MANUEL KIPER

Biometrische Identifikation –

Ein reizvoller Gedanke: Statt Passwörtern, Geheimnummern oder Chip-Karte benötigt man nur noch einen Fingerabdruck oder das eigene Gesicht, um sich vorm Computer auszuweisen. Aber – wie immer – hat die Angelegenheit natürlich einen Haken.

Big Brother – jener Diktator, der in George Orwells Roman ›1984‹ alles und jeden beobachten ließ – stützt sich neuerdings auf die Biologie. Die letztjährige Auseinandersetzung um die Anlage einer bundesweiten Gen-Datei im Rahmen der Strafverfolgung zeigte dabei nur die Spitze neuer Daten- und Persönlichkeitsschutz-Probleme, die sich aus der technischen Realisierung biologiegestützter Identifizierungs- und Überwachungssysteme ergeben.

Die Gen-Analyse erlaubt heute die Entschlüsselung geringster Spuren biologischen Materials und ihre Zuordnung zu einer bestimmten Person – dauert allerdings noch zwei Wochen und ist teuer. In Sekundenschnelle hingegen können heute bereits andere messbare ›Körperdaten‹ wie Stimme, Gesicht, Iris, Fingerkuppen und so weiter ausgewertet und sogenannte biometrische Identifikationen vorgenommen werden, etwa für systematische Zugangskontrollen oder eine automatisierte Anwesenheitserfassung. Zusammen mit den digitalen Datenspuren, die jede Telekommunikation hinterlässt, und mit den wachsenden Gen-Datensammlungen lassen sich so Persönlichkeitsprofile gewinnen und Überwachungsverfahren werden denkbar, die die Visionen von ›Brave New World‹ und ›Big Brother is Watching You‹ weit in den Schatten stellen.

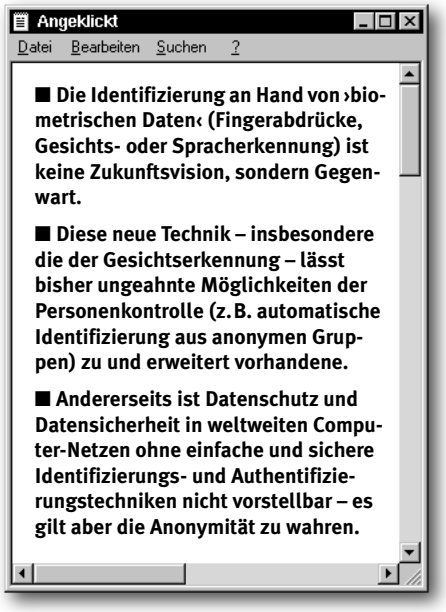
Biometrie wird jetzt eingeführt

Dass die biometrische Identifikation keine Zukunftsmusik ist, sondern genau jetzt eingeführt wird und dabei Passworte oder persönliche Identifikations-Nummern (PIN) ergänzt oder auch ersetzt, zeigt das Beispiel der Dresdner Bank: Seit Anfang dieses Jahres testet deren Frankfurter Zentrale einen ›Procash‹-Geldautomaten von Siemens-Nixdorf mit einer Iris-Erkennungs-Software der amerikanischen Firma Sensar. Eine Video-Kamera nimmt die Regenbogenhaut des menschlichen Auges am Geldautomaten auf, 266 Strukturmerkmale werden digitalisiert und mit einer bereits gespeicherten Vorlage verglichen. Fällt dieser Vergleich positiv aus, wird die Auszahlung freigeschaltet – ein Vorgang der nicht einmal zwei Sekunden dauert.

Mit der Iris liegt diesem biometrischen Identifizierungs-Verfahren ein statisches, also unveränderbares, biologisches Merkmal zu Grunde, das mit weit über 200 zu differenzierenden Strukturmerkmalen der Identifizierung über den Fingerabdruck weit überlegen ist (denn bei diesem – ebenfalls statischen – Verfahren können nur rund 40 Strukturmerkmale genutzt werden).

Auf der diesjährigen CeBIT in Hannover wurde aber auch ein Zugangssystem namens ›BioID‹ des Berliner Unternehmens DCS vorgestellt. Dieses System arbeitet ›multimodal‹ – soll heißen: Sowohl statische wie auch dynamische (sich verändernde) biologische Merkmale der zu identifizierenden Person werden genutzt. Konkret werden das Gesicht, die Stimme und die Lippenbewegungen beim Sprechen zur Erstellung eines biometrischen Datensatzes und zur eindeutigen Identifikation herangezogen. Ein System also, das gewissermaßen die Fortentwicklung jener ›multimodalen Identifikation‹ ist, die schon die ›Sieben Geißlein‹ der Gebrüder Grimm anwendeten: Sie arbeiteten mit einer Schlüsselnachricht (»Eure Mutter ist wieder da!«), hoher Stimme und weißer Pfote ...

Bezeichnenderweise nennt sich ein ähnliches multimodales System, das als ›High-Tech-Pförtner‹ von der Fraunhofer-



Gesellschaft in Erlangen entwickelt wurde, ›Sesam‹ (Synergetische Erkennung durch Standbild, Akustik und Motorik).

Die neuen Identifikations-Techniken

Die genannten zwei Verfahren sind nur Beispiele für eine ganze Reihe neuer biologie-gestützter Identifikations-Verfahren, die sekundenschnell arbeiten. Genutzt werden:

Wärmeabstrahlungsmuster ...

... der Blutgefäße in der Gesichtshaut; diese sogenannten Thermogramme werden zum Beispiel von der Firma Technology Recognition Systems angeboten.

Fingerabdruck:

Angeboten wird dazu beispielsweise das System FIU (Fingerprint Identification Unit) von Sony; verarbeitet werden dabei Fingerabdruck, thermische Informationen und die spezielle (Finger-)Drucktechnik einer Person. In den nächsten Jahren soll die Miniaturisierung und der Einbau in die Maus des Computers bewerkstelligt werden. Siemens präsentierte schon auf der CeBIT'97 einen Chip, der mittels 65 000 winzigen Sensoren die Fingerkuppen abtastete, womit ein ›lebendes‹ Schlüsselsystem etwa bei der Handy-Benutzung möglich würde.

Bio-Prox heißt eine neue, bereits vermarktete Schließtechnik für Chefetagen und Gefängnisse. Von der Firma Deister-Electronic in Barsinghausen wird dieses System angeboten, das aus einer Kombination von Chip-Karte und Lesegerät besteht. Die Chip-Karte sagt dem Gerät, wie der persönliche Fingerabdruck aussehen soll; Einlass bekommt nur, wer den richtigen Fingerabdruck auf dem Lesegerät platziert. So ist die Identitätsprüfung bereits nach einer halben Sekunde abgeschlossen, da der richtige Fingerabdruck nicht erst in einer Datenbank gesucht werden muss. Seit Jahren sind solche automatisierten Zugangssysteme schon an Flughäfen wie zum Beispiel in New York installiert. Das kalifornische Unternehmen Identicator

Technology bietet inzwischen auch einen Fingerabdruck-Scanner an, über den Beschäftigte an ihrem Arbeitsplatzrechner Zugang zum Firmennetz erhalten.

Gesichtserkennung:

Kybernetiker vom Max-Planck-Institut in Tübingen, am Zentrum für Neuro-Informatik der Ruhr-Uni Bochum, am MIT in den USA und anderswo arbeiten an Erkennungssystemen auf der Basis von Gesichtstypien (die die Lage markanter Punkte zueinander erfassen) oder sogenannter Eigengesichter (die Eindeutigkeit durch die Überlagerung unterschiedlicher mimischer Ausdrücke eines Gesichts erzielen – siehe Abbildung auf Seite 49).

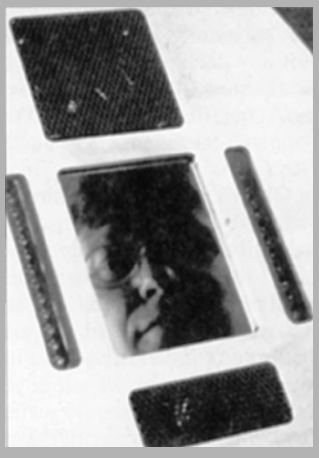
Am Markt werden bereits angeboten: das von der Bochumer ZN GmbH entwickelte ZN-Face, das Gesichtserkennung in weniger als drei Sekunden erlaubt, und das Produkt Phantomas, das ein automatisiertes Duchsuchen großer Bilddatenbestände ermöglicht (dabei werden auch ›ähnliche‹ Gesichter ermittelt). Auch FacsVACS von Siemens-Nixdorf ist bereits zu bekommen und erlaubt die Gesichtserkennung zusammen mit einer persönlichen Chip-Karte – so ist es wohl nur noch eine Frage der Zeit, bis uns ein Geldautomat immer schon dann bedient, wenn wir ihn freundlich anlächeln.

Folgende Systeme wurden bereits installiert: Die Gesichtserkennungstechnik FaceIt der New Yorker Firma Visionics identifiziert Passagiere und Gepäck auf Flughäfen (seit Juli 1997 z. B. am Internationalen Flughafen Malaysia). Auch am Eingang der Berliner Bundesdruckerei identifiziert ein Computer Beschäftigte an Hand ihres Gesichts. »Fratze schneiden? Zwecklos. Brille auf? Keine Chance. Dreitagebart? Aussichtslos. Dem computergesteuerten Türsteher ZN-Face macht niemand etwas vor!«, begeisterte sich die Wirtschaftswoche.

An der Ruhruniversität Bochum ist unter der Leitung von Professor Christoph von der Malsburg bereits eine Weiterentwicklung des elektronischen Pförtners erfolgreich. Mit dem neuen System namens PersonSpotter lassen sich Gesichter aus einer größeren Menge heraus automatisch verfolgen und identifizieren – auch im Halbprofil. Dabei können bislang zwölf Video-Bilder pro Sekunde abgetastet werden und es lassen sich bis zu acht Personen in der Minute identifizieren – selbst wenn sie sich bewegen oder maskiert sind. Von den amerikanischen Streitkräften ist Malsbergs Programm jüngst als das beste und präziseste Gesichtserkennungs-Programm ausgezeichnet worden.

Iris-Mustererkennung mit einem Iris-Scanner:

John Daugman an der Universität Cambridge hat mit Iris-Scannern Zugangskontrollen für Gebäude, für Sicherheitszonen, für die eindeutige



Links oben: Fingerabdruck-Scanner von Compaq
Links und unten: Gesichtserkennung und mehr – das multimodale BioID-System (genannt auch der ›elektronische Pförtner) ...

Zuordnung persönlicher Dokumente, für Kraftfahrzeug-Diebstahlsicherungen, für die Sicherung von Telekommunikation und anderes entwickelt. Die bereits genannte amerikanische Firma Sensar hat einen Iris-Scanner unter dem Namen Irisdent für die Verwendung in Banken weltweit patentieren lassen. Die amerikanische Citybank testete den Scanner als erste Bank in Los Angeles. Im Gefängnis von Cook County, Illinois, müssen die Häftlinge bereits in jedem Trakt Augen-Lesegeräte passieren. Die ebenfalls mögliche Identifikation mittels eines Retina-Scans (= Netzhautabtastung) ist zwar versucht worden, aber wegen der Ausleuchtung des inneren Auges gesundheitlich nicht zu verantworten.

Tipp- und Unterschriftsverhalten:

An der Universität Regensburg wurde von Professor Bartmann eine Software entwickelt, die Personen durch Analyse von Schreibrhythmus, Anschlagverhalten und weiteren charakteristischen Merkmalen beim Tippen auf einer Tastatur zweifelsfrei identifizieren kann. Die dynamische Unterschriftserkennung (z. B. durch Checkmate oder Countermatch) wird von mehreren Herstellern angeboten; Feldtests (z. B. bei der Post und der Wohlfahrt in Großbritannien) sind positiv verlaufen.

Spracherkennung:

Weit fortgeschritten ist auch die Spracherkennung. Mit ViaVoice von IBM kann mit Sprache und Gesten ein Computer gesteuert werden. VoiceXpress der belgischen Firma Lernout & Hauspie erlaubt Spracherkennung in Kombination mit Textverarbeitung. Das unter Federführung des Forschungszentrums Saarbrücken für Künstliche Intelligenz mit einem Aufwand von bisher 100 Millionen Mark entwickelte sogenannte Verbmobil erlaubt nicht nur die Spracherkennung, sondern gleichzeitig eine Übersetzung in eine Fremdsprache.

All diese Systeme müssen sich allerdings erst systematisch auf die feinen individuellen Sprachmodulationen eines Sprechers einstellen. Und das heißt umgekehrt: Die Schwingungsspektren und Modulationen der Stimme sind ein individueller ›Stimmabdruck‹ und können zur Personen-Identifizierung genutzt werden.

Schweißgeruch:

Eine englische Firma mit dem bezeichnenden Namen Bloodhound Sensors entwickelt zur Zeit Erkennungssysteme für individuellen Schweißgeruch.

DNA-Profiling:

Mit dieser Technik kann aus einer winzigen Spur Erbsubstanz (einem Haar, dem Speichel an einer Zigarette usw.) ein für jeden Menschen charakteristisches Muster erzeugt werden, das dann als Strichcode sichtbar gemacht werden kann. Ausgewertet werden dabei die Merkmale von fünf aus rund dreitausend Mustern eines Zellkerns. Das Ergebnis kann als Zahlenreihe gespeichert und mit anderen Proben verglichen werden. Die Typisierung der DNA-Proben dauert allerdings noch durchschnittlich 14 Tage, so dass dieses Verfahren als Zutrittskontrolle für Gebäude oder zur Prüfung von Zugangsberechtigungen noch chancenlos ist. Die Beschleunigung und Miniaturisierung auch der genetischen Identifikationssysteme schreitet allerdings in großen Sprüngen voran.

Mit diesen in Entwicklung begriffenen oder auf dem Markt bereits erhältlichen modernen biometrischen Identifikations-Techniken wird der Körper selbst zum Ausweis. Die Identität einer Person lässt sich fälschungssicher feststellen, die Anwesenheit einer Person und ihre

jeweilige Kommunikation lassen sich lückenlos überwachen.

Zum Ausmaß biometrischer Datenspeicherung

In Deutschland werden Fingerabdrücke seit Dezember 1992 im BKA-System AFIS gespeichert – von Verbrechern und Asylsuchenden. Von über 2 Millionen ›erkennungsdienstlich behandelten Personen‹ enthält die Kartei des BKA auch Fotografien.

Das Hamburger Software-Haus Dermalog Identification Systems hat Indonesien in die Lage versetzt, die Fingerabdrücke von 35 Millionen Bürgern elektronisch zu erfassen und hat die dortigen Behörden mit einem automatisierten Erkennungssystem für Fingerabdrücke ausgerüstet. Zur Zeit werden auch die brasilianischen Behörden mit einem Fingerabdruck-Erkennungssystem für 150 Millionen Menschen ausgerüstet und das Bundesausfuhramt hat gerade die Test-Installation des Systems im Iran genehmigt ...

Entsprechend ausufernd scheint sich die staatliche Sammelwut bei den ›genetischen Fingerabdrücken‹ zu entwickeln. Als erstes europäisches Land errichtete Großbritannien 1994 eine DNA-Datenbank in Birmingham. Seither wurden dort DNA-Profile von 290 000 Verdächtigen gespeichert. Seit 1998 sollen jährlich 200 000 weitere hinzu kommen, so werden zum Beispiel alle bekannt gewordenen Drogenkonsumenten auf diese Art erfasst.

Seit Anfang 1998 gibt es eine DNA-Datenbank nicht nur in Deutschland, sondern auch in Norwegen, in Belgien, in den Niederlanden und in Österreich. »In der ersten Phase wollen wir besonders schwere Fälle bearbeiten und jene, bei denen wir davon ausgehen, dass der Täter wiederkommen wird [...]. Unser Fernziel ist es, dass jeder der registriert wird, einen DNA-Mundhöhlenabstrich über sich ergehen lassen muss«, hieß es dazu aus dem österreichischen Innenministerium. In Deutschland wurde 1998 mit dem DNA-Identitätsfeststellungsgesetz immerhin ein eher strenger Persönlichkeitsschutz etabliert.

Bei der Video-Überwachung (CF 2/99 ab Seite 4) hingegen fehlt dies praktisch völlig – ihr Ausmaß steigt auch hier zu Lande ständig an. 1976 führte Hannover als erste deutsche Stadt mit 25 ferngesteuert schwenkbaren stationären Zoom-Kameras den Dauereinsatz der Video-Technik ein – unter anderem auch zur Überwachung von ›Rand- und Problemgruppen‹. Ebenfalls seit 1976 überwachen die polizeilichen Beweissicherungs- und Dokumentationstrupps Demonstrationen mit kleinen Video-Kameras und fertigen damit gestochen scharfe Portrait-Aufnahmen an. Und auch wenn in Deutschland der betrieblichen Video-Überwachung von Beschäftigten erhebliche datenschutzrechtliche Hürden entgegen stehen und die Gerichte heimliche Überwachung nur als letztes Mittel innerbetrieblicher Kontrolle anerkennen, so wird doch auch hier die Video-Überwachung in Kaufhäusern, Spielbanken und so weiter immer lückenloser. Und sie kann beliebig mit am Markt käuflicher Software zur automatischen Personenerkennung gekoppelt werden.

Ein ›Eigengesicht‹, das zur Gesichtserkennung herangezogen wird, entsteht durch Überlagerung von Gesichtern mit unterschiedlicher Mimik, so werden die Gesichtspartien herausgefunden, die weitgehend unveränderlich bleiben.

Die in Großbritannien vorhandenen automatischen Personen-Identifizierungs-Techniken versetzen die britische Regierung heute schon, so eine Untersuchung an der Universität Hull, in die Lage, jeden einzelnen Menschen auf den Inseln zu kontrollieren. Dabei haben moderne Video-Kameras nicht nur Infrarot-Ansicht, Fernbedienung, Zoom und automatische Verfolgung im Repertoire, sondern lassen sich auch mit elektronischen Personenerkennungs-Systemen kombinieren, deren Software in der Lage ist, ›normales‹ von verdächtigem Verhalten zu unterscheiden. Alles in allem sind in Großbritannien bereits 300 000 Überwachungs-Kameras installiert – mehr als 200 000 sollen es in Deutschland sein!

Ende letzten Jahres startete in einem Londoner Stadtteil das Mandrake-Projekt. Dort wurden 240 Video-Kameras gekoppelt mit Gesichtserkennungs-systemen installiert und sollen das Auftauchen bekannter Verbrecher automatisch feststellen und den Behörden melden.

Bedenklich ist all das vor allem, wenn verschiedene biometrische Datensammlungen gekoppelt werden. In den USA zum Beispiel liegen über vier Millionen digitalisierte Bilder von Führerscheininhabern in einer Datenbank in Massachusetts und werden vom MIT benutzt, um damit das Projekt Photobook zur sekundenschnellen Identifikation zu entwickeln.

Nicht zuletzt machen Computer-Firmen wie Lotus mit ›Awareness‹-Technologien (awareness = Einblick) die PC-Arbeit an anderen Arbeitsplätzen durchsichtig. Konkret: Man kann (Berechtigung vorausgesetzt) auf den eigenen PC-Bildschirm genau das holen, was zur Zeit gerade an einem anderen PC-Ar-

beitsplatz auf dem Bildschirm passiert. Diese Technik erleichtert nicht nur die Kooperation zwischen verschiedenen Arbeitsplätzen, sondern auch die heimliche Überwachung durch Vorgesetzte.

Einen Vorgeschmack hierfür geben Programme wie Win-Protocol oder WinWhatWhere, die Echtzeit-Monitoring (monitoring = Beobachtung) erlauben, also einem Kontrolleur jederzeit die aktuellen Bildschirmansichten liefern können oder auch Angaben über geöffnete Dateien, Tastaturanschläge, Mausbewegungen und so weiter (siehe dazu auch CF 12/98 ab Seite 18). Verbunden mit der kommenden biometrischen Zugangskontrolle am Computer und vielleicht noch einer Video-Kamera wird hier lückenlose personenbeziehbare Kontrolle am Bildschirmarbeitsplatz technisch realisierbar. In den USA setzt jedes dritte befragte Unternehmen bereits irgendeine Spionage-Software zur Kontrolle ihrer Arbeitnehmer ein.

Die Vorteile biometrischer Authentifizierung

Die biometrische Identifikation von Personen wird einerseits unter Überwachungs- und Kontrollgesichtspunkten eingesetzt, sie wird gleichzeitig aber auch voran getrieben als Methode zum verbesserten Schutz von Informationen, Schutz von Systemen vor unberechtigtem Zugriff/Zugang und damit als ein wichtiges Element der Datensicherheit. Je nach Zielsetzung lassen sich also biometrie-gestützte Sicherheits-›Architekturen‹ mit einem hohen Maß an Persönlichkeitsschutz entwickeln oder Datensammlungen zur möglichst lückenlosen Personenüberwachung.

Das ist die Kehrseite der (Kontroll-) Medaille: Soll die Informationsgesellschaft funktionieren und soll beispielsweise das elektronische Einkaufen (= eCommerce – siehe dazu CF 8/98 ab Seite 10) perspektivisch eine Rolle spielen, dann werden sichere und einfach zu handhabende Indentifikations-Techniken gebraucht, damit es vertrauenswürdige Kommunikation und authentifizierten (eindeutig einer Person zugeordneten) Geldtransfer geben kann.

Die Nutzung biometrischer Merkmale wäre dabei von erheblichem Vorteil. Passwörter werden vergessen oder an unsicherer Stelle verwahrt und Chip-Karten gehen verloren oder werden gestohlen. Biologische Merkmale hingegen können weder gestohlen noch vergessen werden. Werden mehrere Faktoren miteinander kombiniert, so lassen sich mit Hilfe der Biometrie höchst sichere, einfache und dennoch sogar Anonymität bewahrende (!) Authentifizierungs-Systeme aufbauen.

So kann zum Beispiel der Fingerabdruck (nur) auf einer Chip-Karte gespeichert sein; bei der Benutzer-Authentifizierung wird dann lediglich überprüft, ob der Fingerabdruck des Benutzers mit den auf der Karte gespeicherten Informationen übereinstimmt. Für den Fall der Übereinstimmung wird vom System ein dem Benutzer unbekanntes, zufällig erzeugtes Passwort von der Karte gelesen – bei einem solchen mobilen Authentifizierungssystem muss also nicht auf eine zentrale Identifizierungsdatei zugegriffen werden.

Da heut zu Tage Passwörter allein schon mit im Internet kursierenden Hacker-Tools leicht geknackt werden können, brächte ein auf Biometrie gestütztes System von persönlichen Schlüsseln und Kennungen einen erheblichen Zugewinn an Datensicherheit. Dies betrifft die Zugangsberechtigungen in firmeninternen Netzwerken ebenso wie den Zugriff auf Firmennetze von mobilen Computern und Telearbeitsplätzen aus, die sichere Dateiablage bei sensiblen Daten und anderes mehr. Die wirksame Verschlüsselung sensibler Daten wird dadurch allerdings nicht ersetzt, sondern nur ergänzt.

Das Gesetz zur digitalen Signatur (SigG) – der dritte Artikel des Informations- und Kommunikationsdienstegesetzes – schreibt den Einsatz von biometrischen Verfahren für die sichere Bestätigung einer Identität zwar nicht ausdrücklich vor, aber nach heutigem Wissensstand ist die Biometrie tatsächlich am besten geeignet, zuverlässig automatisch zu bestätigen, dass der ein elektronisches Dokument (z.B. eine Überweisung) ›Unterschreibende‹ tatsächlich der ist, der er zu sein vorgibt. Der biometrischen Authentifizierung sollte deshalb zukünftig bei Kauf, Zeugnis, Testament und anderen rechtsverbindlichen Akten eine wesentliche Rolle zukommen.

Biometrie und Persönlichkeitsrechte

Dies setzt allerdings voraus, dass bei der Einführung biometrischer Verfahren die Persönlichkeitsrechte gewahrt bleiben. Da biometrische Daten sich möglicherweise ein Leben lang nicht verändern werden, verfolgen uns gespeicherte biometrische Erkenntnisse ebenso wie gespeicherte Medizin- oder Gen-Daten.

Nun müssen biometrische Daten nicht unbedingt etwas über die Persönlichkeit enthüllen. Selbst bei Gen-Daten ist der prognostische Wert gespeicherter Informationen umstritten und zum Teil nichtig. Im Hinblick jedoch auf einzelne Krankheiten, auf Veranlagungen und Einzelrisiken ist und bleibt der prognostische Gehalt – etwa für Lebensversicherungen oder Arbeitgeber – durchaus wertvoll.

In gleicher Weise mag sich herausstellen, dass andere biometrische Daten – gespeicherte Körperdaten und Körperreaktionen – im Einzelfall nicht nur Aussagen zur Identität zulassen, sondern auch Aussagen beispielsweise zum Gemütszustand, zur gesundheitlichen Verfassung oder zum Charakter ermöglichen; der ›Lügendetektor‹ spricht hier Bände. Insofern ist also in jedem Fall sicherzustellen, dass die als ›Daten-Krill‹ (so in einer Wissenschaftszeitschrift benannt nach dem frei schwebenden winzigen Plankton der Weltmeere, von deren Massen sich die riesigen Wale ernähren) anfallenden biometrischen Daten ähnlich wie Gen- und Medizindaten einem umfassenden Persönlichkeitsschutz unterworfen werden. Schweigepflicht und Vertraulichkeit des Umgangs muss

in Hinblick auf alle biometrischen Daten verpflichtend werden. Die Verknüpfung mit anderen Daten zu einem nicht autorisierten Zweck muss organisatorisch und technisch ausgeschlossen, Körpermerkmale dürfen nicht zu Personenkennziffern werden. Es muss unmöglich sein, aus zusammengefassten biometrischen Identifkationen auf eine natürliche Person zurückzuschließen. Sicherzustellen ist auch, dass biometrische Daten nicht unbemerkt erhoben und nicht ohne Erfordernis gespeichert werden

Somit bleiben Datenschutz und informationelle Selbstbestimmung wichtige zu schützende Rechtsgüter im Zusammenhang mit biometrischen Datensammlungen. Seit dem 22. 3. 1997 ist spezialgesetzlich denn auch der Einsatz der DNA-Analyse im Strafverfahren rechtlich geregelt. Molekulargenetische Untersuchungen dürfen durchgeführt werden, so weit sie zur Feststellung der Abstammung oder der Tatsache, ob aufgefundenes Spurenmaterial von dem Beschuldigten oder dem Verletzten stammt, erforderlich sind. Die Datei wird nur mit solchen Daten gespeist, die im Zuge von Strafverfahren nach den strengen Vorschriften der Strafprozessordnung erhoben worden sind. Sie stellen sicher, dass nur jener kleine Teil der DNA analysiert werden darf, der allein zur Identifizierung erforderlich ist und der darüber hinaus keinen prognostischen Wert hat. Das Ausgangsmaterial muss nach der Analyse vernichtet werden. Damit ist zugleich die Erstellung von Persönlichkeitsprofilen ausgeschlossen, die für Zwecke der aktuellen Strafverfolgung nicht benötigt werden.

Fazit

Begriffe wie Natural Computing, BioID und andere schöne Namen kaschieren möglicherweise nur einen stärker beobachtenden ›Big Brother‹. Die heute aus Gen-Analyse, Biometrie und digitaler Vernetzung zu gewinnenden Persönlichkeitsdaten sind so aussagekräftig, dass diese Daten ein ›Eigenleben‹ entwickeln könnten. So gilt es, die Frage zu beantworten, wie die Nutzung dieser Daten zu anderen als den ursprünglichen (zugelassenen) Zwecken verhindert werden kann.

Außer für gerichtliche Gen-Analysen fehlen bislang noch spezialgesetzliche Regelungen in Hinblick auf biometrische Datensammlungen im staatlichen Bereich. Gleiches gilt für die biometrischen Datensammlungen im privaten Bereich. Allerdings sind die entsprechenden Vorschriften des Bundesdatenschutzgesetzes zu beachten und die Grundsätze der Datensparsamkeit und des Einsatzes möglichst datenschutzfreundlicher Technologien zu beachten. Bei der betrieblichen Einführung oder dem Einsatz biometrischer Verfahren sind auch die Mitbestimmungsrechte der Betriebs- und Personalräte zu wahren. Betriebs- und Dienstvereinbarungen sollten in diesen Fällen den Persönlichkeitsschutz sicherstellen und könnten dabei gleichzeitig ein Mehr an Datensicherheit für den Betrieb etablieren.

Dr. Manuel Kiper ist Technologie- und Arbeitsschutzberater bei der BTQ Niedersachsen. Kontaktadresse:
BTQ Niedersachsen, Donnerschweer Str. 84, 26123 Oldenburg, Telefon 04 21 / 8 20 68
eMail: **kiper@btq.de**