

# Herausforderung für den Datenschutz?

*Biometrische Verfahren sind nicht neu. Die Kriminalistik setzt bereits seit dem 19. Jahrhundert biometrische Daten für die Aufklärung von Verbrechen ein, indem sie den Fingerabdruck von Verdächtigen mit denen vergleicht, welche sie am Tatort sicherstellt. Allerdings war ein Vergleich des gefundenen Fingerabdrucks mit einer Vielzahl von Fingerabdrücken von möglichen Tätern lange Zeit mit immensem Aufwand verbunden.*



Bild: Pixelquelle

*Besonders schützenswerte Personendaten dürfen vom Staat nur bearbeitet werden, wenn eine formelle gesetzliche Grundlage es erlaubt.*

VON MARIA WINKLER

Erst die moderne Informationstechnologie ermöglicht es, auf effiziente Art rasch ein Ergebnis zu erzielen. Die modernen Methoden der Speicherung und Verknüpfung von Daten, gepaart mit dem Bedürfnis nach eindeutiger Zuweisung einer virtuellen Identität zu einer bestimmten natürlichen Person, machen biometrische Verfahren auch ausserhalb der Kriminalistik interessant.

Biometrische Verfahren ermöglichen die eindeutige Identifizierung einer Person über körpereigene, einmalige Kennzeichen, welche untrennbar mit dieser Person verbunden sind. Während die damit einhergehenden Möglichkeiten insbesondere von den Anbietern entsprechender Technologien bejubelt werden, wecken sie in den betroffenen Personen häufig Ängste darüber, welche Möglich-

keiten sich demjenigen eröffnen, der über diese Daten verfügen kann. Aus Datenschutzkreisen kommen daher auch oft Bedenken gegen diese Art der Datenbearbeitung. Werden biometrische Verfahren zweckmässig und verhältnismässig eingesetzt, so sind diese Bedenken zu einem grossen Teil ungerechtfertigt. Im Gegenteil – biometrische Verfahren können durch korrekte Anwendung den Datenschutz unterstützen.

Die Normen des Datenschutzes bezwecken den Schutz des Rechts auf informationelle Selbstbestimmung – somit das Recht der betroffenen Person zu bestimmen, wer welche Daten in welcher Form über sie bearbeiten darf. Personendaten gemäss Datenschutzgesetz sind alle Angaben über eine bestimmte oder bestimmbare Person. Werden besonders



## Maria Winkler

ist mag. iur. und geschäftsführende Partnerin der IT & Law Consulting GmbH in Zug und Luzern. Nach dem Studium der Rechtswissenschaften in Graz (Österreich)

spezialisierte sie sich nach einigen Jahren Berufspraxis auf rechtliche Themen an der Schnittstelle zwischen Informationstechnologie und Recht. Sie unterstützt Unternehmen für die Ausarbeitung von Verträgen im Informatikbereich und berät diese für rechtliche Fragestellungen, welche sich aus dem Einsatz oder der Entwicklung von Informationstechnologie ergeben. Maria Winkler ist zudem Dozentin für Informatikrecht an der Hochschule für Wirtschaft (HSW) Luzern und unterrichtet insbesondere Themen wie Urheberrecht, Datenschutzrecht und Recht im Internet. Kontakt: maria.winkler@itandlaw.ch

schützenswerte Personendaten (zum Beispiel Daten über die Gesundheit, die Rassenzugehörigkeit, die Religion, die politische Einstellung, über strafrechtliche Sanktionen) bearbeitet, dann sind besondere Vorkehrungen zu deren Schutz zu treffen.

Besonders schützenswerte Personendaten dürfen vom Staat nur bearbeitet werden, wenn eine formelle gesetzliche Grundlage es erlaubt. Privatpersonen, welche regelmässig besonders schützenswerte Personendaten bearbeiten, müssen die Datensammlung beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) anmelden, wenn die betroffene Person von Bearbeitung keine Kenntnis hat und keine gesetzliche Verpflichtung für die Bearbeitung besteht. Zudem dürfen besonders schützenswerte Personendaten nicht ohne Rechtfertigungsgrund an Dritte weitergegeben werden. Es stellt sich nun die Frage, ob biometrische Daten automatisch als besonders schützenswert zu qualifizieren sind.

Neben dem Fingerabdruck, der Handunterschrift, dem Gesichtsbild und der DNA werden in biometrischen Verfahren und Systemen weitere biometrische Merkmale wie die Iris, die Handgeometrie, das Tipverhalten, das Stimmprofil oder der Gang zur Identifikation und zur Authentifizierung verwendet. Die Erhebung dieser Daten erfolgt mit Hilfe von Kameras, Mikrofonen, Tastaturen oder speziellen Sensoren. Die so gewonnenen Daten, also der Fingerabdruck oder das Gesichtsbild, bezeichnet man als biometrische Rohdaten, welche vor ihrer Verwendung mittels mathematischer Methoden in so genannte Templates weiterverarbeitet werden. Dabei handelt es sich um einen komprimierten Datensatz, welcher die für einen Vergleich wesentlichen Daten enthält, aber üblicherweise keine unmittelbaren Rückschlüsse auf eine bestimmte Person erlaubt, da beim Umwandlungsprozess diesbezügliche Informationen verloren gehen.



**Fingerabdruck oder das Gesichtsbild bezeichnet man als biometrische Rohdaten, welche vor ihrer Verwendung mittels mathematischer Methoden als Templates weiterverarbeitet werden.**

Biometrische Rohdaten können besonders schützenswerte Personendaten sein, wenn sich aus ihnen direkt Rückschlüsse über die Gesundheit, die Rassenzugehörigkeit, die Religion und die politische Gesinnung der betroffenen Person machen lassen. Aber auch die Verknüpfung mit anderen Informationen oder der Verarbeitungszweck, zum Beispiel eine Verwendung im Rahmen der Strafverfolgung, kann biometrische Rohdaten zu besonders schützenswerten Personendaten machen.

Die in Templates enthaltenen Informationen lassen hingegen ohne weitere Informationen keine unmittelbaren Aussagen und Rückschlüsse auf die betroffene Person zu, weshalb per se ein viel geringeres Risiko einer Persönlichkeitsverletzung besteht. Die Qualifikation als besonders schützenswert kann zudem nur durch diese Zusatzinformationen oder den Verarbeitungszweck folgen.

Das Datenschutzgesetz verlangt weiter, dass Personendaten nur zu dem Zweck bearbeitet werden, zu welchem sie erhoben werden. Zudem muss die Bearbeitung verhältnismässig erfolgen – sie muss für den angestrebten Zweck geeignet und erforderlich sein und den geringstmöglichen Eingriff in die Rechte der betroffenen Person darstellen. Personendaten dürfen ausserdem nur rechtmässig beschafft werden, und die bearbeitende Person hat sich von deren Richtigkeit zu vergewissern.

Für die Beurteilung der Datenschutzkonformität biometrischer Systeme können aus dem bisher Gesagten die folgenden (Mindest-)Anforderungen abgeleitet werden:

Biometrische Rohdaten enthalten oft mehr Informationen, als zur Erreichung des angestrebten Zwecks erforderlich sind. Wenn es der Verarbeitungszweck zulässt, ist daher biometrischen Verfahren der Vorzug zu geben, welche auf Templates basieren. Die Rohdaten sind so rasch als möglich zu löschen.

Biometrische Daten sollen nicht ohne Wissen der betroffenen Person beschafft werden. Für die Erfassung biometrischer Daten ist somit den Verfahren der Vorzug zu geben, an welchen die betroffene Person unmittelbar mitwirken muss.

Das System sollte so gestaltet sein, dass eine Verwendung der biometrischen Daten zu einem anderen als dem ursprünglich beabsichtigten Zweck vermieden wird.

Auf eine zentrale Speicherung von Templates in einer Datenbank sollte verzichtet werden, wenn der angestrebte Zweck auch mit einer Speicherung der Templates auf Chipkarten oder einem anderen, nur der betroffenen Person zugänglichen Medium erreicht werden kann.

Biometrische Daten müssen gleich bei der Registrierung verschlüsselt und vor dem Zugriff unberechtigter Dritter geschützt werden. Das Belauschen oder das Einspielen von gefälschten Daten muss mit geeigneten Massnahmen verhindert werden.

## Links

«Einige Datenschutzaspekte für die Verwendung von biometrischen Daten im Privatsektor», zu finden auf der Website des EDÖB unter <http://www.edoeb.admin.ch/dokumentation/00445/00509/00510/00815/index.html?lang=de>  
«Stand der nationalen und internationalen Diskussion zum Thema Datenschutz für biometrische Systeme» auf der Website des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, abrufbar unter <http://www.datenschutzzentrum.de/download/tabga.pdf>

Fehler durch die Zulassung Unberechtigter oder die Abweisung Berechtigter sind durch sorgfältige Testverfahren und durch die Wahl eines geeigneten Parameters für den Übereinstimmungsgrad so gering wie möglich zu halten.

Für die Ausübung staatlicher Gewalt – insbesondere für die Strafverfolgung und beim Strafvollzug – kann im öffentlichen Interesse von den oben genannten Anforderungen abgewichen werden. Allerdings ist der Staat auch in diesem Bereich strikt an das Gesetz gebunden. Oberstes Prinzip ist dabei die Unantastbarkeit der Menschenwürde. Sie unterscheidet sich von anderen Grundrechten dadurch, dass es keine verfassungsrechtliche Legitimation für deren Einschränkung gibt – das gilt auch für das staatliche Handeln.

Die Menschenwürde ist dann verletzt, wenn der Mensch als Objekt, zu einem blossen Mittel oder zu einer vertretbaren Grösse herabgewürdigt wird. In der Fachliteratur wird übereinstimmend die Meinung vertreten, dass eine umfassende Katalogisierung der biometrischen Merkmale der Bevölkerung durch den Staat ohne Zweckbindung gegen die Menschenwürde verstossen würde.

Grundsätzlich haben biometrische Systeme und Verfahren das Potenzial, den Datenschutz dadurch zu fördern, dass sie als Zugriffssicherung zu personenbezogenen Daten verwendet werden. Man spricht in diesem Zusammenhang von so genannten Privacy Enhancing Technologies (PET). Gemeint sind Technologien, welche durch Transparenz, Datenvermeidung und Datensparsamkeit den Datenschutz fördern. Als Beispiel können PDAs genannt werden, welche die darauf gespeicherten persönlichen Daten durch biometrische Sensoren sichern.

Grundsätzlich können keine allgemeingültigen Aussagen gemacht werden, wann biometrische Systeme und Verfahren datenschutzkonform sind. Letztendlich muss im Einzelfall beurteilt werden, ob ein bestimmtes System angesichts des angestrebten Zwecks eine datenschutzkonforme Bearbeitung der biometrischen Daten bietet. ■