SCHRIFTENREIHE
DER STIFTUNG
DER HESSISCHEN
RECHTSANWALTSCHAFT

BAND 3

Schwimmen mit Fingerabdruck?

Die biometrischen Herausforderungen für das Recht der Gegenwart und Zukunft

Beiträge von
Yoan Hermstrüwer
Hanjo Hamann
Rahel M.K. Diers

Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar.

Herausgeber: Stiftung der Hessischen Rechtsanwaltschaft
Reihe: Schriftenreihe der Stiftung der Hessischen Rechtsanwaltschaft
Band 3

Hermstrüwer, Yoan / Hamann, Hanjo / Diers, Rahel M.K.
Schwimmen mit Fingerabdruck? – Die biometrischen Herausforderungen für das Recht der Gegenwart und Zukunft
ISBN 978-3-86376-016-8
Hinweis: Die Arbeit gibt ausschließlich die persönliche Ansicht des Autors wieder.

Alle Rechte vorbehalten
1. Auflage 2012
© Optimus Verlag, Göttingen
URL: www.optimus-verlag.de
Printed in Germany
Papier ist FSC zertifiziert (holzfrei, chlorfrei und säurefrei,
sowie alterungsbeständig nach ANSI 3948 und ISO 9706)

Das Werk, einschließlich aller seiner Teile, ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes in Deutschland ist ohne Zustimmung des Verlages unzulässig und strafbar. Dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Vorwort des Herausgebers

Die Stiftung der Hessischen Rechtsanwaltschaft hat ihren studentischen Aufsatzwettbewerb diesmal unter einen ungewöhnlichen Titel gestellt. Biometrie ist sicherlich kein Thema, mit dem sich junge Juristen in ihrer Ausbildung intensiv beschäftigen. Dennoch, oder gerade deswegen, hatte dieses Thema seinen ganz speziellen Reiz. Es gingen die unterschiedlichsten Beiträge ein, und jeder dieser Beiträge beleuchtete das Thema auf seine eigene, ganz spezielle Weise unter den verschiedensten Aspekten. Die Stiftung hat angesichts der herausragenden Qualität der eingereichten Beiträge das von ihr ausgelobte Preisgeld mehr als verdoppelt und insgesamt 5 Preise vergeben; die Beiträge, welche mit dem ersten und dem zweiten Preis ausgezeichnet wurden, möchten wir in diesem Band der interessierten Leserschaft vorstellen.

Der Rahmen des Themas wurde in den Ausschreibungsbedingungen wie folgt beschrieben:

Bundesinnenminister Wolfgang Schäuble propagierte 2008 die Speicherung ausnahmslos aller Fingerabdrücke im Zuge der Einführung des elektronischen Personalausweises. Ein Jahr zuvor verabschiedete der Bundestag das neue Passgesetz und die Schriftstellerin und Juristin Juli Zeh erhob Verfassungsbeschwerde gegen die Speicherung nur zweier Abdrücke. Biometriebasierte Identifikationsstrategien gewinnen im Bereich privater und öffentlicher Angebote grundsätzliche Bedeutung und stellen das Recht vor neue Herausforderungen. Ein Beispiel aus Hessen macht dies deutlich: Darf die Stadt Bad Orb Dauernutzungskarten für ihr Schwimmbad unter der „Auflage“ anbieten, dass die Nutzer/innen ihren Fingerabdruck zur automatisierten Zugangskontrolle zur Verfügung stellen? Reicht es außerdem für die Freiwilligkeit der Einwilligungserklärung (§ 4a BDSG) aus, dass Badegästen, die dazu nicht bereit sind, die Möglichkeit eröffnet ist an der Pforte zu klingeln und zu warten bis ein Bademeister öffnet?

Die hessische Kommunalaufsicht und der hessische Datenschutzbeauftrage haben hierzu ihre Auffassung dargetan. Wie aber stellt sich die Lage außerhalb von Bad Orb bundes- und europaweit sowie international dar, wenn private Anbieter/innen (etwa: Videotheken) privilegierte Zahlungsstrategien unter der „Auflage“ anbieten, dass der Kunde seinen Fingerabdruck preisgibt? Welche Alternativen für eine Zahlung ohne Fingerab-

druck sind hier notwendig? Was halten Sie davon, dass man in die USA überhaupt nur unter Preisgabe des Fingerabdrucks fliegen kann?

Über die Frage des „Ob“ hinaus stellt sich die Frage des „Wie“. Welche Sicherungen (§ 9 BDSG und Anlage) müssen getroffen, welche Evaluierungen vorgenommen werden, damit „der“ Nutzer gegebenenfalls seinen Fingerabdruck nicht „verliert“ und „er“ in Zukunft von vermeintlich von ihm autorisierten rechtsgeschäftlichen Erklärungen nicht eingeholt wird? Etwa, weil der Fingerabdruck gefälscht oder der Finger abgetrennt wurde?

Klärungsbedürftig ist auch,

- inwieweit der Einsatz biometrischer Identifikationsstrategien der Sicherheit, Qualität und Verfügbarkeit von Waren und Dienstleistungen dienen kann und darf (etwa im Fall Bad Orb, dass die Benutzung des Schwimmbads kostengünstiger angeboten werden kann, weil die Pforte nicht ständig besetzt sein muss);
- ob die Aufnahme des Fingerabdrucks in ein Ausweisdokument gerechtfertigt ist, weil er die Fälschungssicherheit erhöht.

Diese Fragen konnten Ausgangspunkt der Beiträge sein – mußten es aber nicht.

Die bei der Stiftung eingereichten Beiträge wurden von Frau Prof. Dr. Viola Schmid, LL.M. (Harvard) vom Fachgebiet Öffentliches Recht (Schwerpunkt Cyberlaw) der Technischen Universität Darmstadt begutachtet. Auf ihre Empfehlung wurden zwei der preisgekrönten Aufsätze für diesen Band ausgewählt.

Frankfurt am Main, den 23. Mai 2012

Für den Vorstand

Dr. Mark C. Hilgard
- Rechtsanwalt -

Vorwort des Jurymitglieds Prof. Dr. Viola Schmid

Einige Fragen und Antworten des Aufsatzwettbewerbs der Stiftung der Hessischen Rechtsanwaltschaft 2011/2012 lassen sich der Reihenfolge der termini des Themas gemäß schildern. Hervorzuheben ist, dass dieses Vorwort und die Auswahl der Beiträge die Freude am (technik)rechtlichen und-politischen Diskurs widerspiegeln will. Es geht in diesem Band und im Vorwort nicht um den Anspruch auf wissenschaftliche Vollständigkeit der Darstellung aller rechtlich vertretbaren Positionen zum Thema – bzw. um eine Bewertung unterschiedlicher Argumentationen. Im Einzelnen:

„Schwimmen mit Fingerabdruck?“ ist ein realitätsorientiertes Szenario, das den hessischen Datenschutzbeauftragten wie die hessische Kommunalaufsicht in 2011 beschäftigt hat. Eine hessische Stadt wollte die Nutzung von Dauerkarten für ein Schwimmbad mit Fingerprintverfahren kontrollieren. Unbestritten stellen sich grundlegende Fragen der Freiwilligkeit der Einwilligung (§ 4a BDSG) der Dauerkartenbesitzer/innen. Eine solchen Nutzung des Fingerabdrucks zur Authentifizierung im Kontext der Entgegennahme von kommunalen Leistungen der sogenannten Daseinsvorsorge ist genauso innovativ wie umstritten. Beide ausgezeichneten Beiträge greifen dieses Szenario unter unterschiedlichen Aspekten auf. Der Beitrag von Yoan Hermstrüwer und Hanjo Hamann reflektiert die Option des „Data Cash“ wenn die Verbilligung des Eintritts in ein Schwimmbad durch die Erhebung und Nutzung biometrischer Merkmale in Aussicht gestellt wird. Der Beitrag von Rahel Maria Katharina Diers betont nicht den ökonomischen, sondern den (verfassungs-) und datenschutzrechtlichen Vorder- bzw. Hintergrund, wenn die Ungeeignetheit („leichte Herstellung von Plagiaten“), die fehlende Erforderlichkeit („Einführung von Karten mit Passfoto“) und die fehlende Verhältnismäßigkeit im engeren Sinne gerügt wird. Beide Beiträge repräsentieren so ökonomische und rechtliche Perspektiven – die durchaus zu unterschiedlichen Argumentationslinien führen: … „Der Schwimmbadbetreiber, der sich durch die Einholung einer Einwilligung eine Kostenersparnis erhofft, wird versuchen, die Verweigerung der Einwilligung als relativen Verlust erscheinen zu lassen.“ (Hermstrüwer /Hamann). Losgelöst vom Schwimmbadszenario ist beiden Arbeiten die Erkenntnis gemein, dass es

biometrische Herausforderungen für das Recht gibt. Beide Beiträge zeichnen sich durch die Analyse der differenzierten Einsatzszenarien von Biometrie aus. Insbesondere Diers unterscheidet transparent zwischen staatlichem und privatem Bereich und dort wiederum zwischen Dienstleistungs- (Convenience) und Mitarbeiterszenarien. Kennzeichnend für den Beitrag von Hermstrüwer/Hamann ist die informationstechnologische und ökonomische Analyse der Vor- und Nachteile des Einsatzes von Biometrie. Nicht überraschend kommen beide Beiträge zu dem Ergebnis, dass die Herausforderungen, die Biometrie dem Recht stellt, noch nicht gemeistert sind. Als ein Ergebnis dieses Aufsatzwettbewerbs kann festgehalten werden, dass beide Beiträge „Zuflucht" im Recht suchen. Der Beitrag von Hermstrüwer / Hamann entwirft eine dogmatische Grundlage für eine Interpretation von § 4a BDSG (Entscheidungsforschung) und hofft auf europäisches Datenschutzrecht („Das europäische Datenschutzrecht wird darüber entscheiden, ob wir die allgegenwärtige Vermessung unseres Körpers hinnehmen …"). Der Beitrag von Diers realisiert: „der politische Wille von heute ist das Recht von morgen". Dies mag, muss aber nicht so sein. Jedenfalls aber soll Regulativ des Zukunftsrechts vergangenes Recht sein („Das Recht der Historie ist das Regulativ des Rechts der Zukunft"). Deutlich wird mit dem Rekurs auf Europa- bzw. Vergangenheitsrecht, dass beide Beiträge die Herausforderungen im Grundsatz anerkennen. Belegt wird diese Analyse durch die Darstellung des

Rechts der Gegenwart. Biometrierecht ist keine Materie, die nicht alle Bürger und Bürgerinnen der Bundesrepublik Deutschland unmittelbar berührt bzw. zu einem Zeitpunkt in ihrem Leben berühren wird. Die Ausstellung einer staatsbezogenen Identität erfolgt beim Reisepass nur noch unter der Bedingung der Preisgabe biometrischer Daten (§ 16a Satz 2, § 4 Abs. 3 PaßG). Dieses „Identifikations- und Verifikationsmodell" bietet sich aus einer informationstechnologischen, sicherheitspolitischen und wettbewerbspolitischen Perspektive für das Nachdenken über das

Recht der Zukunft an. Zu prüfen wird sein – und das ist beiden Beiträgen gemein – in wie weit die Technologie fälschungssicher bzw. fehler"frei" zu arbeiten fähig ist. (Stichwort Fehlerraten). Nach Evaluation der Chancen, Risiken und Folgen des Einsatzes von Biometrie wird der potentielle Beitrag zur Etablierung eines Raums der Freiheit, der Sicherheit und des Rechts (Art. 67 AEU) zu konturieren sein. Die Herausforderung könnte sein, dass der etwa im Flugverkehr (IATA-Modell des „Checkpoint of the Future") gewollte, globale Einsatz an den Inhalten von Art. 67 AEU gemessen wird: „in dem die Grundrechte und die verschiedenen Rechtsordnungen und –traditionen der Mitgliedsstaaten geachtet werden". Die Grundrechte und Rechtsordnungen könnten verlangen, dass biometrische Anwendungen außer in privaten Hochsicherheitsumgebungen dem öffentlichen Sektor vorbehalten bleiben. Und zu diesen Rechtstraditionen könnte – um den Zirkel zum Ausgangspunkt des

Themas wie dieses Vorworts zu schließen – auch die Datenschutzkultur gehören. So findet sich im aktuellen Tätigkeitsbericht des Hessischen Datenschutzbeauftragten folgender Kommentar zum Schwimmbadszenario: „Zudem widerspricht die Nutzung eines derartigen Systems nach meiner Ansicht der Datenschutzkultur! Wie soll Kindern der Grundsatz der Datensparsamkeit nahegebracht werden, wenn sie schon beim Schwimmbadbesuch Fingerabdrücke abgeben sollen?[1]“ Vielleicht ist dieser Grundsatz der Datensparsamkeit (auf Bundesebene § 3a BDSG) de lege lata zugrundezulegen, de lege ferenda in einer Welt allzeitiger und allgegenwärtiger (Informations)Technologisierung indes neu zu konturieren?

Darmstadt, im April 2012

Prof. Dr. Viola Schmid, LL.M. (Harvard)
- Technische Universität Darmstadt; Fachgebiet Öffentliches Recht -

[1]Michael Ronellenfitsch (Hrsg), Vierzigster Tätigkeitsbericht vorgelegt zum 31.12.2011, S. 134.

Inhalt

BEITRAG VON RAHEL M.K. DIERS

BEDEUTUNG VON BIOMETRIE IM RECHT DER GEGENWART UND ZUKUNFT

Beitrag von
Yoan Hermstrüwer
Hanjo Hamann

Biometrie und Autonomie
Die Vermessung der Person zwischen Datenschutzrecht und Entscheidungsforschung

Zu den Autoren:

Die Autoren sind gegenwärtig Promotionsstudenten am Max-Planck-Institut zur Erforschung von Gemeinschaftsgütern in Bonn. **Yoan Hermstrüwer** studierte Jura und Islamwissenschaften in Freiburg, Paris und Bonn. Seine Interessenschwerpunkte liegen in den Gebieten des Internetrechts, des internationalen Wirtschaftsrechts, des Verfassungsrechts und der sozialwissenschaftlichen Methoden im Recht. **Hanjo Hamann** studierte Jura in Heidelberg und Hamburg und arbeitete studienbegleitend in wirtschaftsberatenden Sozietäten in Frankfurt/M., Hamburg und Shanghai. Seine Interessen liegen insbesondere im Unternehmensrecht, in der Verhaltensforschung und in der Programmierung.

Zum Inhalt:

Biometrie birgt Risiken. Zur Handhabung dieser Risiken und zur Entwicklung geeigneter Regulierungsinstrumente kann das Recht wertvolle Impulse aus der Verhaltensforschung gewinnen. Der Beitrag unterscheidet biometrische Systeme rechtlich danach, welchen Grad an Entscheidungsfreiheit sie dem Einzelnen belassen. Im Rahmen einer Auslegung des deutschen und europäischen Datenschutzrechts werden verhaltenswissenschaftlich belegte Entscheidungsrestriktionen und deren Bedeutung für den rechtlichen Umgang mit Biometrie beleuchtet.

1 Einleitung: Biometrie und Entscheidungsforschung

Welche Herausforderungen stellt die Biometrie dem Recht der Gegenwart und der Zukunft? Biometrie ist Technik. Jede Technik birgt Risiken. Das Recht ist gefordert, solche Risiken zu beherrschen, ohne technische Innovation im Keime zu ersticken. Möchte man technische Risiken beherrschbar machen, muss man sich der Frage stellen: Ist es die Technik als solche, die gefährlich ist, oder sind es die menschlichen Entscheidungen über den Umgang mit Technik? Grundsätzlich kann man versuchen, die Unterscheidung zwischen Mensch und Technik zu dekonstruieren; Mensch und Technik lassen sich dann als *hybride Assoziation* beschreiben.[2] Nicht die Waffen töten; nicht allein die Menschen töten; es ist die *Verflechtung* von Mensch und Waffe.[3]

Der Rechtsordnung aber fiele es schwer, solche Verflechtungen als Normadressaten in den Blick zu nehmen. Funktion des Rechts ist schließlich in erster Linie die *Verhaltenssteuerung*,[4] die Beeinflussung menschlicher Entscheidungen. Daher muss das Recht versuchen, die Kategorien Mensch und Technik in der Kategorie *Verhalten* zu reformulieren. Wenn das Recht Vorgaben an die Technik macht, werden zumeist nicht die technischen Geräte geregelt, sondern die Entscheidungen derjenigen, die solche Geräte herstellen. Ist das Produkt einmal auf dem Markt, kann das Recht noch die Entscheidungen über den Umgang mit diesen technischen Geräten steuern. So mag der Gesetzgeber versuchen, individuelle Entscheidungen über die Teilnahme an biometrischen Verfahren zu beeinflussen. Er kann etwa regeln, dass Menschen über die Verarbeitung biometrischer Merkmale informiert werden müssen. Ob solche Informationspflichten ihr Ziel erreichen, setzt aber empirisches Wissen darüber voraus, wie Menschen Entscheidungen über die Preisgabe biometrischer Daten treffen.

„Neuere Ansätze […] versprechen komplementäre und ergiebigere Instrumente, um Entscheidungsverhalten im Datenschutz zu verstehen.“[5] Diese Ansätze beruhen auf den Erkenntnissen verschiedenster Disziplinen, die hier unter dem Begriff *Entscheidungsforschung* zusammengefasst werden; gemeint sind alle wissenschaftlichen Fachrichtungen, die sich mit menschlichen Entscheidungen befassen.[6] Der vorliegende Beitrag soll die Einsichten der Entscheidungsforschung für das Biometriedatenschutzrecht fruchtbar machen. Es ist ein erster Versuch, die „überempirische Zweckidee, an der das

---

2 *Johnson*, Soc Prob's 1988, 298; vgl. *Karavas*, Grundrechtsschutz im Web 2009, 301, 312.
3 *Latour*, Comm Knowl 2/1994, 29, 30; *ders.*, Hoffnung der Pandora 2002, 236.
4 *Rüthers*, Rechtstheorie 2008, 75 ff.; *Somek*, Rechtliches Wissen 2006, 11.
5 *Acquisti*, IEEE Sec Priv 6/2009, 82 (Übers. d. Verf.).
6 *Acquisti*, IEEE Sec Priv 6/2009, 82, 84 nennt beispielhaft “economics, behavioral decision research, psychology, usability, human-computer interaction, and so forth”.

Recht zu messen ist“[7], mit der Entscheidungswirklichkeit zu konfrontieren. Diese juristisch-empirische Herangehensweise soll angemessene rechtliche Lösungsansätze für die Herausforderungen der Biometrie aufzeigen; zugleich wird sie die Rechtsdogmatik insgesamt vor eine neue Herausforderung stellen: die Rezeption von Erkenntnissen der Entscheidungsforschung durch das Recht.

[7] *Radbruch*, Rechtsphilosophie 2003, 54.

Beitrag von

Rahel Maria Katharina Diers

Bedeutung von Biometrie im Recht der Gegenwart und Zukunft

Zur Autorin:

Rahel M. K. Diers, am 09.05.1988 in Itzehoe geboren, erwarb 2008 das deutsch-französische Doppelabitur, bevor sie sich zum Studium der Rechtswissenschaften an der Universität Heidelberg entschloss. Sie legte die Zwischenprüfung als Semesterbeste ab und wechselte für die Examensvorbereitung an die Universität Münster.

Zum Inhalt:

In den nächsten Jahren wird der Einsatz der biometrischen Systeme sowohl im öffentlichen als auch im privaten Sektor stetig steigen. Den dadurch bedingten Herausforderungen muss sich das Datenschutzrecht bereits heute stellen und einen möglichst proaktiven Charakter gewinnen. Ein Überblick über die unterschiedlichen Anwendungsfelder der Biometrie ergibt, dass trotz der bereichsspezifischen Komplexität eine konsequente Überprüfung mit den verfassungsrechtlichen Grundsätzen prinzipiell ausreicht, um das erforderliche Schutzniveau aufrecht zu erhalten. Eine Rückbesinnung auf diese Grundsätze kann damit eine Antwort auf die technischen und einfachgesetzlichen Herausforderungen bieten.

1 Einleitung

„Who controls the past controls the future, who controls the present controls the past“.[190]

Durch die rasante technische Entwicklung der letzten Jahrzehnte ist das von George Orwell bereits 1949 dargestellte Szenario eines Überwachungsstaates längst realisierbar. Die biometrischen Identifikationssysteme könnten zu einer vollständigen staatlichen Erfassung und Speicherung sämtlicher Körpermerkmale der Bürger genutzt werden. Eine Vorstellung, die durch alltägliche Viedoüberwachung öffentlicher Plätze, Ortungssysteme, Bewegungsprofile, RFID-Chips und Rasterfahndungen nicht mehr abwegig erscheint, aber dadurch seine rechtliche Brisanz in keiner Weise verliert („Wir befinden uns auf einem Weg von einem Rechtsstaat hin zu einem systematischen Verdachtsstaat“[191]). Gerade aufgrund dieser „Normalität“ der Registrierung persönlicher Daten ist es unabdingbar aktuelle Entwicklungen in Exekutive, Legislative und im privaten Sektor ständig auf ihre Vereinbarkeit mit dem Grundgesetz, speziell mit dem, seit dem „Volkszählungsurteil“ durch das BVerfG konkretisierten, Recht auf informationelle Selbstbestimmung hin zu überprüfen. Somit muss sich auch die Biometrie den Anforderungen des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG („Die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“[192]) stellen. Diese Befugnis bedarf heutzutage eines besonderen Schutzes, da der technische Fortschritt dem Betroffenen keine ausreichende Kontrolle mehr über die Daten und deren Quantität ermöglicht. Ein Anspruch auf Schutz vor unbefugter Kenntnisnahme, Speicherung und Verarbeitung personenbezogener Daten erfolgt neben dem Persönlichkeitsrecht, auch als „Annexrecht“[193] aus anderen Grundrechten (Berufs-und Gewerbefreiheit, Wissenschafts-, Kunst und Religions-, allg. Handlungsfreiheit). Die Freiheitsrechte können wegen ihrer Konzeption je nach Konfliktlage durch Auslegung und Anwendung angepasst werden. Sie verlieren somit nicht ihre Anwendungsmöglichkeit oder Relevanz bezüglich der modernen Informations-, und Kommunikationstechnik. Vielmehr charakterisiert sie das „Wechselspiel zwischen dem programmatischen Gehalt der Norm und den kulturellen, sozialen, politischen, ökonomischen, technologischen, ökologischen u.a. Rahmenbedingung, auf die sie inhaltlich bezogen sind“[194].

---

[190] *Orwell, George,* 1984, Book 1,. Chapter 3. (1949).
[191] *Tauss,* Datenschutz im Spannungsfeld von Freiheit und Sicherheit, S. 4.
[192] *BVerfGE* 65, 1 (42).
[193] Zu diesem Begriff: Vgl. *Bull*, Informationsgesellschaft, S. 25.
[194] Vieweg/Gerhäuser/*Hoffmann-Riem*, Digitale Daten in Geräten und Systemen, S.42.

Spätestens seit dem 11. September hat der Bedarf nach zuverlässigen Personenidentifizierungstechnologien in sicherheitsrelevanten Bereichen, insbesondere zur Terrorismusbekämpfung neben der langjährigen[195] Anwendung im Bereich der Strafverfolgung, eine neue Dimension erreicht und ist seither von hoher gesellschaftlicher und politischer Bedeutung. Ihre Einsatzfelder sind neben dem öffentlichen Sektor gerade auch im betrieblichen Bereich (Zutrittskontrolle, Arbeitszeiterfassung, Zugangssicherung) von steigender Bedeutung. Bei zunehmender Personalisierung von Dienstleistungen und Geräten wird im Privaten ebenfalls zur Sicherheits-, Effektivitäts- und Komfortsteigerung auf biometrische Authentifizierungssysteme zurückgegriffen, an Stelle der Verwendung klassischer Authentifizierungsvorgänge (durch Besitz/Wissen von Passwörtern, PIN). Nicht nur in Hinblick auf die Definition der sog. „sensiblen Daten" gem. § 3 Abs. 9 BDSG sind die Grundlagen der Biometrie somit zunächst erläuterungsbedürftig.

1.1 Biometrie

Biometrie[196] ist die automatisierte Messung von natürlichen, hoch charakteristischen, physiologischen oder verhaltenstypischen Merkmalen (Fingerabdrücke, Irismuster, Gesichtsgeometrie, Stimme, Schrift, aber auch DNA[197]) von Menschen zum Zwecke der Identifizierung von Personen.[198] Trotz prozessualer Unterschiede der biometrischen Authentifizierungssysteme lassen sie sich grob kategorisieren. Im Rahmen des „Enrolments" (Registrierungsprozess) werden die Referenzdaten optisch, thermisch, chemosensorisch, akustisch oder drucksensitiv gewonnen und gespeichert.[199] Die Anzahl fehlgeschlagener Versuche (False Enrolement Rate „FER") kann durch mangelnde oder verfälschte (z.B. Verschmutzung) Merkmale des Trägers entstehen. Eine angenommene Fehlerquote von 2 bis zu 10 Prozent[200] beruht naturgemäß auf empirischen Erfahrungswerten und korreliert mit Vorauswahl der Versuchspersonen und Versuchsbedingungen. Ein objektiver Wert[201] ist daher schwer zu ermitteln. Die Referenzdaten werden entweder in vollständiger Form als Roh- oder image data (z.B. beim Gesichtsbild, Fingerabdruck) oder in extrahierter Form (Templates[202]) gespeichert. Beim späteren Vergleichs- prozess (Matching) werden die aktuellen Daten mit den gespeicherten Referenzdaten verglichen. Dabei gibt es zwei Möglichkeiten. Im Prozess der sog. Identifikation (1:n Abgleich) wird die Person aus einer vorgegebenen Menge von Indi-

[195] 1858 erster Vorschlag zur Nutzung des Fingerabdrucks in der Kriminalistik, siehe *Busch*, Biometrische Systeme, S. 8.
[196] Aus dem Griechischen: *bios* (Leben) und *metron* (Maß).
[197] Ablehnend: *Albrecht*, Biometrische Verfahren,S .47; *Nanavati*/*Thieme*/*Nanavati*, Biometrics, S.153.
[198] Vgl. Hornung/Möller/*Hornung* §4 PassG Rn. 41; ISO-Definition: „ automated recognition of individuals based on their behavioral and biological characteristics, http://www.3dface.org/media/vocabulary.html.
[199] Vgl. *Behrens/Roth*, Biometrische Identifikation, S.19.
[200] *Heibey/Quiring-Kock,* Authentisierung, S.10; *Mansfield*, How to achieve test results in real-life?.
[201] Dazu: *Laßmann*, Biometrische Verfahren, S.8.
[202] *Petermann*/*Sauter*, Biometrische Identifikation S.19.