Datenschutz

Biometrie am Arbeitsplatz – sichere Kontrollverfahren versus ausuferndes Kontrollpotential

Dr. Gerrit Hornung, LL. M. (Edinburgh)/Rechtsanwalt Dr. Roland Steidle*, Kassel/Frankfurt/M.

Biometrische Verfahren werden in Zukunft am Arbeitsplatz vermehrt eingesetzt werden, insbes. bei Zugangskontrollsystemen. Das BAG *hat im Beschluss v. 27. 1. 04 entschieden, dass derartige Systeme auch dann mitbestimmungspflichtig sind, wenn sie im Kundenbetrieb eines Unternehmens eingesetzt werden. Die Entscheidung enthält keine inhaltlichen Kriterien für die Zulässigkeit biometrischer Zugangskontrollen und deren Gestaltung. Der Beitrag geht diesen Fragen nach.*

1. Einleitung

Biometrische Verfahren sind keine ganz neue Technologie. In der Kriminalistik wird bereits seit Beginn des letzten Jahrhunderts mit Fingerabdrucksverfahren gearbeitet, die mittlerweile auch in automatisierter Form ablaufen[1]. Überdies dient die Biometrie schon seit geraumer Zeit zur Absicherung von Hochsicherheitsbereichen gegen unbefugten Zutritt. Neu ist, dass die Verfahren durch ihre technische Weiterentwicklung vor der Einsatzreife für den Masseneinsatz stehen. Die potentiellen Anwendungsfelder sind nahezu uneingrenzbar. Sie reichen von Zugangs- und Zugriffskontrollen über den Einsatz in Führerscheinen und Identitätspapieren[2], die Vermeidung von Doppelbezügen staatlicher Leistungen[3] und die Aktivierung von Chipkarten bis hin zu Bezahlfunktionen in der Gastronomie[4].

Der Einsatz von Biometrie bringt am Arbeitsplatz Chancen und Risiken mit sich[5]. Beide resultieren aus der grundsätzlich unlösbaren Verbindung eines biometrischen Datums mit dem zugehörigen Merkmalsträger. Diese Bindung führt dazu, dass eine echte Identifikation einer Person vorgenommen werden kann. Anders als die sonst üblichen Legitimationsmechanismen Besitz (z. B. eines Ausweises oder einer Chipkarte) und Wissen (einer PIN oder eines Passwortes) können biometrische Merkmale grundsätzlich weder verloren noch weitergegeben werden. Das eröffnet größere Sicherheit für Kontrollbereiche. Außerdem erhöht sich die Authentizität von Handlungen, die biometrisch legitimiert werden. Biometrie lässt sich weiterhin zur Sicherung sensibler Daten einsetzen, wenn bspw. Speichermedien oder -bereiche gesichert werden, die Geschäftsgeheimnisse oder höchstpersönliche Daten eines Beschäftigten enthalten.

Diesen positiven Effekten stehen Risiken für die Merkmalsträger gegenüber. Durch die lebenslang unlösliche Bindung des biometrischen Merkmals an die Person besteht die erhöhte Gefahr der – eventuell heimlichen – dauerhaften Überwachung, der Ansammlung umfänglicher Datenbestände und der Bildung von Verhaltensprofilen eines Betroffenen. Im Fall der Kompromittierung eines biometrischen Merkmals bleibt lediglich der Rückgriff auf ein noch nicht benutztes Merkmal. Das bedingt jedoch eine neue Infrastruktur. Bisweilen können sich aus biometrischen Daten Rückschlüsse auf Eigenschaften des Betroffenen ergeben, wenn diese „überschießende Daten" enthalten[6]. Diese Risiken sind i. d. R. keine zwangsläufige Folge des Einsatzes von Biometrie, sie können jedoch direkt durch ihn herbeigeführt werden. Ihnen muss deshalb durch eine datenschutzfreundliche Ausgestaltung der Systeme, technische Schutzmechanismen und wo nötig durch rechtliche Absicherungen begegnet werden.

2. Grundlagen

2.1 Datenschutz im Betrieb

Dem Schutz personenbezogener Daten kommt am Arbeitsplatz herausragende Bedeutung zu, weil sich ein Beschäftigter den Risiken für seine informationelle Selbstbestimmung im Arbeitsverhältnis kaum entziehen kann. Beschäftigte stehen in einem Abhängigkeitsverhältnis zum AG und verbringen einen wesentlichen Teil des täglichen Lebens am Arbeitsplatz. Trotz dieser Besonderheiten be-

* Die Autoren sind Mitglieder der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) an der Universität Kassel.

1 S. zum Automatischen Fingerabdruck-Identifizierungssystem (AFIS) *Weichert,* DuD 1999, 167.

2 Durch die Verordnung (EG) Nr. 2252/2004 v. 13. 12. 2004 (Abl. EG L 385, 1) werden die EU-Staaten zur Einführung biometrischer Daten des Gesichts und des Fingerabdrucks in ihre Reisepässe verpflichtet. S. zum Problemfeld Biometrie auf Identitätsdokumenten *Reichel/Roßnagel/Müller*, Der Digitale Personalausweis, 2005, i. E.; *Hornung*, Die digitale Identität, 2005, i. E.; *ders.*, Biometric Identity Cards, in: *Paulus/Pohlmann/Reimer* (Hrsg.), Securing Electronic Business Processes, 2004, 47 ff.; *ders.*; KJ 2004, 344, 355 ff.; *Roßnagel/Hornung*; DuD 2005, 69 ff.; *Golembiewski/Probst*, Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfeststellungen (Gutachten des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein), abrufbar unter http://www.datenschutzzentrum.de/download/Biometrie_Gutachten_Print.pdf.

3 Die Niederlande geben bspw. bereits seit 1997 Asylbewerberausweise mit biometrischen Daten zur Leistungsausgabe und Aufenthaltskontrolle aus, s. *Weichert*, CR 1997, 369, 373. Im Rahmen der Ausgabe von Hilfslieferungen durch den UN-Flüchtlingskommissar in Pakistan werden die Iris-Scans der Antragsteller gespeichert, vgl. *Woodward/Orlans/Higgins*, Biometrics. Identity Assurance in the Information Age, 2003, 287 f.

4 S. http://www.heise.de/newsticker/meldung/39192/.

5 Für eine allgemeine Einführung in die Rechtsfragen der Biometrie vgl. *Albrecht*, Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz 2003; *Hornung,* KJ 2004, 344 ff.

6 Diese können im Einzelfall auch „besondere Arten personenbezogener Daten" darstellen (§ 3 Abs. 9 BDSG), s.u. 4.2. Praktische Probleme ergeben sich, weil einige der verwendeten Merkmale bei einem bestimmten Prozentsatz der Bevölkerung nicht oder nicht in hinreichender Ausprägung vorhanden sind, s. dazu *Büro für Technikfolgenabschätzung beim BT (TAB)*, Biometrische Identifikationssysteme. Sachstandsbericht, BT-Drs. 14/10005, 25; *TeleTrust,* Kriterienkatalog – Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren, 2002 (abrufbar unter http://www.teletrust.de/publikat.asp?id=40600), 7; *Däubler,* Gläserne Belegschaften? Datenschutz für Arbeiter, Angestellte und Beamte, 2002, Rn. 288 ff.; *Sietmann,* c't 5/2002, 146.

7 Ein solches steht zwar zum wiederholten Mal in einem Koalitionsvertrag einer Bundesregierung, (s. zuletzt auszugsweise AuR 2002, 456 f.), ist jedoch in Kürze nicht zu erwarten; dazu *Tinnefeld/Viethen,* NZA 2000, 977; *Simitis,* in: *ders.* (Hrsg.), BDSG, 5. Aufl. 2003, EinI. Rn. 20, 108; *ders.,* AuR 2001, 429; S.a. *Bartel,* RDV 2003, 37.

steht aber kein spezielles Arbeitnehmerdatenschutzgesetz[7], so dass das allgemeine Datenschutzrecht herangezogen werden muss. Dieses normiert zum Schutz der personenbezogenen Daten in § 4 Abs. 1 BDSG ein generelles Verbot mit Erlaubnisvorbehalt. Ihre Verwendung ist danach grundsätzlich verboten und nur dann zulässig, wenn sie durch eine Rechtsvorschrift oder eine Einwilligung des Betroffenen ausdrücklich erlaubt ist. Der Begriff der „Rechtsvorschriften" wird durch das *BAG* weit ausgelegt und umfasst auch TV, BV oder Dienstvereinbarungen[8].

2.1.1 Datenverwendung aufgrund einer Einwilligung

Eine Datenverwendung aufgrund einer Einwilligung setzt nach § 4a Abs. 1 Satz 1 BDSG voraus, dass diese auf der „freien Entscheidung" des Betroffenen beruht[9]. Vor allem im Arbeitsverhältnis ist die Freiwilligkeit einer erteilten Einwilligung problematisch, da ein Beschäftigter u. U. eine Einwilligung allein deshalb erteilt, weil er Repressalien des AG befürchtet[10]. Aufgrund der Anforderungen der Informiertheit und Bestimmtheit einer individuellen Einwilligung kommt ihr im Arbeitsverhältnis jedoch ohnehin nur eine untergeordnete Rolle zu. Im Arbeitsvertrag enthaltene pauschale Einwilligungen sind in aller Regel unwirksam, und spezifische Einwilligungen werden regelmäßig daran scheitern, dass nicht alle möglichen und zukünftig auftretenden Datenverwendungen konkret vorausgesehen und geregelt werden können.

Es steht zu erwarten, dass biometrische Kontrollsysteme nicht so in einen Betrieb eingeführt werden, dass ihr Einsatz von der Einwilligung einzelner Beschäftigter abhängig ist. Denn die betriebliche Datenverarbeitung und die Arbeitsabläufe können nur dann sinnvoll gestaltet werden, wenn sich ihre Zulässigkeit weitgehend einheitlich bestimmt. Wegen der Mitbestimmungsrechte der Beschäftigtenvertretungen wird die Verwendung personenbezogener Daten daher regelmäßig mittels Betriebs- oder Personalvereinbarungen als anderer Rechtsvorschrift nach § 4 Abs. 1 BDSG legitimiert werden[11].

2.1.2 Datenverwendung aufgrund § 28 BDSG

Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG[12] ist die Verwendung personenbezogener Daten zur Erfüllung eigener Geschäftszwecke zulässig, sofern sie der „Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient"[13]. Der Zweck eines Arbeitsverhältnisses liegt vor allem in der leistungsgerechten Erbringung der Arbeitskraft durch den Beschäftigten gegen eine adäquate Entlohnung entspr. dem Arbeitsvertrag und den zugrundeliegenden TV und BV[14]. Der AG darf jedenfalls bestimmte Basisdaten über die Person des Beschäftigten und Stammdaten, die für den künftigen Verlauf des Arbeitsverhältnisses erforderlich sind, verwenden[15] und zur Kontrolle der Arbeitsleistung die Verwendung der betrieblichen Arbeitsmittel in gewissen Grenzen kontrollieren[16].

Neben der Leistungserfassung durch die Verwendung personenbezogener Daten können je nach Einzelfall noch weitere Zwecke für das Arbeitsverhältnis dienlich sein[17]. Wenn die vom AG verfolgten Zwecke zu einer Datenverwendung führen, so ist die Zweckbestimmung der Daten konkret festzulegen. Es darf nicht allgemein auf „das Arbeitsverhältnis" Bezug genommen[18], und die Daten dürfen nur zweckentsprechend verwendet werden.

Wann genau die Datenverwendung dem so ermittelten Zweck eines Vertragsverhältnisses „dient", lässt das Gesetz offen. Es besteht weitgehend Einigkeit, dass die Daten zur Erfüllung der Pflichten oder zur Wahrnehmung der Rechte aus dem Vertragsverhältnis tatsächlich erforderlich sein müssen[19]. Erforderlichkeit bedeutet andererseits keine absolut zwingende Notwendigkeit, sondern ein bei vernünftiger Betrachtung zu bejahendes Angewiesensein auf die in Frage stehenden Mittel. Somit ist eine Datenverwendung erforderlich, wenn sie ein geeignetes Mittel zur Zweckerreichung ist, für das es keine sinnvolle und zumutbare Alternative gibt[20].

Auch in diesem Fall ist noch nicht entschieden, wie die Datenverwendung zur Erreichung des Zweckes konkret auszusehen hat und ob Persönlichkeitsrechte der Beschäftigten einer Kontrolle im Einzelfall entgegenstehen. Insbes. wenn sich die Zweckbestimmung eines Vertragsverhältnisses nur mittelbar ergibt, sind die gegenseitigen Rechte und Pflichten im Rahmen einer Interessenabwägung gegenüberzustellen. Im Arbeitsverhältnis ist zwischen dem Informa-

8 *BAG*, DB 1986, 2080 (2082); so auch *Bitkom,* Die Nutzung von Email und Internet im Unternehmen – Rechtliche Grundlagen und Handlungsoptionen, 2003, 10.

9 Dies bedeutet mehr als das Fehlen von Willensmängeln i. S. d. §§ 119 ff. BGB und umfasst auch ein unzulässiges Unter-Druck-Setzen, s. *Däubler,* NZA 2001, 877.

10 *Lorenz,* JZ 1997, 281 f. mit Einzelbeispielen; *Däubler,* Internet und Arbeitsrecht, 2001, Rn. 331 ff.; *ders.,* RDV 1999, 249: *Tinnefeld/Ehmann*, Einführung in das Datenschutzrecht, 3. Aufl. 1998, 212; *Hanau/Hoeren,* Private Internetnutzung durch AN, 2003, 57; *Roßnagel/Pfitzmann/Garstka,* Modernisierung des Datenschutzrechts, 2001, 92; *Gola,* RDV 2002, 111. Die freiwillige Einwilligung als Zulässigkeitstatbestand war daher stets starker Kritik ausgesetzt, s. *Simitis* (Fn. 7) § 4a Rn. 2 m. w. N.

11 Art. 29 Gruppe, Gruppe für den Schutz von Personen bei der Verarbeitung von personenbezogenen Daten, eingesetzt durch die EG-Datenschutzrichtlinie 95/46/RG: Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten, Arbeitspapier 5062/01/DE, (WP 48), v. 13. 9. 2001, 27; *Däubler* (Fn. 10), Rn. 334; *ders.,* (Fn. 6), Rn. 135, 786; Bitkom (Fn. 8), 19.

12 § 28 BDSG gilt über § 12 Abs. 4 BDSG auch im „dienst- oder arbeitsrechtlichen Rechtsverhältnis" der Beschäftigten des Öffentlichen Dienstes und damit einheitlich für Beschäftigte in privaten und öffentlich-rechtlichen Betrieben. Zur Systematik im Einzelnen s. *Simitis* (Fn. 7) § 27 Rn. 22 ff.

13 Diese Zulässigkeitsnorm wird aufgrund ihrer generalklauselartigen Formulierung und der erforderlichen Interessenabwägung zu Recht kritisiert, da sie eine Datenverwendung nicht wie vom Gesetzgeber beabsichtigt einschränkt, sondern durch ihre fehlende Bestimmtheit vielfach erst ermöglicht S. dazu *Simitis* (Fn. 7), Einl. Rn. 101 ff.; *Tinnefeld,* DuD 2002, 231 ff.; *Lambrich/Cahlik,* RDV 2002, 287.

14 *Hanau/Hoeren* (Fn. 10), 52; *Däubler* (Fn. 10), Rn. 217.

15 *Gola/Schomerus*, BDSG, 7. Aufl. 2002, § 28 Rn. 18; *Simitis* (Fn. 7) § 28 Rn. 97, 101 ff.

16 Darunter fallen im Grundsatz auch die Verkehrsdaten von Telekommunikationseinrichtungen, s. *BAG* v. 13.1.1987, AP Nr. 3 zu § 23 BDSG, Bl. 4 f.; *Gola/Schomerus* (Fn. 15), § 28 Rn. 16; *Büllesbach,* in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, 2003, Kap. 6.1, Rn. 82.

17 Zu den einzelnen in der Literatur als zulässig erachteten Zwecken s. *Raffler/Hellich,* NZA 1997, 862; *Hanau/Hoeren* (Fn. 10), 52, 58; *Däubler* (Fn. 10), Rn. 217; Bundesbeauftragter für den Datenschutz, Datenschutzrechtliche Grundsätze bei der dienstlichen/privaten Internet- und E-Mail-Nutzung am Arbeitsplatz, 2003, 1; *Rieß,* in: *Roßnagel* (Fn. 16), Kap. 6.4, Rn. 31; *Post-Ortmann,* RDV 1999, 106; *Bijok/Class,* RDV 2001, 54. Genannt werden bspw. die Verwirklichung geplanter Kosteneinsparungen, der Schutz von Betriebsgeheimnissen, die Möglichkeit zur Kontrolle eines Verbots oder des Umfangs einer erlaubten Privatnutzung von Internet/Telefon, die Gewährleistung der Datensicherheit einer Datenbank, die Optimierung betrieblicher TK-Einrichtungen und die Kontrolle von Mobbing und Belästigungen per E-Mail.

18 *Däubler,* NZA 2001, 876.

19 So bereits *Wronka/Hörle,* BDSG, 1977, § 23 Anm. 1. Der Grundsatz der Erforderlichkeit ist Ausprägung des verfassungsrechtlichen Verhältnismäßigkeitsprinzips und daneben in Art 6 Abs. 1 lit. c der EG-Datenschutzrichtlinie (Fn. 11) verankert. S.a. *Simitis* (Fn. 7), § 28 Rn. 85, 91.

20 *Gola/Schomerus* (Fn. 15), § 28 Rn. 34.

21 *Gola/Schomerus* (Fn. 15), § 28 Rn. 19.

tionsinteresse des AG und dem Anspruch der Beschäftigten auf Persönlichkeitsrechtsschutz nach § 75 Abs. 2 BetrVG abzuwägen[21].

2.1.3 Betriebliche Mitbestimmung

Letztlich erfährt die informationelle Selbstbestimmung Beschäftigter einen Schutz durch die Beschäftigtenvertretungen. Beim Einsatz eines biometrischen Kontrollsystems im Betrieb können deren Mitwirkungs- und Mitbestimmungsrechte das Direktionsrecht des AG bereits bei der Einführung eines Datenverarbeitungssystems begrenzen[22].

Zu den Gesetzen, über deren Durchführung der BR für die Beschäftigten im Privatrechtsverhältnis nach § 80 Abs. 1 Nr. 1 BetrVG zu wachen hat, gehören auch datenschutzrechtliche Bestimmungen[23]. Mitbestimmungsrechte ergeben sich insoweit vor allem bei Fragen der Ordnung des Betriebs und des Verhaltens der AN im Betrieb (§ 87 Abs. 1 Nr. 1 BetrVG) und bei der Einführung und Anwendung technischer Einrichtungen, die dazu „bestimmt sind“[24], das Verhalten oder die Leistung der AN zu überwachen (§ 87 Abs. 1 Nr. 6 BetrVG)[25]. Mit diesen Rechten sollen unzulässige Eingriffe in das Persönlichkeitsrecht der AN präventiv verhindert und zulässige Eingriffe auf das notwendige Maß reduziert werden[26].

Daneben kommt § 75 Abs. 2 BetrVG eine entscheidende Rolle für den Datenschutz im privatrechtlichen Arbeitsverhältnis zu. BR und AG haben „die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten AN zu schützen und zu fördern“[27]. Die Norm geht dabei über ein reines Abwehrrecht hinaus. Die freie Entfaltung der Persönlichkeit der AN ist nicht nur zu schützen, sondern auch aktiv zu „fördern“. AG und BR sind danach gleichermaßen verpflichtet, die Arbeitsbedingungen im Betrieb positiv datenschutzfreundlich zu gestalten[28].

2.2 Biometrische Verfahren

Biometrie ist die automatisierte Messung von natürlichen, hoch charakteristischen, physiologischen oder verhaltenstypischen Merkmalen von Menschen zum Zweck der Unterscheidung von anderen Personen[29]. Fingerabdrucksverfahren sind dabei am weitesten verbreitet[30]. Verwendet werden daneben vor allem Gesicht, Iris, Handgeometrie, Stimme und Handschrift[31]. Der Gesichtserkennung wird ein zunehmendes Potential eingeräumt[32]. Nicht jede Videoüberwachungsanlage ist ein biometrisches System. Dazu ist vielmehr erforderlich, dass die Gesichter der erfassten Personen automatisiert mit Referenzdaten abgeglichen werden und nicht nur eine Überwachung durch eine Kontrollperson vor einem Monitor erfolgt.

Im betrieblichen Umfeld ergibt sich eine Vielzahl von Möglichkeiten für den Einsatz von Biometrie[33]. Denkbar sind bspw. Zutrittskontrollen am Betriebseingang oder zu bestimmten Sicherheitsbereichen, das Single-Sign-On an PC-Arbeitsplätzen, die Sicherung von Speichermedien[34], die Absicherung der Authentizität von Handlungen der Mitarbeiter (z. B. bei elektronischen Signaturverfahren[35]) und der Kunden[36] sowie die automatisierte Kontrolle von Besuchern.

Biometrische Systeme laufen im Wesentlichen identisch ab[37]. Zunächst werden im Rahmen des sog. Enrolments Referenzdaten des Merkmalsträgers gewonnen und gespeichert[38]. Dies kann in vollständiger (Roh- oder Volldatensätze) oder extrahierter (sog. Templates) Form erfolgen. Eine weitere Möglichkeit besteht in der Verwendung templatefreier Verfahren[39]. Dabei wird aus den biometrischen Rohdaten ein kryptographischer Schlüssel berechnet und mit diesem ein beliebiger Text verschlüsselt. Dieser Text wird im Klartext und in seiner verschlüsselten Form als Referenzdatensatz gespeichert (Klartext-Chiffrat-Paar).

Beim späteren Vergleichsprozess (Matching) werden die aktuell erhobenen Daten mit den gespeicherten Referenzdaten verglichen. Eine Möglichkeit ist, diese zentral zu speichern. Dann werden vor Ort die biometrischen Daten erhoben und an eine zentrale Recheneinheit gesandt, die das Matching vornimmt. Die Referenzdaten können aber auch dezentral auf einer Chipkarte gespeichert werden. Dann kann das Matching an unterschiedlichen Stellen erfolgen. Entweder wird eine Kontrolleinheit verwendet, die die Referenzdaten aus der Karte ausliest und das Matching vornimmt. Oder die Kontrolleinheit sendet umgekehrt die erhobenen Daten an die Karte, und die Überprüfung findet in der Karte statt (Matching-On-Card). Außerdem gibt es für bestimmte Einsatzumgebungen Verfahren, bei denen die Chipkarte nicht nur über einen Mikrochip zum Matching,

22 Zu den einzelnen Mitwirkungsmöglichkeiten *Wedde*, in: *Roßnagel* (Fn. 16), Kap. 6.3, Rn. 1 ff.; *Däubler* (Fn. 10), Rn. 108 ff. Für die Angestellten im Öffentlichen Dienst *Däubler* (Fn. 10), Rn. 143 ff.; *Hartig*, in: *Roßnagel* (Fn. 16), Kap. 6.2, Rn. 12 ff. Zu den landesrechtlichen Besonderheiten *Thannheiser,* CF 3/1999, 16 ff. Im Folgenden werden nur die Rechte des BR abgehandelt. Für die Rechte des Personalrats gelten weitgehend dieselben Grundsätze.

23 *BAG* AP Nr. 29 zu § 80 BetrVG 1972, st. Rspr.; *Linnenkohl,* RDV 1990, 61, 65; *Däubler* (Fn. 10), Rn. 108 f.; *Bitkom* (Fn. 8), 10; *Fitting/Kaiser/Heither/Engels/Schmidt* (Hrsg.), Betriebsverfassungsgesetz, 2002, § 80 Rn. 7; *ErfK-Hanau/Kania,* 2001, § 80 BetrVG Rn. 3.

24 S. ausführlich *Däubler* (Fn. 10), Rn. 287 ff.; *ders.,* K&R 2000, 327. Trotz dieser Formulierung ist eine Überwachungsabsicht des AG nicht erforderlich. Es genügt die bloß objektive Möglichkeit zur Überwachung, vgl. *BAG* AP Nr. 2 zu § 87 BetrVG 1972, st. Rspr.

25 In § 75 Abs. 3 Nr. 17 BPersVG findet sich eine dem § 87 Abs. 1 Nr. 6 BetrVG entspr. Regelung für das Bundesrecht.

26 *Bitkom* (Fn. 8), 10.

27 Bei der Auslegung dieser Norm sind grundgesetzliche Wertungen wie das Recht auf informationelle Selbstbestimmung zu berücksichtigen.

28 *Hanau/Kania,* (Fn. 23), § 75 BetrVG Rn. 9; *FKHES* (Fn. 23), § 75 Rn. 74.

29 *TAB* (Fn. 6), 9. S.a. *Albrecht* (Fn. 5) m. w. N.; *Woodward/Orlans/Higgins* (Fn. 3), 27.

30 *Woodward/Orlans/Higgins* (Fn. 3), 213 nennen einen Marktanteil von 1/3.

31 Erprobt wird auch die Erkennung von Bewegungsmustern beim Gang, Hand- und Gesichtsvenenmustern, Geruch, Tippverhalten und Ohrmuschelkontur, s. *Woodward/Orlans/Higgins* (Fn. 3), 115 ff.

32 Diese wird auch von der International Civil Aviation Organization (ICAO) für den weltweiten Einsatz in Reisedokumenten favorisiert.

33 S. zum Einsatz im Betrieb *Steidle,* Die datenschutzkonforme Gestaltung von Multimedia-Assistenzsystemen im Betrieb, Kap. 10.9.2, i. E. 2005.

34 Es gibt inzwischen eine Reihe von USB-Speichern, die über einen Fingerabdruck-Sensor verfügen.

35 Vgl. § 17 Abs. 1 Satz 1 SigG i. V. m. § 15 Abs. 1 Satz 1, 3 SigV.

36 Hier kommt Biometrie etwa zur Sicherung von Online-Banking zum Einsatz.

37 S. zum Folgenden *Behrens/Roth*, in: *dies.* (Hrsg.), Biometrische Identifikation, 2001, 10 ff.; *Gundermann/Probst*, in: *Roßnagel* (Fn. 16) Kap. 9.6, Rn. 8 ff.; *Albrecht* (Fn. 5), 35 ff.; *Woodward/Orlans/Higgins* (Fn. 3), 28 ff.; *Hornung,* KJ 2004, 344, 346 ff. Auf eine Darstellung der spezifischen Funktionsweise und Besonderheiten der jeweiligen Verfahren wird an dieser Stelle verzichtet. S. insoweit die Beiträge in *Woodward/Orlans/Higgins*, ebd., Kap. 3-7; *Albrecht*, ebd., 39 ff. *Behrens/Roth*, ebd., II. Teil.

38 Schlägt dies fehl, so wird der prozentuale Anteil der fehlgeschlagenen Versuche als False Enrolment Rate oder Failure to Enrol Rate (FER) bezeichnet. Ein Fehlschlag kann durch Fehler des Systems bedingt sein. Es gibt bei den meisten Merkmalen aber auch einen gewissen Prozentsatz der Bevölkerung, der dieses entweder überhaupt nicht oder nicht in hinreichender Ausprägung für die biometrische Authentifikation besitzt.

39 *Albrecht/Probst*, in: *Behrens/Roth* (Fn. 37), 39 f.; *Gundermann/Probst*, in: *Roßnagel* (Fn. 16), Kap. 9.6, Rn. 24 f.; *Albrecht* (Fn. 5), 56 f.

40 Das ist in absehbarer Zeit nur für den Fingerabdruck realistisch. Hier existieren auch erste Prototypen, vgl. *TAB* (Fn. 6), 12; *Janke*, in: *Nolde/Leger* (Hrsg.), Biometrische Verfahren, 2002, 206 ff.

sondern auch über einen Sensor verfügt[40]. Dann kann auf eine Kontrolleinrichtung völlig verzichtet werden.

Biometrische Systeme dienen der Authentifikation (Bezeugung der Echtheit) eines Merkmalsträgers. Diese kann durch zwei Verfahren geschehen, nämlich durch Verifikation oder Identifikation[41]. Bei der Verifikation findet ein Vergleich der im Einzelfall erhobenen Daten mit einem konkreten Referenzdatensatz statt (1:1). Es wird überprüft, ob es sich bei einer Person um diejenige handelt, für die sie sich ausgibt. Die Identifikation hingegen erfolgt durch Vergleich der erhobenen Daten mit allen Referenzdaten (1:n). Hierbei wird festgestellt, um welche Person es sich tatsächlich handelt.

Aufgrund von Messfehlern, zu geringen Merkmalsausprägungen und anderen Ungenauigkeiten ergibt sich beim Matching niemals ein eindeutiges Ergebnis. Biometrische Verfahren arbeiten mit relativen Übereinstimmungsgraden und können deshalb Falschakzeptanzen und -zurückweisungen nie ganz ausschließen. Die Wahrscheinlichkeit einer ungerechtfertigten Zurückweisung wird als False Rejection Rate (FRR), die einer ungerechtfertigten Akzeptanz als False Acceptance Rate (FAR) bezeichnet[42]. Beide Raten sind von der Grundgenauigkeit des Systems und dem Wert abhängig, der für eine hinreichende Übereinstimmung festgelegt wird (Schwellwert). Je höher dieser liegt, desto geringer wird die FAR. Das ist etwa für die Zugangssicherung zu Hochsicherheitsbereichen erwünscht. Gleichzeitig steigt jedoch die FRR an. Dies ist für die Benutzer problematisch, da sich das Risiko erhöht, einen erneuten Zugangsversuch machen zu müssen, dabei unter Verdacht zu geraten oder sogar insgesamt zurückgewiesen zu werden. Aus Sicht der Merkmalsträger ist deshalb eine geringe FRR vorteilhaft[43]. In diesem Fall steigt jedoch die FAR an, was zu Sicherheitsproblemen führen kann. Die beiden Fehlerraten beeinflussen sich also gegenseitig, und die optimale Systemeinstellung kann nur nach den konkreten Einsatzbedingungen ermittelt werden.

Neben diesen Problemen des manipulationsfreien Betriebs können sich Bedrohungen durch Angriffe auf den Matchingprozess ergeben. Ein Angreifer kann dabei drei Ziele verfolgen, nämlich die Gewinnung von Daten zur missbräuchlichen Verwendung, das Absenden von Daten mit vorgetäuschter Authentizität und die Manipulation übertragener Daten[44]. Ein möglicher Angriffspunkt ist zunächst der Sensor. Hier besteht die Gefahr einer Systemüberwindung durch Fake-Angriffe (Nachahmung des Merkmals[45]) oder Datenakquisitions-Angriffe (Einspielen von Daten, die anderweitig beschafft wurden). Bei der Verwendung von Chipkarten ist darüber hinaus die Schnittstelle ein Schwachpunkt. Werden Daten mitgeschnitten und danach erneut ins System eingespielt, so spricht man von einem Replay-Angriff. Daneben ist denkbar, dass ein Angreifer übertragene Daten während der Kommunikation so verändert, dass beide Seiten die jeweils empfangenen Daten für authentisch halten. Dies wird als Man-in-the-middle-Angriff bezeichnet.

3. Der Beschluss des BAG v. 27. 1. 2004

In dem Sachverhalt, der dem *BAG*[46] zugrunde lag, ging es um eine AG, die bei einer Kundin laufend Wartungsarbeiten durchzuführen hatte. Die Kundin richtete unter Beteiligung des bei ihr gebildeten BR ein Fingerabdrucksverfahren zur Zugangskontrolle ein und vereinbarte mit der AG, dass dieses auch von deren AN einzusetzen war. Die AG erteilte ihren AN eine entspr. Weisung. Auf Antrag des BR untersagte das ArbG der AG im Wege der einstweiligen Verfügung, AN bei der Kundin einzusetzen, soweit von diesen verlangt wurde, Fingerabdrücke zu hinterlegen. In der Folgezeit wurde den AN der Zugang ohne Abgabe von Fingerabdrücken dadurch ermöglicht, dass sie von Beschäftigten der Kundin durch die Personalschleuse begleitet wurden. Im Hauptsacheverfahren beantragte der BR, es zu unterlassen, AN bei der Kundin einzusetzen, soweit von ihnen verlangt werde, dass sie dort über ein biometrisches System Fingerabdrücke hinterlegen müssten.

Das *BAG* bejaht einen entspr. Anspruch aus § 87 Abs. 1 Nr. 1 und Nr. 6 BetrVG. Damit wurde höchstrichterlich die Mitbestimmungspflichtigkeit des Einsatzes eines biometrischen Zugangskontrollsystems festgestellt, wobei die Besonderheit darin bestand, dass das System in einem (externen) Kundenbetrieb eingesetzt wurde. Der *Senat* erkannte eine Frage der Ordnung des Betriebs nach § 87 Abs. 1 Nr. 1 BetrVG[47]. Der Begriff des Betriebs nach § 87 Abs. 1 Nr. 1 BetrVG sei nicht räumlich, sondern „funktional" zu verstehen und erfasse deshalb auch außendienstliche, „betriebliche" Tätigkeiten in anderen Betrieben[48]. Ein im Kundenbetrieb errichteter BR könne mangels Mandats und Verhandlungsmöglichkeit die Interessen der auf Grund von Werkverträgen dort tätigen fremden AN regelmäßig nicht wahrnehmen. Es mache auch keinen Unterschied, ob ein AG seinen im Außendienst beschäftigten Mitarbeitern selbst bestimmte Vorschriften hinsichtlich ihres Verhaltens in den Räumlichkeiten von Kunden mache oder ob er sie anweise, die dort geltenden Regeln zu beachten. Schließlich könne die AG nicht einwenden, ihr selbst seien die Verhaltensregeln durch den Kunden vorgegeben. Sie habe vielmehr als Vertragspartner des Kunden die Möglichkeit, darauf Einfluss zu nehmen, unter welchen Bedingungen „ihre" AN dort arbeiteten. Dementsprechend obliege es ihr, durch eine entspr. Vertragsgestaltung sicherzustellen, dass die ordnungsgemäße Wahrnehmung der Mitbestimmungsrechte des BR gewährleistet seien. Hiergegen sei vorliegend verstoßen worden.

Das Gericht konstatiert auch einen Verstoß gegen die Mitbestimmung bei der Einführung einer technischen Einrichtung zur Verhaltensüberwachung nach § 87 Abs. 1 Nr. 6 BetrVG. Die Durchführung der Überwachungstätigkeit durch einen Dritten schließe die Mitbestimmung ebenso wenig aus wie die Tatsache, dass die Überwachung in erster Linie oder gar ausschließlich im Interesse des Dritten erfolge. In der Anweisung der AG an „ihre" AN, sich der biometrischen Zugangskontrolle zu unterziehen, liege somit die Anwen-

41 S. *Probst*, DuD 2000, 322; *Behrens/Roth* (Fn. 37), 10 ff.; *Woodward/Orlans/Higgins* (Fn. 3), 7 f.; *Albrecht* (Fn. 5), 38.

42 *Gundermann/Probst*, in: *Roßnagel* (Fn. 16), Kap. 9.6, Rn. 14 ff.; *Woodward/Orlans/Higgins* (Fn. 3), 35 ff. Grundsätzlich zu Fehlerraten und ihrer Messung *TeleTrusT* (Fn. 6), 9 ff.

43 Eine Ausnahme besteht bspw. dann, wenn der Merkmalsträger das biometrische Verfahren selbst zur Zugangssicherung zu eigenen Daten verwendet. In diesem Fall besteht sein vorrangiges Interesses in einer niedrigen FAR.

44 Zu Motiven und Methoden der unterschiedlichen Angriff s. etwa *Schneier*, C.ACM 8/1999, 136; *Daum*, in: *Nolde/Leger* (Fn. 40), 189 ff.; *Thalheim/Krissler/Ziegler*, c't 11/2002, 114, 115 f.; *Woodward/Orlans/Higgins* (Fn. 3), 13 f.

45 Beispiele sind Silikonfinger, Tonbandaufnahmen, Photos und Kontaktlinsen mit fremden Irismustern, vgl. *Gundermann/Probst*, in: *Roßnagel* (Fn. 16), Kap. 9.6, Rn. 20; *Thalheim/Krissler/Ziegler*, c't 11/2002, 114 ff.

46 1 ABR 7/03, AuR 2004, 106, 238 = DuD 2004, 433 ff.

47 Darunter fallen regelmäßig Regelungen über das Betreten und Verlassen des Betriebs, s. BAGE 54, 36 (44 f.); AP BetrVG 1972 § 87 Ordnung des Betriebes Nr. 17 und Nr. 7.

48 S. zur allgemeinen Definition des Betriebs als organisatorischer Einheit, innerhalb derer ein AG allein oder mit den AN mit Hilfe von technischen oder immateriellen Mitteln bestimmte arbeitstechnische Zwecke verfolgt, die sich nicht in der Befriedigung von Eigenbedarf erschöpfen, *BAG* AP Nr. 5 zu § 1 BetrVG 1972, st. Rspr.; ErfK-*Eisemann*, (Fn. 23), § 4 BetrVG Rn. 2; *Etzel*, in: *Leinemann* (Hrsg.), Kasseler Handbuch zum Arbeitsrecht, Band 2, 1997, II, 7.1 Rn. 1; *FKHES* (Fn. 23), § 1 Rn. 63.

dung einer technischen Überwachungseinrichtung gem. § 87 Abs. 1 Nr. 6 BetrVG.

4. Rechtskonforme biometrische Systeme am Arbeitsplatz

Der Entscheidung des *BAG* ist sowohl im Ergebnis als auch in der Begründung beizustimmen. Allerdings beschränkt sich der Inhalt des Beschlusses entspr. dem Antrag des BR auf das grundsätzliche Bestehen der Mitbestimmung. Es werden keine inhaltlichen Kriterien für die Zulässigkeit der Verwendung von Biometrie am Arbeitsplatz aufgestellt. Derartige Kriterien für die rechtskonforme Gestaltung der Systeme sind jedoch für die Praxis immens wichtig, da sie die Basis für die Verhandlungen zwischen AG und BR und ggf. für die Entscheidung der Einigungsstelle bilden müssen[49].

4.1 Die Rechtsprechung des BAG zur Videoüberwachung am Arbeitsplatz

Auch wenn bisherige Videoüberwachungssysteme regelmäßig keine biometrischen Systeme im eigentlichen Sinne sind (s.o.), besteht doch eine zumindest teilweise vergleichbare Interessenlage auf Seiten des AG und der Beschäftigten. Deshalb ergibt sich eine Reihe von Parallelen. Eine Videoüberwachung birgt für die Betroffenen Gefahren, da Daten erhoben werden können, ohne dass der Betroffene davon Kenntnis hat oder an der Erhebung aktiv mitwirken muss. Dies widerspricht dem datenschutzrechtlichen Transparenzprinzip. Werden vermehrt Videokameras am Arbeitsplatz eingesetzt, so kann dies zu einem Anpassungsdruck aller Beschäftigten an ein erwartetes, normgemäßes Verhalten führen, da nicht klar ist, wie die Daten verwendet werden und ob sich an ein vom AG nicht erwünschtes Verhalten Folgen anknüpfen. Dieser Anpassungsdruck beeinträchtigt das in Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG geschützte allgemeine Persönlichkeitsrecht, das in § 75 Abs. 2 BetrVG gerade für die freie Entfaltung der Persönlichkeit am Arbeitsplatz konkretisiert ist[50].

Während sich die Beobachtung öffentlich zugänglicher Räume nach § 6b BDSG richtet, besteht keine spezielle Norm für private Einrichtungen. Im Arbeitsverhältnis bestimmt sich die Zulässigkeit also zumeist nach allgemeinen Regeln, insbes. nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG[51]. Rspr. und Lehre haben hierzu Grundsätze entwickelt, die § 6b BDSG weitgehend entsprechen[52], jedoch in einigen Punkten restriktiver sind. Die heimliche Überwachung durch versteckte Kameras ist grundsätzlich ebenso unzulässig[53] wie Kameras, die ohne konkreten Anlass jederzeit eingeschaltet werden können oder ausschließlich zum Zweck der lückenlosen und dauerhaften Kontrolle der Beschäftigten verwendet werden[54]. Eine disziplinäre Verhaltens- und Leistungskontrolle darf nur bei besonders begründetem Anlass mit enger zeitlicher Begrenzung erfolgen[55]. Bei Verstößen gegen diese Regeln dürfen die gewonnen Erkenntnisse nicht zur Grundlage arbeitsrechtlicher Maßnahmen wie einer Kündigung gemacht werden[56].

Liegen überwiegende schutzwürdige Interessen des AG vor, so kann im Einzelfall eine heimliche Überwachung zulässig sein, wenn diese das einzig mögliche Mittel zur Rechtsverfolgung ist. Dies kann bei einem konkreten Verdacht von Straftaten der Fall sein[57]. Dabei reicht der vermutete Diebstahl geringfügiger Werte nicht aus[58], wohl aber ein erheblicher Warenverlust[59]. Möglich ist eine Regelung von Videoüberwachung im Rahmen einer BV. Diese findet ihre Grenzen im allgemeinen Persönlichkeitsrecht der Beschäftigten und den grundlegenden Prinzipien des BDSG als einem Mindeststandard des Datenschutzes[60]. Sie muss deshalb den beschriebenen Grundsätzen entsprechen.

4.2 Gestaltungskriterien für biometrische Systeme

Bei der Einrichtung biometrischer Systeme sind einerseits die Interessen des AG an einer effektiven Kontrolle des Zugangs zu Verarbeitungsbereichen zu berücksichtigen. Andererseits haben AG und BR gem. § 75 Abs. 2 BetrVG die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten AN zu schützen und zu fördern[61]. Hierzu zählt deren Recht auf informationelle Selbstbestimmung.

AG und Beschäftigte haben ein Interesse an technischer Sicherheit und hoher Funktionstüchtigkeit des eingesetzten Verfahrens. Dieses muss hinreichend geringe Fehlerraten gewährleisten und über Sicherungen gegen Angriffe verfügen[62]. Je nach Risiko eines Angriffs kann es ratsam sein, auf adaptive Systeme zu verzichten, bei denen die Referenzdaten kontinuierlich angepasst werden. Auch Matching-On-Card kann problematisch sein, weil dabei der Karte, die lediglich das Prüfergebnis nach außen sendet, vertraut werden muss. Wird ein Verfahren eingeführt, dass wegen zu geringer Merkmalsausprägung nicht auf alle Beschäftigen angewendet werden kann, so müssen effektive Alternativverfahren bereitgehalten werden. Zur Erprobung der Funktionsfähigkeit bieten sich Tests im Betrieb an.

Unter dem Kriterium der Erforderlichkeit des Einsatzes ist zunächst nach alternativen Absicherungen zu suchen, weil biometrische Verfahren im Verhältnis zu anderen Kontrollmechanismen regelmäßig eingriffsintensiver sind. Sofern keine gesonderte BV zur Biometrie besteht, kann die Rspr. des *BAG* zur Videoüberwachung im Rahmen der Interessenabwägung des § 28 Abs. 1 Satz 1 BDSG auf andere Formen der Kontrolle Beschäftigter wie biometrische Zugangskontrollen übertragen werden. Trotz der erheblichen Intensität eines Eingriffs in das Persönlichkeitsrecht können somit die Interessen des AG überwiegen. Dies kann der Fall sein, wenn eine biometrische Kontrolle erforderlich ist, also ein geeignetes Mittel zur Zweckerreichung darstellt, für das es keine sinnvolle und zumutbare Alternative gibt. Im Fall des *BAG* dürfte es dagegen an der Erforderlichkeit fehlen, weil die Kundin der AG offensichtlich zu einer alternativen

49 Vgl. zu den folgenden datenschutzrechtlichen Gestaltungskriterien allgemein *Hornung*, KJ 2004, 344, 351 ff.; s. auch *ders.*, 2005, (Fn. 2), Kap. 4.2.2.4.

50 S. zu den Risiken eines Anpassungsdrucks für die demokratische Gesellschaft auch BVerfGE 65, 1 (43).

51 *V. Zezschwitz*, in: *Roßnagel* (Fn. 16), Kap. 9.3, Rn. 74, 92 f. Die Datenschutzbeauftragten des Bundes und der Länder fordern demgegenüber schon seit einigen Jahren eine spezielle Regelung für die Videoüberwachung nichtöffentlicher Räume, s. DuD 2000, 305; S. auch *Steidle* (Fn. 33), Kap. 10.7.3.

52 Ausführlich *BAG*, NZA 2004, 1278 = NJW 2005, 313ff.; *Tinnefeld,* DuD 2002, 234; *Wedde,* DuD 2004, 21 ff.; *Däubler,* NZA 2001, 878.

53 *BAG*, a. a. O.; LAG *Baden-Württemberg*, BB 1999, 1439; LAG *Köln*, BB 1997, 476; *Bäumler,* RDV 2001, 68; *Däubler* (Fn. 6), Rn. 294, 312.

54 *BAG 7. 10. 1987* - 5 AZR 116/86 , DB 1988, 403; dazu *Buschmann*, AiB 1988, 210 ff.; *FKHES* (Fn. 23), § 75 Rn. 80.

55 S. *v. Zezschwitz*, in: *Roßnagel* (Fn. 16), Kap. 9.3, Rn. 98.

56 LAG *Baden-Württemberg*, RDV 2000, 27; LAG *Hessen*, RDV 2002, 86.

57 LAG *Baden-Württemberg*, BB 1999, 1439; OstLG Bayern, RDV 2002, 313; *v. Zezschwitz*, in: *Roßnagel* (Fn. 16), Kap. 9.3, Rn. 98.

58 LAG *Köln*, BB 1997, 476.

59 *BAG*, RDV 2003, 293; *BAG*, Fn. 54; *BAG*, DuD 2003, 705; *Tammen,* RDV 2000, 16.

60 Zur Regelungskompetenz der Betriebsparteien ausdrücklich *BAG*, NZA 2004, 1278 ff.; *BAG*, RDV 1992, 178, nichtamtl. LS; *Tammen,* RDV 2000, 16.

61 Vgl. zu den hieraus resultierenden Abwägungsprozessen *Albrecht* (Fn. 5), 198 ff.; s.a. *Hornung*, KJ 2004, 344, 354 f.

62 So kann z. B. dem Problem der Fake-Angriffe mit Lebenderkennungssystemen begegnet werden, s. *Breitenstein,* in: *Nolde/Leger* (Fn. 40), 45, 50; *Albrecht* (Fn. 5), 55; *Woodward/Orlans/Higgins* (Fn. 3), 142 ff.

63 Zur Verwendung einer alternativen Technik bei fehlender Erforderlichkeit *Däubler,* (Fn. 6), Rn. 289 f.

Ablaufgestaltung bereit war, indem sie die AN persönlich in Empfang nahm[63]. Wäre das nicht gegeben, könnte das Interesse der AG überwiegen, wenn sie ansonsten einen Kunden verliert.

Kommt man zu dem Ergebnis, dass die Einrichtung des biometrischen Systems grundsätzlich zulässig ist, so bedeutet dies nicht, dass jede denkbare technische Umsetzungsvariante legitimiert ist. Die Datenverwendung ist strikt auf den tatsächlich erforderlichen Umfang zu begrenzen. Hierzu muss eine präzise Zweckbestimmung der Verwendung der biometrischen Daten erfolgen, etwa ausschließlich zur Zugangskontrolle eines bestimmten Fertigungsbereiches. Andere Verwendungszwecke – in diesem Fall etwa zur Arbeitszeitkontrolle – sind dann unzulässig. Die Zweckbestimmung ist nach Möglichkeit technisch abzusichern, um eine missbräuchliche Datenverwendung sicher auszuschließen[64].

Der tatsächliche Umgang mit den Daten ist in der Folge daraufhin zu untersuchen, ob er über das zur Zweckerreichung erforderliche Maß hinausgeht. In einer Vielzahl von Situationen wird sich das Interesse des AG bspw. auf die Prüfung der grundsätzlichen Zutrittsberechtigung beschränken. In diesem Fall muss das Zugangskontrollsystemen lediglich überprüfen, ob die Referenzdaten der kontrollierten Person in einem Pool von Daten der Berechtigten enthalten sind[65]. Eine Individualisierung der Referenzdaten ist dann nicht erforderlich. Diese sind somit zu anonymisieren. Wenn hierdurch die Identifizierung eines konkreten AN vollständig und technisch sicher ausgeschlossen wird, kann dies sogar dazu führen, dass das Mitbestimmungsrecht des BR entfällt[66]. Dies dürfte allerdings die Ausnahme sein. Überdies ist die Information und Beteiligung der Beschäftigten aus Akzeptanzgründen zu empfehlen. Muss eine Identifizierung der konkret kontrollierten Person stattfinden, so können häufig Pseudonyme verwendet werden, die lediglich in bestimmten Situationen, etwa beim Verdacht auf eine Straftat oder weisungswidrige Handlung, den Klarnamen zugeordnet werden[67].

Auf die Anlage einer zentralen Referenzdatenbank biometrischer Daten ist nach Möglichkeit zu verzichten. Zentrale Datenbanken erhöhen das Risiko von Zweckentfremdungen[68]. Außerdem machen sie interne und externe Angriffe attraktiv und damit wahrscheinlicher. Als Alternative kommt die dezentrale Speicherung auf Chipkarten wie Betriebsausweisen oder anderen Token in Betracht[69]. Hierdurch kann auch das Authentisierungsmittel Sein (Biometrie) mit dem Besitz (des Ausweises) kombiniert und so ein höherer Grad an Sicherheit hergestellt werden. Auch der zusätzliche Einsatz einer PIN oder eines Passwortes ist denkbar.

Bei der Auswahl des biometrischen Merkmals ist zu berücksichtigen, inwieweit dieses Zusatzinformationen über den Betroffenen preisgibt. Wenn das verwendete Datum Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben enthält (vgl. § 3 Abs. 9 BDSG), so schließt § 28 Abs. 6 BDSG die Verarbeitung unter Berufung auf die Zweckbestimmung des Arbeitsvertrages ausdrücklich aus. Stattdessen ist – wenn keine BV besteht – eine individuelle Einwilligung erforderlich, die von jedem AN verweigert werden kann. Dies ist jedoch kaum mit den Erfordernissen einer einheitlichen Gestaltung der betrieblichen Abläufe vereinbar.

Inwieweit aus biometrischen Daten auf die Gesundheit des Merkmalsträgers geschlossen werden kann, ist wissenschaftlich umstritten[70]. Unterstellt man entspr. Zusammenhänge, so ließe sich einwenden, dass die Systeme diese und andere Zusatzinformationen im Normalbetrieb nicht erfassen und verarbeiten. Es verbleibt aber das Risiko von Zweckentfremdungen, insbes. bei einer Speicherung in zentralen Datenbanken. Eindeutig ist schließlich bspw., dass Gesichtsdaten Informationen über die rassische und ethnische Herkunft des Betroffenen enthalten. De lege lata können diese im Betrieb damit nur auf der Basis von BV und individuellen Einwilligungen eingesetzt werden.

Eng verbunden mit der Frage von Zusatzinformationen ist die nach der Verwendung von Templates und templatefreien Verfahren. Wenn bei der Berechnung der Templates substantielle Teile der Volldatensätze entfernt werden und diese nicht rekonstruierbar sind, sind sie unter dem Gesichtspunkt der Datensparsamkeit vorzugswürdig. Das gilt umso mehr für die Verwendung templatefreier Verfahren, die keine personenbezogenen biometrischen Referenzdaten speichern. Allerdings verbleibt in beiden Fällen das Problem, dass zum Matching in aller Regel die Rohdaten des Betroffenen erhoben und verarbeitet werden müssen[71].

Von größter Bedeutung ist die Transparenz der Datenerhebung. In Übertragung der Rspr. des *BAG* zur Videoüberwachung am Arbeitsplatz ist die heimliche Kontrolle der Beschäftigten mittels biometrischer Identifikationssysteme grundsätzlich unzulässig. Das datenschutzrechtliche Transparenzgebot wird verletzt, wenn Daten „im Vorbeigehen" erhoben werden können. Der Einsatz offener Systeme und die vollständige Information der Beschäftigten ist letztlich auch im Interesse des AG, weil die Unsicherheit über Ob und Umfang der Überwachung den Betriebsfrieden gefährden kann. Unter dem Gesichtspunkt der Transparenz ist insbes. die Gesichtserkennung kritisch zu sehen[72]. Hier muss nach Möglichkeit gewährleistet werden, dass die verwendeten Systeme auch technisch eine heimliche Kontrolle ausschließen. Vorzugswürdig sind im Ergebnis Systeme, die das biometrische Merkmal mitwirkungsgebunden erheben, also etwa die Merkmalspräsentation am Sensor in einer definierten Art und Weise erfordern, die nicht ohne Kenntnisnahme des Betroffenen möglich ist.

Schließlich ist die Einrichtung biometrischer Systeme ohne Gewährleistung hinreichender Mechanismen der Datensicherung unzulässig[73]. Im Rahmen der vorzunehmenden Interessenabwägung kön-

64 So sollten die Daten nach Zwecken getrennt vorgehalten werden, sog. „informationelle Gewaltenteilung", *Däubler* (Fn. 6), Rn. 130, 394 ff. mit Einzelbeispielen; *Steidle* (Fn. 33), Kap. 10.3.2.

65 Vgl. *Gundermann/Köhntopp*, DuD 1999, 143, 147.

66 S. *Albrecht* (Fn. 5), 208 f.

67 S. zum Einsatz von Pseudonymen *Bizer*, in: Simitis (Fn. 7), § 3 Rn. 225 ff.; *Scholz*, Datenschutz beim Internet-Einkauf, 2003, 190 ff. m. w. N.

68 *Bizer*, DuD 2002, 44; *Golembiewski/Probst* (Fn. 2), 69 f., 72; *Woodward/Orlans/Higgins* (Fn. 3), 40; *Albrecht* (Fn. 5), 162 ff.; *Hornung*, KJ 2004, 344, 352 f.; 357.

69 Hierbei greifen die Transparenzpflichten aus § 6c BDSG ein, wenn Matching-On-Card stattfindet oder die Karten über Sensoren verfügen. S. hierzu *Hornung*, DuD 2004, 15, 16.

70 Es werden bspw. Zusammenhänge zwischen bestimmten Fingerabdruckmustern und chronischen Magen-Darm-Beschwerden, Leukämie, Rubella-Syndrom und Brustkrebs genannt. Aus Irisdaten sollen sich Erkenntnisse über Erkrankungen wie Diabetes, Arteriosklerose und Bluthochdruck ergeben. S. näher *Woodward/Orlans/Higgins* (Fn. 3), 202 f.; *Gundermann/Probst*, in: *Roßnagel* (Fn. 16), Kap. 9.6, Rn. 26. m. w. N.

71 S. dazu, und zum Problem des Personenbezugs biometrischer Daten insgesamt *Hornung*, DuD 2004, 429 ff.; *Steidle* (Fn. 33), Kap. 14.7.

72 *Albrecht/Probst*, in: *Behrens/Roth* (Fn. 37), 32; *Woodward*, Super Bowl Surveillance. Facing Up to Biometrics, abrufbar unter http://www.rand.org/publications/IP/IP209/, 2001, 7 ff.

73 S. *Albrecht* (Fn. 5), 200 m. w. N.

nen die Interessen des AG nur überwiegen, wenn er umgekehrt die erforderlichen Vorkehrungen zum Schutz der sensiblen Daten gegen Missbrauch trifft. Dabei sind die Anforderungen aus § 9 BDSG und der zugehörigen Anlage zu berücksichtigen. Zutritt und Zugang zu biometrischen Systemen sind organisatorisch und technisch zu sichern, unbefugte Zugriffe durch Sicherungsfunktionen auszuschließen und es ist eine getrennte Verarbeitung von anderen Datenbeständen zu gewährleisten.

4.3 Praktische Umsetzung durch Betriebs- und Dienstvereinbarungen

Die praktische Umsetzung inhaltlicher Gestaltungskriterien für ein biometrisches Zugangskontrollsystem erfolgt am besten in einer BV, da der BR wegen seiner Mitbestimmung nach § 87 Abs. 1 Nr. 1 und Nr. 6 BetrVG ohnehin zu beteiligen ist. Inhalt der Vereinbarung sollten insbes. die folgenden Punkte sein:

- Die transparente Erläuterung der Umstände und Gesichtspunkte, die die Erforderlichkeit der Einführung des biometrischen Systems in der konkreten betrieblichen Situation begründen.
- Die konkrete und abschließende Festlegung des Verwendungszwecks.
- Der Ausschluss von Verhaltens- und Leistungskontrollen mittels des Systems.
- Die Erläuterung der Funktionsweise des Systems (erstmalige Datenerhebung, Datenspeicherung, Kontrollsituationen, Maßnahmen zur Datensicherung).
- Eine regelmäßige Evaluation der Leistungsfähigkeit des Systems.
- Die Verpflichtung des AG, alternative Zugangsmechanismen einzurichten, falls sich einer oder mehrere Beschäftigte als zur biometrischen Erkennung ungeeignet erweisen.
- Die Festlegung konkreter Aufklärungspflichten des AG über Zweck, Ablauf und Funktionsweise des biometrischen Verfahrens. Diese können etwa durch die Erstellung einer Broschüre umgesetzt werden. Denkbar ist auch die Mitwirkung des BR bei der Unterrichtung der Beschäftigten.
- Art und Umfang der Mitwirkung des betrieblichen Datenschutzbeauftragten.
- Bestimmungen über die Löschung von Daten, beispielsweise nach dem Ausscheiden von Mitarbeitern.

Eine wertvolle Hilfe für die Praxis könnte die Entwicklung von MusterBV sein, die Leitlinien für kleine und mittlere Betriebe bieten[74].

5. Ausblick

Biometrische Verfahren werden in absehbarer Zeit nicht nur im Bereich der hoheitlichen Identifikation mittels Ausweispapieren, sondern auch im betrieblichen Umfeld in großem Maße eingesetzt werden. Alle Beteiligten an der betrieblichen Mitbestimmung haben ein hohes Interesse daran, Rechtssicherheit über die Zulässigkeit des Einsatzes zu erlangen. Die genannten Kriterien können hierfür Leitlinien bilden. Letztlich ist jedoch ihre Ausformung und weitere Konkretisierung auf die Besonderheiten des jeweiligen betrieblichen Umfelds unumgänglich.

Zu diesem Zweck ist eine möglichst frühzeitige Information der Beschäftigtenvertretung durch den AG von größter Wichtigkeit. Damit werden nicht nur rechtliche Unsicherheiten und Verzögerungen

74 Hierzu gibt es derzeit Aktivitäten des Arbeitskreises Recht der AG 6 des Teletrust e. V. unter Leitung von Frau Dr. *Astrid Albrecht* (BSI).

[Zusammenfassung/Summary auf S. 240]

Übermittlung von Arbeitnehmerdaten im Konzernverbund im Rahmen eines konzerneinheitlichen Datenverarbeitungssystems

Fachanwalt für Arbeitsrecht Dieter Hummel/Rechtsanwalt Sönke Hilbrans, Berlin

Vielfältige Aufgaben der Konzernspitze, wie z. B. das Personalcontrolling, werden insbes. bei heterogener IT-Landschaft in den Konzernunternehmen durch die Erfassung personenbezogener Daten von AN direkt bei der Konzernspitze, bspw. mittels eines konzerneinheitlichen Business-Warehouse-Systems oder HR-Systems, erleichtert. Die zentrale Verarbeitung personenbezogener Daten erscheint dabei nur gerechtfertigt, wenn, was häufig genug umstritten ist, personenbezogene Daten der Mitarbeiter in den Unternehmen für originäre Aufgaben der Konzernspitze benötigt werden. Können sich Konzernbetriebsrat und AG nicht auf eine Konzernbetriebsvereinbarung einigen, gilt die Einsetzung einer Einigungsstelle als Mittel der Wahl. Neben den Erfordernissen des Arbeitnehmerdatenschutzes wirft dabei auch die sachliche Kompetenz der Einigungsstelle Fragen auf, denen dieser Beitrag nachgeht.

I. Datenschutzrechtliche Vorfragen

1. Der Konzern ist datenschutzrechtlich „Dritter“

Bei der Einführung technischer Einrichtungen zur Arbeitnehmerdatenverarbeitung ist der BR regelmäßig nach § 87 Abs. 1 Satz 1 Nr. 6 BetrVG zu beteiligen. Ein Konzern selbst ist nicht AG, diese Rolle nimmt das jeweilige Konzernunternehmen ein. Diese Rollenverteilung spiegelt sich in der Verteilung der datenschutzrechtlichen Verantwortung: § 2 Abs. 4 Satz 1 BDSG stellt alleine auf die speichernde Stelle als selbständige natürliche oder juristische Person ab. Ungeachtet der wirtschaftlichen Verflechtungen ist allein das mit dem AN vertraglich verbundene Unternehmen und nicht der Konzern diejenige Stelle, die personenbezogene Daten der AN erhebt und speichert. Auch eine noch so ausgeprägte ökonomische Einheit begründet mithin keine Informationseinheit[1], denn der Gesetzgeber hat

1 *Simitis* in: Simitis u. a., BDSG, 5. Aufl. (2003), § 2 Rn. 139.

Der folgende Text wurde im Heft 6 der AuR beim Aufsatz von Hornung/Steidle durch ein Versehen der Redaktion nicht mit abgedruckt:

durch gerichtliche Verfahren wie im Fall des BAG vermieden, sondern es wird durch die Einbeziehung in die Prozesse der Entscheidungsfindung auch die Akzeptanz der Systeme durch die Beschäftigten gefördert. Letzteres ist im allseitigen Interesse, weil ein hohes Maß an Kooperationsbereitschaft nicht nur die Effektivität der biometrischen Systeme erhöht, sondern auch dem Betriebsklima dient.