 2003, S. 327.
[WP03] Artikel-29-Datenschutzgruppe: Stellungnahme zur Biometrie (WP80) 2003.
[Zi09] Ziebarth, DuD 2009, 25, S. 29; zustimmend Roßnagel u.A., DuD 2009, 536, S. 539.