

Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz beim Einsatz biometrischer Verfahren

Dr. jur. Astrid Albrecht
Am Weitgarten 59, 53227 Bonn
aalbrechtlaw@aol.com

Abstract: Der Beitrag befasst sich mit biometrischen Authentifizierungsverfahren zwischen Wahrung von Persönlichkeitsrechten einerseits und der Eignung zum Nachweis von Authentizität im elektronischen Rechtsverkehr insbesondere bei der Verwendung elektronischer Signaturen andererseits. Ein Vergleich mit herkömmlichen Authentifizierungsmechanismen wie dem Prinzip Besitz und Wissen ergibt entscheidende Schwächen dieser Verfahren, da diese im Gegensatz zu biometrischen Verfahren keine unmittelbare Personenbindung und damit keine Personenverifikation zulassen. Auf der anderen Seite können sich durch die direkte Personenbindung biometrischer Merkmale besondere Gefährdungen der Persönlichkeitsrechte der Nutzer ergeben. Der Einsatz biometrischer Verfahren wird daher einer kritischen datenschutzrechtlichen Würdigung unterzogen. Im Rahmen der Sicherheitsanforderungen an biometrische Verfahren findet das Konzept der Privacy-Enhancing-Technologies besondere Berücksichtigung.

1. Problemstellung

Die Informationstechnologie ist als „Querschnittstechnologie“ nicht nur von fachspezifisch technischem, sondern auch von rechtlichem Interesse. Die elektronische Abwicklung bedeutsamer Verträge und Vereinbarungen nimmt stetig zu. Im papiergebundenen Rechtsverkehr, d.h. im Schriftverkehr, werden Authentizität und damit Urheberschaft vor allem durch die biometrische Handlung der eigenhändigen Unterschrift gewährleistet. Durch diese wird der Zusammenhang zwischen Erklärung und deren Urheber vermittelt. Im elektronischen Rechtsverkehr funktionieren diese althergebrachten Mittel zur Schaffung von Rechtssicherheit nicht mehr. Im Internet als „körperlosem Sozialraum“ ist die eindeutige Identifizierung des Geschäftspartners im Gegensatz zum realen Kaufhaus für alle Beteiligten dabei ungleich wichtiger. Denn aus der Körperlosigkeit ergeben sich spezifische, in der Offline-Welt nicht existente Risiken. Manipulationen an elektronischen Dokumenten hinterlassen grundsätzlich keine Spuren. Beim ungesicherten EDV-Verkehr besteht keine Gewähr dafür, dass ein versendetes Dokument unverändert beim Empfänger ankommt. Insbesondere besteht das Problem, den Urheber einer elektronischen Willenserklärung zweifelsfrei festzustellen. In zivil- und beweisrechtlicher Hinsicht ist dies jedoch notwendig, um Willenserklärungen einem bestimmten Rechtssubjekt zurechnen und in prozessualer Hinsicht die Urheberschaft auch nachweisen zu können. Elektronische Signaturen werden in diesem Zusammenhang nicht zuletzt durch deren rechtliche Anerkennung vor allem in § 126a BGB (elektronische Form) und § 292a ZPO (Anscheinsbeweis) besondere Bedeutung zugemessen, unterscheiden sich aber entscheidend von der eigenhändigen Unterschrift: die Verwendung eines Signaturschlüssels ist grundsätzlich nicht wie die eigene Hand an den Erklärenden unmittelbar gebunden. Biometrische Verfahren bieten sich hier deshalb an, weil diese im Gegensatz zu

Methoden wie PINs, Passwörtern und Besitzelementen die unmittelbare Bindung einer elektronischen Transaktion an die Person ermöglichen.

Den Vorteilen einer solchen direkten Authentifizierung steht die regelmäßige Verwendung personenbezogener Daten gegenüber. Aus der unmittelbaren Personenbindung heraus können daher besondere Gefährdungen erwachsen. Zu den diesbzgl. noch nicht abschließend geklärten Fragen gehört etwa der datenschutzrechtlich entscheidende Aspekt eines Personenbezugs biometrischer Daten. Zudem hängt die Risikobewertung biometrischer Daten entscheidend vom Verarbeitungsmodus sowie davon ab, in wessen Zugriffsbereich die Daten gespeichert werden. Klassische Kernbereiche des Schutzes der informationellen Selbstbestimmung können gleichfalls berührt sein, von denen hier einige exemplarisch andiskutiert werden.

2. Authentizität im Rechtsverkehr durch biometrische Handlungen

Im herkömmlichen Rechtsverkehr erlangt die biometrische Handlung der eigenhändigen Unterschrift Bedeutung bei der „klassischen“ Schriftform gemäß § 126 BGB. Diese dient dem Nachweis und der Sicherung von Rechten und Pflichten der Parteien. Das traditionelle Vertrauen in die so abgebildete eigenhändige Unterschrift zeigt sich u.a. darin, dass zahlreiche Vereinbarungen im Privatverkehrsverkehr trotz überwiegender Formfreiheit schriftlich abgeschlossen werden. Im Sinne von Beweissicherheit ist daher der besondere Grund für die faktische Bedeutung der Schriftform in dem Bedürfnis der Parteien zu sehen, das Erklärte oder Vereinbarte beweissicher zu halten¹. Im elektronischen Rechtsverkehr bedient sich der Aussteller eines elektronischen Dokuments im Gegensatz zur eigenen Hand technischer Hilfsmittel wie einer Chipkarte und Geheimzahlen wie z.B. PINs. Dabei fehlt es prinzipiell an einer Realisierung der klassischen Sicherungsfunktionen der Schriftform². Zu diesen gehören vor allem die Identitätsfunktion, die den Aussteller einer Erklärung erkennen lässt, und die Beweisfunktion, mit der das vorgenommene Rechtsgeschäft beweiskräftig dokumentiert wird. Insbesondere fehlt der unmittelbare Zusammenhang zwischen Text und Urheber, der sonst über die eigenhändige Unterschrift hergestellt wird.

3. Elektronische Signaturen im elektronischen Rechtsverkehr

Um das für die Teilnehmer am elektronischen Rechtsverkehr ebenfalls bestehende Bedürfnis, Gewissheit über Authentizität und Urheberschaft eines elektronischen Dokuments herzustellen, sind daher technische Maßnahmen erforderlich, die die Individualisierung Parteien gewährleisten sowie diese für Beweiszwecke nachweis- und verwertbar machen. Die Rechtsverbindlichkeit und der Beweiswert einer elektronischen Transaktion hängen dabei ganz entscheidend von der tatsächlichen Sicherheit der eingesetzten technischen Verfahren und Komponenten ab³. In diesem Rahmen gelangt die elektronische Signatur an Bedeutung. Diese stellt nach § 2 Nr.1 SigG⁴ in

¹ Bizer, Beweissicherheit im elektronischen Rechtsverkehr, 141 ff.

² Bizer, Digitale Dokumente im elektronischen Rechtsverkehr, 151.

³ Bizer in Bizer/Miedbrodt: Die digitale Signatur im elektronischen Rechtsverkehr, 136 ff., 145; so auch Nocke, Gesetzliche Schriftform und elektronische Willenserklärung, 322 ff., 335.

⁴ Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, vom 16.05.2001, BGBl. I 2001, S. 876.

Anlehnung an die EG-Signaturrechtlinie⁵ „Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind“ dar. Jedenfalls ab der Stufe der fortgeschrittenen elektronischen Signatur nach § 2 Nr.2 SigG kann grundsätzlich das Problem der Integrität gelöst werden, da hier die nachträgliche Veränderung eines elektronisch signierten Dokumentes zwar nicht verhindert, jedoch festgestellt werden kann.

Die hinreichend sichere Verknüpfung eines elektronisch signierten Dokumentes mit dem Signierenden kann dadurch jedoch nicht gewährleistet werden. Die Authentizität der elektronisch signierten Willenserklärung hängt dabei entscheidend von dem eingesetzten Authentifizierungsverfahren ab, mit dem der Signiervorgang in Gang gesetzt wird. Daher ist gemäß § 17 I SigG bei der qualifizierten Signatur der Einsatz sicherer Signaturerstellungseinheiten vorgeschrieben, die den Signaturschlüssel „gegen unberechtigte Nutzung des Signaturschlüssels schützen“ sollen. IdR werden hier Wissens- und Besitzelemente verwendet. Diese können jedoch nur eine mittelbare Authentifizierung des Rechtssubjekts durchführen. Verbleibende Restrisiken der nur abgeleiteten Erkennung der handelnden Person und des daraus entstehenden Missbrauchspotenzials werden nicht zuletzt durch die Festlegung von Sorgfaltspflichten für den PIN-Inhaber oftmals auf diesen abgewälzt. Dies kann zu ungerechter Haftungs- und Beweislastverteilung zu dessen Lasten führen, wie Erfahrungen mit der Rechtsprechung zum EC-Karten-Missbrauch hinlänglich gezeigt haben⁶. Neben Wissens- und Besitzelementen können aber auch biometrische Merkmale eingesetzt werden, wenn sie mit einem Besitzelement verknüpft werden und gewissen Mindestsicherheitsanforderungen genügen, § 15 I 1 SigG. Diese umfassen eine Evaluierung nach Common Criteria (EAL 4 mit Mechanismenstärke mittel bis hoch).

Die Herstellung der notwendigen Funktionsäquivalenz der elektronischen Form nach § 126a BGB im Sinne einer Abbildung der rechtlich bestimmten sozialen Funktionen der eigenhändigen Unterschrift durch eine andere Technik⁷ muss bei der Verwendung lediglich von Wissens- und Besitzelementen bei der Signaturerzeugung bezweifelt werden. Die besondere Eigenschaft der eigenhändigen Unterschrift, Authentizität durch die unmittelbare Personenbindung tatsächlich herstellen zu können, und der damit verbundene soziale Vertrauenstatbestand, können durch eine derartige Signatur nicht ohne weiteres adäquat abgebildet werden⁸.

Im zivilprozessualen Bereich stützt sich § 292a ZPO auf die qualifizierte elektronische Signatur. § 292a ZPO kann als „vorgezogener Anscheinsbeweis“ qualifiziert werden⁹, da ein allgemeiner Erfahrungssatz bzgl. der Sicherheit qualifizierter Signaturverfahren, von dem auf die Echtheit der elektronischen Willenserklärung geschlossen werden könnte, mangels umfassenden Einsatzes elektronischer Signaturen noch nicht besteht. Der Gesetzgeber aber vertraut darauf, dass die Rahmenregelungen des Signaturgesetzes für qualifizierte Signaturen ausreichend sind, um ein entsprechendes Maß an technischer und organisatorischer Sicherheit zu garantieren¹⁰. Zwar sollte allein der einfache Einwand des Signaturschlüssel-Inhabers, er habe die mit seiner Signatur versehene Erklärung nicht abgegeben, aus Gründen der Rechtssicherheit nicht grundsätzlich zur vollen Beweislast für die Herkunft der Signatur seitens des Empfängers führen. Jedoch kann eine ungerechtfertigte Beweislastverteilung insofern eintreten, als sich der Signaturschlüssel-Inhaber auch an solchen Signaturen festhalten lassen muss, die ohne sein Wissen mit seinem

⁵ Richtlinie 1999/93 EG des Europäischen Parlaments und des Rates vom 13.12.1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. EG L 13/12 vom 19.01.2000.

⁶ Albrecht, Biometrie zum Nutzen für Verbraucher? DuD 2000, 332 ff.

⁷ Bizer, Beweissicherheit im elektronischen Rechtsverkehr, 141 ff., 147 Fußnote 28.

⁸ Bizer, Der gesetzliche Regelungsbedarf digitaler Signaturverfahren, DuD 1995, 459 ff., 462.

⁹ So die Einordnung bei Roßnagel, in Roßnagel, Recht der Multimedia-Dienste, 5. Teil SigG, § 1 Rz. 44.

¹⁰ Fischer-Dieskau u.a., Elektronisch signierte Dokumente als Beweismittel im Zivilprozess, MMR 2002, 709 ff., 710

Signatur Schlüssel erstellt worden sind. Manipulationen gehen aufgrund § 292a ZPO zu Lasten des Berechtigten, ohne dass es für diese Folge technisch belastbare Sicherheiten gäbe¹¹.

Die Verwendung biometrischer Verfahren zur Durchführung einer echter Personenverifikation könnte demnach sowohl in materiell- als auch prozessrechtlicher Hinsicht zu höherer Rechtssicherheit führen. Technisch hinreichend sichere biometrische Systeme könnten dazu beitragen, dass eine elektronische Transaktion tatsächlich an die berechtigte Person gebunden ist und eine missbräuchliche Verwendung etwa von Signaturschlüsseln jedenfalls ohne wissentliches Mitwirken des Signaturschlüssel-Inhabers nicht ohne weiteres möglich ist.

4. Sicherheit biometrischer Systeme

Sollen biometrische Verfahren tatsächlich zu höherer Rechtsverbindlichkeit und besserer Beweissicherheit im elektronischen Rechtsverkehr beitragen, müssen diese selbst gewissen Sicherheitsanforderungen genügen. Zudem benötigen auch datenschutzgerechte Systeme sichere Informationstechnologie, jedoch folgt auf die Umsetzung informationstechnischer Sicherheit nicht unmittelbar und ohne weiteres ein datenschutzgerechtes System.

Aus Sicht der Datensicherheit ist zunächst die enge Bindung biometrischer Merkmale an die Person zu begrüßen¹². Wenn tatsächlich sichergestellt ist, dass eine korrekte Zuordnung der Identität einer Person zu den Referenzdaten erfolgt, können biometrische Verfahren die zuverlässige Überprüfung leisten, ob es sich um die entsprechende Person handelt. Andererseits können kompromittierte körperliche Merkmale eines Nutzers grundsätzlich nicht wie eine Geheimzahl ausgetauscht oder widerrufen werden. Zudem ist die Menge der zur Verfügung stehenden Merkmale prinzipiell begrenzt. Die für den Grad der erreichbaren Datensicherheit entscheidende Sicherheit der Systeme selbst hängt in großem Maße vom Schutz der Referenzdaten und den Vergleichsmechanismen ab. Zunächst müssen diese tatsächlich von den Merkmalen der Person stammen, der sie zugeordnet sind. Zudem muss ihre Integrität, d.h. ihre Unverfälschtheit, beim Einlernen, aber auch anschließend stets gewährleistet sein. Schließlich dürfen die Eingabedaten, die die Sensoren aus den biometrischen Merkmalen gewinnen, nicht abgehört und wiedereingespielt aber auch nicht mit oder ohne Mitwirkung des Nutzers einfach reproduziert werden können.

4.1. Erkennungsleistung und Überwindungssicherheit

Zuverlässigkeit und Sicherheit biometrischer Systeme hängen grundsätzlich von Wahrscheinlichkeiten ab und muss kalibriert werden. Die Falschzurückweisungsrate (FRR) gibt an, welcher prozentuale Anteil von Versuchen von korrekten Benutzern fälschlicherweise abgewiesen wird. Die Erkennungsleistung wird hier üblicherweise bei einem Prozentsatz von größer als 7 % als schwach, bei kleiner als 1 % als sehr stark klassifiziert¹³. Die Falschakzeptanzrate (FAR) gibt den Prozentsatz an, bei welchem Anteil von Versuchen eine

¹¹ Gesellschaft für Informatik, Stellungnahme zum Gesetzentwurf „Formvorschriften des Privatrechts“, DuD 2001, 38 ff., 39.

¹² Köhntopp, Technische Randbedingungen für einen datenschutzgerechten Einsatz biometrischer Verfahren, 177 ff., 180.

¹³ Munde, Die Evaluation biometrischer Systeme, 145 ff., 153.

Falsch-Erkennung erfolgt, d.h. eine falsche Identität zugewiesen wird. Bei einem Prozentsatz von größer als 5 % wird die Erkennungsleistung hier als schwach, bei einem Prozentsatz von kleiner als 0,3 % als sehr stark bezeichnet¹⁴. Beide Raten korrelieren insoweit miteinander, als dass eine hohe FAR eine niedrige FRR zur Folge hat und umgekehrt¹⁵. Die Einstellung der Fehlerraten biometrischer Systeme ist vor allem abhängig von der gewählten Anwendung. Wird also z.B. in Hochsicherheitsbereichen die FAR niedrig eingestellt, hat dies eine hohe FRR und damit eine geringere Bequemlichkeit für den Nutzer zur Folge. Bei einer niedrigen FRR hingegen ergeben sich höhere Zahlen von Falschakzeptanzen. Vielfach wird als Einstellung des biometrischen Systems die möglichst kleine sog. „Equal-Error-Rate“ (EER) verwendet, bei dem beide Fehlerraten, FAR und FRR, gleich sind.

Neben der Erkennungsgüte ist darüber hinaus die Überwindungssicherheit eines biometrischen Systems ein entscheidender Faktor für die Sicherheit des Systems. Die verschiedenen Angriffe auf ein biometrisches System betreffen u.a. die Erfassung des Merkmals und dessen Fälschung sowie die Datenübertragung vom Sensor.

4.2. Sicherheitsinfrastruktur

Vertrauen in biometrische Systeme bedarf schließlich einer Abstützung u.a. durch organisatorische Maßnahmen. Anerkannte Evaluierungskriterien und deren Bestätigung durch unabhängige Stellen im Rahmen einer Zertifizierung können zu Vertrauen beitragen. Evaluation wird grundsätzlich als wichtiger Baustein beim Aufbau und Betrieb von Infrastruktur-Einrichtungen der Informationsgesellschaft betrachtet¹⁶. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im Jahre 2000 u.a. aus dem Projekt „BioIS“ technische Evaluierungskriterien entwickelt, die sich gegenwärtig im Entwurfsstadium befinden und auch im Rahmen internationaler Gremien weiterentwickelt werden¹⁷. Als Zertifizierungsinstanz kann ebenfalls das BSI genannt werden, das zur Förderung der Sicherheit in der Informationstechnik u.a. die Aufgabe hat, die Sicherheit von informationstechnischen Systemen oder Komponenten zu prüfen und zu bewerten sowie Sicherheitszertifikate zu erteilen, vgl. § 3 I Nr.3 BSIG.

Daneben kommt die Etablierung eines Gütesiegels zur Funktionalität biometrischer Systeme in Betracht. Dieses könnte neben der Gewährleistung der Grundfunktionalität auch den Schutz gegen Angriffe mit geringem Aufwand, den Grundschutz der eingespeicherten biometrischen Daten sowie den Nachweis einer leicht nachvollziehbaren Mindestqualität bestätigen¹⁸.

4.3. Privacy-Enhancing-Technologies

Bei der Diskussion über Sicherheit biometrischer Systeme im Zusammenhang mit Datenschutz sollte auch das Konzept der Privacy-Enhancing-Technologies (PET) mit einbezogen werden.

¹⁴ Munde, Die Evaluation biometrischer Systeme, 145 ff., 153.

¹⁵ Köhntopp, Technische Randbedingungen für einen datenschutzgerechten Einsatz biometrischer Verfahren, 177 ff., 180.

¹⁶ Deutscher Bundestag, Enquete-Kommission Zukunft der Medien in Wirtschaft und Gesellschaft, Sicherheit und Schutz im Netz, BT-Drs. 13/11002, 55.

¹⁷ BSI, Technische Evaluierungskriterien zur Bewertung und Klassifizierung biometrischer Systeme, Entwurf Version 0.6 (14.9.2000).

¹⁸ Giesecke/Kalo/Lassmann, Erfahrungen mit biometrischen Systemen, 378 ff., 386 f.

Diese werden definiert als ein zusammenhängendes Ganzes von informations- und kommunikationstechnologischen Maßnahmen, die die Privatsphäre schützen, indem sie personenbezogene Daten eliminieren oder vermindern oder unnötige bzw. unerwünschte Verarbeitung personenbezogener Daten verhindern, ohne Verlust der Funktionsfähigkeit des Informationssystems¹⁹. Während also biometrische Systeme bei geeigneter Gestaltung zur Realisierungshilfe und einem wichtigen Baustein für PET werden können, kann dieses Konzept auch auf die technische Gestaltung biometrischer Systeme selbst angewendet werden. Unter anderem sind hier die benannte Evaluierung und Zertifizierung von biometrischen Systemen, die personenbezogene Daten verwenden, sowie Maßnahmen der Verschlüsselung einzubeziehen.

5. Persönlichkeitsschutz

Die Ambivalenz der biometrischen Technologie zeigt sich insbesondere im Bereich des Datenschutzes. Biometrie ermöglicht zwar einerseits eine datenschutzgerechte und personengebundene Authentifizierung, begründet aber andererseits neuartige Datenschutzrisiken. Im spezifischen Datenschutzkontext können biometrische Systeme etwa zur Bekämpfung des sog. Identitätsdiebstahls eingesetzt werden. Dieser bezeichnet ein Vorgehen, bei dem jemand Personendaten, die einem anderen zugeordnet sind, verwendet, um etwa finanzielle Transaktionen vorzunehmen. Könnten diese Daten mittels biometrischer Systeme besser vor Entwendung geschützt werden, wäre ein Missbrauch voraussichtlich nicht mehr ohne weiteres und jedenfalls nicht mehr allein durch Erlangen bloß personenbezogener Kennnummern möglich. Andere, bei den herkömmlichen Verfahren nicht vorkommende Risiken können jedoch aus dem hier möglichen „Angewachsensein“ elektronischer Transaktionen entstehen²⁰. Bzgl. des erwähnten Identitätsdiebstahls könnten neue Risiken etwa dann entstehen, wenn biometrische Daten einer Person erlangt und diese wiederum zum Zweck des Identitätsdiebstahls missbraucht werden.

5.1. Personenbezug biometrischer Daten

Der Schutzbereich der informationellen Selbstbestimmung als Kernbereich des Datenschutzes ist erst dann betroffen, wenn es sich um personenbezogene Daten handelt. Nach § 3 I BDSG sind solche „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbar natürlichen Person“. Die EG-Datenschutzrichtlinie gibt einen Anhaltspunkt dafür, wann eine Person als bestimmbar anzusehen ist. Artikel 2 a) besagt: „(...) als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind“²¹.

Grundsätzlich ist eine direkte Identifizierung eines Menschen anhand eines körperlichen Merkmals

¹⁹ Borking, Privacy-Enhancing-Technologies (PET), DuD 2001, 607 ff., 610.

²⁰ Kumbrock, Der „unsichere Anwender“ – vom Umgang mit Signaturverfahren, DuD 1994, 20 ff., 28 im Hinblick auf die mögliche Erhöhung der Sicherheit elektronischer Signaturen durch die Verwendung biometrischer Verfahren und dem gleichzeitig bestehenden Widerspruch zu Freiheitsrechten.

²¹ Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG 1995 Nr. L 281 S. 31 vom 23.11.1995.

möglich, das in einem biometrischen Datensatz verarbeitet wird²². Ein solches bezieht sich im Original immer nur auf eine einzige bestimmte Person²³. Aus diesem Grund erscheint es angebracht, biometrische Angaben stets als personenbezogene Daten anzusehen und folgerichtig jegliche Verarbeitung und Nutzung dieser Daten als einen rechtlich legitimationsbedürftigen Eingriff in das Recht auf informationelle Selbstbestimmung zu begreifen²⁴.

Hinsichtlich biometrischer Templates kann ein Personenbezug grundsätzlich durch zusätzliche Identifizierungs- und Adressierungsinformationen entstehen sowie durch einen Vergleich mit neuen Templates, wenn dadurch ein Rückschluss auf den Betroffenen iSv § 3 I BDSG ermöglicht wird. Ob dies der Fall ist, hängt stark von dem Verwendungszusammenhang und der Nutzbarkeit des Templates ab. Diese sind wiederum abhängig davon, wo das Template abgelegt, d.h. gespeichert ist und wer potenziellen Zugriff auf die Daten hat. Während bei einer Identifikation, also bei der Frage nach „Wer ist die Person?“ auf eine Datenablage in einer Datenbank nicht verzichtet werden kann, ist bei Verifikationsverfahren („Ist die Person diejenige für die sie sich ausgibt?“) auch die dezentrale Speicherung möglich. Schließlich ist die sog. Selbstauthentifizierung zu nennen, bei der zusätzlich der gesamte Erkennungsvorgang auf der mobilen Speichereinheit selbst abläuft. Solange aus existenten Daten der Betroffene noch bestimmbar ist, ist grundsätzlich von einem Personenbezug iSv § 3 I BDSG auszugehen.

Für einen möglichst umfassenden Schutz der informationellen Selbstbestimmung erscheint es somit sinnvoll, in Zukunft biometrische Daten, Rohdaten wie Templates, ausdrücklich als personenbezogene Daten im Sinne des § 3 I BDSG zu kodifizieren. Dies ist von Art. 2 a) EG-Datenschutzrichtlinie abgedeckt²⁵ und folgt u.a. dem kanadischen Datenschutzrecht, in dem personenbezogene Daten als „the address, fingerprints or blood type of the individual“ definiert und somit biometrische Merkmale klar in den Schutzbereich des Gesetzes mit einbezogen werden²⁶.

5.2. Risikobewertung, Datenvermeidung und -sparsamkeit

Je nach gewählter Lösung ist neben der Bestimmung des Personenbezugs auch das Risikopotenzial biometrischer Daten differenziert zu beurteilen. Ebenfalls abhängig von der Art der Speicherung und Verarbeitung der Daten kann zudem den Geboten der Datenvermeidung und der Datensparsamkeit mehr oder weniger genügt werden. Nach § 3a BDSG dürfen Datenverarbeitungssysteme keine oder so wenig personenbezogene Daten wie möglich erheben, verarbeiten oder nutzen. Das bedeutet, dass in Umsetzung des Verhältnismäßigkeitsprinzips diese technisch so zu gestalten sind, dass keine oder so wenig wie möglich personenbezogene Daten anfallen (Systemdatenschutz). Zudem ist von den Möglichkeiten der Anonymisierung (§ 3 VI BDSG) und Pseudonymisierung (§ 3 VI a BDSG) Gebrauch zu machen, soweit möglich und angemessen, vgl. § 3a, 2 BDSG, um den Schutz betroffener Personen präventiv sicherzustellen.

Bei einer zentralen Datenablage ist vor allem das latente Missbrauchsrisiko als problematisch anzusehen. Ein zentraler Abgleich ermöglicht es, Bewegungsprofile zu erstellen, auch über die

²² Borking, Privacy Enhancing Technologies (PET), DuD 2001, 607 ff., 611.

²³ Bis auf die äusserst seltenen Fälle, in denen ein biometrisches Merkmal einer Person zu 100 % demjenigen einer anderen Person gleicht.

²⁴ Weichert, Biometrie – Freund oder Feind des Datenschutzes? CR 1997, 369 ff., 372.

²⁵ Begründung zu Art. 2 des geänderten Vorschlags, vgl. Dammann-Simitis, EG-Datenschutzrichtlinie, Anm. 106 unter a).

²⁶ Privacy Act 1980-81-82-83, c. 111, Sch. II "1".

Zwecke der Identifizierung hinaus²⁷. Die Schaffung einer zentralen biometrischen Datenbank würde einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen darstellen, wobei genau zu prüfen wäre, ob eine solche nicht gänzlich unzulässig wäre. In diesem Zusammenhang ist die Entscheidung des Gesetzgebers zu sehen, bei Zulassung weiterer biometrischer Merkmale in Personaldokumenten die Einrichtung einer bundesweiten Datei der erfassten biometrischen Daten zu untersagen, vgl. § 4 IV 2 PassG und § 1 V 2 PersonalausweisG²⁸.

Bei einer dezentralen Speicherung kann dem Selbstbestimmungsrecht des Anwenders in hohem Maße Genüge getan werden²⁹. Jedenfalls sind unzulässige Speicherung oder Zweckänderungen ohne Mitwirkung des Betroffenen in diesem Fall ausgeschlossen, da sich die biometrischen Daten in dessen Verfügungsgewalt befinden. Auch unter dem Gesichtspunkt der Datensicherheit ist die dezentrale Speicherung der biometrischen Templates weniger verletzlich als die zentrale Ablage³⁰. Unbefugte könnten allerdings den Datenträger, auf dem das Template abgelegt ist, entwenden. Bei nicht hinreichender Sicherung der biometrischen Daten auf dem Token selbst könnten diese Zugriff auf die Daten erhalten und sie weiterverwenden, etwa für ein Wiedereinspielen der Daten. Die Anwesenheit des Betroffenen zu einem bestimmten Zeitpunkt an einem bestimmten Ort oder dessen angeblicher Zugriff auf Daten könnten so vorgetäuscht werden. Dies aber würde den Betroffenen in seinem Recht auf informationelle Selbstbestimmung insoweit verletzen, als dadurch Angaben über ihn selbst verfälscht würden.

Im Falle der lokalen Lösung bei der Selbstauthentifizierung verbleiben die biometrischen Daten stets im Verfügungsbereich des Betroffenen. Sie müssen auch nicht zum Zwecke des Abgleichs ausgelesen werden. Daher würde dessen Recht auf informationelle Selbstbestimmung hiermit am besten gewährleistet. Zusätzlich verringerte sich das Angriffsrisiko, da der Angreifer nunmehr nicht mehr in die Übermittlung der Daten an eine Datenbank eingreifen oder die Datenbank selbst angreifen könnte³¹. Für einen Missbrauch müsste z.B. das biometrische Merkmal des Berechtigten selbst gefälscht werden und dem Sensor gegenüber präsentiert werden.

5.3. Diskriminierung

Ein weiterer datenschutzrechtlicher Grundsatz kann im Zusammenhang mit der Verwendung biometrischer Daten berührt werden. Das Recht auf informationelle Selbstbestimmung schützt vor jeglicher Stigmatisierung und einer daraus erwachsenden Rechtfertigungslast³². Ein Betroffener kann durch den Einsatz biometrischer Verfahren dadurch diskriminiert werden, dass sein körperliches Merkmal für die biometrische Erkennung nicht oder nicht so gut geeignet ist wie bei der übrigen Benutzergruppe, und dadurch das konkret eingesetzte biometrische System bei ihm nicht oder nicht fehlerfrei funktioniert. Falschzurückweisungen sind aufgrund der technischen Besonderheiten biometrischer Verfahren prinzipiell nicht zu vermeiden, s.o. Dies kann zu negativen Rückschlüssen auf das körperliche Merkmal des Betroffenen und zu dessen Ausgrenzung innerhalb der Benutzergruppe führen³³.

²⁷ Weichert, Die Wiederbelebung des Personenkennzeichens, RDV 2002, 167 ff., 172.

²⁸ Geändert durch das Gesetz zur Bekämpfung des internationalen Terrorismus, BGBl. 2002 I Nr. 3 vom 11.01.2002, S. 361 ff., vgl. BT-Drs. 14/7386, 7.

²⁹ So auch CNIL, 22e rapport d'activité 2001, 168 f.

³⁰ Bizer, Selbstauthentifizierende Ausweiskarte, DuD 2002, 44.

³¹ S. zu den Angriffsmöglichkeiten auch 2. Kapitel § 4 III. 2.

³² Burchard, Verfassungsrechtliche Interessenabwägung im Informationsrecht, KritV 1999, 239 ff., 243.

³³ ULD, Positionspapier zum Antiterrorgesetz der Bundesregierung, 12.

5.4. Unbemerkte Erhebung und Überwachung

Eine vom Betroffenen unbemerkte Erhebung biometrischer Daten würde dessen Recht auf informationelle Selbstbestimmung ebenfalls beeinträchtigen und zudem das Risiko der Überwachung erhöhen. Gemäß § 4 II BDSG muss die Erhebung personenbezogener Daten grundsätzlich beim Betroffenen selbst erfolgen. Dies macht eine unbemerkte Erhebung in der Regel unzulässig. Dies gilt sowohl für die Erstellung des Referenzdatensatzes als auch für die spätere Datenerhebung zum Zwecke der Wiedererkennung³⁴. Würden Personen ohne ihr Einverständnis mittels derartiger Verfahren identifiziert, läge darin somit ein grundsätzlich unzulässiger Eingriff in das Recht der informationellen Selbstbestimmung. Ob eine verdeckte, d.h. nicht-kooperative Erfassung eines körperlichen Merkmals überhaupt möglich ist, hängt von dem eingesetzten biometrischen System ab³⁵. Es kommt darauf an, ob dieses ein solches Verfahren verwendet, das eine aktive Mitwirkung des Betroffenen, d.h. einen Körperkontakt oder eine spezielle Haltung des Körpers im Sinne einer Aufnahmeposition erfordert.

6. Fazit und Ausblick

Die herausragende Eigenschaft biometrischer Authentifizierungsmechanismen besteht darin, unmittelbar an die Person gebundene körperliche Merkmale zu verwenden und damit eine echte Verifikation zu ermöglichen. Wenn Authentizität nicht nur im elektronischen Rechtsverkehr, sondern auch im Hinblick auf die notwendige Datensicherheit mittels Biometrie erhöht werden soll, müssen gleichzeitig die potenziellen Gefährdungen für den Persönlichkeitsschutz angemessen berücksichtigt werden. In jedem Fall muss bei der Verwendung biometrischer Daten eine sorgfältige Abwägung zwischen den schutzwürdigen Interessen des Betroffenen und den berechtigten Interessen der verantwortlichen Stelle zur Wahrung der Persönlichkeitsrechte der Betroffenen führen. Zur Realisierung erlangt neben gesetzlichen Regelungen, deren notwendiger Umfang zukünftig noch näher zu betrachten ist, vor allem die zunehmende Technisierung des Datenschutzes unter Realisierung des Konzepts der Privacy-Enhancing-Technologies besondere Bedeutung. Biometrische Authentifizierungsmethoden werden schließlich nur dann eine wesentliche Rolle im elektronischen Rechtsverkehr einnehmen können, soweit gleichzeitig der Schutz der Persönlichkeitsrechte der Betroffenen sichergestellt wird.

Literaturverzeichnis

- Albrecht, A.*, Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, Dissertation Universität Frankfurt April 2003, i.E. Nomos 2003, Reihe Frankfurter Studien zum Datenschutz, hrsg. von Prof. Dr. Dr. hc. Sprios Simitis
- Dies.*, Biometrie zum Nutzen für Verbraucher?, DuD 2000, S. 332 ff.
- Bizer, J.*, Der gesetzliche Regelungsbedarf digitaler Signaturverfahren, DuD 1995, S. 459 ff.
- Ders.*, Beweissicherheit im elektronischen Rechtsverkehr, S. 141 ff., in: Haratsch, A./Kugelman, D./Repkewitz, U.: Herausforderungen an das Recht der Informationsgesellschaft, Boorberg Stuttgart 1996

³⁴ Gundermann/Probst, Brennpunkte des Datenschutzes, Rz. 98.

³⁵ Die Datenschutzbeauftragten des Bundes und der Länder, Entschließung der 63. Konferenz, 6.

Ders., Das Schriftformprinzip im Rahmen rechtsverbindlicher Telekooperation, DuD 1992, S. 169 ff.

Ders., Digitale Dokumente im elektronischen Rechtsverkehr, S. 148 ff., in: Kröger, Detlef (Hrsg.): Internet für Rechtsanwälte und Notare, Hermann Luchterhand Verlag GmbH, Neuwied u.a. 1997

Ders., Selbstauthifizierende Ausweiskarte, DuD 2002, S. 44

Bizer, J./Miedbrodt, A., Die digitale Signatur im elektronischen Rechtsverkehr – Deutsches Signaturgesetz und Entwurf der Europäischen Richtlinie, S. 136 ff., in: Kröger, Detlef/Gimmy, Marc A. (Hrsg.): Handbuch zum Internetrecht: Electronic Commerce – Informations-, Kommunikations- und Mediendienste, Springer Berlin u.a. 2000

Die Datenschutzbeauftragten des Bundes und der Länder, Entschließung der 63. Konferenz vom 07.03.-08.03.2002: Biometrische Merkmale in Personalausweisen und Pässen

Bobrowski, M., Biometrie und Verbraucherschutz, DuD 1999, S. 159

Borking, J., Privacy-Enhancing-Technologies (PET), DuD 2001, S. 607 ff.

Burchard, D., Verfassungsrechtliche Interessenabwägung im Informationsrecht, KritV 1999, S. 239 ff., 243

Commission Nationale de l'Informatique et des Libertés (CNIL), 22e rapport d'activité Paris 2002

Dammann, U./Simitis, S., EG-Datenschutzrichtlinie, Kommentar, Nomos Baden-Baden 1997

Fischer-Dieskau, S., u.a., Elektronisch signierte Dokumente als Beweismittel im Zivilprozess, MMR 2002, S. 709 ff.

Gesellschaft für Informatik, Stellungnahme zum Gesetzesentwurf "Formvorschriften des Privatrechts", DuD 2001, S. 38 ff.

Giesecke, H.-J./Kalo, H./Lassmann, G., Erfahrungen mit biometrischen Systemen, S. 378 ff., in: Nolde, V./Leger, L.: Biometrische Verfahren, Körpermerkmale als Passwort, DWD 2002

Gundermann, L./Probst, Th., Brennpunkte des Datenschutzes, Kapitel 9 in: Roßnagel, A.: Handbuch des Datenschutzrechts, C.H. Beck München 2003

Kiper, M., Biometrische Identifikation, CF 8-9/1999, S. 46 ff.

Köhntopp, M., Technische Randbedingungen für einen datenschutzgerechten Einsatz biometrischer Verfahren, S. 177 ff., in: Horster, P.: Sicherheitsinfrastrukturen, Vieweg 1999

Kumbruck, Ch., Der „unsichere Anwender“ – vom Umgang mit Signaturverfahren, DuD 1994, 20 ff., 28

Langenbach, Ch.J./Ulrich, O. (Hrsg.), Elektronische Signaturen – Kulturelle Rahmenbedingungen einer technischen Entwicklung, Springer Berlin u.a. 2002

Munde, A., Die Evaluation biometrischer Systeme, S. 145 ff., in: Nolde, V./Leger, L.: Biometrische Verfahren, Körpermerkmale als Passwort, DWD 2002

Nocke, C., Gesetzliche Schriftform und elektronische Willenserklärung – Neue Formvorschriften für den eCommerce, S. 322 ff. in: Nolde, Veronika/Leger, Lothar (Hrsg.): Biometrische Verfahren – Körpermerkmale als Passwort, Deutscher Wirtschaftsdienst Köln 2002

Roßnagel, A. (Hrsg.), Recht der Multimedia-Dienste, Kommentar zum IuKDG und zum MDSStV, C.H. Beck München 2001

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Positionspapier zum Antiterrorgesetz der Bundesregierung, Kiel 07.12.2001, www.datenschutzzentrum.de

Weichert, Th., Biometrie-Freund oder Feind des Datenschutzes, CR 1997, S. 369 ff.

Ders., Die Wiederbelebung des Personenkennzeichens, RDV 2002, S. 167 ff.