Oktober 2015
10. Jahrg.
71732
Seite 293-408

ZfWG

Zeitschrift für Wett- und Glücksspielrecht

European Journal of Gambling Law

5

dfv Mediengruppe · Frankfurt am Main

Oktober 2015
10. Jahrg.
Sonderbeilage 3 / 2015
Seite 1 – 32

ZfWG
Zeitschrift für Wett- und Glücksspielrecht

Biometrische Zugangskontrollen Datenschutz – Rechtliche Fragen – Praktische Umsetzung

Tagungsdokumentation

Inhalt

Vorwort

Biometrische Zugangskontrollen

Datenschutz – Rechtliche Fragen – Praktische Umsetzung

I.

Der hiermit einer (noch) breiteren Fachöffentlichkeit vorgelegte Band versammelt die Beiträge der Referenten der Veranstaltung zu biometrischen Zugangskontrollen am 10. September 2015 im Haus der Bundespressekonferenz in Berlin. Insbesondere vor dem Hintergrund der geplanten Datenschutz-Grundverordnung der EU sowie dem zunehmenden Einsatz biometrischer Systeme war es hohe Zeit für eine Bestandsaufnahme zu den vielfältigen Fragen, die biometrische Zugangskontrollen an die Rechtswissenschaft und -praxis, aber auch und gerade an die Experten aus Wirtschaft und Technologie stellen. Um das Spannungsverhältnis zwischen der steigenden Attraktivität biometrischer Systeme und den erheblichen Vorbehalten gegenüber derartigen Technologien abzubilden, war es Ansatz und Ziel der Tagung, die rechtlichen und die technischen Fragenstellungen durch Vertreter aus Praxis, Wissenschaft und Politik im Zusammenhang erörtern zu lassen.

Während Ausgangspunkt der Debatte hinsichtlich biometrischer Systeme historisch der Einsatz dieser Verfahren durch Hoheitsträger ist, sollte im Verlauf der Veranstaltung gerade auch die Verwendung im Privatsektor beleuchtet werden. Dennoch waren Veranstalter und Organisatoren außerordentlich auf Grund der umfangreichen Erfahrungswissens der öffentlichen Hand im Umgang mit biometrischen Zugangskontrollen und einer möglichen Orientierung der Privatwirtschaft an eben diesen Erfahrungswerten außerordentlich dankbar, dass sich der zuständige Abteilungsleiter im Bundesministerium des Innern, Herr Martin Schallbruch, bereitfand, eine politische Keynote an die Anwesenden zu richten. Herr Schallbruch stellte insbesondere die Akzeptanz in der Bevölkerung gegenüber biometrischen Verfahren heraus, die sich aus deren Zuverlässigkeit und Sicherheit ergibt. Auf Grund dieser steigenden Akzeptanz würden auch die Anwendungsfelder im hoheitlichen Bereich, wie die automatisierte Grenzkontrolle EasyPass, weiterhin ausgebaut.

II.

Das Thema der Veranstaltung und des vorliegenden Bandes ist in jeder Hinsicht anspruchsvoll und verlangt nach begrifflichen Vorklärungen, die indes weder auf einen statischen Befund zurückgreifen noch unangreifbar sind: Vom Begriff der biometrischen Daten sollen alle Daten zu physischen, physiologischen und verhaltenstypischen Merkmalen eines Menschen erfasst sein, welche die eindeutige Identifizierung einer Person ermöglichen. Biometrische Erkennung durch ein biometrisches System verfolgt das Ziel, eine mittels automatisierter Messung durch ein spezifisches Merkmal bestimmte Person von anderen unterscheidbar zu machen. Der Vorteil biometrischer Verfahren gegenüber anderen Authentisierungsmöglichkeiten ergibt sich aus der mangelnden Übertragbarkeit biometrischer Daten.[1] Unterschieden werden biometrische Verfahren, die mit physiologischen Merkmalen arbeiten, und solche, die verhaltensbezogene Merkmale verwenden. Verfahren, die mit physiologischen Merkmalen arbeiten, beruhen in der Regel auf der Verwendung passiver Merkmale, die mit dem Gesicht, der Iris, dem Finger oder der Hand im Zusammenhang stehen. Verhaltensbezogene Merkmale beruhen dagegen grundsätzlich auf einem aktiven Tun wie der Unterschrift, dem Einsatz der Stimme oder dem Anschlagsrhythmus an einer Tastatur.[2]

Dabei ist Grundprinzip der biometrischen Erkennung bei allen Systemen gleich. Alle biometrischen Systeme enthalten unabhängig von ihrem oft sehr individuellen technologischen Aufbau die Komponenten der Personalisierung oder Registrierung des Nutzers im System (Enrolment), die Erfassung der biometrisch relevanten Eigenschaften einer Person und die Erstellung von Datensätzen (Templates) sowie den Vergleich der aktuell präsentierten mit den zuvor abgespeicherten Daten (Matching). Die Erfassung biometrischer Merkmale erfolgt sowohl bei der erstmaligen Erfassung zur Erstellung des sog. Referenzdatensatzes als auch bei der späteren Erfassung zur Wiedererkennung durch Sensoren wie Kamera, Mikrofon, Tastatur, Druckpads, Geruchssensoren oder Fingerabdrucksensoren.[3]

Biometrische Systeme können als Verifikationssysteme oder als Identifikationssysteme ausgelegt sein. Bei einem Verifikationssystem gibt der Nutzer eine Identität vor, zu der im System eine Referenz vorliegt. Sofern biometrische Systeme mit einem authentischen Dokument kombiniert werden, kann die biometrische Referenz (z. B. Passfoto) auf diesem Dokument abgelegt sein. Zum Zeitpunkt der Verifikation wird ein Vergleich mit genau diesem einen Referenzbild durchgeführt (1:1 Vergleich). Bei einem Identifikationssystem hingegen wird das erfasste Bild mit vielen

1 „Grundsätzliche Funktionsweise biometrischer Verfahren“, zuletzt abgerufen unter: https://www.bsi.bund.de/cln_174/DE/Themen/Biometrie/AllgemeineEinfuehrung/allgemeineeinfuehrung_node.html am 4.9.2015.

2 Ebenda.

3 „Grundsätzliche Funktionsweise biometrischer Verfahren“, zuletzt abgerufen unter: https://www.bsi.bund.de/cln_174/DE/Themen/Biometrie/AllgemeineEinfuehrung/allgemeineeinfuehrung_node.html am 4.9.2015.

eingelernten Bildern verglichen und aus dieser Menge das am besten passende Muster ermittelt (1:n Vergleich).[4]

III.

Im Kontext dieser Zunahme an Einsatzfeldern im öffentlichen und privaten Bereich befasste sich der erste Themenkomplex der Veranstaltung mit den verfassungsrechtlichen wie einfachgesetzlichen Rahmenbedingungen biometrischer Zugangskontrollen.

Prof. Dr. Gerrit Hornung, Lehrstuhlinhaber für Öffentliches Recht, IT-Recht und Rechtsinformatik an der Universität Passau, konstatierte in diesem Zusammenhang, dass viele gesetzliche Grundlagen zur Personenidentifizierung die Nutzung biometrischer Daten nicht oder zumindest nicht hinreichend spezifisch regeln. Auch sei nicht klar, wie im Rahmen der EU-Datenschutz-Grundverordnung die Begrifflichkeit der biometrischen Daten definiert werden wird. Angesichts der wachsenden Bedeutung dieser Daten und des Gebots der Normenbestimmtheit bedürfe es zwingend einer trennscharfen Definition. Insbesondere im Hinblick auf die Frage, ob biometrische Daten den Gesundheitsdaten zuzuordnen sind und damit erhöhte Anforderungen für die Zulässigkeit einer Datenverarbeitung gelten, sei eine Klärung wünschenswert.

An diese grundsätzlichen Erwägungen anschließend stellte Dr. Vera Jungkind, Rechtsanwältin und Partnerin bei Hengeler Mueller, die datenschutzrechtlichen Voraussetzungen bei der Erhebung und Verarbeitung biometrischer Daten dar. Sie zeigte auf, dass biometrische Gesichtserkennungsverfahren wegen ihrer Zuverlässigkeit speziell zum Schutz gesperrter Spieler am Referenzbeispiel von Spielhallen dort praktisch in Betracht kommen. Dieses Beispiel veranschauliche allerdings auch, dass sich die Interessen der Praxis und die datenschutzrechtlichen Anforderungen häufig konträr gegenüber stehen. Einerseits werde durch biometrische Erkennungsverfahren ein hohes Maß an Zuverlässigkeit geschaffen, ohne zugleich ein Zugangshemmnis für die nicht gesperrten Spieler herbeizuführen, indem eine individuelle Ausweiskontrolle jedes Besuchers vermieden wird. Andererseits bedürfe es hierzu einer pauschalen Erhebung und Verarbeitung der biometrischen Gesichtsdaten jeglicher Spielhallenbesucher, um diese mit den Daten der gesperrten Spieler abzugleichen. In einem datenschutzrechtlich sensibilisierten Rechtsraum wie Deutschland gestalte sich die Rechtfertigung einer solchen generellen Datenerhebung schon traditionell als schwierig. Dennoch rechtfertigten die Interessen der Spielhallenbetreiber – insbesondere das wirtschaftliche Interesse an einem möglichst geringen Zugangshemmnis für die nicht gesperrten Spieler – im Ergebnis wohl die pauschale Datenerhebung, sofern die Daten nur für den Abgleich mit der Sperrdatei erhoben werden und keine dauerhafte Speicherung erfolgt.

IV.

Im Zentrum des zweiten Themenkomplexes der Veranstaltung standen die technischen Möglichkeiten biometrischer Systeme. Passend hierzu hatte Herr Schallbruch bereits in seiner Keynote den internationalen Erfolg deutscher Technologien im Hinblick auf biometrische Verfahren herausgestellt.

Dr. Michael Schneider, Senior Director Marketing Strategy & Operations der Bundesdruckerei GmbH, machte deutlich, dass das Portfolio der Bundesdruckerei GmbH weit über die Herstellung (klassischer) biometrischer Ausweise hinausgeht. Von besonderer Relevanz in diesem Zusammenhang ist das auf der CEBIT 2015 erstmals vorgestellte Modell, bei dem die biometrischen Daten dezentral auf dem Kartenchip selbst gespeichert werden. Anhand dieser sog. „Match-on-Card"-Verfahren zeigt sich das Zusammenspiel der technischen Ausgestaltung und datenschutzrechtlichen Vorgaben. So findet hier der für biometrische Systeme typische Abgleichs- und Identifizierungsvorgang allein auf der Karte selbst statt. Mittels dezentraler Speicherungsmöglichkeiten dieser Art kann Vorbehalten wegen etwaiger Missbrauchsrisiken wirksam begegnet und gleichzeitig der Grundsatz der Datensparsamkeit gewahrt werden.

Als Vertreter der Privatwirtschaft hat Dr. Jürgen Pampus, Vice President Sales & Marketing der Cognitec Systems GmbH, in technischer Hinsicht auf das Anwendungsbeispiel von Frau Dr. Jungkind Bezug genommen und über seine Praxiserfahrungen im Umgang mit anonymen Gesichtserkennungsverfahren referiert. Die Cognitec Systems GmbH hat für ein Pilotprojekt der Merkur Spielothek bereits eine Technologie entwickelt, die anstelle der manuellen Ausweiskontrolle mit einer automatischen Gesichtserkennungssoftware arbeitet. Sie liest die biometrischen Gesichtsdaten der Spielhallenbesucher aus und gleicht diese mit den Fotos der Sperrliste abgleicht (sog. „face in the crowd"). Im Hinblick auf die datenschutzrechtliche Zulässigkeit ist es bei diesem System insbesondere von Bedeutung, dass die Technologie für den Abgleich nicht mit den biometrischen Rohdaten arbeitet, sondern diese für den Abgleich auf sog. „Templates" reduziert, wodurch ein unzulässiger Erkenntnisgewinn aus den Überschussinformationen der Rohdaten schon technisch ausgeschlossen ist.

Besonders wertvoll waren schließlich auch die Erläuterungen von Dr. Waldemar Grudzien, Direktor des Bundesverbandes deutscher Banken e. V., die deutlich machten, dass biometrische Erkennungsverfahren nicht nur zur Sicherung von Räumen oder Grenzbereichen Anwendung finden können. Vielmehr böten sich – wenn auch bisher noch kaum praktiziert – biometrische Verfahren ebenfalls zur Identitätsverifizierung bei Zahlungsvorgängen an. Einer rasanteren Entwicklung in diesem Bereich steht aktuell wohl noch die hohe Verbreitung PIN- und TAN-gebundener Zahlungssysteme entgegen. Dennoch lassen bestimmte Indikatoren den Schluss zu, dass zukünftig auch in Deutschland im Bereich des „Private Bankings" der Einsatz von biometrischen Systemen zunehmen wird. Vorboten einer derartigen Entwicklung seien Apps wie „Apple Pay". Mittels dieser Anwendung können Nutzer sich bereits seit 2014 mit ihrem Fingerabdruck auf dem Apple-Smartphone legitimieren und so Zahlungsaufträge erteilen.

Zum Abschluss der Veranstaltung stellte Thomas Walloschke, Principal Business Development Manager der Fujitsu Technology Solutions GmbH, mit dem Handvenenscanner einen technisch äußerst innovativen Ansatz der biometrischen Erkennung vor. Im Rahmen dieses Verfahrens wird die Struktur des Venenmusters innerhalb der menschlichen Handfläche mit Hilfe eines Nahinfrarotstrahls, der das zum Herzen zurückfließende Blut absorbiert, erfasst. Da auf diese Weise gleichzeitig ein Lebendtest integriert wird, bietet sich die Technologie wegen der geringen Gefahr der Umgehung an, um besonders sensible Bereiche zu sichern. In

4 *Busch*, in: Busch/Heibey/Quiring-Kock/Kniess/Herzog, Biometrische Authentisierung, 2. Auflage 2010, S. 5.

Deutschland wird der Handvenenscanner beispielsweise zur Zutrittskontrolle für autorisiertes Personal an Flughäfen genutzt. In Ländern mit einer geringeren Sensibilität für datenverarbeitende Anwendungen, wie z. B. in Brasilien oder der Türkei, werde diese Technologie bereits zur Verifizierung an Geldautomaten oder gar zur Zeiterfassung von Arbeitnehmern im Betrieb genutzt.

V.

Der bisherige Diskurs zu biometrischen Daten und Verfahren, dessen Bestandsaufnahme der vorliegende Band dient, zeigt ein vielschichtiges Bild. Die zahlreichen Facetten der Materie müssen auch in Zukunft weiter in rechtlicher und technischer Hinsicht erschlossen werden. Auszutarieren sind dabei die stets die Interessen an Sicherheit und informationeller Selbstbestimmung. Bei der Gewichtung dieser Aspekte spielt stets auch die Provenienz der Protagonisten eine entscheidende Rolle, ansonsten ließe sich der unterschiedliche Verbreitungsgrad biometrischer Technologien in den verschiedenen Jurisdiktionen und Märkten kaum hinreichend erklären.

RA Dr. Dirk Uwer, LL.M., Düsseldorf

Beiträge

Martin Schallbruch, Berlin*

Keynote für die Veranstaltung „Biometrische Zugangskontrollen“

Datenschutz – Rechtliche Fragen – Praktische Umsetzung

I. Einführung

Als wir im Jahr 2005 den biometrischen Reisepass in Deutschland eingeführt haben, waren der Widerstand gegen den Einsatz und die Kritik an der Biometrie groß. Ob die biometrische Technik generell überhaupt Vorteile bei der Identifizierung besitzt, war heftig umstritten. Die Biometrie würde von den Bürgerinnen und Bürgern nicht angenommen werden; sie würden an der Nutzung biometrischer Systeme scheitern, weil diese Systeme zu kompliziert seien. Identifizierungen anhand von biometrischen Daten dauere zu lange, die Abfertigungen und Kontrollen an Flughäfen würden verzögert, anstatt vereinfacht zu werden. Zugespitzt formuliert: die Biometrie sei ein Irrweg. Sie werde sich nicht durchsetzen können und über kurz oder lang wieder verschwinden.

Und wie stellt sich die Situation heute dar? Biometrische Identifizierungs- und Sicherungssysteme sind in unserem Alltag präsenter denn je. Unsere Bürgerinnen und Bürger nutzen den biometrischen Pass ganz selbstverständlich. Wir haben mit EasyPASS bei unserer Grenzkontrolle eine biometrie- und kryptografiebasierte Identitätsverifikation installiert, die von den Bürgerinnen und Bürger angenommen und genutzt wird. Biometriebasierte Identifizierungssysteme arbeiten heute sehr schnell, sind zuverlässig und beschleunigen dadurch die Identifizierungsprozesse.

Im privaten Bereich nutzen Menschen -insbesondere in der jüngeren Generation- ganz selbstverständlich ihre Fingerabdrücke oder ihren Iris-Scan zur Entsperrung Ihrer Smartphones, Tablets und Computer. Die ersten Smartphones, die eine Identifizierung und Autorisierung per Fingerabdruck ermöglichten, kamen in Deutschland übrigens erst im Oktober 2013 heraus. Nicht mal ein Jahr später können Sie diese Smartphones bereits bei zwei Banken dazu nutzen, mit Ihrem Fingerabdruck online Ihr Konto einzusehen und Überweisungen zu tätigen. Offenbar sind unsere Bürgerinnen und Bürger doch technikoffener und lernfähiger als mancher Kritiker im Jahr 2005 glaubte. Die Akzeptanz der Biometrie ist nämlich groß in Deutschland:

Im August 2014 konnte sich laut einer repräsentativen Umfrage des Bitkom jeder zweite Bundesbürger ab 14 Jahren vorstellen, bargeldlose Zahlungen und Transaktionen mit ihren biometrischen Daten abzusichern.

Außerdem sprachen sie sich dafür aus, sensible Daten mit Hilfe der Biometrie zu verschlüsseln. Beeindruckt hat mich insbesondere, dass vor allem auch ältere Verbraucher sich für eine solche Nutzung von Fingerabdrücken und Iris-Scans aussprachen. Auch die Industrie und Wirtschaft hat das Marktpotenzial der Biometrie erkannt:

- Etabliert sind heute z. B. der Abgleich der Unterschriftsdynamik, der Abgleich von Fingerabdrücken, Gesicht und Stimme oder auch die Handvenenerkennung, also der Abgleich eines Venenmusters einer Hand und mit einem gespeicherten Referenzmuster.
- Künftig möchte z. B. Google smarte Kontaktlinsen mit einem Lichtsensor ausstatten, der die Iris des Kontaktlinsenträgers scannt. Dieser Scan soll dann mit dem hinterlegten Iris-Scan der Person abgeglichen werden.
- Yahoo z. B. arbeitet an sogenannten Bodyprints. Hierbei wird Software entwickelt, die ganz normale Touchscreens von Smartphones in einen Scanner verwandeln kann, mit der Körperteile (z. B. das Ohr beim Telefonieren) gescannt und mit einem gespeicherten Referentmuster verglichen wird
- Ein anderer Hersteller will das kontaktlose Bezahlen per Herzschlag authentifizieren und dazu ein Armband ein-

* Auf Seite 32 erfahren Sie mehr über den Autor.

setzen, das seinem Träger heute bereits die biometrische Anmeldung an den technischen Geräten des Kunden ermöglicht.

Allein im Biometrie-Markt im Bereich der Mobilfunkgeräte gehen Schätzungen davon aus, dass im Jahr 2017 weltweit 9,1 Milliarden US-Dollar erzielt werden können; für 2020 rechnen die Fachleute mit 33,3 Milliarden US-Dollar Umsatz.

Erlauben Sie mir noch einen Hinweis: Deutsche Unternehmen, welche im Bereich der Biometrie tätig sind, verteidigen ihre Spitzenposition in dem dynamischen Markt sehr gut und vertreiben Ihre Produkte weltweit.

II. Der staatliche Einsatz der Biometrie

Es gibt hohes Bedürfnis nach sicherer Identifizierung sowohl im staatlichen als auch im privaten Bereich. Auf den privaten Bereich werde ich nachher eingehen, zunächst möchte ich Ihre Aufmerksamkeit auf den Einsatz und die Nutzung der Biometrie in staatlichen Identitätsdokumenten lenken.

Nach den verheerenden Anschlägen des 11. September 2001 setzte sich die Einführung biometrischer Pässe durch. Heute werden in allen 28 EU-Staaten biometrische Reisepässe an die insgesamt rund 500 Millionen Einwohner ausgegeben.

In Deutschland haben wir den elektronischen Reisepass bereits 2005 eingeführt. Zunächst nur mit gespeichertem Lichtbild; seit 2007 werden zusätzlich zwei Fingerabdrücke gespeichert. Auf diese gespeicherten biometrischen Daten haben ausschließlich hoheitlichen Stellen Zugriff. Diese Behörden (z. B. Polizeien des Bundes und der Länder) dürfen auf die Daten lediglich zugreifen, um die Echtheit des Personalausweises oder die Identität des Inhabers zu überprüfen. Die so erhobenen Daten sind unverzüglich zu löschen, wenn die Prüfung der Echtheit des Personalausweises oder der Identität des Inhabers beendet ist (§ 16a PaßG).

Wir haben aus Gründen des Datenschutzes keine zentrale Fingeradruck-Datenbank. Die in den Passbehörden bei Beantragung erhobenen Fingerabdrücke sind spätestens nach Aushändigung des Passes an die Bürgerinnen und Bürger zu löschen (§ 16 PaßG). Auch der Passproduzent, die Bundesdruckerei, hat sämtliche zur Produktion benötigten personenbezogenen und selbstverständlich erst recht die biometrischen Daten mit Abschluss der Herstellung des jeweiligen Passes zu löschen (§ 16 PaßG).

Bei der Datenerfassung, -prüfung und -übermittlung der personenbezogenen und biometrischen Daten stellen wir sicher, dass stets neuste Technik zur Sicherstellung des Datenschutz und der Datensicherheit genutzt wird. Denn die Vertraulichkeit und Unversehrtheit der Daten sowie die Feststellbarkeit der übermittelnden Stelle müssen wir gewährleisten.

Jährlich reisen immer mehr Menschen beruflich oder privat über Landesgrenzen mit Ihren biometrischen Reisedokumenten hinweg. Diesen steten Aufwuchs müssen wir bei den Grenzkontrollen effizient bewältigen.

Automatisierte Grenzkontrollen müssen daher drei Anforderungen erfüllen: sie müssen

- rasch,
- reibungslos und
- sicher erfolgen.

In Deutschland haben wir dafür das System EasyPASS entwickelt. Heute können Sie an den Flughäfen Frankfurt am Main, Düsseldorf, Köln/Bonn, Hamburg, Berlin und München 122 EasyPASS-Kontrollspuren zur automatisierten Grenzkontrolle nutzen, so genannte eGates. In München sind 18 weitere Kontrollspuren für die Erweiterung des Terminals 2 vorgesehen, die im April 2016 eröffnet werden soll. Die biometrie- und kryptografiebasierte Identitätsverifikation überprüft die Identität der Reisenden auf Grundlage des gespeicherten Gesichtsbildes. Auch Gültigkeit und Echtheit des elektronischen Reisedokuments werden überprüft.

EasyPASS können volljährige Staatsangehörige der Mitgliedstaaten der EU, der Europäische Wirtschaftsgemeinschaft und der Schweiz nutzen, die im Besitz eines elektronischen Reisepasses sind. Dabei wird das Reisedokument vom Reisenden auf ein Lesegerät gelegt. Der Reisende betritt eine Schleuse, in der eine Kamera sein Gesicht mit dem im Chip gespeicherten Lichtbild vergleicht. Sofern die Identitätsfeststellung erfolgreich war und keine polizeilich relevanten Erkenntnisse zur Person vorliegen, öffnet sich der Ausgang der Schleuse. Die Grenzkontrolle ist vollzogen.

Die automatisierte Grenzkontrolle ist sehr sicher und einfach zu handhaben. Das System hat mindestens drei Vorteile:

- Die Reisenden können die Grenze schneller passieren,
- die Schalter für manuelle Kontrollen werden entlastet,
- dadurch verringern sich auch hier die Wartezeiten für die Reisenden.

Wesentlich ist, dass bei der Verwendung von EasyPASS keine personenbezogenen Daten gespeichert werden, auch keine biometrischen Daten. Eine Speicherung der Daten erfolgt nur im Rahmen des EasyPASS-Registered Travelers Programs für volljährige Reisende aus Drittstaaten, mit denen eine Gegenseitigkeitserklärung zur Nutzung automatisierter Grenzkontrollverfahren besteht. Solche bilateralen Kooperationen wurden mit den Vereinigten Staaten von Amerika und der Sonderverwaltungszone Hongkong der Volksrepublik China (visumsfrei) geschlossen. Reisende aus diesen Staaten können sich für das Programm registrieren und – sofern die Bundespolizei bei Überprüfung ihrer Daten keine Sicherheitsrisiken sieht – können sie die kostenfreie automatisierte Grenzkontrolle mit ihrem elektronischen Reisepass nutzen. Nur bei EasyPASS-RTP werden also die persönlichen Daten jener Reisenden, die sich freiwillig für das Programm registrieren lassen, in der EasyPASS-RTP-Datenbank der Bundespolizei gespeichert.

EasyPASS ist eine deutsche Entwicklung, ebenso wie der elektronische Reisepass und der 2010 eingeführte Personalausweis mit Online-Ausweisfunktion. In beiden Ausweisdokumenten wird eine Sicherheitstechnologie verwendet, die international ein hohes Ansehen genießt. Ihre Fälschungssicherheit wird weltweit anerkannt.

Biometrische Verfahren müssen auf sehr hohem Niveau vor Fälschung und Missbrauch zuverlässig geschützt werden. Unter anderem aus diesem Grund führt das BSI seit einigen Jahren Projekte zu den technischen Aspekten biometrischer Verfahren durch, wie zum Beispiel BioFinger und BioFace.

Daneben untersuchen wir auch in Feldstudien biometrische Verfahren auf ihre Praxistauglichkeit in konkreten Anwendungen, so zum Beispiel die Verfahren der Fingerabdruck-, Gesichts- und Iriserkennung in Verbindung mit Personaldokumenten.

III. Einsatz der Biometrie im privaten Bereich

Auch im privatwirtschaftlichen Bereich ist der Bedarf nach sicherer Identifizierung hoch. In den verschiedensten Branchen werden bereits biometrische Verfahren verwendet.

- Die biometrische Zugangskontrolle zu Gebäuden, besonders gesicherter Räumen bzw. Bereichen oder Systemen ist bereits Realität.
- Banken nutzen, wie eingangs gesagt, vermehrt Biometrie für den Online-Zugang zu Konten und die Autorisierung von Transaktionen.
- Nach § 8 des Glücksspielstaatsvertrags sind Spielbanken und Veranstalter von Sportwetten und Lotterien mit besonderem Gefährdungspotential verpflichtet, gesperrte Spieler am Spiel zu hindern. Hierzu wurde ein übergreifendes Sperrsystem, in welches Eigen- und Fremdsperren eingetragen werden, geschaffen. Das Casino in Bad Homburg setzt zur Erfüllung der Verpflichtung seit 2004 ein Gesichtserkennungssystem im Automatensaal ein, mit dessen Hilfe Personen, die sich einer freiwilligen Selbstsperre unterzogen haben, das Spielen zu untersagen.

Unabhängig von ihrem Einsatzgebiet sind biometrische Systeme technisch stets höchstkomplex, aufgrund der Sensibilität der biometrischen Daten sind besonders hohe Sicherheitsanforderungen an sie zu stellen, ihre Implementierung und ihr Betrieb sind mit hohen Kosten verbunden. Zahlreiche technische, rechtliche und datenschutzrechtliche Vorgaben sind zu klären und zu beachten. Letzteres ist Gegenstand der beiden folgenden Beiträge.

Deshalb möchte ich an dieser Stelle nur ein paar Fragen in den Raum stellen:

- Wie stellt man sicher, dass keine Rohdaten, sondern nur reduzierte Referenzdaten (Templates) verwendet werden?
- Wie kann man den Anfall von Überschussinformationen (z. B. Informationen über den Zutritt) ausschließen?
- Welche Verfahren, die eine unbemerkte Erfassung der biometrischen Daten ausschließen, müssen verwendet werden?
- Welche rechtlichen Probleme ergeben sich bei einer zentralen Speicherung der biometrischen Daten?
- Wie kann man eine dezentrale Speicherung der Templates erreichen? Ist es notwendig, dass das Medium,
- auf welchem die Templates gespeichert sind, in der alleinigen Verfügungsgewalt des Nutzers (z. B. Chipkarte) liegt?
- Welche Art Verschlüsselung oder sonstige Sicherung muss zum Schutz der biometrischen Daten eingesetzt werden?

IV. Identitätsnachweis per eID-Funktion

Ich frage mich allerdings auch, ob die private Wirtschaft nicht anstelle von biometrischen Verfahren den elektronischen Identitätsnachweis nutzen könnte. Schließlich haben hier staatliche Stellen die personenbezogenen Daten erhoben und garantieren damit quasi den Identitätsnachweis und die Richtigkeit der Daten. Mit der Online-Ausweisfunktion des Personalausweises haben wir 2010 eine vertrauenswürdige staatliche Sicherheitsinfrastruktur geschaffen.

Mittlerweile besitzen über 40 Millionen Menschen in Deutschland eine eID-fähige Ausweiskarte: über 36 Millionen Personalausweise und über 4 Millionen Aufenthaltstitel im Scheckkartenformat wurden bereits ausgegeben. Die eID-Funktion wurde eingeführt, damit die Bürger sich im Internet oder an Automaten einfach und sicher ausweisen können. Auf dem Sicherheitsgewinn lag unser Hauptaugenmerk. Aber für die Anbieter von eID-Diensten und deren Nutzer hat die eID-Funktion weitere Vorteile: sie spart Zeit und beschleunigt durch die automatisierte Übernahme von persönlichen Daten aus den Melderegistern die Prozesse.

In Anwendungsgebieten, in denen biometrische Verfahren verwendet werden, könnte meines Erachtens auch die eID-Funktion eine interessante Alternative sein. Ein Beispiel ist die Zutrittskontrolle, mit der bestimmte Personen Zutritt zu Gebäuden oder technischen Infrastrukturen erhalten.

In der Praxis heißt das:

- Autorisierte Personen registrieren sich mit Hilfe des Personalausweises und ihrer PIN an zugangsbeschränkten Bereichen oder Infrastrukturen mit ihrem Namen und Geburtsdatum.
- Auch das dienste- und kartenspezifische Kennzeichen (der pseudonyme Zugang) des Personalausweises kann für die Registrierung und die Wiederanmeldung genutzt werden. So kann eine personengebundene Zuordnung auch ohne die Übermittlung persönlicher Daten gewährleistet werden.
- Genutzt wird die staatliche Infrastruktur, es werden weder weitere Smartcards benötigt, noch Benutzernamen und Passwörter.

Wir sind davon überzeugt, dass wir mit dem Online-Ausweis ein zukunftsfähiges Sicherheitselement für den elektronischen Identitätsnachweis geschaffen haben, das wichtige Mehrwerte für alle Nutzer bietet.

Gleichwohl sehen wir auch Optimierungsbedarfe. Deshalb hat das Bundesinnenministerium eine neue Software für den Online-Ausweis bereitgestellt, die deutlich schneller, schlanker und einfacher funktioniert. Wir unterstützen zudem die Entwicklung von Massenverfahren, denn hier sorgt die eID-Funktion für besonders hohe Effizienzsteigerungen.

Drei Beispiele möchte ich nennen:

- Das Bundesamt für Justiz hat 2014 die Online-Bestellung von Führungszeugnissen ermöglicht.
- Im Bundesverkehrsministerium wird das Projekt i-Kfz umgesetzt, die internetbasierte Kfz-An-, Um- und Abmeldung mit eID-Funktion. Die Online-Außerbetriebsetzung ist seit 1.1.2015 möglich. Nach Planungen des BMVI sollen 2016 die Wiederzulassung online angemeldeter Kfz und danach die Zulassung von Kfz realisiert sein.
- Als letztes Beispiel möchte ich Ihnen das BAföG-Rückzahlungsverfahren des Bundesverwaltungsamtes nennen, das dieser Tage live geschaltet wird.

Sicher sind wir bei der Etablierung der eID-Funktion noch nicht auf der „Zielgraden“, aber wir arbeiten daran.

V. Großer Bedarf an vertrauenswürdigen Identitätsnachweisen

Die Suche nach sicheren Identitäten bzw. vertrauenswürdigen Identitätsnachweisen beschäftigt uns alle.

Das zeigt das Programm der Veranstaltung deutlich.

Prof. Dr. Gerrit Hornung, LL.M., Kassel*

Chancen und Risiken der Biometrie aus rechtlicher Sicht

Grundlagen und aktuelle Herausforderungen

Nachdem biometrische Verfahren über viele Jahre eher Nischenanwendungen waren, existiert nunmehr eine Vielzahl von Systemen und Verfahren, die in immer mehr Lebensbereichen Verwendung finden. Diese Entwicklung hat auch in der Rechtswissenschaft und der Rechtsanwendung zu vielen Diskussionen gerade im Bereich des Datenschutzrechts geführt. Aus rechtlicher Perspektive ist die Biometrie freilich ambivalent und offenbart sowohl Chancen als auch Risiken. Der Beitrag wirft einen grundsätzlichen Blick auf die Biometrie und erörtert ausgewählte rechtliche Probleme.

I. Grundlagen

Biometrie lässt sich verstehen als die automatisierte oder teilautomatisierte Erkennung von Menschen anhand hochcharakteristischer, physiologischer oder verhaltenstypischer Merkmale.[1] Gegenüber der „natürlichen" Gesichts- und Stimmerkennung – Menschen haben irgendwann im Laufe der Evolution gelernt, sich gegenseitig anhand derartiger Merkmale zu erkennen – ist die Automatisierung das entscheidende Kriterium. Diese begann bei der Erkennung der Fingertopographie[2] und setzte sich nach und nach bei anderen biometrischen Charakteristika[3] durch. Inzwischen existiert eine große Bandbreite von Eigenschaften des menschlichen Körpers, die entsprechend verwendet werden können. Neben Finger-, Hand- und Gesichtstopographie sind dies z. B. die Struktur der Iris oder der Handvenen, das Muster der Netzhaut, die Dynamik der Unterschrift oder des Gangs, die Besonderheiten des Tippverhaltens oder der menschlichen Stimme, sowie je nach Definition die Molekülstruktur der menschlichen DNA.[4]

1. Technischer Ablauf

Auf der Ebene der technischen Sensoren unterscheiden sich diese Verfahren erheblich. Demgegenüber ist aus rechtlicher Perspektive die gemeinsame Struktur wichtiger.[5] Auf der ersten Stufe (Enrolment) wird eine biometrische Referenz erstellt und gespeichert. Diese Speicherung kann in unterschiedlicher Form erfolgen. Eine wesentliche Unterscheidung ist die zwischen einer zentralen Datenbank und der dezentralen Speicherung beispielsweise auf einer Chipkarte. Eine weitere Frage ist die nach dem Inhalt der biometrischen Referenz. Je nach System kann es sich dabei um ein biometrisches Sample (vollständige Repräsentation des biometrischen Charakteristikums, etwa ein Gesichtsfoto), ein biometrisches Template (eine bestimmte Menge markanter Kennzeichen aus dem Sample, z. B. die Endungen und Verzweigungen der Papillarleisten des Fingers) oder schließlich ein aus diesen Daten abgeleiteter Datensatz sein, der als solcher grundsätzlich keine biometrischen Daten mehr enthält.

Die eigentliche Erkennung findet im Rahmen des Matchings (Vergleich) statt. Dabei werden zunächst neue Vergleichsdaten erhoben. Die biometrische Erkennung bietet sodann zwei grundlegende Funktionsweisen: Identifikation und Verifikation.[6] Bei der Identifikation werden die Vergleichsdaten mit allen in einer Datenbank hinterlegten Datensätzen abgeglichen (1:n-Vergleich). Demgegenüber beschränkt sich die biometrische Verifikation auf einen Abgleich mit nur einer biometrischen Referenz (1:1-Vergleich), die durch den Betroffenen präsentiert wird (wie etwa beim Reisepass) oder ihm sonst zugeordnet ist. Die „biometrische Behauptung" beschränkt sich bei der Verifikation also auf eine konkrete Identität. Kann diese nicht bestätigt werden, bleibt die Identität offen oder muss anderweitig ermittelt werden.

Beim Matching wird praktisch niemals eine vollständige Übereinstimmung oder Nicht-Übereinstimmung festgestellt. Biometrische Systeme ergeben also keine eindeutige Entscheidung, wie beispielsweise bei der Eingabe eines Passworts. Fehler können auf unterschiedlichen Ebenen auftreten (Verschmutzung des Sensors, unterschiedliches Mitwirkungsverhalten der Betroffenen, Probleme der Implementierung oder der Genauigkeit der verwendeten Algorithmen).[7] Dementsprechend kommen biometrische Falsch-Akzeptanzen und Falsch-Rückweisungen vor und werden mit der Falschübereinstimmungs-Rate (FMR) und Falschnichtübereinstimmungs-Rate (FNMR) gemessen. Diese sind abhängig von dem Grad an Übereinstimmung, der für eine Akzeptanz verlangt wird (Schwellwert). Sie können deshalb je nach Anwendungssituation (Hochsicherheits- oder Convenience-Anwendung) gesteuert werden. Eine ungenügende Ausprägung der biometrischen Charakteristika kann die biometrische Erkennung unter Umständen auch ganz vereiteln. Die Failure to Enroll Rate (FTE) beschreibt den Anteil fehlgeschlagener Enrolmentversuche.

2. Anwendungsfälle

Aus rechtlicher Perspektive lassen sich biometrische Systeme prinzipiell überall dort verwenden, wo es im Rechts- und Geschäftsverkehr auf die Identität oder bestimmte Eigenschaften oder Berechtigungen einer Person ankommt.

Aus Unternehmenssicht lässt sich beispielsweise zwischen der Identifizierung von Kunden, Mitarbeitern und Dritten

* Der Text ist im Zusammenhang mit dem BMBF-Projekt „Multi-Biometriebasierte Forensische Personensuche in Lichtbild und Videomassendaten (MisPel)", FKZ 13N12064, entstanden. Auf Seite 32 erfahren Sie mehr über den Autor.

1 *Hornung*, Die digitale Identität, 2005, 75 m. w. N.; aus der technischen Literatur z. B. *Jain/Ross/Nandakumar*, Introduction to Biometrics, 2011, 2.

2 Das FBI begann Anfang der 1970er Jahre mit dem Aufbau automatisierter Systeme (AFIS), s. *Jain/Ross/Nandakumar* (Fn. 1), 93.

3 Die Terminologie ist inzwischen durch das Harmonized Biometric Vocabulary standardisiert (ISO/IEC 2382-37, s. http://www.christoph-busch.de/standards.html).

4 Zu den verschiedenen Charakteristika und Verfahren z. B. *Jain/Ross/Nandakumar* (Fn. 1), 30 ff.

5 S. zum Folgenden *Jain/Ross/Nandakumar* (Fn. 1), 3 ff.

6 S. *Jain/Ross/Nandakumar* (Fn. 1), 10 ff.

7 Zu Fehlerquellen und Fehlerraten *Jain/Ross/Nandakumar* (Fn. 1), 13 ff.

unterscheiden. Unternehmen identifizieren ihre Kunden, um zu wissen, mit wem sie Verträge abschließen (z. B. bei kreditorischen Risiken) oder um einzelne Transaktionen abzusichern (Überweisungen oder elektronisch signierte Willenserklärungen). Weitere Fälle sind Einlasskontrollen zu Gebäuden, Transportmitteln oder bestimmten Sicherheitsbereichen, aber auch elektronische Bezahlverfahren. Eine Identifizierung von Mitarbeitern findet insbesondere bei der Zutrittskontrolle am Betriebseingang oder in einzelnen Betriebsbereichen statt. Im Rahmen der Arbeitstätigkeit kann es etwa beim Single-Sign-On, bei der Absicherung von Speichermedien oder ebenfalls bei elektronischen Signaturen zur Verwendung von Biometrie kommen. Dritte Personen identifizieren Unternehmen regelmäßig im Rahmen der Gefahrenabwehr, also beispielsweise bei der Durchsetzung von Hausverboten oder der Diebstahlsbekämpfung. Daneben kann eine solche Erkennung auch auf Initiative des Dritten erfolgen, wenn dieser sich etwa freiwillig in die Sperrdatei einer Spielbank eintragen lässt („Selbstsperre" nach § 8 Abs. 2 GlüStV, die nach § 23 Abs. 1 GlüStV zum Eintrag in eine Sperrdatei und nach § 20 Abs. 2 S. 1 GlüStV zum Ausschluss vom Spielbetrieb führt).[8]

Interessanterweise lässt sich dieselbe Dreiteilung auch auf die staatliche Perspektive anwenden. Auch hier werden „Kunden" (im Sinne von Antragstellern) identifiziert. Dies erfolgt bei der Beantragung von Sozialleistungen, bei sonstigen Verfahren wie der universitären Prüfungsverwaltung, bei Einlasskontrollen und Bezahlverfahren. Auch bei der Identifizierung von Mitarbeitern ergeben sich keine wesentlichen Unterschiede zur Unternehmenssicht. Die Identifizierung von Dritten zeigt sich zum einen bei der Ausstellung biometrische Identitätspapiere[9] und der Anlegung entsprechender Register, zum anderen bei der staatlichen Gefahrenabwehr und Strafverfolgung. Letzteres wird für Fingerabdrücke schon sehr lange durchgeführt; aktuell konzentrieren sich einige Forschungsaktivitäten auf die Gesichtserkennung.[10]

II. Chancen und Risiken aus rechtlicher Sicht

Nimmt man zunächst eine nicht anwendungsbezogene, sondern mehr konzeptionelle Perspektive ein, so handelt es sich aus rechtlicher Sicht bei der Biometrie um eine ambivalente Technologie.[11] Diese eröffnet Chancen, birgt jedoch auch Risiken. Chancen und Risiken knüpfen an dieselbe Eigenschaft biometrischer Charakteristika an: die (grundsätzlich)[12] feste und (grundsätzlich) lebenslange Bindung an einen Menschen.

Diese Bindung eröffnet Chancen in vielen Rechtsbereichen, weil sie – entsprechend hohe Erkennungsraten und Überwindungssicherheit vorausgesetzt[13] – ein Mittel zur sicheren Identifizierung von Menschen mit und gegen ihren Willen darstellt. Für beides gibt es im Rechtssystem legitime und völlig übliche Anwendungsfälle: Strafverfolgung und Gefahrenabwehr (Identifizierung von Straftätern und Störern),[14] Rechtssicherheit im elektronischen Rechtsverkehr (Eröffnung von Bankkonten,[15] Absicherung qualifizierter elektronischer Signaturen), aber auch der Schutz sensibler personenbezogener Daten. Wenn biometrische Systeme in diesem letzten Bereich eingesetzt werden, tragen Sie also gerade zum Datenschutz bei.[16]

Die genannte Bindung führt jedoch auch zu rechtlichen Risiken.[17] Neben dem nicht zu unterschätzenden Problem, dass eine zu starke Technikgläubigkeit zu erheblichen Schwierigkeiten für denjenigen führen kann, der durch das System zu Unrecht erkannt oder nicht erkannt wurde, liegen die Probleme insbesondere im Bereich der Persönlichkeitsrechte. Da biometrischer Charakteristika fest mit dem Menschen verbunden sind, eignen sie sich zur Identifizierung in jedem Lebensbereich. Ohne technische Schutzinstrumente (insbesondere bei der Speicherung biometrischer Samples oder Templates, die nach allgemein bekannten Algorithmen erstellt werden) besteht ein erhebliches Risiko der Verwendung als allgemeines Personenkennzeichen und der Erstellung von Persönlichkeitsprofilen. Mit Blick auf das Recht auf informationelle Selbstbestimmung ist beides hochgradig problematisch.[18] Überdies kann es problematisch sein, wenn das legitime Verbergen der Identität erschwert wird (Anmeldung unter anderem Namen, aber mit demselben Fingerabdruck nach Aufnahme in ein Zeugenschutzprogramm; Identifizierung von verdeckten Ermittlern).[19]

Weitere Risiken ergeben sich für bestimmte biometrische Charakteristika. Da das Gesicht in aller Regel unverdeckt bleibt, kann es in der Öffentlichkeit mit hochauflösenden Kameras aus der Distanz oder mit miniaturisierter Technologie aus der Nähe unbemerkt und ubiquitär erfasst werden.[20] Bestimmte Charakteristika stehen zumindest in dem Verdacht, so genannte Zusatzinformationen (über die Gesundheit, Behinderungen, Eigenschaften und Anlagen) zu

8 Näher *Peters*, JR 2002, 177; zur Überwachungspflicht der Spielbank s. OLG Hamm, 4.12.2006 – 22 U 250/05, VersR 2007, 552; zur Evaluierung des Sperrsystems s. *Fiedler*, ZfWG 2015, 188; zu Sperren in Spielhallen *Ennuschat*, GewArch 2015, 97.

9 S.u. 3.4.

10 Z. B. die BMBF-Projekte „Multi-Biometrische Gesichtserkennung (GES-3D)" und „Multi-Biometriebasierte Forensische Personensuche in Lichtbild und Videomassendaten (MisPel)"; das BKA führte schon 2006/2007 das Projekt „Gesichtserkennung als Fahndungshilfsmittel – Foto-Fahndung" durch.

11 S. monographisch z. B. *Albrecht*, Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, 2003; *Meuth*, Zulässigkeit von Identitätsfeststellungen mittels biometrischer Systeme durch öffentliche Stellen, 2006; *Hornung* (Fn. 1), 178 ff., 246 ff., 346 ff.; *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller, Der Digitale Personalausweis, 2005, 106 ff., 223 ff.; *Art. 29-Datenschutzgruppe*, Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien; *Herrmann*, Möglichkeiten und Grenzen des Einsatzes biometrischer Verfahren unter strafprozessualen Gesichtspunkten, 2013; *Held*, Intelligente Videoüberwachung, 2014.

12 Das Problem der Langzeitstabilität (Veränderung biometrische Charakteristika durch natürliche Alterungsprozesse, Verletzungen oder gewollte Operationen) bleibt hier außer Betracht.

13 Beide Fragen werden hier nicht weiter behandelt, sind aber nicht nur technisch, sondern auch rechtlich essenziell; s. *Hornung* (Fn. 1), 179 ff.

14 Zum Einsatz der Biometrie *Herrmann* (Fn. 11); s. a. *Hornung/Desoi/Pocs*, in: Brömme/Busch, BIOSIG 2010, 83 ff.

15 Zum Bankenbereich s. *Grudzien*, DuD 2015, 7; die BaFin erwähnt im Rundschreiben 4/2015 Biometrie erstmals als Möglichkeit der starken Authentifizierung.

16 Zu dieser Ambivalenz bereits *Weichert*, CR 1997, 369.

17 S. z. B. *Hornung*, KJ 2004, 344, 350 ff.; *TeleTrusT*, White Paper zum Datenschutz in der Biometrie, 2008, 10 ff.

18 Näher *Hornung* (Fn. 1), 159 ff., 180 ff.; zu Profilbildung und Personenkennzeichen s. a. BVerfG, 16.7. 1969 – 1 BvL 19/63, BVerfGE 27, 1 (6); 15.12.1983 – 1 BvR 209/83 u. a., BVerfGE 65, 1 (53).

19 Der BND erarbeitet seit 2014 Verfahren, um zum Schutz von Klarnamen-Legenden die biometrische Gesichtserkennung im Internet zu verhindern, s. https://netzpolitik.org2015/strategische-initiative-technik-wir-enthuellen-wie-der-bnd-fuer-300-millionen-euro-seine-technik-aufruesten-will/.

20 Zu sog. Smart Cameras s. aus rechtlicher Sicht *Hornung/Desoi*, K&R 2011, 153 ff.; *Bier/Spiecker gen. Döhmann*, CR 2012, 610; *Spiecker gen. Döhmann*, K&R 2014, 549; *Held* (Fn. 11).

offenbaren.[21] Jedenfalls wenn die DNA als biometrisches Charakteristikum aufgefasst wird, sind entsprechende Zusammenhänge offensichtlich. Schließlich besteht ein Risiko für Menschen, die eine individuell schlechtere Erkennungsrate für ein bestimmtes Charakteristikum aufweisen. Ohne entsprechende technische Schutzmechanismen ergeben sich Gefahren der Verzögerung, des Zusatzaufwand oder der unberechtigten Verdächtigung.

Nicht alle diese Risiken treffen auf alle Einsatzszenarien, Systeme und Verfahren zu. Es besteht ein Unterschied, ob man zu Unrecht an einer Spielbank abgewiesen oder durch die Polizei verhaftet wird. Wichtig ist auch die Frage der Freiwilligkeit, weil z. B. die freiwillige Verwendung des Fingerabdrucks zur Entsperrung mobiler Endgeräte zumindest dann rechtlich unproblematisch ist, wenn die erfassten biometrischen Referenzen auf dem Gerät unter der Kontrolle des Betroffenen verbleiben.[22] Ein erheblicher Unterschied besteht schließlich zwischen automatisierten und solchen Systemen, bei denen ein Mensch eine Letztentscheidung fällt. Die Frage der Fehlerraten lässt sich rechtlich ebenfalls nicht eindeutig beantworten, weil in bestimmten Situationen eine Falsch-Rückweisung zu erheblichen Nachteilen führen kann (Grenz- oder Zugangskontrolle), in anderen Situationen jedoch gerade die Falsch-Akzeptanz (polizeiliche Fahndung).

Aus datenschutzrechtlicher Perspektive dürfte schließlich die Frage des Aufbaus großer Datenbanken mit biometrischen Samples das größte Problem darstellen. Solange die biometrische Erkennung in spezifischen, rechtlich durchstrukturierten Situationen Identifizierungen erleichtert, an denen ein legitimes Interesse besteht, so werden sich die rechtlichen Anforderungen vielfach auf die technische Ebene verlagern (Erkennungsgenauigkeit, Schutz gegen Zweckentfremdung, Datensicherheit).[23] Demgegenüber eröffnen große Datenbanken erhebliche Risiken der Profilbildung für große Menschengruppen; dies ist nicht nur individuell-grundrechtlich, sondern auch gesellschaftlich relevant.

III. Ausgewählte rechtliche Problemlagen

Biometrische Systeme werfen eine Vielzahl von Rechtsfragen in unterschiedlichen Bereichen auf. Von diesen werden im Folgenden einige exemplarisch beleuchtet.

1. Grundrechte

Ohne dass dies hier im Detail ausgeführt werden kann, sollte man für die weitere rechtliche Analyse im Hinterkopf behalten, dass der Einsatz biometrischer Verfahren praktisch immer grundrechtlich relevant ist. Wenn und soweit die entsprechenden Verfahren personenbezogene Daten verwenden,[24] ist der Schutzbereich des Rechts auf informationelle Selbstbestimmung eröffnet. Dies ist in sehr vielen Fällen der Fall und insbesondere auch dort gegeben, wo biometrische Daten so in andere personenbezogene Datenformate umgerechnet werden, dass nicht auf die biometrischen Charakteristika zurückgeschlossen werden kann.

Insbesondere die genannten Fehlerraten können zu Problemen mit den Gleichheitsgrundrechten führen, wenn keine effektiven Alternativverfahren bereitgestellt werden.[25] Daneben kann es mittelbar zu Eingriffen in viele weitere Grundrechte kommen. Dies hängt vom Einsatzzweck ab und kann beispielsweise die Ein- und Ausreisefreiheit oder das Asylrecht (Art. 11 GG,[26] Art. 2 I GG[27] bzw. Art. 16a GG, bei Grenzkontrollen), die Versammlungsfreiheit (Art. 8 GG, bei Anreisekontrollen oder der biometrischen Überwachung der Teilnehmer)[28] oder das Recht auf Gewährleistung eines menschenwürdigen Existenzminimums (Art. 1 I GG i. V. m. Art. 20 I GG,[29] bei einer Identifizierung zur Gewähr von Sozialleistungen) betreffen.

2. Reichweite bestehender Rechtsgrundlagen

Eine übergreifende Rechtsfrage besteht darin, ob bestehende Ermächtigungsgrundlagen für die Erhebung und Verwendung personenbezogener Daten auch die Erhebung und Verwendung gerade biometrischer Daten zulassen. Dies ist zum einen eine methodische Frage der Auslegung, zum anderen auch ein Verfassungsproblem.[30]

Verfassungsrechtlich betrifft dies die Anforderungen an die Bestimmtheit von Ermächtigungsgrundlagen. Das BVerfG hat diese Anforderungen über die Jahre verschärft und verlangt einen umso höheren Grad an Bestimmtheit, je intensiver der mit der staatlichen Maßnahme verbunden Grundrechtseingriff ist. Für die Eingriffsintensität hat das Gericht in inkrementeller Innovationstätigkeit[31] ein inzwischen gefestigtes Set an Kriterien entwickelt: relevant sind danach die Gestaltung der Einschreitschwellen, die Zahl der Betroffenen („Streubreite“, insbesondere bei unverdächtigen Dritten) und die individuelle Beeinträchtigung. Letztere hängt davon ab, ob die Betroffenen als Person anonym bleiben, ob sie einen Anlass für die Datenerhebung gegeben haben, welche Daten erfasst werden und welche Nachteile den Grundrechtsträgern drohen oder von ihnen nicht ohne Grund befürchtet werden. Das Problem soll an zwei Beispielen verdeutlicht werden, stellt sich aber auch in vielen anderen Rechtsbereichen (etwa hinsichtlich der „Identitätskontrolle“, die Spielbanken gemäß § 20 Abs. 2 S. 2 GlüStV durchzuführen haben).

---

21 Näher FIDIS Deliverable D3.10: Biometrics in identity management, http://www.fidis.net/resources/deliverables/, 2007, 83; speziell zur Retina *Friedewald/Wawrzyniak/Pallas*, DuD 2014, 482; aus rechtlicher Sicht *Hornung* (Fn. 1), 185 ff., 276 f.

22 Zur Nutzung von Biometrie mit Smartphones s. *Busch*, DuD 2014, 475.

23 S. noch unten 4.

24 S. zum Personenbezug biometrischer Daten *Hornung*, DuD 2004, 15.

25 Dazu am Beispiel biometrischer Identitätspapiere *Hornung* (Fn. 1), 199 ff.

26 Dieser umfasst auch die Einreise, s. BVerfG, 7.5.1953 – 1 BvL 104/52, 25.1.1977 – 1 BvR 210/74 u. a., BVerfGE 2, 266, 273; 43, 203, 211; s. *Hornung*, in: Hornung/Möller, PassG/PAuswG, 2011; Einf. Rn. 24 ff. m. w. N.

27 Als Grundlage der Ausreisefreiheit, s. BVerfG, 16.1.1957 – 1 BvR 253/56, BVerfGE 6, 32.

28 Zur Videoüberwachung von Versammlungen z. B. OVG NRW, 23.11.2010 – 5 A 2288/09, DVBl 2011, 175; VG Berlin, 5.7.2010 – 1 K 905.09, NVwZ 2010, 1442; VG Berlin, 26.4.2012 – VG 1 K 818.09, ZD 2012, 444; zur Gefahr durch „exzessive Observationen und Registrierungen“ BVerfG, 14.5.1985 – 1 BvR 233, 341/81, BVerfGE 69, 315 (349); s. a. *Kutscha*, KJ 2011, 223.

29 BVerfG, 9.2.2010 – 1 BvL 1/09 u. a., BVerfGE 125, 175.

30 Diese Fragen hängen zusammen, weil die Entscheidung über die (richterliche) Methode der Rechtsanwendung wegen der Verfassungsbindung der Judikative immer auch eine verfassungsrechtliche Frage ist.

31 S. aus grundrechtstheoretischer Sicht *Hornung*, Grundrechtsinnovationen, 2015, 309 ff.; dort auch m. w. N. zu den einzelnen Entscheidungen.

a) § 100h Abs. 1 S. 1 Nr. 1 StPO

§ 100h Abs. 1 S. 1 Nr. 1 StPO erlaubt unter bestimmten Voraussetzungen die Herstellung von „Bildaufnahmen" außerhalb von Wohnungen. Es ist anerkannt, dass dies auch Videoaufnahmen umfasst.[32] Weder der Wortlaut noch die Entstehungsgeschichte der Vorschrift geben aber einen Hinweis auf die nachfolgende automatisierte Auswertung des gewonnenen Bildmaterials.[33]

Mit Blick auf die oben genannten Kriterien liegt in einer biometrischen Analyse sicherlich ein intensiverer Eingriff in die Persönlichkeitsrechte der Betroffenen. Wie stark dieser Effekt ist, hängt vom konkreten Verwendungszweck der Biometrie ab. Dies kann z. B. die reine Personenerkennung ohne Identifizierung sein (um das Auffinden von Menschen in sehr umfassendem Videomaterial zu ermöglichen), die Wiedererkennung einer markierten Person in demselben oder einem anderen Video, der Abgleich mit während eines Ermittlungsverfahrens gespeicherten Lichtbildern oder die Suche in großen Lichtbilddatenbanken.[34]

Alle diese Verwendungszwecke sind technische Fortentwicklungen, bei denen sich die Frage stellt, ob für sie neue strafprozessuale Ermächtigungsgrundlagen erforderlich sind. Dieses Problem taucht bei technikspezifischen Ermächtigungsgrundlagen auch ansonsten auf. Das BVerfG hat insoweit mehrfach entschieden, dass derartige Normen zumindest in bestimmtem Umfang auch den Einsatz technisch fortentwickelter Erhebungsinstrumente rechtfertigen.[35] Überträgt man dies auf den hiesigen Fall, so spricht einiges dafür, zumindest die ersten der genannten Verwendungszwecke als von § 100h Abs. 1 S. 1 Nr. 1 StPO erfasst anzusehen, zumal die Norm relativ hohe Anforderungen statuiert und § 101 StPO verfahrens- und organisationsrechtliche Absicherungen enthält. Flächendeckende Kontrollen (im Sinne eines Live-Abgleichs mit biometrischen Datenbanken)[36] oder gar die Anlage einer solchen Datenbank selbst können aber keinesfalls auf § 100h Abs. 1 S. 1 Nr. 1 StPO gestützt werden.

b) § 6b BDSG

Ein vergleichbares Problem stellt sich für die allgemeine Rechtsgrundlage für die Videoüberwachung in § 6b BDSG. Abs. 1 gestattet die „Beobachtung" öffentlich zugänglicher Räume durch Videoüberwachungsanlagen. Betrachtet man diese Formulierung isoliert, so deutet der Wortlaut eher darauf hin, dass eine weitere Analyse des erhobenen Bildmaterials überhaupt nicht gestattet ist. Genau in diesem Sinne hat das OVG Hamburg den vergleichbaren § 8 Abs. 3 S. 1 HmbPolDVG interpretiert. Aus der Formulierung, die Polizei dürfe Straßen, Wege und Plätze „mittels Bildübertragung offen beobachten", folge, dass sich jede spätere Verwendung des Bildmaterials auf das bloße Betrachten der Bilddaten beschränken müsse. Insbesondere sei damit „jegliche Form der automatisierten Auswertung ausgeschlossen".[37] Der Begriff der Biometrie wird hier nicht genannt, ihr Einsatz aber der Sache nach für unzulässig erklärt.

§ 6b BDSG ist demgegenüber anders strukturiert. Abs. 3 legitimiert die „Verarbeitung oder Nutzung von nach Abs. 1 erhobenen Daten". Begrifflich wird damit eine automatisierte Bildanalyse umfasst. Auch der Gesetzgeber erwähnte 2001 biometrische Verfahren und ging insoweit offenbar davon aus, dass der Tatbestand einen technischen Fortschritt mit umfasst.[38] Dies führt zu einer doppelten Abwägung: Sowohl hinsichtlich der Videoüberwachung selbst (Abs. 1), als auch hinsichtlich der biometrischen Auswertung (Abs. 3) dürfen keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Diese Abwägungen sind getrennt durchzuführen, weil der Einsatz biometrischer Systeme regelmäßig zu einer erheblichen Vertiefung des Eingriffs führt.[39] Die Abwägung kann also ergeben, dass die Beobachtung selbst zulässig, die automatisierte Analyse aber unzulässig ist.

3. Arbeitsrecht

Im Arbeitsrecht werfen insbesondere biometrische Zugangskontrollen rechtliche Probleme auf. Das Beschäftigtendatenschutzrecht ist in Deutschland nach wie vor nur rudimentär in § 32 BDSG geregelt. Während die Norm für innerbetriebliche Ermittlungsverfahren immerhin einige Vorgaben enthält, beschränkt sie sich im Übrigen darauf, die Erhebung und Verwendung derjenigen Daten zu gestatten, die für die Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses „erforderlich" sind. Unter welchen Umständen der sehr unbestimmte Begriff der Erforderlichkeit ein biometrisches Zugangskontrollsystem legitimiert, lässt sich der Norm selbst kaum entnehmen und bleibt dementsprechend der Rechtsprechung überlassen.[40] Während der vorläufig letzten Reformdiskussion 2011 gab es mehrere Vorschläge für spezifische Regelungen zur Biometrie,[41] die jedoch mit dem gesamten Gesetzgebungsverfahren scheiterten.

Damit gelten für die Verwendung biometrischer Daten der Beschäftigten die allgemeinen Regeln. Gemäß § 4 Abs. 1 BDSG bedarf es für die Erhebung und Verwendung einer Einwilligung oder einer Legitimation durch eine Rechtsvorschrift (Verbotsprinzip). Die Einwilligung ist als Instrument wenig geeignet, weil ihre Freiwilligkeit im Arbeitsverhältnis problematisch sein kann und sie prinzipiell widerruflich ist. Da die Reichweite von § 32 BDSG häufig zweifelhaft sein wird (s. o.) und die Einführung biometrischer Systeme ohnehin praktisch immer mitbestimmungspflichtig ist, wird in der Praxis regelmäßig der Weg über eine entsprechende Betriebs- oder Dienstvereinbarung gewählt.[42] Diese

32 KK-*Bruns*, § 100h Rn. 3 m. w. N.
33 Zum vergleichbaren Problem bei polizeirechtlichen Videoüberwachungsnormen s. *Held* (Fn. 11), 184 ff.
34 Diese Szenarien wurden im Projekt MisPel (Fn. 10) erforscht.
35 Z. B. BVerfG, 12.4.2005 – 2 BvR 581/01, BVerfGE 112, 304 (315 ff.).
36 Insoweit kann eine Parallele zur automatisierten Kennzeichenerkennung gezogen werden, die expliziter Normen bedarf, s. BVerfG, 11.3.2008 – 1 BvR 2074/05, 1254/07, BVerfGE 120, 378.
37 OVG Hamburg, 22.6.2010 – 4 Bf 276/07, MMR 2011, 128, 131; die Revisionsentscheidung (BVerwG, 25.1.2012 – 6 C 9/11, BVerwGE 141, 329) befasst sich nicht mit dieser Frage.
38 BT-Drs. 14/5793, 62.
39 S. näher *Hornung/Desoi*, K&R 2011, 153, 157.
40 S. näher *Albrecht* (Fn. 11), 198 ff.; *Riesenhuber*, BeckOK Datenschutzrecht, § 32 BDSG Rn. 136 ff.
41 Der Regierungsentwurf (BT-Drs. 17/4230) enthielt in § 32h nur wenige Regelungen, nämlich eine Zweckbindung auf betriebliche Gründe der Autorisierung und Authentifikation (da dies Zweck der Biometrie per se ist, wäre dies keine Einschränkung gewesen) und eine Löschungspflicht nach Zweckerreichung (die man auch aus allgemeinen Regeln ableiten kann). Zwar gestattete der Entwurf eine Einwilligung nur für Lichtbilder. Wegen der allgemeinen Zwecke hätte dies aber keine Rolle gespielt. § 16 des Entwurfs von Bündnis90/Die Grünen (BT-Drs. 17/4852) beschränkte den Einsatz demgegenüber auf die Autorisierung und Authentifizierung in „besonders sicherheitsrelevanten Bereichen". Eine Erhebung biometrischer Daten zur Zeiterfassung sollte unzulässig sein.
42 Zu deren Ausgestaltung s. *Albrecht*, JurPC 2007, Web-Dok. 55/2007.

kann als Rechtsvorschrift im Sinne von § 4 Abs. 1 BDSG[43] die Erhebung und Verwendung legitimieren, wenn sie sich ihrerseits im Rahmen der Regelungskompetenz der Parteien bewegt.[44]

Die Mitbestimmungspflicht folgt aus § 87 Abs. 1 Nr. 1 BetrVG (Ordnung des Betriebs und des Verhaltens der Arbeitnehmer im Betrieb) und Nr. 6 (Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen). Das BAG zieht den Anwendungsbereich insoweit relativ weit und bejaht eine Mitbestimmungspflicht auch dann, wenn ein Arbeitgeber seine Beschäftigten anweist, in einem externen Betrieb das dort vorhandene biometrische Zugangskontrollsystem zu verwenden.[45] Der Kundenbetrieb zählt insoweit (funktional) zum Betrieb des Arbeitgebers. Auch spielt es keine Rolle, dass das biometrische System weder durch den Arbeitgeber selbst noch in seinem Interesse betrieben wird.

Während die grundsätzliche Mitbestimmungspflichtigkeit damit geklärt ist (und z. B. auch in Österreich besteht),[46] existiert bislang keine Rechtsprechung zu einzelnen Gestaltungskriterien und -anforderungen für biometrische Systeme im betrieblichen Umfeld.[47]

4. Biometrische Identitätspapiere und Grenzkontrollen

Die meisten Menschen kommen das erste Mal mit der Biometrie in Berührung, wenn sie Reisepässe und Personalausweise beantragen. Nach den Anschlägen des 11. September entfalteten die USA erheblichen politischen Druck auf andere Staaten, um diese zur Einführung biometrischer Reisedokumente zu bewegen.[48] Für Reisepässe existiert inzwischen eine europäische Regulierung in Form einer Pass-Verordnung,[49] deren primärrechtliche Zulässigkeit der EuGH bejaht hat.[50] Demgegenüber steht die Einführung biometrischer Daten in nationale Personalausweise in der Kompetenz der Mitgliedstaaten; die Pass-Verordnung findet insoweit gemäß Art. 1 III 2 keine Anwendung.[51]

Im deutschen Recht regeln § 4 PassG und § 5 PAuswG detailliert die Speicherung biometrischer Daten in Pässen und Personalausweisen. Diese Normen werfen einige Rechtsfragen auf,[52] sind aber prinzipiell ein Beispiel für eine detaillierte und normenklare Regelung des Umgangs mit derartigen Daten. Die Identitätsprüfung wird ebenfalls detailliert geregelt. § 16a PassG und § 17 PAuswG enthalten eine strikte Zweckbindung der im Chip gespeicherten Daten (Überprüfung der Echtheit des Dokuments und der Identität des Passinhabers).[53] Daneben wird für bestimmte Behörden (Polizei, Zollverwaltung, Pass-, Personalausweis- und Meldebehörden) explizit die Befugnis geregelt, einzelne Schritte der biometrischen Erkennung durchzuführen: Auslesen der Daten aus dem Chip, Erheben der neuen Daten des Passinhabers und Vergleich der Datensätze. Im Anschluss sind die Daten unverzüglich zu löschen; dies gilt auch, wenn die Identität des Inhabers nicht positiv festgestellt werden konnte.[54] Angesichts der Gesetzgebungsgeschichte ist eindeutig, dass sowohl der Abgleich der Daten mit erkennungsdienstlichen Dateien, als auch die Aufbewahrung zu Zwecken der Gefahrenabwehr oder Strafverfolgung absolut unzulässig sind.[55]

Die Frage biometrischer Datenbanken (die bei der Ausstellung biometrische Identitätspapiere mit relativ wenig Aufwand angelegt werden können) wird durch die Pass-Verordnung nicht geregelt.[56] In Deutschland sind die Gesichtsdaten dezentral in Pass- und Personalausweisregistern gespeichert. Demgegenüber werden Fingerabdrücke vom Hersteller nach Herstellung (§ 16 Abs. 3 S. 2 PassG, § 26 Abs. 3 S. 2 PAuswG) und von der Behörde nach Aushändigung (§ 16 Abs. 2 S. 3 PassG, § 26 Abs. 2 PAuswG) gelöscht. Eine Speicherung bei anderen Stellen ist unzulässig (§ 16 Abs. 2 S. 1 PassG, § 26 Abs. 1 S. 1 PAuswG), und nach Kontrollen sind die Daten sofort zu löschen (§ 16a S. 3 PassG, § 17 S. 4 PAuswG). Damit dürfen Fingerabdrücke nach der Übergabe an den Inhaber ausschließlich im Dokument selbst gespeichert werden; einzige Ausnahme ist die kurzzeitige Verarbeitung bei Kontrollen.

Das Verbot bundesweiter biometrischer Datenbanken in § 4 Abs. 3 S. 3 PassG, § 26 Abs. 4 PAuswG ist folglich nur für die Gesichtsdaten relevant. Diese Regelung ist, auch wenn sie einen deutschen Sonderweg darstellt,[57] verfassungsrechtlich geboten. Das ergibt sich aus den Risiken zentraler biometrischer Datenbanken[58] und der restriktiven Rechtsprechung des BVerfG zur Zulässigkeit einer begrenzten DNA-Datenbank Vorbestrafter.[59]

---

43 BAG, 30.8.1995 – 1 ABR 4/95, BAGE 80, 366; 20.12.1995 – 7 ABR 8/95, BAGE 82, 36.

44 Dazu *Scholz/Sokol*, in: Simitis, BDSG, 4. A. 2014, § 4 Rn. 17 m. w. N.

45 BAG, 27.1.2004 – 1 ABR 7/03, BAGE 109, 235; s. näher *Hornung/Steidle*, AuR 2005, 201, 204 f.; *Hornung*, KJ 2004, 344, 354 f.; kritisch *Besgen/Langner*, SAE 2006, 233.

46 OGH, 20.12.2006 – 9 ObA 109/06d, AuR 2007, 398 m. Anm. *Hornung*.

47 S. dazu unten 4 sowie *Steidle*, Multimedia-Assistenten im Betrieb, 2005, 232 ff.; *Hornung/Steidle*, AuR 2005, 201, 205 ff.

48 Gegenüber 25 mit den USA eng verbündeten Staaten bestand das Druckmittel in der (im Enhanced Border Security and Visa Reform Act fixierten) Drohung, das Visa-Waiver-Abkommen aufzukündigen, das es Staatsangehörigen ermöglicht, ohne Visum in die USA einzureisen.

49 VO (EG) Nr. 2252/2004 v. 13.12.2004, ABl. EU Nr. L 385 v. 29.12.2004; geändert durch VO (EG) Nr. 444/2009, ABl. EU Nr. L 142 v. 6.6.2009; s. *Roßnagel/Hornung*, DÖV 2005, 983 ff.; *Pallasky*, Datenschutz in Zeiten globaler Mobilität, 2007, 30 ff.; *Altmann*, Freiheitsbeschränkung durch den Reisepass?, 2010; zur Umsetzung *Hornung*, DuD 2007, 181; zu den völker- und europarechtlichen Bezügen *Hornung*, in: Hornung/Möller (Fn. 26), Einf. Rn. 10 ff.

50 EuGH, 17.10.2013 – C-291/12, NVwZ 2014, 435.

51 Dieses angesichts des Wortlauts und der fehlenden Kompetenz bei Verabschiedung (die Union darf erst seit dem Vertrag von Lissabon Bestimmungen für Personalausweise erlassen: Art. 77 III AEUV) eher selbstverständliche Ergebnis hat der EuGH explizit festgestellt, s. EuGH, 16.4.2015 – C-446/12 u. a., ZD 2015, 420.

52 S. *Hornung*, in: Hornung/Möller (Fn. 26), § 4 PassG Rn. 35 ff.

53 Näher *Hornung*, in: Hornung/Möller (Fn. 26), § 16a PassG Rn. 11 ff.

54 *Hornung*, in: Hornung/Möller (Fn. 26), § 16a PassG Rn. 21 (str.).

55 Der Bundesrat hatte beides gefordert, s. BR-Drs. 16/1/07, 3 f.; näher *Hornung*, in: Hornung/Möller (Fn. 26), § 16a PassG Rn. 4 ff., 13.

56 EuGH, 16.4.2015 – C-446/12 u. a., ZD 2015, 420; näher *Hornung*, DuD 2007, 181, 184 f.; *ders.*, in: Hornung/Möller (Fn. 26), § 4 PassG Rn. 67 ff.

57 Viele Staaten nutzen zentrale Datenbanken v. a. zum Abgleich vor der Ausstellung neuer Identitätspapiere, um „Doppelidentitäten" zu verhindern. Daneben existieren weitere große Datenbanken, z. B. das FBI-Projekt „Next Generation Identification", in dem die Fingerabdrücke von Bewerbern für staatliche (und neuerdings auch viele private) Stellen gespeichert werden, s. www.heise.de/-2823448.html.

58 *Konferenz der Datenschutzbeauftragten*, DuD 2002, 247; *Albrecht* (Fn. 11), 159 ff., 162 f.; *Roßnagel/Hornung* (Fn. 11), 136 ff.; *Hornung* (Fn. 1), 191 ff.; *ders.*, KJ 2004, 344, 352 f.; unlängst wurden in den USA bei einem Angriff 5,6 Mio. Fingerabdruckdaten kompromittiert, s. www.heise.de/-2824581.html.

59 BVerfG, 14.12.2000 – 2 BvR 1741/99 u. a., BVerfGE 103, 21; hierzu *Faber*, RDV 2003, 278, 280 ff.; s. a. EGMR, 4.12.2008 – 30562/04, EuGRZ 2009, 299.

5. Biometrie in der Datenschutzreform

Jenseits derartiger spezifischer Regelungen wird sich die Zulässigkeit des Einsatzes biometrischer Systeme in Zukunft maßgeblich nach der europäischen Datenschutz-Grundverordnung richten,[60] die sich derzeit in den Verhandlungen des Trilogs befindet.[61] Die Positionen der Kommission, des Parlaments und des Rats enthalten leicht abweichende Bestimmungen des Begriffs der biometrischen Daten in Art. 4 Nr. 11. Die Kommission definiert diese als „Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen eines Menschen, die dessen eindeutige[62] Identifizierung ermöglichen, wie Gesichtsbilder oder daktyloskopische Daten".[63] Das Parlament fügt hinzu, dass es sich um „personenbezogene" Daten handeln muss;[64] dies dürfte im Regelungskontext an sich eindeutig sein. Der Rat schlägt dagegen vor, als Konkretisierung nur „mit speziellen technischen Verfahren gewonnene personenbezogene Daten" zu erfassen.[65] Dies verengt den Anwendungsbereich in sinnvoller Weise, da mutmaßlich einfache Gesichtsbilder (wie private Fotos) die Definition des Rats nicht erfüllen.

Wesentliche Unterschiede offenbaren sich bei den Anforderungen, die die Institutionen an die Erhebung und Verwendung biometrischer Daten stellen. Im Entwurf der Kommission findet sich als einzige zusätzliche Anforderung, dass nach Art. 33 I, II lit. c eine Datenschutz-Folgenabschätzung durchzuführen ist.[66] Das Parlament nimmt biometrische Daten dagegen in den Katalog der „besonderen Datenkategorien" auf. Dies hat neben der Datenschutz-Folgenabschätzung viele weitere erhöhte Anforderungen zur Folge.[67] Der Rat folgt diesem Vorschlag nicht, sondern schließt sich der Position der Kommission an. Dementsprechend bleibt abzuwarten, welche Position sich im Trilog durchsetzen wird. Dies wird einen erheblichen Einfluss auf die Anwender haben, auch wenn zu berücksichtigen ist, dass biometrische Daten bereits heute vielfach unter den Begriff der „besonderen Arten personenbezogener Daten" (§ 3 Abs. 9 BDSG) fallen.[68] Wie allgemein bei der Datenschutzreform werden sich die konkreten Auswirkungen wegen der vielfach generalklauselartigen Formulierungen erst in der praktischen Anwendung durch Datenschutzaufsichtsbehörden und Gerichte zeigen.

IV. Ausblick

Angesichts der fortschreitenden technischen Entwicklung und des erheblichen Interesses an sicherer und einfacher Identifizierung in vielen Lebensbereichen steht zu erwarten, dass sich biometrische Systeme in der Zukunft weit verbreiten werden. Ob diese Entwicklung positiv oder negativ zu sehen ist, lässt sich nicht prinzipiell beantworten, sondern ist eine Frage der technischen Gestaltung.

Verläuft diese ungeregelt und unter dem Paradigma einer permanenten Identifizierung des Menschen auf Schritt und Tritt in allen sozialen Kontexten, so droht die Dystopie ubiquitärer Beobachtung insbesondere im öffentlichen Raum. Vor allem die Verbreitung miniaturisierter Kameras (erkennbar am Beispiel von Google Glass)[69] ist insoweit eine erhebliche Herausforderung. Der Abgleich so aufgenommene Bilder mit Gesichtsbildern im Internet erlaubt es, in Sekundenschnelle Informationen über Menschen in der eigenen Umgebung abzurufen.[70] Das Problem des (fehlenden) „Vergessens" im Internet[71] wird so allgegenwärtig.

Demgegenüber lässt sich durch eine Mischung aus rechtlichen und organisatorischen Rahmenbedingungen sowie einer grundrechtsfreundlichen technischen Gestaltung Biometrie unter Vermeidung vieler der beschriebenen Risiken einsetzen. Rechtliche Regelungen (Betriebs- und Dienstvereinbarungen, AGB und sonstige Vertragsklauseln, gesetzliche Regelungen insbesondere dort, wo staatliche Schutzpflichten bestehen) können zulässige und unzulässige Einsatzfelder abstecken, Erhebungs- und Verwendungsbefugnisse spezifizieren, Zweckentfremdungen verbieten, unbeteiligte Dritte schützen, Transparenz für die Betroffenen herstellen und ihre Rechte auf Auskunft und Löschung sichern. Organisatorische Instrumente sind insbesondere die Einbindung von Betriebs- und Personalräten (die auch aus Akzeptanzgründen sinnvoll ist) sowie von Datenschutz- und IT-Sicherheitsbeauftragten. Auch effektive gerichtliche Kontrollverfahren sind hier zu nennen.

Wie bei vielen anderen technischen Innovationen reichen rechtliche und organisatorische Instrumente jedoch nicht aus. Vielmehr bedarf es nach dem Grundsatz des privacy by design einer datenschutzfreundlichen Technikgestaltung, die die Betroffenen vielfach effektiver vor Missbrauch schützt: Was technisch nicht möglich ist, muss rechtlich nicht verboten werden.[72]

Technische Gestaltungskriterien zum Schutz der Betroffenen können auch den Interessen der Betreiber dienen. Dies gilt insbesondere für die technische Leistungsfähigkeit, die die Nachteile von Falsch-Akzeptanzen und Falsch-Rückweisungen minimiert. In anderen Bereichen muss ein Ausgleich widerstreitender Interessen gefunden werden.[73] Eine datensparsame Gestaltung kann vielfach sowohl auf die zentrale Speicherung, als auch auf die Speicherung biometrischer Sample verzichten, indem Chipkarten und templa-

60 Für die Datenverarbeitung bei Polizei und Justiz soll eine Richtlinie gelten (dazu *Bäcker/Hornung*, ZD 2012, 147), die sich aber ganz überwiegend nicht mit den Erhebungsbefugnissen befasst.

61 S. als Zwischenstand zur umfangreichen und ausdifferenzierten Diskussion *Hornung*, in: Scholz/Funk, DGRI Jahrbuch 2012, 2013, 1 ff.; zur Videoüberwachung *Seifert*, DuD 2013, 650.

62 Da die Akteure sich der Fehlerraten bewusst sind, ist dies sicher nicht wörtlich zu verstehen.

63 KOM(2012) 11 endg.

64 P7_TA-PROV(2014)0212.

65 Position vom 15.6.2015, 9565/15.

66 Zu Kriterien für eine solche Abschätzung s. *Art. 29-Datenschutzgruppe* (Fn. 11), 36 ff.

67 U.a. Einschränkungen bei der Einwilligung, eine Beschränkung des Profilings sowie die Pflicht zur Bestellung eines Datenschutzbeauftragten. Außerdem ist die Verarbeitung der Daten ein Regelbeispiel für eine „erhöhte Risikoeinschätzung".

68 S. *Hornung* (Fn. 1), 274 ff.

69 S. z. B. *Schwenke*, K&R 2013, 685; *ders.*, DuD 2015, 161.

70 S. z. B. http://www.zeit.de/digital/mobil2014-02/google-glass-gesichtserkennung-kommt: „Gesichtserkennung für Google Glass soll Sextäter zeigen"; s. a. *Art. 29-Datenschutzgruppe*, Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten.

71 Allgemein *Hornung/Hofmann*, JZ 2013, 163 ff.; s. nunmehr EuGH, 13.5.2014 – C-131/12, NJW 2014, 2257.

72 S. *Borking*, DuD 1998, 636; *ders.*, DuD 2001, 607; *Hansen*, in: Roßnagel, HB Datenschutzrecht, 2003, Kap. 3.3; in Bezug auf die europäische Reform *Hornung*, in: Friedewald/Pohoryles (Hrsg.), Privacy and Security in the Digital Age, 2014, 181 ff.

73 S. zu den Anforderungen und Gestaltungskriterien insoweit *Hornung* (Fn. 1), 178 ff., 346 ff.; *Schumacher/Unverricht*, DuD 2009, 308; *Art. 29-Datenschutzgruppe* (Fn. 11), 11 ff., 34 ff.; zum Einsatz am Arbeitsplatz *Hornung/Steidle*, AuR 2005, 201, 205 ff.; zur Idee einer gestuften Kontrolle bei Smart Cameras *Roßnagel/Desoi/Hornung*, DuD 2011, 694.

tefreie Verfahren[74] eingesetzt werden. Bei der Merkmalsauswahl lassen sich Kriterien wie das Problem der Zusatzinformationen oder der intransparenten Datenerhebung adressieren.[75] Letzteres ist auch bei der biometrischen Erkennung zu vermeiden. Schlussendlich ergeben sich bereits heute aus § 9 BDSG und der entsprechenden Anlage Anforderungen an die Datensicherung. Da hier eine Risikoabwägung unter Angemessenheitsgesichtspunkten durchzuführen ist, ist der besondere Charakter der gespeicherten biometrischen Daten zu berücksichtigen und kann zu erhöhten Anforderungen führen.

Nicht alle datenschutzfreundlichen Optionen werden sich in allen Verwendungsszenarien eignen. Sie bilden aber eine Art Baukasten, der bei der Entscheidung über die Einführung und Konfiguration eines biometrischen Systems beachtet werden sollte. Letztlich sind diese datenschutzrechtlichen Anforderungen immer auch Akzeptanzkriterien. Zumindest in Deutschland und Europa werden Systeme kaum akzeptiert werden, die gegen den Willen der Betroffenen datenschutzunfreundlich gestaltet werden – während sich umgekehrt durch ein entsprechende Design die Chance eröffnet, eine innovative Technologie im Interesse aller Beteiligten zu implementieren.

74 Zu den Möglichkeiten einer „Biometric Template Protection" s. *Busch u. a.*, DuD 2011, 183 ff.

75 S. aus Datenschutzsicht zu den einzelnen Charakteristika *Art. 29-Datenschutzgruppe* (Fn. 11), 21 ff.

RAin Dr. Vera Jungkind, Düsseldorf*

Biometrische Zugangskontrollen

Chance oder Gefahr für den Datenschutz?

Spätestens mit der Einführung des biometrischen Reisepasses im Herbst 2005 gelangten Authentifizierungsverfahren auf Grundlage von biometrischen Merkmalen in den Fokus der breiten Öffentlichkeit. Derartige Verfahren werden längst auch im Bereich der Privatwirtschaft genutzt, um den Zugang zu Räumlichkeiten oder technischen Systemen zu sichern und zu kontrollieren. In den wenigsten Fällen steht für biometrische Systeme eine spezialgesetzliche Grundlage zur Verfügung, sodass sich deren Zulässigkeit nach den allgemeinen Vorschriften, in datenschutzrechtlicher Hinsicht insbesondere nach §§ 4, 28 BDSG, beurteilt. Speziell in Spielhallen kommen biometrische Zugangskontrollen wegen ihrer Zuverlässigkeit zum Schutz gesperrter Spieler praktisch in Betracht. Dieses Beispiel veranschaulicht allerdings auch, dass sich die Interessen der Praxis und die datenschutzrechtlichen Anforderungen häufig konträr gegenüber stehen.

I. Biometrische Daten als personenbezogene Daten i. S. d. BDSG

Biometrische Zugangskontrollen werden dadurch ermöglicht, dass biometrische Daten einem bestimmten Menschen zugeordnet werden können. Biometrische Daten sind in der Regel einzigartig, untrennbar und dauerhaft mit dem Körper verbunden, nicht verlierbar, nicht vergessbar, nicht geheim zu halten, nicht übertragbar, nicht veränderbar. Hierzu gehören alle Daten über physische, physiologische und verhaltenstypische Merkmale einer Person, die deren eindeutige Identifizierung zulassen.[1] Klassische Beispiele für biometrische Daten, die sich aus physiologischen Merkmalen ergeben, sind der Fingerabdruck, die Hand- oder Gesichtsgeometrie, die Netzhaut oder die Iris. Um biometrische Merkmale handelt es sich auch bei der Stimme, der Sprechweise oder der Gangart einer Person. Biometrische Daten sind somit regelmäßig personenbezogene Daten i. S. d. § 3 Abs. 1 BDSG,[2] es sei denn, sie liegen nur als Template oder in chiffrierter Form vor und es ist daher auszuschließen, dass die betroffene Person durch diese Daten identifiziert werden kann.[3]

Biometrische Daten sind sensibel: Sie bergen die Gefahr des Identitätsdiebstahls, z. B. in Form der nichtautorisierten Nutzung fremder Charakteristika (wodurch biometrische Zugangs- oder Identitätskontrollen überwunden werden können), sowie die Gefahr der Auswertung der in biometrischen Daten enthaltenen Zusatzinformationen, insbesondere Gesundheitsdaten. Biometrische Daten können als Kennung in unterschiedlichen Anwendungen und Datenbanken verwandt werden und erlauben die Verknüpfung von Daten und Erstellung von Personen- und Bewegungsprofilen. Bei biometrischen Zugangskontrollen ist je nach Ausgestaltung auch die Diskriminierung von Personen, die ein bestimmtes biometrisches Merkmal nicht aufweisen, möglich, wenn keine Alternativanwendung angeboten wird.

Dennoch sind biometrische Daten in der Regel nicht zugleich besondere personenbezogene Daten nach § 3 Abs. 9 BDSG.[4] Dazu gehören Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Die Aufzählung ist abschließend.[5] Die genannten Arten von Daten wurden vom Gesetzgeber als besonders sensibel bewertet, weshalb ihnen einzelfallunabhängig ein besonderer Schutz gewährt wird,

* Die Autorin dankt Herrn Rechtsreferendar Marten Franke für die Unterstützung bei der Erarbeitung des Vortrags. Auf Seite 32 erfahren Sie mehr über die Autorin.

1 *Schild*, in: Wolff/Brink, BDSG, 2013, § 3 Rn. 10.

2 *Gola/Klug/Körffer*, in: Gola/Schomerus, BDSG, 12. Auflage 2015, § 3 Rn. 6; *Schild*, in: Wolff/Brink (Fn. 1), § 3 Rn. 10.

3 Art. 29-Datenschutzgruppe, WP 80, S. 5 (dort in Fn. 11); *Dammann*, in: Simitis, BDSG, 8. Auflage 2014, § 3 Rn. 73.

4 *Schild*, in: Wolff/Brink (Fn. 1), § 3 Rn. 151.

5 *Schild*, in: Wolff/Brink (Fn. 1), § 3 Rn. 151; *Simitis*, in: Simitis (Fn. 3), § 3 Rn. 256.

indem erhöhte Anforderungen an die Wirksamkeit einer Einwilligung und die Rechtfertigung von deren Erhebung, Verarbeitung und Nutzung gestellt werden.[6]

Auch wenn biometrische Daten hinsichtlich der vorstehend dargestellten Missbrauchsgefahr und daraus resultierenden Schutzbedürftigkeit mit Gesundheitsdaten vergleichbar sind, lässt die Definition und abschließende Aufzählung der besonderen Arten personenbezogener Daten solche Erwägungen gerade nicht zu. Missbrauchspotential und Schutzbedürftigkeit sind keine Tatbestandsmerkmale des § 3 Abs. 9 BDSG. Aus der Einordnung als „reguläre" personenbezogene Daten folgt auch nicht zwangsläufig ein geringeres Schutzniveau. Die Rechtfertigungstatbestände der §§ 28, 29 BDSG enthalten stets eine Interessenabwägung. Die erhöhte Schutzbedürftigkeit biometrischer Daten ist – unabhängig davon, ob es sich um besondere Arten personenbezogener Daten i. S. d. Legaldefinition handelt – in diese Abwägung einzustellen.

Soweit gesperrte Spieler in der Sperrdatei eines Spielhallenbetreibers geführt werden, ist damit nicht ohne weiteres eine Aussage über deren Gesundheitszustand (Spielsucht) getroffen. Vielmehr ist danach zu differenzieren, nach welchen Kriterien die Personen in die Sperrdatei aufgenommen werden. Soweit dies z. B. aufgrund eines Hausverbots wegen ungebührlichen Verhaltens geschieht oder aufgrund einer Selbstsperre, deren Gründe dem Spielhallenbetreiber nicht bekannt sind, ist damit nicht ohne weiteres eine Aussage zur Spielsucht verbunden.

Vereinzelt lässt sich aufgrund biometrischer Daten eine Aussage über den Gesundheitszustand einer Person treffen. So kann z. B. der Augenhintergrund einer Person Rückschlüsse auf Diabetes oder Bluthochdruck zulassen. In diesen Fällen handelt es sich ausnahmsweise um personenbezogene Daten besonderer Art.

II. Datenschutzrechtliche Rechtfertigung biometrischer Zugangskontrollen

Hintergrund der Überlegung, in Spielhallen biometrische Zugangskontrollen einzurichten, ist die Verpflichtung der Spielhallenbetreiber, gesperrten Spielern den Zutritt zur Spielhalle zu verwehren.[7] Herkömmlicherweise erfolgt die Zugangskontrolle durch den Abgleich des Personalausweises bzw. des Reisepasses mit einer Sperrliste. Dies schafft in der Praxis jedoch ein erhebliches Zugangshemmnis für nicht gesperrte Spieler, in dessen Folge die Spielhallenbetreiber Umsatzrückgänge verzeichnen und die Gefahr besteht, dass die Spieler ins illegale Spiel abwandern. Ein biometrisches Erkennungssystem könnte daher eine Alternative zur Zugangskontrolle durch Ausweisvorlage sein.

Durch biometrische Zugangskontrollen kann gerade im Referenzbeispiel Spielhallen ein hohes Maß an Zuverlässigkeit ohne Zugangshemmnis geschaffen werden. Hierzu bedarf es einer Erhebung der biometrischen Gesichtsdaten jeglicher Spielhallenbesucher, um diese mit den Daten der gesperrten Spieler abzugleichen. In einem datenschutzrechtlich sensibilisierten Rechtsraum wie Deutschland gestaltet sich die Rechtfertigung einer solch generellen Datenerhebung traditionell als schwierig. Dennoch können die Interessen der Spielhallenbetreiber – insbesondere das wirtschaftliche Interesse an einem möglichst geringen Zugangshemmnis für die nicht gesperrten Spieler – die pauschale Datenerhebung im Ergebnis rechtfertigen, sofern die Daten der nicht gesperrten Spieler nur für den Abgleich mit der Sperrdatei erhoben und nicht dauerhaft gespeichert werden.

1. Rechtfertigungsbedürftige Verfahrensschritte

Unabhängig von der individuellen technischen Gestaltung gliedern sich sämtliche biometrische Erkennungsverfahren in drei Phasen der Datenverarbeitung, die jeweils der datenschutzrechtlichen Rechtfertigung bedürfen. Zunächst werden im Rahmen des sog. „Enrolments" die Rohdaten des Nutzers im System registriert (Erheben). Anschließend werden aus diesen Rohdaten die für das jeweilige Erkennungsverfahren relevanten Referenzdaten, sog. „Templates", gewonnen (Verarbeiten). Im letzten Schritt, dem sog. „Matching", werden die jeweils präsentierten Daten mit den zuvor abgespeicherten Referenzdaten verglichen (Erheben und Verarbeiten).[8] In diese drei Phasen der Datenverarbeitung sind auch biometrische Systeme zur Zugangsregelung in Spielhallen gegliedert.

Vorstellbar ist z. B. eine Gesichtserkennungssoftware, die aus den Echtzeitvideobildern des Eingangsbereichs Gesichtsbilder extrahiert und diese mit den Referenzdaten der gesperrten Spieler abgleicht (siehe zu einer für ein Pilotprojekt der Merkur Spielothek bereits entwickelten Technologie den Beitrag von Pampus, Zugangskontrolle mittels anonymer Gesichtserkennung, S. 22).

Sowohl das Erheben der Rohdaten bei den zu sperrenden Spielern als auch die Verarbeitung dieser Rohdaten zu Referenzdaten bedürfen nach § 4 Abs. 1 BDSG einer datenschutzrechtlichen Rechtfertigung, ebenso das temporäre Erheben der Vergleichsdaten bei sämtlichen Besuchern der Spielhalle.

2. Datenschutzrechtliche Rechtfertigung

Die datenschutzrechtliche Zulässigkeit der beschriebenen Phasen der Datenverarbeitung kann sich für einen privaten Systembetreiber aus einer wirksamen Einwilligung nach § 4a BDSG oder aus dem Erlaubnistatbestand des § 28 Abs. 1 S. 1 Nr. 2 BDSG ergeben.

a) Einwilligung

Denkbar ist, von gesperrten Spielern eine Einwilligung in die Erhebung der Rohdaten und deren Verarbeitung zu Referenzdaten einzuholen. Dazu müsste der Betroffene ausdrücklich in die Erhebung seines Lichtbilds und Extraktion der biometrischen Daten zur Erstellung einer Referenzdatenbank einwilligen. Die Freiwilligkeit einer solchen Einwilligung ist jedoch fraglich. Bei sog. Fremdsperren, bei denen Angehörige oder Dritte die Spielersperre beantragen, z. B. bei Spielsucht oder Überschuldung mit existenziellen Auswirkungen auf die Familie, scheint die Einwilligung schon a priori ausgeschlossen.

---

6 *Gola/Klug/Körffer*, in: Gola/Schomerus (Fn. 2), § 3 Rn. 56.

7 Diese Verpflichtung besteht in mehreren Bundesländern und ergibt sich aus den Spielhallengesetzen des jeweiligen Bundeslandes. Vgl. hierzu beispielsweise § 5 Abs. 3 SpielhG Schleswig-Holstein, § 6 Abs. 6 S. 1 SpielhG Berlin und § 4 Abs. 1 S. 2 Nr. 5 SpielhG Bremen.

8 Bundesamt für Sicherheit in der Informationstechnik, Grundsätzliche Funktionsweise biometrischer Verfahren, https://www.bsi.bund.de/cln_174/DE/Themen/Biometrie/AllgemeineEinfuehrung/allgemeineeinfuehrung_node.html, zuletzt abgerufen am 22.9.2015.

Aber auch bei einer Selbstsperre auf Initiative des Spielers erfüllt das Handeln des Betroffenen unter Umständen nicht die hohen Anforderungen an die Freiwilligkeit, wenn die Selbstsperre nur bei Einwilligung in die Erhebung und Verarbeitung biometrischer Daten durchgeführt und keine Alternative zur biometrischen Zugangskontrolle angeboten wird. Die Verknüpfung mit einer Leistung lässt die Freiwilligkeit der Einwilligung nicht per se entfallen. Soweit die Selbstsperre aber aufgrund von Spielsucht existenzielle Bedeutung für die Privat- und Vermögenssituation des Spielers hat, spricht viel dafür, dass die Verknüpfung von Sperre und Einwilligung eine die Freiwilligkeit ausschließende Zwangswirkung mit sich bringt.[9]

Die Einholung einer ausdrücklichen Einwilligung sämtlicher Spielhallenbesucher in die Erhebung der Vergleichsdaten zum Abgleich mit den Referenzdaten scheidet schon mangels Praxistauglichkeit aus. Erforderlich wäre, dass jeder Besucher schriftlich oder zumindest mündlich noch vor Datenerhebung erklärt, hiermit einverstanden zu sein. Das hieraus resultierende Zugangshemmnis wäre mindestens genauso intensiv wie individuelle Ausweiskontrollen.

Mit einem wesentlich geringeren Zugangshemmnis wäre die konkludente Einwilligung der Besucher verbunden. Vorstellbar wäre z. B. das Anbringen von Schildern mit dem Hinweis, dass der Eingangsbereich der Spielhalle videoüberwacht ist und der Besucher mit dem Betreten der Räumlichkeiten in diese Überwachung und das damit verbundene Auslesen seiner Gesichtsdaten und deren Abgleich mit einer Referenzdatenbank einwilligt. In dem Betreten der Spielhalle in Kenntnis dieser Maßnahmen wäre die Einwilligung des Besuchers in diese Maßnahmen zu sehen.

Grundsätzlich gibt es im Datenschutzrecht die Möglichkeit der konkludenten Einwilligung.[10] Allerdings wäre es mit erheblichen Risiken verbunden, hier mit einer solchen Lösung zu arbeiten: So hat das OVG Lüneburg jüngst entschieden, dass selbst bei Hinweisen auf Videoüberwachung, „nicht die Schlussfolgerung gezogen werden [kann], dass jeder Betroffene allein durch das Betreten des Gebäudes konkludent in die Datenerhebung und -verarbeitung seiner Bildaufnahme einwilligt."[11] In Anwendung dieser Rechtsprechung scheidet daher eine konkludente Einwilligung erst recht aus, wenn – wie im Anwendungsfall der Spielhallen – während der Echtzeitvideoüberwachung zusätzlich noch biometrischen Gesichtsdaten ausgelesen und mit einer Referenzdatenbank abgeglichen werden.

b) Interessenabwägung nach § 28 Abs. 1 S. 1 Nr. 2 BDSG

aa) Erhebung der Referenzdaten der gesperrten Spieler

Die Erhebung von Referenzdaten der gesperrten Spieler kann auf den Erlaubnistatbestand des § 28 Abs. 1 S. 1 Nr. 2 BDSG gestützt werden, da es um die Verarbeitung personenbezogener Daten zur Erfüllung eigener Geschäftszwecke geht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder gelangt in einer Entschließung zu der Überzeugung, dass die Erhebung biometrischer Referenzdaten nur bei Vorliegen einer wirksamen Einwilligung nach § 4a BDSG erfolgen könne.[12] Hiernach wäre es schon a priori ausgeschlossen, eine Erhebung biometrischer Referenzdaten auf eine Erlaubnisnorm wie § 28 Abs. 1 S. 1 Nr. 2 BDSG zu stützen. Dieses Normverständnis ist allerdings abzulehnen, da der Wortlaut des § 28 Abs. 1 BDSG die Anwendbarkeit der Erlaubnistatbestände einzig an das Vorliegen personenbezogener Daten und die Erfüllung eigener Geschäftszwecke knüpft.[13] Insbesondere besteht keine Hierarchie zwischen den Rechtfertigungstatbeständen Einwilligung und Interessenabwägung. Hinsichtlich der Art der Daten statuiert lediglich § 28 Abs. 6 BDSG verschärfte Rechtfertigungsvoraussetzungen für die Erhebung und Verarbeitung besonderer personenbezogener Daten. Soweit keine besonderen personenbezogenen Daten betroffen sind,[14] ist § 28 Abs. 1 S. 1 Nr. 2 BDSG anwendbar.

Der Spielhallenbetreiber hat ein berechtigtes Interesse i. S. d. § 28 Abs. 1 S. 1 Nr. 2 BDSG an der Erhebung und Verarbeitung der biometrischen Daten der gesperrten Spieler. Berechtigt ist jedes tatsächliche Interesse wirtschaftlicher oder ideeller Natur.[15] Für Spielhallen besteht überwiegend die Verpflichtung zur Zugangskontrolle.[16] Diese begründet das berechtigte Interesse der Betreiber, durch die Erhebung und Verarbeitung der biometrischen Referenzdaten die Voraussetzungen zu schaffen, um ihrer gesetzlichen Verpflichtung gerecht zu werden.

Zur Wahrung dieses berechtigten Interesses ist die Erhebung der biometrischen Referenzdaten auch erforderlich. Zu verneinen wäre dies nur, wenn das Ziel der Datenverarbeitung auch durch eine weniger intensive Maßnahme erreicht werden könnte und diese Alternative dem Systembetreiber zumutbar wäre.[17] Wegen der geringeren Zahl pro Person erhobener Daten und der niedrigeren Eingriffsintensität handelt es sich beim ausschließlichen Erheben der Personalausweisdaten (z. B. Name und Adresse) im Vergleich zum kumulativen Erheben von Ausweisdaten und biometrischen Gesichtsdaten um ein milderes Mittel. Das ausschließliche Erheben von Personalausweisdaten hätte jedoch zur Folge, dass das Verfahren der biometrischen Zugangskontrolle in Spielhallen gänzlich ausscheidet. Ohne Referenzdatenbank ist das „Matching" schon denklogisch ausgeschlossen. Eine Zugangskontrolle könnte somit nur durch die Prüfung des Personalausweises jedes einzelnen Besuchers gewährleistet werden. Die Personalausweiskontrolle ist aber nicht in gleicher Weise wie eine biometrische Zugangskontrolle zum Ausschluss gesperrter Spieler geeignet, z. B. aufgrund des Risikos der Verwendung fremder bzw. gefälschter Ausweise oder wegen eines Fehlers des Kontrollpersonals. Die Personalausweiskontrolle ist dem Systembetreiber als Alternative auch nicht zumutbar, weil die individuelle Kontrolle jedes Besuchers ein massives Zugangshemmnis schafft, welches – wie die Praxis bereits gezeigt hat – die wirtschaftliche Betätigungsfreiheit einschränkt und zu erheblichen Umsatzrückgängen führt.

Die schutzwürdigen Interessen der gesperrten Spieler an dem Ausschluss der Erhebung und Verarbeitung biometrischer Daten überwiegen nicht. Im Rahmen dieser Interessenabwägung ist hinsichtlich des berechtigten Interesses

9 *Taeger*, in: Taeger/Gabel, BDSG, 2. Auflage 2013, § 4a Rn. 56 f.
10 *Taeger*, in: Taeger/Gabel (Fn. 13), § 4a Rn. 41 ff.; *Kühling*, in: Wolff/Brink (Fn. 1), § 4a Rn. 50; a. A.: *Simitis*, in: Simitis (Fn. 3), § 4a Rn. 44.
11 OVG Lüneburg, 29.9.2014 – 11 LC 114/13, CR 2015, 39, 40 Rn. 37.
12 87. Konferenz der Datenschutzbeauftragten des Bundes und der Ländern, Biometrische Gesichtserkennung durch Internetdienste – Nur mit Wahrung des Selbstbestimmungsrechts Betroffener!, S. 1 f., Stand: 27.3.2014.
13 *Gola/Klug/Körffer*, in: Gola/Schomerus (Fn. 2), § 28 Rn. 2.
14 Siehe dazu oben I.
15 *Wolff*, in: Wolff/Brink (Fn. 1), § 28 Rn. 59.
16 Siehe dazu oben II.1.
17 *Simitis*, in: Simitis (Fn. 3), § 28 Rn. 108.

der gesperrten Spieler an einer datenschonenden Zugangskontrolle zu berücksichtigen, dass die biometrische Gesichtserkennung das informationelle Selbstbestimmungsrecht beeinträchtigt, insbesondere weil keine nichtbiometrische Alternative besteht. Allerdings steht die biometrische Gesichtserkennung wegen des höheren Schutzniveaus im Einklang mit dem Gesetzeszweck der Landesspielhallengesetze, einen Beitrag zur aktiven Suchtprävention zu leisten.[18] Zugunsten der Spielhallenbetreiber ist in die Interessenabwägung einzustellen, dass die Auferlegung der Zugangskontrollen ohnehin schon eine erhebliche (wirtschaftliche) Belastung ist. Zumindest bei der konkreten Ausgestaltung der Zugangskontrollen muss den Spielhallenbetreibern daher ein gewisses Maß an Flexibilität zugestanden werden.

Die Missbrauchsgefahr kann durch technische und organisatorische Sicherheitsvorkehrungen reduziert werden, z. B. durch Schrumpfung der Rohdaten zu „Templates" und Löschung der zur Gewinnung dieser „Templates" erhobenen Rohdaten. Auch kann sich der Betreiber bestimmten Selbstbeschränkungen unterwerfen, insbesondere: (i) keine Weitergabe von biometrischen Daten an Dritte, (ii), keine Speicherung und Auswertung von biometrischen Zusatzinformationen, (iii) kein Hinzuspeichern und Verknüpfen mit sonstigen Daten der Person, (iv) strikte Zweckbindung, keine Zweckänderung, (v) überprüfbare Löschung innerhalb festgesetzter Löschfristen oder nach Zweckfortfall (z. B. Ende der Sperre). Sofern die erforderlichen Sicherheitsvorkehrungen getroffen werden, ist das grundsätzliche Missbrauchsrisiko nicht als besonders schwerwiegend einzustufen.

bb) Erhebung und Abgleich der Vergleichsdaten aller Spielhallenbesucher

Die Interessen der Spielhallenbesucher sind anders gelagert als die der gesperrten Spieler.

Im Rahmen der Referenzdatenerhebung erheben und verarbeiten die Spielhallenbetreiber biometrische Daten von gesperrten Spielern, um ihre Pflicht zur Durchsetzung der Spielersperre zu erfüllen. Auch wenn hierzu keine Einwilligung eingeholt wird, werden die Daten doch in gewisser Weise auf Veranlassung der betroffenen Personen erhoben und verarbeitet. Im Gegensatz hierzu hat die pauschale Datenerhebung/-auswertung bei sämtlichen Spielhallenbesuchern keinen konkreten Anlass. Der weit überwiegende Teil der Besucher ist nicht gesperrt, muss sich aber dennoch der Erhebung und Auswertung der biometrischen Gesichtsdaten aussetzen, um einer legalen Freizeitbeschäftigung nachzugehen.

Trotz der darin liegenden Beeinträchtigung des informationellen Selbstbestimmungsrechts sämtlicher Spielhallenbesucher hat die Erhebung biometrischer Vergleichsdaten im Hinblick auf die nicht gesperrten Spieler auch eine datenschonende Komponente. Die Alternative zur Erhebung biometrischer Vergleichsdaten wäre die individuelle Ausweiskontrolle jedes Spielhallenbesuchers. Hiermit wäre zwingend eine Offenbarung der Identität verbunden, die beim automatisierten Erheben biometrischer Vergleichsdaten im Hinblick auf die nicht gesperrten Spieler vermieden würde. Der Spielhallenbesucher muss dem Spielhallenpersonal nicht Name, Geburtsdatum und Adresse offenbaren, bleibt dem Personal gegenüber also „anonym".

Um Gefahren wie den Identitätsdiebstahl, die Auswertung von Zusatzinformationen und die Erstellung von Bewegungsprofilen zu minimieren, muss im privaten Bereich dasselbe Schutzniveau wie im öffentlichen Bereich gewährleistet werden. § 17 S. 4 PAuswG sieht vor, dass die zur Echtheitskontrolle beim Ausweisinhaber erhobenen Vergleichsdaten nach Beendigung der Prüfung unverzüglich zu löschen sind. Nichts anderes kann hinsichtlich der erhobenen biometrischen Vergleichsdaten in Spielhallen gelten.

Sofern diese Sicherheitsvorkehrungen getroffen werden, überwiegt vor dem Hintergrund des datenschonenden Charakters, der Zuverlässigkeit und der weniger schweren wirtschaftlichen Folgen einer biometrischen Gesichtserkennung auch im Hinblick auf das kurzfristige Erfassen und Abgleichen der biometrischen Vergleichsdaten das schutzwürdige Interesse der Spielhallenbetreiber. Im Ergebnis sind diese Phasen der biometrischen Datenverarbeitung mithin ebenfalls gem. § 28 Abs. 1 S. 1 Nr. 2 BDSG gerechtfertigt.

3. Potentiell entgegenstehende landesrechtliche Spielhallengesetze

Zu klären ist das Verhältnis der datenschutzrechtlichen Rechtfertigung zu den diesbezüglichen Vorgaben der landesrechtlichen Spielhallengesetze. Die Rechtslage ist unterschiedlich. Teilweise gibt es die Verpflichtung der einzelnen Spielhallenbetreiber, individuelle Sperrlisten zu führen, z. B. in Berlin, Schleswig-Holstein, Bremen, Baden-Württemberg (geplant), teilweise bundeslandweite Sperrsysteme für alle Spielhallen eines Bundeslandes, z. B. in Hessen (OASIS) oder Rheinland-Pfalz. Vereinzelt gibt es keine gesetzliche Sperrpflicht, z. B. in Bayern (hier nur freiwillige Hausverbote durch die Spielhallenbetreiber).

Soweit in einigen Bundesländern eine individuelle Sperrliste zu führen ist, ist die Zulässigkeit der Erhebung biometrischer Daten als Referenzdaten nicht eindeutig geregelt. In Schleswig-Holstein dürfen nach § 5 Abs. 3 SpielhG zum Zwecke der Kontrolle einer Selbstsperre die zur Identifizierung der betreffenden Personen erforderlichen personenbezogenen Daten erhoben und für die Dauer der Sperre gespeichert und im Rahmen einer Zutrittskontrolle entsprechend § 5 Abs. 2 SpielhG verwendet werden. Dies scheint die Erhebung biometrischer Daten und biometrische Zugangskontrollen einzuschließen. Jedenfalls bei Minderjährigen ist das Aufenthaltsverbot in Spielhallen durch die Vorlage eines amtlichen Ausweispapiers *oder eine vergleichbare Identitätskontrolle* zu gewährleisten. Die Ausweiskontrolle ist also nicht die einzige Möglichkeit. Eine entsprechende Regelung fehlt für gesperrte Spieler. Es ist jedoch kein Grund ersichtlich, warum nicht auch bei diesen anstelle von Ausweiskontrollen vergleichbare Systeme zum Einsatz kommen können, zu denen dann auch biometrische Zutrittskontrollen zu zählen wären. Vergleichbares gilt in Berlin nach § 6 Abs. 6 und Abs. 4 SpielhG.

Was die Erhebung biometrischer Daten als Vergleichsdaten angeht, ist eine Videoüberwachung zur Zutrittskontrolle explizit zulässig (§ 7 Abs. 1 SpielhG Schleswig-Holstein). Allerdings ist problematisch, ob dies eine ausreichende gesetzliche Grundlage für die Extrahierung der Gesichtsbilder

18 Vgl. beispielhaft Gesetzesbegründung zur Selbstsperre in Sachsen-Anhalt: LT-Drs. Sachsen-Anhalt 6/914, 13.3.2012, S. 66.

und deren Abgleich mit der Sperrdatei ist, insbesondere bzgl. der nicht gesperrten Spieler. Regelungen zur Speicherung, Löschung und Zweckbindung von biometrischen Daten fehlen. Hier sind das BDSG und die oben dargestellten Grundsätze anzuwenden.

Sofern demgegenüber in einzelnen Bundesländern (bisher in Hessen und Rheinland-Pfalz) landesweite, zentrale Sperrdateien bestehen, sind die Spielhallenbetreiber verpflichtet, diese zu nutzen. Sie haben keinen direkten Einfluss der Spielhallenbetreiber auf die Struktur des Sperrsystems (insbesondere auf die Art der abzugleichenden Daten), sondern unterliegen einem bußgeldbewehrten Anschlusszwang. Lichtbilder dürfen nach § 11 Abs. 1 Nr. 6 HSpG zwar als Referenzdaten erhoben werden. Die Extrahierung von biometrischen Referenzdaten (Gesichtsgeometrie) aus diesen Lichtbildern ist aber nicht ausdrücklich geregelt (in Rheinland-Pfalz Erhebung von Lichtbildern nur mit Einwilligung). Videoüberwachung ist zur Zutrittskontrolle explizit zulässig (§ 7 Abs. 1 HSpG), sonstige Vorgaben zur Art und Weise der Zugangskontrolle gibt es in Hessen nicht (in Rheinland-Pfalz müssen bei Einlasskontrollen die Personalien festgestellt und mit der Sperrdatei abgeglichen werden). Allerdings ist problematisch, ob dies eine ausreichende gesetzliche Grundlage für die Extrahierung der Gesichtsbilder und deren Abgleich mit der Sperrdatei ist, insbesondere bzgl. der nicht gesperrten Spieler. Ausdrücklich ausgeschlossen sind biometrische Zugangskontrollen damit aber ebenfalls nicht. Bei Minderjährigen geht die Gesetzesbegründung zwar von „ausnahmsloser Ausweiskontrolle“ aus, auf gesperrte Spieler bezieht sich dies jedoch nicht.[19] Regelungen zur Speicherung, Löschung und Zweckbindung von biometrischen Daten fehlen.

Auch hier sind das BDSG und die oben dargestellten Grundsätze anzuwenden. Daher sind biometrische Zugangskontrollen auch hier grundsätzlich zulässig. Die Erhebung und Verarbeitung personenbezogener Daten ist bei privaten Unternehmen (nicht-öffentlichen Stellen, § 1 Abs. 2 Nr. 3 BDSG) vorrangig durch das BDSG geregelt. Das BDSG ist nur gegenüber besonderen datenschutzrechtlichen Regelungen des Bundes subsidiär (§ 1 Abs. 3 S. 1 BDSG), nicht aber gegenüber Landesrecht. Ohnehin ist die Kompetenz der Länder für das Spielhallenrecht derzeit beim Bundesverfassungsgericht auf dem Prüfstand. Gleichwohl diente es der Rechtsklarheit, biometrische Zugangskontrollen und deren Anforderungen (bundesgesetzlich) ausdrücklich zu regeln. Dies gilt insbesondere auch im Hinblick auf Bundesländer wie Bremen, wo Ausweiskontrollen verpflichtend sind (§ 4 Abs. 1 Nr. 5 BremSpielhG).

4. Benachrichtigung der Betroffenen

Von der Frage der Zulässigkeit der Datenverarbeitung zu trennen ist die Pflicht zur Benachrichtigung der Betroffenen über (i) die Identität der verantwortlichen Stelle, (ii) den Zweck der Datenerhebung und -verarbeitung sowie (iii) potentielle Datenempfänger (§ 4 Abs. 3 Satz 1 BDSG). Da bei der Erhebung der Referenzdaten regelmäßig die Mitwirkung des gesperrten Spielers erforderlich sein wird und er dadurch davon Kenntnis erlangt, wird die Benachrichtigungspflicht in erster Linie beim Erheben der Vergleichsdaten der nicht gesperrten Spielhallenbesucher und deren Abgleich mit der Referenzdatenbank virulent. Die individuelle Information jedes einzelnen Spielhallenbesuchers ist z. B. durch Handzettel oder mündliche Ansprache denkbar, was aber nicht gerade praxistauglich erscheint. Ob ein Aushang ausreichend ist, wird davon abhängen, wie deutlich sichtbar dieser ist, d. h. es kommt auf Platzierung, Größe, Text/Symbolik, Sprache(n) und Lichtverhältnisse an.

19 LT-Drs. 18/5186, S. 14.

Dr. Michael Schneider, Bundesdruckerei GmbH, Berlin*

Effektiv und nutzerfreundlich

Biometrie schützt Zugänge zu Gebäuden und Systemen

Biometrische Zugangskontrollen werden zunehmend als Möglichkeit zur Umsetzung gesetzlich geforderter Zugangsbeschränkungen abseits klassischer Hochsicherheitsanwendungen verstanden. Dieser Artikel diskutiert die technischen Komponenten eines Gesamtsystems zur biometrischen Zugangskontrolle und gibt praktische Beispiele für mögliche Realisierungen. Schwerpunkte liegen dabei auf den Aspekten Sicherheit, Compliance, Einfachheit sowie Datenschutz.

I. Einleitung

Die Kontrolle und Beschränkung der Zugänge zu Gebäuden und technischen Systemen gewinnen an Bedeutung. Gründe hierfür sind neben einem gestiegenen Sicherheitsbedürfnis zunehmend auch verschärfte Compliance-Vorgaben, die die explizite Erteilung von Zutrittsrechten (im Sinne von Positivlisten) oder die Durchsetzung von Zutrittsbeschränkungen (im Sinne von Negativlisten) für bestimmte Nutzergruppen fordern. Compliance-Vorgaben können gesetzlicher Natur sein, aber auch aus den Bedürfnissen sonstiger interner sowie externer Stakeholder erwachsen.

Bestehende technische Lösungen zur Kontrolle von Zugängen, wie Passcodes oder elektronische Ausweise mit einfacher RFID-Funktion, besitzen entscheidende Nachteile bei der Prüfung personenbezogener Berechtigungen. Die Möglichkeit der problemlosen Weitergabe von Passcodes und Ausweisen an andere Personen begünstigt eine missbräuchliche Verwendung. Dies ist nicht nur aus Sicher-

* Auf Seite 32 erfahren Sie mehr über den Autor.

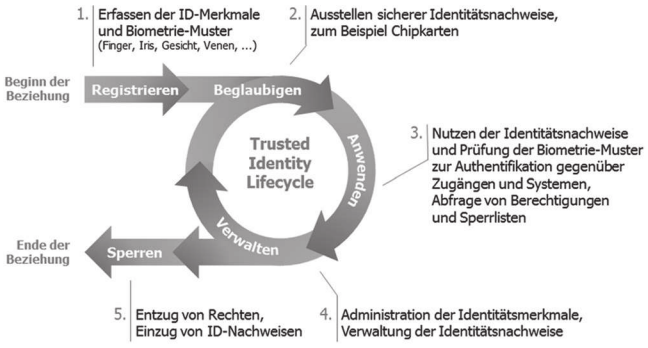
heitsgründen, sondern insbesondere auch aus Compliance-Sicht problematisch.

Abhilfe schafft hier die Nutzung biometriebasierter Prüfverfahren, die ein unveränderliches körperliches Merkmal der zu überprüfenden Person wie beispielsweise einen Fingerabdruck oder die spezifische Gesichtsgeometrie berücksichtigen. Da diese Merkmale in der Regel untrennbar und eindeutig mit einer bestimmten Person verknüpft sind, ist eine Weitergabe nicht ohne weiteres möglich. Für den Anwender sind solche Verfahren zudem einfacher zu nutzen, da das Merken von Passwörtern sowie die Gefahr des Vergessens entfallen.

Bei der konkreten Ausgestaltung biometrischer Zutrittskontrollsysteme ergeben sich vier kritische Erfolgsfaktoren im Spannungsfeld zwischen Effektivität und Nutzerfreundlichkeit:

- Sicherheit: Kann die technische Lösung bestehende Zugangsregelungen zuverlässig durchsetzen und eine Umgehung wirkungsvoll verhindern?
- Compliance: Wird Prüfpflichten belegbar nachgekommen, um Haftungsrisiken bei Verstößen zu minimieren, sowohl in automatischen als auch in manuellen Prozessen?
- Einfachheit: Können die Aufnahme der Identitäten und Verwaltung der Berechtigungslisten sowie die Nutzung der Zutrittskontrolle ohne Spezialkenntnisse durchgeführt werden?
- Datenschutz: Werden biometrische Personeninformationen ausreichend geschützt hinterlegt und sicher genutzt?

Von Relevanz bei der Beurteilung dieser Fragen ist dabei neben dem eigentlichen biometrischen Prüfverfahren insbesondere die Gestaltung des Gesamtsystems inklusive seiner Verwaltungs- und Hintergrundprozesse. Dieser Artikel diskutiert aus technischer Sicht die Komponenten eines biometrischen Zutrittskontrollsystems entlang des allgemeinen „Trusted Identity Lifecycle“. Er beschreibt die grundsätzlichen Schritte vertrauenswürdiger identitätsbasierter Anwendungen.



Der „Trusted Identity Lifecycle“ gliedert sich in die folgenden 5 Phasen:

1. Initiale Identitätsprüfung: Prüfung der Personenidentität des Nutzers und Erfassung der biometrischen Referenzmuster

2. Ausstellung von ID-Token: Ausgabe eines digitalen oder physischen Identifizierungsmerkmals (so genannten Token), wie einer Chipkarte, mit der sich der Nutzer später gegenüber dem Zutrittskontrollsystem ausweisen kann (entfällt bei einer zentralen Speicherung der biometrischen Referenzmuster, siehe Diskussion Kapitel IV)

3. Anwendung: Nutzung der Identifizierungsmerkmale und Prüfung der biometrischen Referenzmuster zur Freigabe des Zugangs

4. Verwaltung: Verwaltung der ID-Token und Berechtigungen, ggf. Neuausstellung von ID-Token oder Aktualisierung von biometrischen Referenzmustern

5. Löschung: Entzug von ID-Token und Rechten bzw. Sperrvermerken, Löschung der Daten aus dem System

Im Folgenden werden die einzelnen Phasen näher diskutiert sowie Beispiele für eine konkrete Umsetzung gegeben.

II. Identitätsprüfung

Grundsätzlich ist bei jeder Art der Zugangskontrolle zu verhindern, dass sich Personen mit fälschlicherweise behaupteten Identitäten Zugang zu einem geschützten Bereich erschleichen, beispielsweise, weil die tatsächliche Identität auf einer Sperrliste vermerkt ist oder die behauptete Identität Zugang über eine Positivliste erlaubt.

Da bei der biometrischen Zugangskontrolle die Gewährung des eigentlichen Zugangs über die Prüfung eines biometrischen Merkmals des Benutzers erfolgt, ist hier bei der initialen Aufnahme der biometrischen Referenzmuster sicherzustellen, dass die Muster der korrekten Person aufgenommen werden. Selbst bei integrierten oder an sich sogar anonymen Biometrieverfahren ist daher in der Regel zunächst eine Prüfung der Personenidentität erforderlich.

Das Mittel der Wahl zum Nachweis der Identität ist dabei in aller Regel ein offizielles Ausweisdokument wie der Personalausweis oder ein Reisepass. Abhängig von den konkreten Anforderungen an Sicherheit und Compliance gilt es dabei insbesondere, Umgehungsversuche durch die Vorlage falscher oder manipulierter Dokumente zu verhindern.

Eine manuelle Prüfung von Ausweisdokumenten ist dabei aus vielen Gründen problematisch: Zusätzlich zu mangelnder Belegbarkeit sowie unzureichender Prüfqualität durch Zeitdruck im Tagesgeschäft fehlt insbesondere bei ungeschulten Anwendern das Wissen über Echtheitsmerkmale von Ausweisdokumenten. Dies gilt besonders, wenn auch ausländische Ausweispapiere zu überprüfen sind. Für eine effiziente und belastbare Prüfung empfiehlt sich daher der Einsatz technischer Hilfsmittel:

1. Im Rahmen von Online-Anwendungen

Soll eine Vorregistrierung von Nutzern zum Beispiel über ein Webportal oder einen Online-Kiosk erfolgen, so bietet sich die Nutzung der eID-Funktionalität des deutschen Personalausweises oder des elektronischen Aufenthaltstitels an. Diese Funktionalität kann über eine Webservice-Schnittstelle in beliebige Web-Anwendungen integriert werden und von jedem PC mit Webbrowser und geeignetem Lesegeräte aus genutzt werden. Sie erlaubt nach Zustimmung des Besitzers das Auslesen von Informationen wie Name, Anschrift und Alter aus dem Personalausweis oder dem elektronischen Aufenthaltstitel.

2. Vor Ort

Für die eigentliche Aufnahme der Biometrie-Muster am Empfang oder einem überwachten Self-Service-Kiosk be-

steht die Möglichkeit, vorgelegte Ausweisdokumente optisch auf Echtheit zu überprüfen. Entsprechende Prüfgeräte, wie sie zum Beispiel von der Bundesdruckerei angeboten werden, können dabei nationale sowie internationale Personaldokumente aus mehr als 160 Ländern innerhalb weniger Sekunden erkennen und prüfen. Ein vollautomatischer Prüfbericht belegt die Echtheitskontrolle nachweislich und bestätigt die Übereinstimmung der Daten im Dokument mit den elektronisch erfassten Daten im System.

III. Ausstellung von ID-Token

Nach Erfassung der biometrischen Referenzmuster müssen diese für die spätere Anwendung aufbewahrt und den Zugangspunkten bereitgestellt werden. Hierzu gibt es verschiedene technische Lösungen, die sich im technischen Aufwand, insbesondere aber auch im resultierenden Schutz der potenziell sensiblen biometrischen Daten unterscheiden.

Aus Anwendersicht ist hierbei insbesondere die sichere Aufbewahrung der biometrischen Muster und die ausreichende Kontrolle über deren Verwendung relevant – letztendlich also die Frage, ob der Nutzer die Hoheit über seine biometrischen Daten behält. Diese Frage ist nicht nur vor dem Hintergrund datenschutzrechtlicher Bestimmungen relevant, sondern spielt auch eine große Rolle bei der Akzeptanz biometrischer Verfahren durch die Anwender.

Abhängig davon, welche Teile der Datenhaltung und Datenverarbeitung sich physisch in der Kontrolle des Nutzers befinden, ergeben sich vier mögliche technische Ansätze mit zunehmendem Grad an Hoheit des Nutzers über seine Daten:

1. Speicherung und Vergleich der Daten im System: keine Datenhoheit

Im einfachsten Fall werden sämtliche Biometrie-Daten ausschließlich im Zutrittskontrollsystem erfasst, gespeichert und bei der Kontrolle verarbeitet. Damit entziehen sie sich vollständig der Kontrolle des Nutzers. Gleichzeitig steigt die Gefahr von Datendiebstahl und Missbrauch. Aus diesen Gründen und der mangelnden Datenhoheit wird diese Variante insbesondere aus Datenschutzgründen als sehr kritisch eingestuft und von vielen Nutzern abgelehnt.

2. Speicherung auf ID-Token, Vergleich im System: mittlere Datenhoheit

In diesem Fall erfolgt die Erfassung der biometrischen Referenzdaten im System, diese werden jedoch im Anschluss auf einem physischen Träger, dem so genannten Token, gespeichert. Diesen trägt der Anwender mit sich, so dass keine zentrale Datenbank mit Biometrie-Daten existiert. Eine Überprüfung kann nur mit Einwilligung des Nutzers erfolgen, da dieser hierzu das Token an ein entsprechendes Lesegerät führen muss. Zur Prüfung werden die biometrischen Referenzmuster aus dem Token ausgelesen und dann innerhalb des Zutrittskontrollsystems ausgewertet. Durch die grundsätzliche Möglichkeit, die Biometrie-Muster aus dem Token auszulesen und unbemerkt vom Nutzer für weitere Dinge zu nutzen, ist die Datenhoheit in diesem Fall als „mittel“ anzusehen.

3. Speicherung und Vergleich auf ID-Token: starke Datenhoheit

Nicht nur die Speicherung der Biometrie-Daten, sondern auch deren Auswertung kann durch einen entsprechenden Token mit integriertem Mikroprozessor übernommen werden. In diesem Fall ist kein Auslesen des Token mehr notwendig; die zu prüfenden Muster werden vielmehr bei jeder Nutzung in den Token übertragen und direkt auf dem Token überprüft. Es erfolgt nur noch eine Rückmeldung, ob sie zu den hinterlegten Referenzmustern passen oder nicht. Durch das Fehlen einer Auslesefunktion sind die Daten auf dem Token sicher verwahrt, so dass diese Architektur eine starke Datenhoheit gewährleistet.

4. Speicherung, Vergleich und Erfassung auf ID-Token: maximale Datenhoheit

In allen bisher genannten Anwendungsfällen liegt es in der Verantwortung des Zutrittskontrollsystems, die initiale Erfassung der Referenzmuster sowie die Erfassung der zu prüfenden Vergleichsmuster vorzunehmen. Dies bedeutet, dass biometrische Daten zumindest temporär im System gehalten und übertragen werden. Der Nutzer muss seinerseits darauf vertrauen, dass diese rückstandslos und schnellstmöglich wieder gelöscht und nicht für andere Zwecke weiterverwendet werden.

Um eine maximale Datenhoheit zu gewährleisten, verfügen modernste Token über eigene Sensoren zur Aufnahme der Biometrie-Muster. Hier erfolgen Aufnahme, Speicherung und Vergleich der Muster einzig auf dem Token, so dass sensible biometrische Daten nie den Verfügungsbereich des Nutzers verlassen. Das Zutrittskontrollsystem stellt an das Token nur noch die Anfrage mit dem Identifizierungswunsch und erhält als Rückmeldung einen Status über die erfolgreiche oder gescheiterte Identifizierung.

Ein Beispiel für solch einen Token zur Gewährleistung maximaler Datenhoheit auf der Basis von Fingerabdrücken hat die Bundesdruckerei auf der CeBIT 2015 vorgestellt. Er hat die Größe einer normalen Kreditkarte und verfügt zusätzlich zu einem Display für Statusmeldungen über einen integrierten Fingerabdrucksensor. Eine eingebaute Antenne übernimmt die berührungslose Kommunikation mit dem Zutrittskontrollsystem und versorgt die Karte gleichzeitig mit Energie, so dass sie ohne integrierte Batterien auskommt und eine unbegrenzte Lebensdauer besitzt.

Bei erstmaliger Benutzung registriert der Nutzer seine Fingerabdrücke direkt auf der Karte. Sie werden dort sicher verschlüsselt hinterlegt. Erhält die Karte von einem Lesegerät die Aufforderung zur Identifikation, wird der Nutzer über einen Hinweistext auf dem Display zur erneuten Auflage des Fingers aufgefordert. Die Daten werden unmittelbar auf der Karte ausgewertet und das Zutrittskontrollsystem über das Ergebnis der Prüfung informiert. So werden zu keinem Zeitpunkt, auch nicht vorübergehend, biometrischen Daten des Nutzers im Zutrittskontrollsystem selbst erfasst, verarbeitet oder gespeichert.

IV. Anwendung

Bei der Anwendung biometrischer Prüfverfahren gilt es zwei wesentliche Aspekte zu betrachten: zum einen die Auswahl des biometrischen Verfahrens selbst und zum an-

deren der Gewährleistung von Vertraulichkeit und Belastbarkeit des Gesamtsystems.

1. Auswahl des biometrischen Prüfverfahrens

Die Anwendung von Biometrie zur Freigabe von Zugängen erfolgt in der Regel durch die Vorlage eines Tokens (siehe Kapitel IV) sowie die Erfassung eines Vergleichsmusters, dass dann im System oder auf dem Token mit dem hinterlegten Referenzmuster verglichen wird.

Bei der Erfassung und Prüfung biometrischer Muster können verschiedenste Verfahren zum Einsatz kommen, die in der Regel ein unveränderliches körperliches Merkmal der zu überprüfenden Person erfassen und zur Wiedererkennung vergleichen. Beispiele für solche Merkmale sind Fingerabdrücke, die Gesichtsgeometrie, die Struktur von Handvenen, Irismuster oder Stimmprofile.

Die existierenden Verfahren unterscheiden sich beispielsweise hinsichtlich

- Anforderungen an die Einsatzumgebung (Beleuchtung, Geräuschpegel, etc.)
- Unterscheidungsleistung (Geschwindigkeit, Fehlerraten, Anzahl unterscheidbarer Individuen, etc.)
- Ansätze zur Manipulationserkennung (insbesondere Lebenderkennung)

Jedes Verfahren hat seine spezifischen Stärken und Schwächen, die es bei einer Entscheidung für oder gegen ein bestimmtes Verfahren zu berücksichtigen gilt. Da der Schwerpunkt dieses Artikels auf der Betrachtung des Gesamtsystems liegt, soll hier lediglich exemplarisch am Beispiel eines bei der Bundesdruckerei für den hoheitlichen Bereich eingesetzten Fingerabdrucklesers auf einige relevante Aspekte eingegangen werden.

Die Nutzung von Fingerabdrücken zur Identifikation hat sich seit Jahren in Anwendungen mit hohem Sicherheitsbedarf bewährt. Insbesondere im staatlichen Umfeld ist diese Technologie seit langem etabliert und akzeptiert. In jüngster Zeit hält sie verstärkt auch im privaten Umfeld Einzug. Vorreiter sind hier die Hersteller von Mobiltelefonen, mit einer guten Nutzerakzeptanz. Dennoch gilt es bei der professionellen Anwendung einige Dinge zu beachten, um Zuverlässigkeit und Nutzerfreundlichkeit der biometrischen Prüfung zu gewährleisten.

Gerade bei einfachen Verfahren können beispielsweise Probleme durch nicht vollständige trockene Finger entstehen. Weitere Fehlerquellen können einfallendes Licht oder eine falsche Positionierung des Fingers gerade bei ungeübten Anwendern sein. Professionelle Prüfgeräte sind auf solche Szenarien optimiert und erzielen auch unter schwierigen Bedingungen gute Ergebnisse mit hohen Erkennungsraten und damit geringen Wiederholversuchen für den Nutzer. Zur Kopplung mit ID-Token (siehe Kapitel IV) verfügen sie darüber hinaus oft über Lesevorrichtungen zur Anbindung von Chipkarten.

2. Vertraulichkeit und Belastbarkeit

Wie oben bereits erläutert, werden biometrischen Daten innerhalb eines Zutrittskontrollsystems idealerweise nur eingeschränkt oder sogar vollständig und ausschließlich unter Hoheit des Nutzers verarbeitet. Für eine effektive Durchsetzung von Zutrittskontrollen müssen jedoch weitere potenziell kritische Daten erhoben, gespeichert, übertragen und verarbeitet werden. Dies umfasst neben Zugangs- oder Sperrlisten auch Daten, die bei der Kommunikation mit den ID-Token oder den einzelnen Komponenten des Systems untereinander anfallen. Diese sind vor beabsichtigtem oder unbeabsichtigtem Mitlesen zu schützen sowie gegebenenfalls für eine spätere Auditierung belegbar zu erheben und manipulationssicher zu speichern.

Für beide Anwendungsfälle – die Verschlüsselung von Nutzer- und Prozessdaten sowie die Belegbarkeit der Integrität elektronischer Aufzeichnungen – existieren praktisch erprobte, zuverlässige technologische Lösungen. Im Zentrum stehen dabei starke kryptographische Verfahren zur Verschlüsselung sowie der so genannten elektronischen Signatur. Zentrales Element für die Sicherheit und Integrität ist dabei, dass die verwendeten öffentlichen Schlüssel von einer vertrauenswürdigen dritten Instanz bestätigt werden, um Manipulationen durch den nachträglichen Austausch von Schlüssel vorbeugen zu können.

Das technologische Mittel der Wahl sind dabei so genannte Verschlüsselungs- und Signaturzertifikate, die von einem akkreditierten Trustcenter, wie es zum Beispiel die Bundesdruckerei unter dem Namen „D-Trust“ betreibt, ausgegeben werden. Sie schützen persönliche Daten auf ID-Token, die (drahtlose) Kommunikation zwischen den Komponenten und verhindern das nachträgliche Verändern von elektronischen Aufzeichnungen in automatischen und manuellen Prozessen.

V. Verwaltung und Löschung

Eine einmalige Identitätsprüfung zur initialen Registrierung ist in der Regel nicht ausreichend für einen zuverlässigen und regelkonformen Betrieb eines biometrischen Zugangskontrollsystems. Angefangen beim Ersatz verlorener oder verlegter ID-Token, der Neuerfassung von biometrischen Merkmalen bei Veränderungen über die Zeit bis hin zur Löschung von Zutrittsrechten und Zutrittsbeschränkungen bei Entfall der Voraussetzungen: In all diesen Fällen kann bei ungenügender Prüfung der Identität Missbrauchspotenzial entstehen.

Dabei ist nicht nur das Erschleichen unerwünschter Berechtigungen ein Problem, auch das ungewollte Entfernen aus einer Positivliste oder Eintragen in eine Sperrliste durch böswillige Dritte gilt es zu verhindern. Nicht zuletzt bei einem Ausfall des Systems durch interne oder externe Faktoren müssen technische und organisatorische Vorkehrungen getroffen werden, um die Zugangsbeschränkung weiterhin durchsetzen zu können.

Vor diesem Hintergrund wird eine Identitätsprüfung entsprechend Kapitel III sowie eine nachweisebare Dokumentation durchgeführter Prüfungen und Maßnahmen entsprechend Kapitel V.2 in aller Regel auch bei der Verwaltung von Nutzern und ID-Token sowie der Verwaltung und Löschung von Zutrittsberechtigungen bzw. Zutrittsbeschränkungen erforderlich sein. Die in den jeweiligen Kapiteln dargestellten Beispiellösungen sind auch hier analog zu verwenden.

VI. Fazit

Um biometrischer Zutrittskontrollen effektiv und nutzerfreundlich zu realisieren, genügt nicht alleine die Auswahl

eines geeigneten biometrischen Prüfverfahrens. Vielmehr ist es erforderlich das System in seiner Gesamtheit detailliert und differenziert zu betrachten. Dabei geht es insbesondere um folgende Fragen: Wie hoch ist die Hürde das System zu überwinden? Wie einfach ist es zu bedienen? Wie sieht es mit dem Datenschutz und der Compliance aus? Mögliche Lösungen sind nie alleine technischer Natur, sondern erfordern immer auch die Berücksichtigung organisatorischer Maßnahmen. Gleichwohl können und sollten diese durch technische Mittel unterstützt, abgesichert sowie belastbar dokumentiert werden.

Der Artikel betrachtet das Thema biometrische Zugangskontrolle aus der Perspektive des technischen Gesamtsystems entlang des „Trusted Identity Lifecycles", weist auf kritische Punkte in der konkreten Anwendung hin und stellt beispielhaft Technologien aus dem Portfolio der Bundesdruckerei als mögliche Lösungsansätze zur Diskussion.

Dr. Jürgen Pampus, Dresden*

Zutrittskontrolle mittels anonymer Gesichtserkennung

I. Einleitung

Die Regelung und Kontrolle des Zutritts zu Casinos und Spielstätten wird immer wichtiger, dabei insbesondere der Abgleich mit Sperrlisten. Hierfür sind verschiedene Lösungen möglich, von der Ausweiskontrolle durch Personal bis zu diversen technischen Systemen. Hier soll untersucht werden, welche Lösungen sich für Spielstätten eignen und wie eine hohe Zuverlässigkeit mit Komfort und dem Schutz persönlicher Daten verknüpft werden kann. Dabei kommen biometrische Systeme, insbesondere Gesichtserkennungstechniken, zum Einsatz.

II. Zugangs- und Zutrittskontrolle

Zugangskontrollsysteme regeln und überprüfen ganz allgemein, ‚wer wann wohin' gehen oder ‚worauf' zugreifen darf. Der Begriff der ‚Zugangskontrolle' wird vor allem in der Informatik verwendet, wenn es um den Zugang zu Informationen oder Informationssystemen geht; auch ‚Zugriffskontrolle' wird gelegentlich verwendet. Hingegen spricht man bei der Regelung und Überprüfung des physischen Zutritts zu Gebäuden, Räumen oder abgegrenzten Geländebereichen von ‚Zutrittskontrolle'. Dieser Begriff soll deshalb im Folgenden verwendet werden, da hier von der Verwendung von biometrischen Verfahren bzw. insbesondere Gesichtserkennungssystemen beim Zutritt zu Gebäuden die Rede sein wird. Biometrische Verfahren werden heute aber auch zur Zugangskontrolle zu Informationen und Geräten wie z. B. Mobiltelefonen benutzt.

Zur Realisierung von Zutrittskontrolle werden eine Reihe verschiedener Methoden verwendet, angefangen vom Augenschein des Pförtners, der alle Zutrittsberechtigten persönlich kennt, bis hin zu ‚eGates' mit Vereinzelung, automatischer Überprüfung des Ausweises und biometrischer Verifikation der Person. Grundsätzlich kann zwischen den folgenden Methoden zur Überprüfung der Berechtigung unterschieden werden:

- Besitz (z. B. Schlüssel, Mitarbeiterausweis, Pass, Token)
- Wissen (z. B. PIN, Passwort)
- Anwesenheit (Biometrie, Personal)
- Kombination von zwei oder mehr Methoden (Stichwort Zweifaktor-Autorisierung).

Weiterhin ist zwischen geschlossenen und offenen Systemen zu unterscheiden. Im ersten Fall ist eine bestimmte Gruppe von Personen im System festgelegt, die zum Zutritt berechtigt sind (z. B. die Mitarbeiter eines Unternehmens). Das offene Verfahren gewährt beliebigen Personen Zutritt, schließt jedoch beispielsweise Personen ohne gültigen Pass aus oder verwehrt einer konkreten Personengruppe den Einlass, welche in einer Negativliste (Nicht-Berechtigung) hinterlegt ist.

Bei der baulichen Gestaltung von Zutrittskontrollsystemen reichen die Möglichkeiten von offenen Eingängen mit Überprüfung ‚on the fly' (etwa durch einen Wachmann oder durch Kamerasysteme) bis hin zu Drehkreuzen, Schleusen oder eGates mit integrierten Ausweislesern, biometrischen Sensoren, Vereinzelungssystemen und Überwachungskameras.

Biometrische Systeme bieten schließlich die Möglichkeit, entweder die Identität der Person zu verifizieren (1:1 Vergleich, gehört dieser Ausweis zu dieser Person?) oder die Person aus einer Gruppe Berechtigter zu identifizieren (1:N Vergleich, ist diese Person Mitglied der Gruppe?). Auch lassen sich mit Gesichtserkennungsverfahren Eigenschaften von Personen bestimmen, die möglicherweise wichtig für die Zutrittsberechtigung sind (z. B. Altersbestimmung, Erkennen von Masken).

Am Beispiel des Zutritts zu Casinos und Spielstätten sollen die Möglichkeiten im Folgenden näher besprochen werden. Hier möchte der Betreiber den Zutritt möglichst offen gestalten und nicht alle Berechtigten registrieren. Gleichzeitig sollen allerdings bestimmte Personengruppen einer Negativliste zugeordnet werden können, um sie von der Teilnahme am Spiel auszuschließen (Spielersperren, Hausverbote). Diesen Personengruppen soll kein Zutritt gewährt werden, möglichst ohne andere Besucher zu beeinträchtigen. Hierbei sind gesetzliche Vorgaben umzusetzen aber auch ökonomische und Sicherheitsinteressen zu berücksichtigen.

An dieser Stelle sei eine Bemerkung zur ‚Fehlerquelle Mensch' erlaubt: Wo immer Zutrittskontrolle durch Wach- oder Empfangspersonal durchgeführt wird, kann es zu unterschiedlichen Fehlern kommen:

* Auf Seite 32 erfahren Sie mehr über den Autor.

– nicht durchgeführte Kontrollen (temporäre Abwesenheit des Personals, Ablenkung)
– fehlerhaft durchgeführte Kontrollen (falscher Ausweis wird nicht erkannt, mangelnde Genauigkeit beim Gesichtsvergleich mit dem Ausweisbild, fehlerhafte Dateneingabe bei maschineller Überprüfung gegen eine Sperrliste)
– bewusste fehlerhafte Kontrollen (Beispiel persönliche Beziehungen).

Auch automatisierte Kontrollen können keine 100-prozentige Sicherheit gewähren, bieten aber zumindest Schutz vor den oben genannten Faktoren.

III. Biometrische Verfahren

Biometrische Verfahren überprüfen persönliche Eigenschaften, die personengebunden (nicht nur personenbezogen) und deshalb nicht übertragbar sind. Dies können physiologische oder verhaltensbestimmte Eigenschaften sein.

Die wichtigsten Eigenschaften, die maschinell überprüft werden können, sind: Fingerabdruck, Gesichtszüge, Irismuster, Retinamuster, Venenstruktur der Hand, Handgeometrie, Stimme, Unterschrift, Tipprhythmus. Im Markt haben sich heute vor allem Fingerprintsensoren, Gesichtserkennungssysteme, Irisscanner, Stimmerkennungssysteme und Venenscanner durchgesetzt. Die Systeme werden je nach Genauigkeit und Benutzerfreundlichkeit in unterschiedlichen Anwendungsbereichen eingesetzt. Typisch ist, dass biometrische Verfahren, richtig eingesetzt, sowohl eine Erhöhung der Sicherheit als auch des Komforts bieten können.

Biometrische Systeme werden vielfältig im hoheitlichen und Sicherheitsbereich eingesetzt, kommen aber immer häufiger auch im privaten und öffentlichen Bereich zum Einsatz. Beispiele für Anwendungsbereiche sind

– Reise- und ID-Dokumente (biometrisches Passbild, Verhinderung von Duplikaten)
– polizeiliche Fahndung (Identifikation von Verdächtigen)
– Grenzkontrolle (Passkontrolle)
– Zugangskontrolle (Authentisierung)
– mobile Authentisierung (‚Wallets', Banking, etc.)
– Zugang zu mobilen Geräten.

Gesichtserkennungssysteme werden in allen genannten Anwendungsbereichen seit vielen Jahren eingesetzt. Darüber hinaus sind bereits zahlreiche weitere Anwendungen entwickelt worden (bzw. befinden sich in der Entwicklung), die ausschließlich durch die Nutzung der Gesichtserkennungstechnik ermöglicht wurden, wie z. B.:

– video-basierte Anwendungen (Video-Überwachung, statistische Messungen von Personenströmen)
– Foto-Album Software (Sortieren von Fotos nach Gesichtern)
– Intelligente Werbebildschirme (zielgruppen-gesteuerte Werbung)
– Service-Roboter (Erkennen von Bezugspersonen)
– Automobile (Fahreridentifizierung, Aufmerksamkeitskontrolle).

Gesichtserkennungssysteme haben dabei gegenüber anderen biometrischen Systemen den Vorteil, dass sie berührungslos und schnell arbeiten, selbsterklärend sind und dass sie darüber hinaus in vielen Bereichen als Erweiterung von Anwendungen genutzt werden können, die mit Fotos oder Videos umgehen. Außerdem können Personeneigenschaften wie Alter und Geschlecht bestimmt und zu statistischen Zwecken verwendet werden.

Gesichtserkennung kann zur Verifikation oder Identifikation von Personen genutzt werden, aber es gibt auch Anwendungen, in denen ‚Anonyme Gesichtserkennung' zum Einsatz kommt. Dabei wird keine Identitätsbestimmung der ‚gesehenen' Personen durchgeführt, d. h. das System kennt keine Namen oder Verknüpfungen zu Namen oder anderen identitätsbestimmenden Daten. Das System generiert statistische Daten, ohne individuelle Inhalte und Details zu speichern. Falls gleichzeitig bestimmte Personen identifiziert werden sollen, werden explizit nur deren Personendaten (Fotos) erfasst und mit deren Zustimmung zur weiteren Nutzung gespeichert.

Hier soll nicht auf die Prinzipien des Datenschutzes eingegangen werden. Es soll jedoch festgehalten werden, dass Produkte, die Gebrauch von Personendaten machen, auf technischer Ebene diese Prinzipien so weit wie möglich unterstützen sollten. Im konkreten Fall der Gesichtserkennung bedeutet das: Die Produkte müssen so konfiguriert werden können, dass Video- und Bilddaten nicht oder nur für die zulässige Dauer gespeichert werden. Es gibt, wie erwähnt, Szenarien, die komplett ohne Bilddatenbank und gespeicherte Personendaten auskommen. Die für die Erkennung automatisch erzeugten Daten (biometrische Templates) können sofort nach einem Abgleich gelöscht werden.

IV. Funktionsweise der Software

Die im Rahmen dieser Ausführungen vorgestellte Software FaceVACS-VideoScan erlaubt es, über angeschlossene Videokameras Gesichter aufzunehmen und zu analysieren. Dabei

– erkennt die Software mehrere Gesichter im Bildausschnitt (‚face in the crowd'),
– berechnet sie Gesichtstemplates von der Videosequenz des Gesichtsausschnitts (‚Face Stream') für jedes Gesicht, das von der Kamera detektiert wurde,
– löscht sie Videoinput, speichert verschlüsselten Gesichtsvektor (Template) für kurze (einstellbare) Zeit,
– vergleicht sie alle Templates mit evtl. vorhandener Bilddatenbank und
– vergleicht sie alle Templates aller Personen gegeneinander.

Aus der Analyse der ‚gesehenen' Gesichter werden Ereignisse erzeugt, die auf Mobilgeräte zur Benachrichtigung gesendet werden, z. B.

– Person aus der Bilddatenbank identifiziert (gesperrte Person), Person soll überprüft werden
– Person mit bestimmten Eigenschaften erkannt (z. B. Alter), Person soll aufgrund der Jugendschutzkontrolle überprüft werden.

Anonyme Gesichtsanalyse kann u. a. die folgenden Daten erzeugen:

– Anzahl der Personen: individuelle Besucher während einer bestimmten Zeitspanne
– Verteilung der Besuchslängen: Besucherzahl in Relation zur Länge der Besuche

- durchschnittliche Transitlänge: *n* Personen brauchen von A nach B eine durchschnittliche Zeit von x
- Altersverteilung der Personen
- Geschlechtsverteilung der Personen.

Ein solches System kann in verschiedensten Anwendungsbereichen eingesetzt werden, z. B.

- für Sicherheit und Zutrittskontrolle (Identifikation von gesperrten Personen)
- zur Messung von Personenfluss und zur Messung von Personenzahlen, Wartezeiten, Transitzeiten (etwa in Flughäfen)
- für Analysen zu Marketingzwecken (Statistik über Besucherzahlen, Alters- und Geschlechtsgruppen, gezielte Werbung, Erkennen von VIP-Kunden).

V. Pilotprojekt Merkur-Spielothek

Für den Zutritt zu Spielstätten gibt es gesetzliche Vorgaben, wonach der Zutritt solchen Personen zu verweigern ist, die auf landesweiten, betreiberspezifischen oder lokalen Sperrlisten registriert sind. In einigen Bundesländern sind diese Vorgaben schon eingeführt, in anderen geplant.

Eine konventionelle Lösung besteht darin, die Ausweise der Besucher zu kontrollieren und einen manuellen Abgleich mit der Sperrliste durchzuführen. Das bedeutet:

- jeder Besucher muss bei jedem Besuch kontrolliert werden
- jeder Besucher muss seine persönlichen Daten offenlegen
- Besucher fühlen sich belästigt
- Zeitverlust für den Besucher durch die Überprüfung
- Personalaufwand für den Betreiber
- fehleranfälliges Verfahren (siehe ‚Fehlerquelle Mensch').

Die erweiterte Forderung lautet daher: Personen auf Sperrlisten soll der Zutritt verweigert werden OHNE die Gesamtheit der Besucher als Problemspieler zu stigmatisieren und durch permanente Kontrollen den Zugang zu beeinträchtigen.

Die innovative Lösung realisiert einen automatischen Gesichtsvergleich mit den Fotos der Sperrliste. Dazu werden von einer Kamera am Eingang die Gesichter aller Besucher aufgenommen und mit den Fotos der Sperrliste verglichen. Bei einem Treffer wird über die mobile Benachrichtigung das Personal informiert; wird kein Treffer erzielt, werden die Daten gelöscht. Diese Lösung hat mehrere Vorteile:

- nur gesperrte Personen müssen persönliche Daten zur Registrierung offenlegen (Ausweis, Foto)
- nur gesperrte Personen werden beim Zutrittsversuch identifiziert
- andere Besucher werden nicht beeinträchtigt
- kein Zeitverlust beim Zutritt
- weniger Personalaufwand, nur im Fall des Treffers muss das Personal aktiv werden
- zusätzlich kann über die automatische Altersschätzung auch noch die Jugendschutzkontrolle unterstützt werden.

VI. Ausblick

Die Ergebnisse der vorliegenden Pilotversuche zeigen, dass die Gratwanderung zwischen höchster Sicherheit einerseits und Benutzerfreundlichkeit sowie Datenschutz andererseits durch die Anwendung von anonymer Gesichtserkennung für die Zutrittskontrolle gemeistert werden kann.

Summary

The article provides an overview of access control systems, in particular systems for physical access control, and how such systems can be best applied at casinos and gaming arcades. While a number of solutions exist that involve human control or electronic devices, biometric technologies offer several advantages. Especially anonymous face recognition allows the implementation of automatic access control that is highly reliable and at the same time, is convenient to use and supports the main principles of privacy protection.

Dr. Waldemar Grudzien, Berlin*

Biometrie im Banking

Ein Plädoyer gegen Vorurteile

I. Einleitung

Das Smartphone als zentrales Gerät für die neuen App-Ökosysteme zieht immer mehr etablierte Märkte auf sich und generiert gänzlich neue Dienstleistungen. Banking und Biometrie erfahren mit der Einführung von Apple Pay seit Oktober 2014 und im Android-Lager seit dem Frühjahr 2015 einen großen Schub: Der Kunde legitimiert sich mit seinem Fingerabdruck am Smartphone und bezahlt. Als erste bieten die Postbank und die Deutsche Bank Touch ID von Apple zum Kontenzugang und sogar zur Autorisierung von Transaktionen an.

Apps werden immer kundenfreundlicher und smarter, die Interaktion mit dem Smartphone erfolgt immer mehr „on the fly", d. h. gestaltet sich zunehmend beiläufig als mit der eigentlichen Aufgabe verbunden: aus dem Eintippen mit einzelnen Tasten wird ein Wischen über das Touchpad, das Eingeben der eigenen Position übermittelt das Smartphone automatisch, die Mauseingabe am PC/Laptop ist ebenfalls in ein Wischen übergegangen. Das Erledigen von Aufgaben „on the fly" mit dem Smartphone befördert die Integration von Biometrie im Smartphone, das über

* Auf Seite 32 erfahren Sie mehr über den Autor.

viele Sensoren verfügt, von denen einige bereits heute biometrisch genutzt werden. Biometrie liefert so in Verbindung mit dem Smartphone ein „Me on the fly“: der Nutzer wird bei der Nutzung des Smartphones beiläufig und ohne ihn zu stören authentifiziert und seine gewollten Transaktionen werden autorisiert. Biometrie macht Banking bequem, meist „convenient“ genannt.

Die biometrischen Verfahren und Methoden selbst haben sich ebenfalls weiter entwickelt. Sensoren wurden weiter miniaturisiert und weisen immer bessere Lebendtests auf. Die Verarbeitungselektronik ist kleiner, schneller und kostengünstiger geworden, Protokolle und Algorithmen wurden neu entwickelt oder verbessert. Gerade für das Banking zentral ist ein interoperables Banking-Biometrie-Protokoll, das zum Beispiel in Form des Biometric Transaction and Authentication Protocol (BTAP) [Bu2010] bereits verfügbar ist.

Es sind mehr Anbieter pro biometrischem Verfahren in den Markt eingetreten, sodass potenzielle Nutzer nun eine breitere Anbieterbasis vorfinden. Zu guter Letzt: Biometrie wird im Banking eingesetzt! Täglich, millionenfach, sicher und komfortabel – nun auch endlich in Deutschland.

1. Sinn eines Banking-Biometrie-Protokolls

Ein Banking-Biometrie-Protokoll verbindet Geschäftsvorfälle des Banking mit der biometrischen Authentifikation. Biometrie, als Messung der Merkmale einer lebendigen Person, bietet inhärent den Vorteil eines One-Time-Passwords (OTP), sodass mit Biometrie auch einzelne Geschäftsvorfälle autorisiert werden können. Im Idealfall verbindet so ein entsprechendes Protokoll die Transaktion eines Geschäftsvorfalls mit den sich ständig verändernden körperlichen Merkmalen einer lebenden Person zu einem OTP für jede Transaktion. Statische Eingaben können durch eine immer dynamische Verbindung mit den lebendigen Merkmalen einer Person ersetzt werden. Ein Beispiel für ein Banking-Biometrie-Protokoll ist das bereits genannte BTAP.

2. Biometrie und Bankregulierung

In Europa gibt es mehrere Regulierungsvorhaben zur IT-Sicherheit bei Banken. Zu nennen sind die Zahlungsdiensterichtlinie PSD sowie die NIS-Richtlinie. Die PSD bindet die Europäische Bankenaufsicht EBA in die IT-Aufsicht ein. Die „Guidelines“ genannten Dokumente der EBA werden in Form von BaFin-Rundschreiben zu Vorgaben für Banken in Deutschland. Dieser Regulierungsweg wurde zum ersten Mal mit den Sicherheitsanforderungen an Zahlungen im Internet beschritten: Aus den „Final guidelines on the security of internet payments“ der EBA vom 19.12.2014 wurde so das BaFin-Rundschreiben zu den Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSI) vom 5.5.2015.

Im BaFin-Rundschreiben wird der Begriff „Starken Kundenauthentifizierung“ folgendermaßen bestimmt:

„Starke Kundenauthentifizierung ist im Sinne dieses Rundschreibens ein Verfahren, das auf der Verwendung zweier oder mehrerer der folgenden Elemente basiert, die als Wissen, Besitz und Inhärenz kategorisiert werden: i) etwas, das nur der Nutzer weiß, z. B. ein statisches Passwort, ein Code, eine persönliche Identifikationsnummer, ii) etwas, das nur der Nutzer besitzt, z. B. ein Token, eine Smartcard, ein Mobiltelefon, iii) eine Eigenschaft des Nutzers, z. B. ein biometrisches Charakteristikum, etwa ein Fingerabdruck. Außerdem müssen die gewählten Elemente unabhängig voneinander sein, d. h. die Verletzung eines Elements darf keinen Einfluss auf das andere bzw. die anderen haben. Mindestens eines der Elemente sollte nicht wiederverwendbar und nicht reproduzierbar (die Inhärenz ausgenommen) sein und nicht heimlich über das Internet entwendet werden können. Das starke Authentifizierungsverfahren sollte so gestaltet sein, dass die Vertraulichkeit der Authentifizierungsdaten gewahrt bleibt.“

Biometrie ist somit für die europäische und nationale Bankenaufsicht neben Wissen und Besitz ein gleichberechtigtes Mittel zur starken Authentifizierung des Kunden.

II. Geräte mit biometrischer Nutzung

Hierunter werden Geräte mit biometrischer Nutzungsmöglichkeit verstanden, d. h., die Geräte verfügen über eingebaute Sensoren, die für biometrische Messungen verwendet werden können. Die wichtigste Gerätegattung stellt das Smartphone dar, das mit einer Vielzahl von Sensoren bestückt wird. Auch die immer stärker aufkommenden Smart Watches und Wearables („Fitnessarmband“) tragen von Hause aus Sensoren mit sich. Viele Smart Watches enthalten Fitness-Sensoren für Beschleunigung und Pulsmessung. Geräte aus dem Smart Home Bereich sollten ebenfalls betrachtet werden. Die Geräteklassen können auch vereint werden und bilden dann zum Beispiel den Bereich der Smart Mobility, der sicherlich auch Bankingfunktionalität bieten wird.

Die beiden „natürlichsten“ Biometriesensoren eines Smartphones sind Mikrofon und Kamera. Biometrisch auswerten lassen sich auch die Tastatureingaben. Einige Smartphones verfügen auch über einen Infrarotsensor zur Pulsmessung, andere auch über einen Fingerabdrucksensor. Mit Siri hat Apple die Spracherkennung hoffähig gemacht. Hinzu kommen meistens auch Gestensensor, Annäherungssensor, Gyroskop, Accelerometer, Kompass, Barometer, Thermometer und Hygrometer, Magnetsensor und RGB-Lichtsensor. Nicht alle Sensoren lassen sich für biometrische Zwecke nutzen. Manche Sensoren können neben der eigentlichen biometrischen Messung auch für Lebendtests verwendet werden. Sensoren ohne biometrischer Ausnutzbarkeit könnten durch intelligente Verknüpfung und Auswertung zur Plausibilität einer Bankingtransaktion dienen – wie die Verknüpfung des Aufenthaltsortes mit der biometrischen Identifikation des Nutzers. In Tabelle 1 sind die gängigsten Sensoren eines Smartphones mit ihrer Messgröße und wenn gegeben, möglicher biometrischer Nutzung gelistet.

Sensor	Misst/beobachtet	Biometrisch nutzbar
Mikrofon	Stimme	Spracherkennung (was? z. B. Ziffernreihenfolge) Sprechererkennung (wer?)
Kamera	Fotos	Augen Gesicht Iris
Tastatur (Touch, Druck)	Schrift / Interaktion	Schrifterkennung / Tippverhalten
Maus	Mausverhalten	Mausverhalten
Infrarotsensor	– Puls	

	– Gesten – Annäherung (Kopf am Smartphone?)	Puls Handbewegungen
Gyroskop	Lage im Raum (Drehbewegungen in allen drei räumlichen Achsen)	
Accelerometer	Bewegung im Raum (Beschleunigungen in allen drei räumlichen Achsen)	Gangerkennung
Barometer	Atmosphärischer Luftdruck	
Thermometer	Temperatur	
Hygrometer	Luftfeuchtigkeit	
Magnetsensor	– Himmelsrichtung Norden (Kompass) – Magnetfeld: Smartphone-Cover zugeklappt?	
RGB-Lichtsensor	Farben Rot, Grün, Blau	
GPS	Aufenthaltsort	
Fingerabdrucksensor	Fingerabdruck	Fingerabdruck

Tabelle 1: Gängige Sensoren in Smartphones

Denkbar und wahrscheinlich ist auch eine „abgestufte Sicherheit" mit Hilfe des Smartphones. In Abbildung 1 ist ein Beispiel dargestellt:

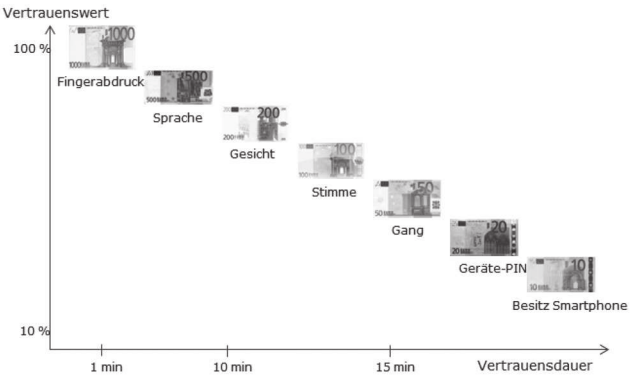


Abbildung 1: Risikobasiertes Ticket – Kombination von Vertrauenswert und Vertrauensdauer in Abhängigkeit des zu autorisierenden Betrages

Allein durch den Besitz des Smartphones darf der Nutzer 5 Euro transferieren. Um 50 Euro zu transferieren, muss sich der Nutzer gegenüber seinem Smartphone durch Besitz, Geräte-PIN und Gang authentifizieren. Das Ticket für 50 Euro ist 15 Minuten lang gültig, nach Ablauf der Frist ist eine erneute Authentifizierung nötig. In diesem Beispiel muss sich der Nutzer für ein Transaktionsvolumen von 1.000 Euro gegenüber seinem Smartphone mit allen Merkmalen authentifizieren, die sein Smartphone messen kann. Das Ticket ist zudem nur 1 Minute kurz gültig. Das muss der Nutzer aber nicht der Reihe nach tun, das Wesen der Biometrie ist ja die „beiläufige" Messung der Körpermerkmale während der Nutzer sein Smartphone nutzt und bei sich trägt.

In Zukunft werden Smartphones und in Kombination mit diesen auch die Wearables und Smartwatches nicht nur ihren Träger, sondern auch dessen Umgebung vermessen und somit Rückschlüsse auf den Träger ziehen können.

III. Vorurteile gegenüber Biometrie im Banking

Im Zusammenhang mit Banking werden zur Biometrie immer wieder die gleichen Vorurteile geäußert, die ich zu entkräften versuche. Im eingangs genannten Banking-Biometrie-Protokoll BTAP sind bereits Maßnahmen umgesetzt, welche die ersten sechs „technisch auflösbaren" Vorurteile widerlegen. Die letzten zwei Vorurteile sind sozioökonomischer Natur und bedürfen einer anderen Erzählung.

1. Vorurteil 1: Biometrie ist unsicherer als PIN

Erläuterung:
Oft wird behauptet, dass die Biometrie nicht so sicher sei wie die Sicherheit wissensbasierter Verfahren, d. h. von PINs und Passworten.

Forderung:
Die Sicherheit der Biometrie muss der Sicherheit wissensbasierter Verfahren ebenbürtig sein.

Lösung:
Als Vergleichsmaßstab für die Sicherheit der Authentisierung wird die PIN herangezogen, da diese das Gros der Banking-Anwendungen absichert. Es gibt drei gute Gründe für die Überlegenheit der Biometrie über der PIN. Erstens ist die Entropie einer vier- oder sechsstelligen PIN recht klein. So verfügt eine sechsstellige[1] numerische PIN (z. B. beim nPA) über eine Entropie von weniger als 20 Bit ($H = L^*\log_2 N$; mit L=6, N=10) [Bu2014].

Die Entropie von biometrischen Charakteristiken ist deutlich größer als die der sechsstelligen PIN:

- Fingerabdruck = 84 Bit [Ratha2001]
- Iris = 249 Bit [Daugman2006]
- Gesichtsbild = 56 Bit [Adler2006]
- Stimme = 127 Bit [Nautsch2015]

Zweitens können PINs weiter gegeben und gestohlen werden, biometrische Charakteristika (d. h. Körperteile) selbst können nicht in dem Sinne weitergegeben werden, dass sie erfolgreich eingesetzt werden könnten. Analoge oder digitale Repräsentationen von einem Charakteristikum, also biometrische Bilder oder Merkmale können gestohlen werden (Beispiel: Fingerabdruck auf Glas oder Fotografie des Gesichts).

Allerdings kann deren erfolgreicher Einsatz durch Lebendtests (d. h. das Abprüfen der „Lebendigkeit" des präsentierten Charakteristikums) verhindert werden. Es wird also geprüft, ob sich eine lebendige Person authentifizieren will oder ob dem Sensor nur ein Artefakt (Foto des Gesichts, Foto der Iris, Gummifinger etc.) dieser Person präsentiert werden soll. Es gibt auch biometrische Verfahren, die nach heutigem Technologiestand keine Latenzbilder hinterlassen. Das sind diejenigen biometrischen Verfahren, die Messungen im Körperinnern und nicht an der Oberfläche vornehmen; dazu zählen Venenverläufe von Handfläche und Finger. Auch die neuen kontaktlosen Fingerbildverfahren („Fingerprint on the fly") zählen dazu. Biometrische Ver-

1 Eine vierstellige PIN verfügt über eine Entropie von 13 Bit.

fahren bieten somit eine Nicht-Abstreitbarkeit (Non-Repudiation) für die Absicherung einer Transaktion, PINs dagegen nicht.

Und drittens überfordern PINs und Passworte das menschliche Gehirn, zumindest dann wenn wir uns zu viele davon merken müssen. Die biometrischen Charakteristika hingegen hat der Mensch immer dabei, er kann sie auch nicht vergessen oder liegen lassen, und auch nicht weitergeben wie PIN und Passwort.

Ergebnis:
Biometrische Verfahren sind sicherer als die PIN.

2. Vorurteil 2: Biometrische Merkmale sind endlich

Erläuterung:
Da der Mensch nur 10 Finger, zwei Hände, zwei Ohren, ein Gesicht etc. hat, ist die Anzahl der für biometrische Anwendungen zur Verfügung stehenden Charakteristika sehr klein. Wird ein Referenzbild gestohlen, zum Beispiel ein Fingerabdruck, stehen nur noch neun weitere Charakteristika dieses Typs zur Verfügung. Wird ein Passwort gestohlen, erzeugt man ein neues. Wird ein Fingerabdruck gestohlen, …

Forderung:
Biometrische Charakteristika müssen so oft verwendet werden können wie PINs und TANs, im Prinzip unendlich oft als ob es sich um One-Time-Passwords handeln würde. Hierzu gehört auch die Forderung nach der Möglichkeit des Rückrufs (Revocation) einer biometrischen Referenz.

Lösung:
Aus diesem Grund sollten nie direkt die Bilder einer Charakteristik (Fingerbild, Gesichtsbild) als Referenz gespeichert werden. Als Referenz wird nicht das biometrische Bild oder ein Template verwendet, sondern ein aus dem biometrischen Bild abgeleiteter pseudonymer Identifikator,[2] so dass ein Rückruf der Referenz und damit ihre unendliche Nutzung möglich werden [ISO 24745-2011] [Br2008].

Durch Verwendung von pseudonymen Identifikatoren (PI) werden die folgenden Eigenschaften biometrischer Verfahren erreicht:

- Vertraulichkeit: Ein PI als gespeicherte biometrische Referenz kann ohne Entschlüsselung für Vergleiche herangezogen werden.
- Erneuerbarkeit: Biometrische Referenzdaten können erneuert und zurück gerufen werden.
- Störabstand (noise robustness): Ein PI ermöglicht den Einsatz der Biometrie in stark gestörter Umgebung (z. B.: hoher Geräuschpegel bei Stimmenbiometrie, starkes Sonnenlicht bei Fingerabdrücken).
- Unlinkability, d. h. Vermeidung von Querbezügen: Beim Abgleich von zwei Datenbanken können PI, die in beiden Anwendungen registriert sind, nicht detektiert werden.
- Nicht-Invertierbarkeit: Das originale biometrische Fingerbild kann aus dem PI nicht rekonstruiert werden.
- Möglichkeit der Autorisierung von einzelnen Transaktionen mit biometrischen Merkmalen: Durch die unendliche Verwendungsmöglichkeit eines variierenden da lebendigen Charakteristikums kann eine biometrische TAN erzeugt werden.

Ergebnis:
Die Verwendung von pseudonymen Identifikatoren ermöglicht den Rückruf biometrischer Referenzen und damit die Nutzung eines biometrischen Charakteristikums unendlich viele Male als OTP.

3. Vorurteil 3: Biometrische Merkmale sind nicht erkennbar

Erläuterung:
Das jeweils für einen Vergleich live aufgenommene biometrische Bild variiert, sodass es oft mit der gespeicherten Referenz nicht übereinstimmt. Die live beobachteten biometrischen Daten *müssen* sogar variieren, denn es wird an einem lebendigen Körper gemessen.

Forderung:
Das biometrische Verfahren muss robust sein gegenüber der Varianz einer biometrischen Charakteristik. D.h., Referenz und live aufgenommene Probe müssen im Rahmen der messtechnischen Fehlertoleranz übereinstimmen.

Lösung:
Zur Stabilisierung der Messergebnisse veränderlicher Parameter (dazu gehören auch Störungen) werden Fehlerkorrekturverfahren eingesetzt. Ein sehr bekanntes Verfahren ist das Hamming-ECC-Verfahren, das bei der Compact Disc verwendet wird.

Ergebnis:
Durch Nutzung eines angemessenen Fehlerkorrekturverfahrens im Banking-Biometrie-Protokoll wird ein stabiler Vergleich von Referenz und Live-Merkmal erreicht.

4. Vorurteil 4: Biometriesensoren sind leicht zu täuschen

Erläuterung:
Es kursieren immer wieder Horrorgeschichten von abgetrennten Fingern oder gar abgehackten Händen von Bankkunden, die von Kriminellen auf den Geldautomaten gelegt werden, um Geld zu erhalten – Bio-Hacking im doppelten Sinne sozusagen. Diesen eher aus der Phantasie entstammenden Schilderungen stehen tatsächlich durch gute Artefakte zu täuschende Sensoren gegenüber. Bekannt geworden sind diverse Gummi-, Silikon- und Gelatinefinger oder auch simple Gesichtsfotos, mit denen die entsprechenden Sensoren getäuscht wurden. Aus diesen Vorurteilen und wahren Schwächen ergibt sich der Gesamteindruck von generell allen leicht zu täuschenden biometrischen Sensoren. Dem ist heute nicht mehr so. Es gibt Sensoren, die einen sicheren Lebendtest aufweisen. Gleichwohl muss die Entwicklung hier weiter gehen, damit möglichst alle für die Nutzung im Banking relevanten biometrischen Verfahren über verlässliche Sensoren verfügen.

Forderung:
Der biometrische Sensor muss robust sein gegen Präsentationen mit Artefakten und toten Körperteilen.

Lösung:
Der biometrische Sensor muss über einen täuschungsresistenten Lebendtest verfügen.

Lebendtests gibt es noch nicht für alle Verfahren, aber bereits für

- Fingerabdruck (Optical Coherence Tomography OCT)[3]

2 Ein pseudonymer Identifikator (PI) ist ein Vektor, der aus der biometrischen Charakteristik abgeleitet ist. Der PI gibt nichts mehr über die Person preis.

3 Messung des äußeren und des inneren Fingerabdrucks, d. h., inkl. Schweißdrüsen und Schweißkanälen.

- Iris (Messung intrinsischer Augenbewegungen),
- Vene – Finger und Handfläche (Messung des Blutsauerstoffgehalts, Messung der Blutflussbewegung),
- Gesicht 3D (Messung der Oberflächengeometrie des Gesichtes).

Derzeit wird ein ISO-Standard[4] zu Lebendtests entwickelt [ISO/IEC 30107], [Busch-2014]. Durch diesen Standard wird die Qualität der Lebendtests vergleichbar.

Ergebnis:
Für einige oft genutzte biometrische Charakteristiken gibt es bereits gute Lebendtests. Es besteht jedoch weiterer Forschungs- und Entwicklungsbedarf für Lebendtests zu weiteren biometrischen Charakteristiken.

5. Vorurteil 5: Biometrie kollidiert mit Datenschutz

Erläuterung:
Oft wird behauptet, dass biometrische Anwendungen nicht datenschutzkonform implementiert werden können. Damit einhergehend kursiert das Vorurteil, dass Biometrie immer zentraler Datenbanken bedarf.

Forderung:
Das biometrische Verfahren muss die Anforderungen des Datenschutzes erfüllen und insbesondere auf die zentrale Speicherung von biometrischen Referenzen verzichten.

Lösung:
Durch die Verwendung eines pseudonymen Identifikators (PI) wird eine pseudonyme Zahl berechnet und die Offenlegung der Information zu einem Körperteil einer Person verhindert. Biometrie bedarf auch nicht der zentralen Speicherung der biometrischen Referenzen, da zum Offline-Vergleich die Referenz den Speicherchip nicht verlässt und zum Online-Vergleich der PI verwendet wird.

Der Standard „ISO/IEC 24745: Biometric Information Protection, (2011)“ beschreibt die datenschutzkonforme Implementierung eines biometrischen Systems.

Ergebnis:
Biometrie kann datenschutzkonform implementiert werden.

6. Vorurteil 6: Biometrie ist proprietär

Erläuterung:
Es wird behauptet, dass es bisher keine Standards gibt, die Biometrieverfahren und alle Zahlungsverkehrs-Anwendungen umfassen.

Hier muss unterschieden werden zwischen der Standardisierungsarbeit auf der „Biometrieseite“, d. h. der Zulieferer der Kreditwirtschaft und dieser selbst für die Anwendungen, derzeit also vornehmlich Zahlungssysteme.

Forderung:
Schaffung und Nutzung biometrischer Standards für alle Elemente der Banking-Biometrie-Kette.

Lösung:
Auf der Zuliefererseite passiert bereits seit geraumer Zeit sehr viel. So arbeiten die drei ISO/IEC Sub Committees 17 (Cards and personal identification), 27 (IT Security Techniques) und 37 (Biometrics) an verschiedenen Standards zusammen, deren Einhaltung kreditwirtschaftliche Betreiber von ihren Zulieferern verlangen sollten:

- Ein Vendor Lock-In durch proprietäre Sensoren wird verhindert durch Verwendung eines BioAPI-Interface gemäß ISO/IEC 19784.
- Verschiedene biometrische Vergleichsalgorithmen können verwendet werden durch Speicherung der biometrischen Referenzdaten in Austauschformaten gemäß der Formatfamilie ISO/IEC 19794 (siehe unten).
- Die Genauigkeit biometrischer Vergleichsalgorithmen kann mit Hilfe eines Leistungstests gemäß ISO/IEC 19795 vergleichend beurteilt werden.
- Die Einhaltung der datenschutzkonformen Speicherung von biometrischen Referenzdaten ist gegeben, wenn das biometrische System gemäß ISO/IEC 24745 implementiert wurde.

ISO 19794-Familie der Austauschformate für biometrische Daten (Biometric data interchange formats)

- Teil 1: Framework [ISO19794-1],
- Teil 2: Finger Minutiae Data [ISO19794-2],
- Teil 3: Finger Pattern Spectral Data [ISO19794-3],
- Teil 4: Finger Image Data [ISO19794-4],
- Teil 5: Face Image Data [ISO19794-5],
- Teil 6: Iris Image Data [ISO19794-6],
- Teil 7: Signature/Sign Time Series Data [ISO19794-7],
- Teil 8: Finger Pattern Skeletal Data [ISO19794-8],
- Teil 9: Vascular Image Data [ISO19794-9],
- Teil 10: Hand Geometry Silhouette Data [ISO19794-10] und
- Teil 11: Signature/Sign Processed Dynamic Data [ISO19794-11].

Mit standardisierten Austauschformaten ist man nicht mehr an Hersteller gebunden, ein Vendor Lock-In wird vermieden. Die Kreditwirtschaft muss von Zulieferern die Einhaltung der o. g. ISO-Formate verlangen.

Auf kreditwirtschaftlicher Seite gibt es einzig beim Betriebssystem der deutschen Debit- und Kreditkarte SECCOS eine Art Standardisierung für Biometrie: Es ist möglich ISO-Kommandos zu integrieren. Da aber bislang in der Deutschen Kreditwirtschaft nur PIN-Prüfungen zur Benutzerauthentikation vorgesehen sind, ist die Möglichkeit einer biometrischen Verifikation derzeit noch nicht vorhanden.

Mit BTAP[5] gibt es bereits ein Protokoll zur Integration von Biometrie als Authentikationskanal in Bankinganwendungen. Weitere Protokolle dürften in anstehenden Forschungsvorhaben der Europäischen Union im Rahmen des Programms Horizon 2020 entwickelt werden.

Ergebnis:
Biometrie ist nicht proprietär.

7. Vorurteil 7: Kunden wollen keine Biometrie

Wann immer Banken im Massenkundenverkehr Biometrie in Piloten oder im Regelbetrieb eingeführt haben, sind die Kunden sehr zufrieden und wollen auf Biometrie nicht mehr verzichten.

Ergebnis:
Kunden sind nicht gegen Biometrie, wollen diese zumeist aktiv wenn angeboten.

---

4 ISO/IEC CD 30107-1 Information Technology – Biometrics – Presentation attack detection – Part 1: Framework.

5 http://www.christoph-busch.de/files/Hartung-BiometricTransaction Protocol-Securware-2010-100420.pdf.

8. Vorurteil 8: Biometrie bringt keine neuen Kunden

Die Frage ist mittlerweile eine Andere. Der Kunde verlangt sichere und zuverlässige Verfahren, die ihn aber nicht mit Sicherheit „belästigen"; der Kunde verlangt bequeme Verfahren. Werden die Banking-Verfahren nicht bequemer, wird sich der Kunde einen Mausklick entfernt Verfahren mit besserer ‚Convenience' zuwenden. Biometrie ist der natürlichste Weg Technik bequemer zu gestalten.

IV. Fazit

Biometrie ist komfortabler als PINs oder Passworte und zudem auch sicherer als diese. Biometrie wird seit Jahren täglich von Millionen von Kunden genutzt – in Japan, Brasilien und der Türkei. Smartphones öffnen der Biometrie im Banking im großen Maßstab die Türen – auch in Deutschland wie erste Anwendungen beispielsweise von Postbank und Deutsche Bank zeigen.

V. Quellen

[Adler2006]
Adler, A., Youmaran, R., Loyka, S.: Towards a measure of biometric information. In: Canadian Conference on Electrical and Computer Engineering (CCECE 2006), pp. 210–213 (2006)

[Br2008]
J. Breebaart, C. Busch, J. Grave, E. Kindt: „A Reference Architecture for Biometric Template Protection based on Pseudo Identities", in BIOSIG-2008, GI-LNI, (2008)

[Bu2010]
C. Busch, D. Hartung: „Biometrische Nachrichten-Authentisierung", in Proceedings of the GI-Sicherheit 2010, LNI, pages 13-24, Berlin, Germany, October (2010)

[Bu2014]
N. Buchmann, C. Rathgeb, H. Baier, C. Busch: Towards electronic identification and trusted services for biometric authenticated transactions in the Single Euro Payments Area, in Proceedings of the 2nd Annual Privacy Forum (APF'14), 2014

[Busch2014]
C. Busch: Related Standards, Handbook of Anti-Spoofing, Springer, 2014

[Daugman2006]
Daugman, J.: Probing the uniqueness and randomness of iriscodes: Results from 200 billion iris pair comparisons. Proc. of the IEEE 94(11), 1927–1935 (2006)

[Nautsch2015]
A. Nautsch, C. Rathgeb, R. Saeidi, C. Busch: Entropy Analysis of I-Vector Feature Spaces in Duration-Sensitive Speaker Recognition, in 40th IEEE ICASSP Conference, 19-24 April 2015, Brisbane, Australia, (2015)

[Ratha2001]
Ratha, N.K., Connell, J.H., Bolle, R.M.: An analysis of minutiae matching strength. In: Bigun, J., Smeraldi, F. (eds.) AVBPA 2001. LNCS, vol. 2091, pp. 223–228. Springer, Heidelberg (2001)

Thomas Walloschke, Berlin*

Your Hand is Your Key – Biometrische Zugangskontrollen

Möglichkeiten und technische Umsetzung

Bekannte biometrische Merkmale wie Iris, Handvenenstruktur oder Fingerabdruck haben weltweit Hochkonjunktur – aktuell steigt die globale Nachfrage nach biometrischen Erkennungssystemen für eine zuverlässige Authentifizierung sprunghaft an. In Unternehmen unterschiedlicher Branchen, wie etwa im Finanzsektor, im Gesundheitswesen, in Apotheken, aber auch in den Sicherheitsbereichen öffentlicher und privater Unternehmen, auf Flughäfen oder im Schulwesen und sogar in Kindergärten kommt die Fujitsu PalmSecure® Sensortechnologie immer häufiger zum Einsatz.

I. „Geldwerte" Handvenenstrukturen

Fujitsu PalmSecure ist eine berührungslose Authentifizierungsmethode basierend auf dem im menschlichen Körper liegenden Venenmuster der Handfläche. Diese Methode erzeugt einen individuellen, persönlichen Identifizierungscode. Die PalmSecure Technologie basiert auf über 20 Jahren Entwicklung und Forschung und wurde im Jahr 2005 zur Marktreife gebracht. Im selben Jahr setzte die Tokio Mitsubishi Bank die Technologie erstmalig in Geldautomaten (ATM) ein.

An den ATMs dieser Bank können registrierte Kunden mittels PalmSecure Sensoren und in Verbindung mit einer Kreditkarte ihre Geldtransaktionen durchführen. Zu diesem Zweck wird zuvor das im Rahmen einer Erstregistrierung erfasste biometrische Handflächenvenenmuster als biometrisches Template im Chip der Kreditkarte gespeichert. Geldtransaktionen erfordern zunächst das Handflächenvenenmuster des Kunden, das über den im ATM intergierten PalmSecure Sensor erfasst wird. Mittels spezieller Algorithmen findet ein Abgleich mit dem im Chip der Kreditkarte gespeicherten biometrischen Template statt. Eine Transaktion kann im Anschluss daran nur stattfinden, wenn das

* Auf Seite 32 erfahren Sie mehr über den Autor.

gescannte Venenmuster mit dem im Chip der Karte gespeicherten biometrischen Template übereinstimmt.

II. Ansprüche an die Biometrie

Biometrische Authentifizierungstechnologie sollte auf den folgenden vier biometrischen Faktoren basieren: Dauerhaftigkeit, Allgemeingültigkeit, Erfassbarkeit und Unterscheidungskraft. Daraus leiten sich die Anforderungen an diese Technologie ab: der biometrische Faktor sollte über einen langen Zeitraum oder sogar bis zum Lebensende unveränderbar sein, jede Person sollte diesen Faktor besitzen und die ausgewählte biometrische Authentifizierungsmethode verwenden können, die biometrische Authentifizierungstechnologie sollte auf Kriterien basieren, die qualitativ messbar sind und der Faktor muss für jede Person, selbst bei Zwillingen, unterschiedlich sein. Die Fujitsu PalmSecure Technologie wurde unter diesen Vorgaben entwickelt und erfüllt diese Ansprüche.

III. Biometrische Qualität

Handflächenvenenmuster sind bei Menschen einzigartig und bieten zugleich mehr als fünf Millionen unterschiedliche Referenzpunkte zur Erkennung. Die Fehlerquote einer Falscherkennung kann damit auf unter eins zu zehn Millionen gesenkt werden. Somit verbannt das Handflächenvenenmuster seine biometrischen „Kollegen" wie den Fingerabdruck und die Iris in Sachen Authentifikationspräzision auf die hinteren Plätze. Auch im Hinblick auf Manipulationssicherheit ist die PalmSecure Technologie einzigartig, da Handvenen unsichtbar innerhalb des Körpers verlaufen und nur bei lebendem Gewebe, das über einen entsprechenden Blutfluss verfügt, erfasst werden.

Im Bereich sehr hoher Anforderungen an die Authentifizierung ermöglicht die kombinierte Nutzung mehrerer Authentifikationsfaktoren, wie weitere biometrische Faktoren, bzw. Smart-, Kredit-, oder Banking-Cards und auch Credentials (Username, PIN, etc.) in sogenannten multimodalen und Multifaktor-Systemen die nahezu einzigartige Erkennung von Menschen unabhängig von Alter, ethnischer Herkunft bzw. Geschlecht.

IV. Biometrie in Brasiliens Bankautomaten

In Brasilen wollte die größte Privatbank Brasiliens, die Banco Bradesco, die Millionenschäden durch Betrug an ATMs nicht mehr hinnehmen und suchte nach einer neuen Sicherheitslösung. Zusammen mit Fujitsu entwickelte Bradesco die erste biometrische ATM-Lösung in Südamerika. Landesweit sind mehr als 48.000 Geldautomaten mit sicheren und hygienischen PalmSecure Sensoren ausgestattet. Über 70 Millionen Kunden haben in Verbindung mit ihrer Bankkarte, auf der das Handflächenvenenmuster als biometrisches Template im Chip gespeichert wird, einen sicheren Zugang zu ihren Konten. Damit konnte die Banco Bradesco ihre bisherigen durch ATM-Betrug entstandenen Kosten gegen Null senken. Bereits nach wenigen Wochen und einer knappen Milliarde Transaktionen wurde kein Betrugsfall mehr registriert. Als wichtiger Zusatznutzen stellte sich durch den Lebendnachweis über PalmSecure ein: bei der ATM-Nutzung durch Rentenbezieher, die Kunden der Banco Bradesco sind, entfällt die schriftliche Lebensbescheinigung an die Rentenversicherung.

V. Palm-ID: Lückenlose Dokumentation verhindert Manipulation

Österreichs Apotheker haben aufgrund gesetzlicher Vorgaben umfangreiche Dokumentationspflichten und Vorkehrungen zu leisten. Schon heute müssen sich Apotheker authentifizieren – etwa per Passwort oder Codekarte. Diese Verfahren sind aber keineswegs robust gegen Manipulationen. Karten lassen sich bekanntermaßen besonders leicht vorsätzlich vertauschen. Passwörter stellen keine hinreichend vertrauenswürdige Authentifizierung sicher. Gefragt war eine Authentifizierungslösung für alle Anwendungen in der Apotheke. Als Lösung kommt für Österreichs Apotheken Palm-ID um Einsatz, basierend auf der PalmSecure Sensor-Mouse. Sie wird gegen die Standard-Mouse ausgetauscht und ein biometrisches Authentifizierungssysteme aus dem Gesundheitswesen für Apotheken installiert. Abschließend erfolgt eine einfache Ersterfassung der legitimierter Personen und Mitarbeiter. Die Fujitsu PalmSecure Technologie minimiert mittels Palm-ID das Fehlerpotenzial im Einzelhandel, da alle Arbeitsschritte, wie die Zubereitung oder Ausgabe von Arzneimitteln, als verlässliche Nachweise im gesamten IT-Anwendungsbereich vertrauenswürdig dokumentiert werden. Insbesondere im Umgang mit verschreibungspflichtigen Arzneien sowie Präparaten, die unter das Betäubungsmittelgesetz fallen, ist ein lückenloser Nachweis unerlässlich. Manipulationen, etwa durch Nachbearbeitung von Rezepten, unberechtigte Rabatte oder Warenentnahmen, gehören auf diese Weise der Vergangenheit an. PalmSecure kann zudem zur einheitlichen Authentifikation der Arbeitszeiterfassung, als Ersatz für den Zutrittscode der Alarmanlage oder zum e-Banking innerhalb der Apotheke verwendet werden.

VI. Biometrie-Einsatz am Büro-Arbeitsplatz und unterwegs

Auch am eigenen Arbeitsplatz-Rechner kann die Authentifizierung über die Pre-Boot-Authentifizierung, die Windows Authentifizierung oder das Single-Sign-on für Applikationen wie SAP mittels Handvenenscan erfolgen. Der PalmSecure Sensor konnte inzwischen auf die Höhe einiger Millimeter verkleinert werden und auf diese Weise erweiterte Fujitsu mit integrierten Sensoren das Produktspektrum der Ultrabooks und Workstations für mobile Nutzer. Damit ist der Sensor jetzt auch für neue Anwendungen verfügbar, die Absicherung des eigentlichen Notebooks ist dabei nur ein Teil eines Ganzen.

VII. Das PalmSecure ID Match Terminal

Sicherheitslösungen bedürfen fallbezogen auch sicherheitsbasierter Geräte. Das PalmSecure ID Match Terminal ist als kompaktes und sicheres Mehrzweckgerät konzipiert bestehend aus einem Touchscreen, einer integrierten Prozessorkarte, einem Multi-Card-Leser und einem Fujitsu PalmSecure Sensor für die Identifizierung und Verifizie-

rung von Personen auf Grundlage des Handflächenvenenmusters. Das Fujitsu PalmSecure ID Match Terminal stellt eine sichere Plattform dar, die aus einem präzise aufeinander abgestimmten Hardware- und Software-Stack besteht und eine gekapselte, sichere Betriebsumgebung für Anwendungen bereitstellt. Basierend auf dem gewünschten Einsatzkonzept können diese Anwendungen entweder autonom auf dem ID Match Terminal bzw. im Client-/Server-Betrieb verteilt zum Einsatz kommen bzw. auch direkt zur Absicherung im Data-Center und der dort laufenden Anwendungen dienen.

Fujitsu bietet damit eine komplette Lösungsplattform, die sich aus Hardware, Software und Services zur Optimierung biometrischer Sicherheitslösungen zusammensetzt: Das ID Match Terminal, mit äußerst effektiver ARM-Technologie, modernsten Sicherheitsfunktionen und den erforderlichen Schnittstellen für Sicherheitsanwendungen ist geeignet für Stand-alone-Betrieb, als Wandgerät oder auch integriert in POS-Systeme für sichere Zahlvorgänge.

Das PalmSecure ID Match Terminal unterstützt schnelle Verifizierungsprozesse und ist in einem Sicherheitsgehäuse mit aktivem Manipulationsschutz untergebracht. Benutzerfreundlichkeit und universelle Einsatzfähigkeit wird durch intuitiven, hygienischen und berührungslosen Betrieb sichergestellt und dient zur Verbesserung der Sicherheit auf physischer, logischer und funktionaler Ebene. Die optionale Verwendung als Match-on-Device-Lösung – das bedeutet: ohne zentrale Datenbank – garantiert größtmöglichen Datenschutz und Datensicherheit und erlaubt damit die Integration in allumfassende Sicherheitslösungen.

VIII. Biometrie und Identität als Einheit

Identitätsmanagement erfordert immer häufiger datenschutzkonforme und zugleich universelle Multi-Faktor-Identitätslösungen. Mithilfe der Identity Lösung PalmSecure truedentity von Fujitsu und OpenLimit werden diese Anforderungen nun sehr einfach unterstützt und für diverse Anwendungen parallel nutzbar. Sowohl aktive als auch passive Identitätskarten (z. B. Smart-, Kredit-, oder Banking-Cards) mit bzw. ohne Datenspeicher können zum Einsatz kommen. Ebenfalls kann auch ohne Identitätskarten jedoch mit Username oder PIN als zweitem Faktor gearbeitet werden. Beliebige Mischformen sind parallel einsetzbar für physische Zugangssysteme ebenso wie zur logischen Authentifizierung an Arbeitsplatzsystemen und Geräten (z. B. Gaming). PalmSecure truedentity garantiert eine sichere Authentifizierung auf der Basis biometrischer Erkennung des Handflächenvenenmusters und der sicheren Übermittlung nichtabstreitbarer Identitäten für nachgelagerte Anwendungen. Bisher verwendete unsichere und ausspähbare Kombinationen z. B. aus Username/Password werden leicht migrierbar. Mehrfach parallel betriebene und mehrfach verwaltete Identitätssilos können künftig mit einheitlichen und echten Identitäten versorgt werden. Damit stehen allen angeschlossenen Anwendungen gleichermaßen einheitliche und global nutzbare Identitäten bedarfsgerecht zur Verfügung. Biometrie basiertes Windows Logon und Single Sign On über Active Directory werden vollumfänglich unterstützt.

IX. Einsatz im Entertainment Sector

Aufgrund zunehmend gesetzlicher Regularien ist absehbar, dass es künftig zu deutlich vermehrter Unterstützung durch biometrisch basiertes Identitätsmanagement bei Spielstätten kommen wird. Hier bieten sich einfache, aber sehr effektive Lösungen aus der Kombination und Auswahl der oben beschriebenen Bausteine an. Im nachfolgenden Beispiel soll angenommen werden, dass eine initiale zentrale Registrierung des Spielers beim ersten Betreten einer Spielstätte bzw. eines Casinos erfolgt. Je nach Unternehmensform führt diese Erstregistrierung zu künftigen Folgenutzungen entweder für eine oder mehrere Spielstätten. Die Erstregistrierung erfolgt am Eingang durch eine biometrische Erfassung. Hierbei bieten sich zwei Varianten an. Im ersten Fall wird das biometrische Handflächenvenenmusters mit dem Geburtsdatum des Spielers verbunden, in einer zweiten Variante kann dies mit einem zweiten biometrischen Faktor, z. B. dem Gesichtsbild, geschehen. Beim wiederholten Zutritt erfolgt der Abgleich mit dem Handflächenvenenmusters und dem jeweils gewählten zweiten Faktor. Innerhalb der Spielstätte können die durch PalmSecure Sensoren ergänzten Spielgeräte allein mithilfe des Handflächenvenenmusters freigeschaltet werden. Das Konzept PalmSecure truedentity ermöglicht hierbei auch den Einsatz eines zentralen Identity-Providers für Spieler unter Beachtung der jeweils erforderlichen Datenschutzanforderungen. Die Spieleridentitäten können sowohl anonym als auch teil- oder vollidentifiziert verwaltet und wiedererkannt werden. Konzepte für große Spielstätten und Stadien sind inzwischen ebenfalls erfolgreich im Einsatz. Hier kommen unterschiedliche Lösungen als zweiter Faktor zum Einsatz, wie z. B. personalisierte Eintrittskarten bei Fußballstadien, die wie ein One-Time-Pad wirken und nach der Zugangskontrolle verfallen.

X. Zusammenfassung

Das Potenzial datenschutzkonformer und einfach einsetzbarer biometrischer Identitätslösungen für Biometrische Zugangskontrollen ist inzwischen für alle Branchen technologisch ausgereift vorhanden. Über 200 Mio. Nutzer dieser PalmSecure Technology bezeugen die Alltagstauglichkeit. Hierunter befinden sich weltweit auch Biometrische Identitätslösungen für den Entertainment Sector im Einsatz.

Die Autoren

Dr. *Waldemar Grudzien* ist Direktor im Geschäftsbereich Retail Banking und Bankentechnologie beim Bundesverband deutscher Banken e.V.

Prof. Dr. *Gerrit Hornung*, LL.M., studierte Rechtswissenschaften und Philosophie an den Universitäten Freiburg und Edinburgh. 2005 Promotion über Rechtsprobleme von Chipkartenausweisen (Wissenschaftspreis 2006 der Deutschen Stiftung für Recht und Informatik). 2004 bis 2006 Referendariat am Hanseatischen Oberlandesgericht. 2006 bis 2011 Geschäftsführer der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) und Habilitand an der Universität Kassel; 2013 Abschluss des Habilitationsverfahren mit der Arbeit Grundrechtsinnovationen. 2011 bis 2015 Professor für Öffentliches Recht, IT-Recht und Rechtsinformatik an der Universität Passau. Seit WS 2015/2016 Professor für Öffentliches Recht, IT-Recht und Umweltrecht an der Universität Kassel.

Dr. *Vera Jungkind* ist Rechtsanwältin und Partnerin der Sozietät Hengeler Mueller Partnerschaft von Rechtsanwälten mbB, Düsseldorf. Sie berät deutsche und internationale Unternehmen zu allen Fragen des Öffentlichen Wirtschaftsrechts, insbesondere zu Datenschutzrecht, Glücksspielrecht, Außenwirtschaftsrecht, Umweltrecht, Sozialversicherungsrecht, Verwaltungsverfahrens- und Verwaltungsprozessrecht. Dr. Vera Jungkind studierte deutsches und französisches Recht an der Universität des Saarlandes und der Université René Descartes, Paris V. Seit 2006 ist sie bei Hengeler Mueller tätig und hat auch Berufserfahrung bei einer Londoner Anwaltskanzlei gesammelt. Sie promovierte 2007 über das Thema Verwaltungsakte zwischen Hoheitsträgern. Sie ist Autorin zu datenschutzrechtlichen Themen im Formularbuch des Fachanwalts Arbeitsrecht (3. Aufl.) und im Beckschen M&A-Handbuch (i.E.).

Dr. *Jürgen Pampus* ist Mit-Gründer der Cognitec Systems und seit der Gründung im Jahre 2002 Vice President Sales & Marketing. Er war nach dem Physik-Studium im Bereich Großrechner und Supercomputer tätig, zunächst als Teamleiter und Consultant bei Control Data Corp., dann bei Siemens, wo er für den internationalen Vertrieb in der Abteilung Scientific Computing verantwortlich war. Bei Siemens war er maßgeblich am Aufbau der Biometrie-Abteilung beteiligt und initiierte im Jahr 1995 die Entwicklung der Gesichtserkennungstechnologie, die heute von Cognitec weiter entwickelt und vermarktet wird. Ab Januar 1998 war er als Sales Director für biometrische Systeme bei plettac electronics.

Martin Schallbruch leitet die Abteilung für Informationstechnik, Digitale Gesellschaft und Cybersicherheit im Bundesministerium des Innern. Als IT-Beauftragter des Ministeriums ist er zudem Stellvertreter der Beauftragten der Bundesregierung für Informationstechnik. Er ist verantwortlich für IT-Strategie und IT-Steuerung der Bundesverwaltung sowie die Zusammenarbeit von Bund und Ländern in IT-Fragen im Rahmen des IT-Planungsrats. Seine Verantwortung erstreckt sich auch auf die Cyber- und IT-Sicherheitspolitik, das Bundesamt für Sicherheit in der Informationstechnik (BSI), die Bundesstelle für Informationstechnik (BIT) sowie Pässe und Personalausweise.

Dr. *Michael Schneider* (geb. 1977) ist bei der Bundesdruckerei zuständig für die Marketing- und Portfoliostrategie. Der Informatiker gestaltet den erfolgreichen Weg des Berliner Unternehmens vom Sicherheitsdrucker zum umfassenden Systemanbieter für ganzheitliche Sicherheitslösungen Made in Germany mit. Dr. Michael Schneider promovierte bei Prof. Dr. Dr. h.c. mult. Wolfgang Wahlster am Deutschen Forschungszentrum für Künstliche Intelligenz in Saarbrücken über das Internet der Dinge. Er beschäftigt sich seit über einem Jahrzehnt in Forschungs- und Leitungsfunktionen mit der Anwendung digitaler Technologien zum Management und Schutz gefährdeter Infrastrukturen. Dr. Michael Schneider engagiert sich in verschiedenen Verbänden und Expertengremien zu Themen wie der intelligenten Vernetzung, Industrie 4.0 sowie vernetzten Service-Welten.

Dirk Uwer ist Rechtsanwalt und Partner der Sozietät Hengeler Mueller. Studium in Trier, Ferrara, Berlin (Dr. iur.), Speyer (Mag.rer.publ.) und Newcastle (LL.M.). Dr. Uwer ist auf das Öffentliche Wirtschaftsrecht spezialisiert und gilt seit vielen Jahren national und international als einer der führenden deutschen Spezialisten für regulierte Industrien. Er ist Autor von mehr als 70 Publikationen (u.a. zum Datenschutzrecht und zu Compliance-Fragen), Lehrbeauftragter an verschiedenen Hochschulen sowie 2015 und 2016 Mitglied des Steering Committee des International Forum on Privacy Law.

Thomas Walloschke, Principal Business Development Manager, Security Solutions bei Fujitsu Technology Solutions.