

Dr. jur. Astrid Albrecht

# Rechtsfragen der Biometrie – Authentizität und Persönlichkeitsschutz

## Einleitung

Im Papier gebundenen Rechtsverkehr wird Authentizität und damit Urheberschaft durch die biometrische Handlung der eigenhändigen Unterschrift gewährleistet. Im elektronischen Rechtsverkehr funktioniert dieses althergebrachte Mittel zur Schaffung von Rechtssicherheit nicht mehr. Aus der Körperlosigkeit bei elektronischen Transaktionen ergeben sich spezifische Risiken, da Manipulationen an elektronischen Dokumenten grundsätzlich keine Spuren hinterlassen. 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 durch deren rechtliche Anerkennung vor allem in § 126 a BGB (elektronische Form) und § 292 a 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 Transaktion an die Person ermöglichen.

Den Vorteilen einer solchen direkten Authentifizierung steht die regelmäßige Verwendung perso-

nenbezogener Daten gegenüber. Aus der unmittelbaren Personenbindung heraus können besondere Gefährdungen erwachsen, die eine besondere datenschutzrechtliche Bewertung biometrischer Daten erfordert.

## Authentizität im Rechtsverkehr durch biometrische Handlungen

Im herkömmlichen Rechtsverkehr erlangt also die biometrische Handlung der eigenhändigen Unterschrift Bedeutung bei der „klassischen“ Schriftform gemäß § 126 BGB. Im elektronischen Rechtsverkehr bedient sich hingegen der Aussteller eines elektronischen Dokuments im Gegensatz zur eigenen Hand technischer Hilfsmittel, wie einer Chipkarte und Geheimzahlen, wie z. B. PINs. Dabei fehlt es an einer Realisierung der klassischen Sicherungsfunktionen der Schriftform wie der Identitätsfunktion, die den Aussteller einer Erklärung erkennen lässt, und der Beweisfunktion, mit der das vorgenommene Rechtsgeschäft beweiskräftig dokumentiert wird.

Beim Einsatz technischer Mittel beruhen erreichbare Rechtsverbindlichkeit und Beweiswert der elektronischen Transaktion ganz entscheidend auf der tatsächlichen Sicherheit des eingesetzten technischen Verfahrens. Bei der elektronischen Signatur hängt die Authentizität der elektronisch signierten Willenserklärung vor allem von dem eingesetzten Authentifizierungsverfahren ab, mit dem der Signiervorgang in Gang gesetzt wird. So ist zwar gemäß § 17 I SigG bei der qualifizierten Signatur der Einsatz sicherer Signaturerstellungseinheiten vorgeschrie-

ben, die den Signaturschlüssel „gegen unberechtigte Nutzung des Signaturschlüssels schützen“ sollen. Die in der Regel verwendeten Wissens- und Besitzelemente können jedoch nur eine mittelbare Authentifizierung des Rechtssubjekts durchführen. Verbleibende Restriktionen der bloß abgeleiteten Erkennung der handelnden Person und des daraus entstehenden Missbrauchspotenzials werden nicht zuletzt durch die Festlegung von Sorgfaltspflichten für den PIN-Inhaber oftmals unberechtigt auf diesen abgewälzt. Nach § 15 I 1 SigG können auch biometrische Merkmale eingesetzt werden, wenn sie mit einem Besitzelement verknüpft werden und gewissen Mindestsicherheitsanforderungen genügen. Bislang mangelt es jedoch an praktischen Anwendungen.

Im zivilprozessualen Bereich stützt sich § 292 a ZPO auf die qualifizierte elektronische Signatur. Bei deren Verwendung wird davon ausgegangen, dass das signierte Dokument auch tatsächlich vom Signaturinhaber stammt, sofern nicht ernstliche Zweifel daran begründet werden können. Hier kann eine ungerechtfertigte Beweislastverteilung insofern eintreten, als sich der Signaturschlüssel-Inhaber auch an solchen Signaturen festhalten lassen muss, die ohne sein Wissen mit seinem Signaturschlüssel erstellt worden sind. Manipulationen gehen daher aufgrund § 292 a ZPO zu Lasten des Berechtigten, ohne dass es für diese Folge nach dem gegenwärtigen Stand technisch belastbare Sicherheiten gäbe.

Die Verwendung biometrischer Verfahren zur Durchführung einer echten Personenverifikation könn-

te somit 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 berechnigte Person gebunden ist.

## **Persönlichkeitsschutz**

Auch mit Blick auf die Datensicherheit ist die enge Personenbindung biometrischer Merkmale zu begrüßen, wenn tatsächlich sichergestellt werden kann, dass ein biometrischer Datensatz unverfälscht und authentisch vom Betroffenen stammt. Aufgrund ihrer dauerhaften Bindung an die Person, den Merkmalsträger, weisen biometrische Daten allerdings eine besondere Brisanz auf.

Durch jede Verwendung personenbezogener Daten wird der Persönlichkeitsschutz des Betroffenen berührt. Das hier betroffene informationelle Selbstbestimmungsrecht beinhaltet das Recht, selbst darüber zu bestimmen, wer auf welche personenbezogenen Daten zugreifen und diese für welche Zwecke verwenden darf. Nach § 3 I BDSG sind personenbezogene Daten solche „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlicher Person“. Artikel 2a) der EG-Datenschutzrichtlinie 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“.<sup>1</sup> Grundsätzlich ist eine direkte

Identifizierung eines Menschen anhand eines körperlichen Merkmals möglich, das in einem biometrischen Datensatz verarbeitet wird. Daher sollten biometrische Angaben stets als personenbezogene Daten angesehen und daher jegliche Verarbeitung und Nutzung dieser Daten als ein rechtlich legitimationsbedürftiger Eingriff in das Recht auf informationelle Selbstbestimmung verstanden werden. Rechtsgrundlage für die Verarbeitung biometrischer Daten können Gesetze, Betriebsvereinbarungen oder die Einwilligung des Betroffenen selbst sein.

## **Zweckbindung und Verhältnismäßigkeit**

Personenbezogene Daten dürfen nur für einen vorab bestimmten Zweck erhoben und verarbeitet werden. Eine Zweckentfremdung ist prinzipiell unzulässig, eine spätere Zweckänderung nur unter ganz bestimmten Voraussetzungen zulässig. Eine Anwendung biometrischer Systeme muss zudem stets verhältnismäßig sein, d. h. für den angestrebten Zweck erforderlich, geeignet und angemessen. Im Verhältnis zueinander abgewogen werden müssen hier die berechtigten Interessen des Betreibers des Systems, etwa die Sicherheit zu erhöhen, gegen die berechtigten Interessen des Betroffenen an einem maximalen Schutz seiner Persönlichkeitsrechte.

## **Risikobewertung, Datenvermeidung und -sparsamkeit**

Das Risikopotenzial biometrischer Daten ist differenziert danach zu beurteilen, zu welchem Zweck und auf welche Art und Weise die Daten gespeichert und verwendet werden. Ebenfalls abhängig von der Art der Speicherung und Ver-

arbeitung der Daten kann zudem den Geboten der Datenvermeidung und der Datensparsamkeit mehr oder weniger genügt werden. Nach § 3 a BDSG dürfen Datenverarbeitungssysteme keine oder so wenig personenbezogene Daten wie möglich erheben, verarbeiten oder nutzen. Zudem ist von den Möglichkeiten der Anonymisierung (§ 3 VI BDSG) und Pseudonymisierung (§ 3 VI a BDSG) Gebrauch zu machen, soweit möglich und angemessen, vgl. § 3 a, 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 Zwecke der Identifizierung hinaus. In diesem Zusammenhang ist etwa 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 PersonalausweisG<sup>2</sup>.

Bei einer dezentralen Speicherung kann dem Selbstbestimmungsrecht des Anwenders in hohem Maße Genüge getan werden. 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.

Im Falle einer lokalen Lösung der sog. selbstauthentifizierenden Token (z. B. match-on-card) verbleiben die biometrischen Daten stets im Verfügungsbereich des Betroffenen. Daher würde dessen Recht

<sup>1</sup> 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.

<sup>2</sup> 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.

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 könnte.

### Diskriminierung

Das Recht auf informationelle Selbstbestimmung schützt vor jeglicher Stigmatisierung und einer daraus erwachsenden Rechtfertigungslast. 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. Falschzurückweisungen können zu negativen Rückschlüssen auf das körperliche Merkmal des Betroffenen und zu dessen Ausgrenzung innerhalb der Benutzergruppe führen.

### Privacy-Enhancing-Technologies (PET)

Bei der Diskussion über Sicherheit biometrischer Systeme sollte auch das Konzept der PET mit einbezogen werden. 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 Informationssystems. Während 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. U.a. sind hier die Evaluierung und Zertifizierung biometrischer Systeme sowie

Maßnahmen des Schutzes der Daten, z. B. durch Verschlüsselung, einzubeziehen.

### Arbeitnehmerdatenschutz

Sollen biometrische Systeme im Arbeitsbereich, etwa als Zutrittskontrolle zum Betrieb eingesetzt werden, müssen zusätzlich besondere Arbeitnehmerschutzregelungen beachtet werden. In jedem Fall muss eine Abwägung der widerstreitenden Interessen im Sinne der o. g. Verhältnismäßigkeit erfolgen. Dies beinhaltet insbesondere die Frage, ob bei objektiver Würdigung ein zwingendes betriebliches Interesse am Einsatz eines biometrischen Systems begründet werden kann. Der Persönlichkeitsschutz der Arbeitnehmer findet sich insbesondere in den Mitbestimmungsrechten der Arbeitnehmervertretung, z. B. bei technischen Einrichtungen, § 87 I Nr. 6 BetrVG, der auch auf biometrische Systeme anwendbar ist.

### Fazit und Ausblick

Die herausragende Eigenschaft biometrischer Authentifizierungsmechanismen besteht also darin, unmittelbar an die Person gebundene körperliche Merkmale zu verwenden und damit eine echte Verifikation der Person 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, de-

ren 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.

#### Weiterführende Literatur:

Albrecht, Astrid: Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, Dissertation 2003, i. E. bei



Nomos Baden-Baden in der Reihe Frankfurter Studien zum Datenschutz, hrsg. von Prof. Dr. Dr. hc. Spiros Simitis; 236 S., 46,- €. ISBN 3-8329-0387-9

Behrens, Michael/Roth, Richard (Hrsg.); Biometrische Identifikation – Grundlage, Verfahren, Perspektiven, Vieweg 2001;

Gundermann, Lukas/Probst, Thomas, Brennpunkte des Datenschutzrechts, Kap. 9 in: Roßnagel, A. (Hrsg.): Handbuch Datenschutzrecht, C. H. Beck München 2003;

Leger, Lothar/Nolde, Veronika (Hrsg.), Biometrische Verfahren, Körpermerkmale als Passwort, Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Deutscher Wirtschaftsdienst 2002;

TeleTrust e. V.: Kriterienkatalog zur Vergleichbarkeit biometrischer Verfahren, vollständig überarbeitete Auflage vom 10.07.2002, download unter <http://www.teletrust.de/publikat.asp?id=40600>. Siehe auch AWW-Informationen 3/2003, S. 4–6

*Dr. jur. Astrid Albrecht, Referentin beim Bundesamt für Sicherheit in der Informationstechnik, Leiterin der AG 6 Biometrische Identifikationsverfahren des TeleTrust e. V., E-Mail: aalbrechtlaw@aol.com*