DuD
Datenschutz und Datensicherheit

Der Personenbezug biometrischer Daten

Zugleich eine Erwiderung auf Saeltzer, DuD 2004, 218ff.

Gerrit Hornung

Bundes- wie Landesdatenschutzgesetze sind in ihrem Anwendungsbereich auf personenbezogene Daten beschränkt. Das entspricht auch dem Anwendungsbereich des Rechts auf informationelle Selbstbestimmung. In Heft 4 der DuD 2004 hat Gerhard Saeltzer sich dazu geäußert, wie sich „der Personenbezug von Daten, auch biometrischer,…fundiert prüfen“ lasse, dabei jedoch die schon länger geführte Diskussion um den Personenbezug biometrischer Daten unerwähnt gelassen. Diese wird im Folgenden näher erörtert.

Gerrit Hornung, LL.M. in European Law
Mitglied der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) an der Universität Kassel
E-Mail: gerrit.hornung@uni-kassel.de

1 Einleitung

Nach der Legaldefinition des § 3 Abs. 1 BDSG sind personenbezogene Daten „Einzelangaben über persönliche oder sachliche Verhältnisse *einer bestimmten oder bestimmbaren natürlichen Person*“. Eine Person ist bestimmt, wenn sie sich aus der Angabe selbst ergibt, bestimmbar, wenn die Identität mit Hilfe anderer Informationen festgestellt werden kann.[1] Sind hierzu technische Verfahren oder wissenschaftliche Erfahrung erforderlich, so reicht es aus, dass sie objektiv am Markt verfügbar sind; wird Zusatzwissen benötigt, so richtet sich der Personenbezug danach, ob dieses der jeweiligen Stelle zugänglich ist.[2]

Dasselbe Datum kann deshalb je nach verantwortlicher Stelle personenbezogen oder nicht personenbezogen sein (*„Relativität“ des Personenbezugs*). Nicht zutreffend ist die Aussage *Saeltzers*,[3] „ohne ein konkretes personenbezogenes Zusatzwissen ist eine Aussage über den Personenbezug von (anonymen) Daten nicht möglich“. Sie ignoriert die stark umstrittene Diskussion darum, ob anonyme und pseudonyme Daten personenbezogen sind.[4] Außerdem kann gerade das Fehlen eines solchen Zusatzwissens die Aussage zulassen, dass ein Personenbezug nicht besteht.

Biometrie ist die automatisierte Messung von natürlichen, hoch charakteristischen, physiologischen oder verhaltenstypischen Merkmalen von Menschen zum Zweck der Unterscheidung von anderen Personen.[5] Die von *Saeltzer* behandelten Videoanlagen verwenden damit ganz überwiegend keine Biometrie, weil bei ihnen keine automatisierte Erfassung stattfindet.

Der Ablauf biometrischer Systeme[6] beginnt mit der Erfassung der biometrischen Referenzdaten, dem Enrolment. Diese Daten werden sodann in einer zentralen Datenbank oder dezentral, beispielsweise auf Chipkarten, gespeichert. Das kann entweder in vollständiger Form (Voll- oder Rohdaten) oder als extrahierter Datensatz (Template) geschehen. Im Rahmen des Matchings erfolgt ein Vergleich der Referenzdaten mit den Daten, die der Betroffene präsentiert.

2 Bisherige Auffassungen

Vertreten wird zunächst die Auffassung, biometrische Daten seien *stets personenbezogen*.[7] Überwiegend wird demgegenüber *zwischen Volldaten und Templates unter-*

[1] Simitis-*Dammann*, BDSG, 2003, § 3 Rn. 21; *Tinnefeld/Ehmann*, Datenschutzrecht, 1998, 184. S.a. Art. 2a DSRL.

[2] Simitis-*Dammann*, § 3 Rn. 31f.; *Gola/Schomerus*, BDSG, 2002, § 3 Rn. 9.

[3] DuD 2004, 218, 221.

[4] Nach einer Auffassung (Simitis-*Dammann*, § 3 Rn. 202f.; *Auernhammer*, BDSG, 1993, § 3 Rn. 47) sind anonyme Daten personenbezogen, solange keine „absolute“ Anonymisierung i.S.v. § 3 Abs. 6, 1. Alt. BDSG vorliegt. Das gelte selbst dann, wenn eine Zuordnung nur mit unverhältnismäßig großem Aufwand möglich sei. Pseudonyme Daten seien stets personenbezogen (Simitis-*Bizer*, § 3 Rn. 223). Nach der – zutreffenden – Gegenauffassung (*Roßnagel/Scholz*, MMR 2000, 721, 725ff.; *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 103; *Gola/Schomerus*, BDSG, 2002, § 3 Rn. 43f.) entfällt im Fall der Anonymisierung jeder Personenbezug. Pseudonyme Daten sind dann personenbezogen, wenn die verantwortliche Stelle über die Zuordnungsregel verfügt, andernfalls wie anonymen Daten zu behandeln.

[5] *Büro für Technikfolgenabschätzung* (*TAB*), Biometrische Identifikationssysteme, BT-Drs. 14/10005, 9. S.a. *Albrecht*, Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, 2003, 31 m.w.N.

[6] S. näher *Albrecht* (Fn. 5), 35ff.; *Gundermann/Probst*, in: Roßnagel, HB Datenschutzrecht, 2003, Kap. 9.6, Rn. 8ff.

[7] *Weichert*, CR 1997, 369, 372. Ebenso noch *Probst* in: Nolde/Leger, Biometrische Verfahren, 2002, 117 (s. aber unten Fn. 10).

schieden. So soll nach einer Ansicht bei Templates ein Personenbezug stets zu verneinen sein,[8] nach einer anderen nur dann bestehen, wenn mit ihnen zusätzliche Identifizierungsinformationen verbunden sind.[9] Bei Volldaten sei hingegen zu differenzieren. Bei Merkmale wie dem Gesicht, „die im Allgemeinen offen liegen und für das menschliche Gehirn leicht zu verarbeiten sind", könne ein Schluss auf eine bestimmte Person kaum je ausgeschlossen werden, „weniger offen liegende Merkmale" wie der Fingerabdruck erforderten hierfür dagegen wie Templates eine zusätzliche Identifizierungsinformation.[10]

Weiter wird die Ansicht vertreten, bei Berücksichtigung grundsätzlich verfügbaren Zusatzwissens, externer Datenverarbeitungskapazitäten und Einsatz von Experten könne die Herstellbarkeit eines Personenbezugs *für Volldaten grundsätzlich nie ausgeschlossen werden*.[11] Bei Templates könne der Betroffene demgegenüber im Fall der zentralen Speicherung über die jeweilige Zuordnungsliste ermittelt werden, im Fall der dezentralen Ablage nur, wenn beim Prüfvorgang gleichzeitig eine Zuordnung zu einer Berechtigtenliste erfolge. Gleiches gälte für Systeme mit biometrischem Sensor auf der Karte, sofern die Daten auch im Verlustfall nicht ausgelesen werden könnten.

3 Analyse

Im Ergebnis kann *keine der erläuterten Auffassungen überzeugen*. Ein Personenbezug von Templates kann nicht grundsätzlich verneint werden, weil auch diese (extrahierte) Informationen über eine Person enthalten und ihr über Zuordnungslisten zugeordnet sein können. Gegen die Annahme eines Personenbezugs ohne Differenzierung spricht, dass dabei spezifische Verfahren ignoriert werden. Zur Überprüfung einer Zugangsberechtigung kann es etwa ausreichen, die Iris-Templates von Mitarbeitern ohne Zuordnungsliste zu speichern und bei der Einlasskontrolle lediglich zu prüfen, ob das präsentierte Merkmal in der Datenbank enthalten ist. Zumindest zwischen den Matchingvorgängen besteht dann für die speichernde Stelle bei ausreichender Größe der Datenbank keine Möglichkeit der Herstellung eines Personenbezugs.[12]

3.1 Differenzierung nach Verfahrensschritten

Im Übrigen konzentrieren sich die erläuterten Ansätze zu sehr auf die unterschiedlichen Merkmale, Speicherungsformen und -orte, anstatt von der Relativität des Personenbezugs auszugehen und im Einzelfall die Bestimmbarkeit des Betroffenen zu analysieren. Hierzu ist es sinnvoll, nach dem *Ablauf des Verfahrens zu differenzieren*.

Bei vielen Verarbeitungsschritten ist der Betroffene bestimmbar, weil er aus unterschiedlichen Gründen identifizierbar sein jeweiliges Merkmal präsentiert. Das gilt zum einen für das Enrolment. Des Weiteren *geht in der Diskussion häufig unter*, dass ganz unabhängig von der Art der Speicherung der Referenzdaten als Volldaten oder Templates, in zentraler oder dezentraler Form *beim Matching* in aller Regel Daten entstehen, die einer bestimmbaren Person zugeordnet sind.

Wenn das Matching unter der Kontrolle der verantwortlichen Stelle stattfindet, so wird die Person, die das Merkmal präsentiert, in aller Regel bestimmbar sein.[13] Werden die Referenzdaten zum Matching aus einem *Chipkartenausweis* ausgelesen, der auch als Sichtausweis fungiert, so sind die neu erhobenen Daten sogar stets personenbezogen. Hierzu ist keine zusätzliche Zuordnung zu einer Berechtigtenliste mittels Kennzahl oder Namens erforderlich, weil der Name des Betroffenen auf dem Ausweis aufgedruckt ist.[14]

Beim Personenbezug der gespeicherten *Referenzdaten* ist demgegenüber zu differenzieren. In dem Moment, in dem ein Referenzdatensatz positiv dem neu erhobenen Vergleichsdatensatz zugeordnet wird, wird er immer dann personenbezogen, wenn jener personenbezogen ist. Wie soeben erläutert, ist dies häufig der Fall. Da allerdings mit dem Vergleichsdatensatz ohnehin Daten vorhanden sind, die zu einem sehr hohen Grad mit den Referenzdaten übereinstimmen, ist hiermit keine weitergehende Gefährdung für die informationelle Selbstbestimmung des Betroffenen verbunden.

Außerhalb von Matchingprozessen sind die gespeicherten Referenzdaten immer dann personenbezogen, wenn ein zentrales System – wie regelmäßig – über eine Zuordnungsliste verfügt. Ist dies nicht der Fall, oder werden Daten außerhalb eines biometrischen Identifikationssystems verarbeitet, kommt es tatsächlich auf den Personenbezug biometrischer Daten „an sich" an. Eine Zuordnung wird dann bei Volldaten regelmäßig leichter möglich sein.

Auch hier kommt es jedoch auf verfügbares Zusatzwissen an. So ist der Fingerabdruck einer bereits erkennungsdienstlich behandelten Person in den Händen der Polizei aufgrund der Möglichkeit einer AFIS-Abfrage personenbezogen. Ohne dieses Zusatzwissen – das nach sozialadäquaten Maßstäben nicht allgemein verfügbar ist – kann eine Zuordnung jedoch normalerweise nicht vorgenommen werden. Das kann auch bei Gesichtsdaten der Fall sein, wenn die verantwortliche Stelle sich im Ausland befindet und keinerlei Informationen über die Identität oder den Herkunftsort des Betroffenen hat.

Unter keinen Umständen kann es darauf ankommen, ob es sich um ein „für das menschliche Gehirn leicht zu verarbeitendes" Merkmal handelt.[15] Bei der Beurteilung der Bestimmbarkeit des Betroffenen ist auf die konkreten Umstände, insbesondere die verfügbaren technischen Verarbeitungsverfahren und Zusatzinformationen, abzustellen. Die erläuterte Auffassung hätte zur Folge, dass die Anwendbarkeit des Datenschutzrechts von den Möglichkeiten einer manuellen Datenverarbeitung auf der Basis menschlich-visuell erfasster Daten abhinge, was unter den Bedingungen moderner Informationsverarbeitung unvertretbar ist.

3.2 Besonderheiten von Templates

Eine gesonderte Beurteilung von Templates kommt nur dann in Betracht, wenn man hierunter ausschließlich Datenextrakte versteht, die substantiell weniger Daten als Volldaten enthalten[16] und es nicht möglich ist, aus ihnen *die Volldaten zurückzukon-*

[8] *Kruse/Peuckert*, DuD 1995, 142, 145.

[9] *Gundermann/Probst* (Fn. 6), Rn. 48. S.a. *TAB* (Fn. 5), 44.

[10] *Gundermann/Probst* (Fn. 6), Rn. 43ff.; *TAB* (Fn. 5), 44.

[11] *Albrecht* (Fn. 5), 157ff.

[12] S. *Gundermann/Köhntopp*, DuD 1999, 143, 147.

[13] Das stellt sich bei automatisierten Kontrollen ohne Aufsicht anders dar.

[14] Das wird übersehen von *Albrecht* (Fn. 5), 160, die lediglich auf die biometrischen Daten abstellt und die Sichtdaten vernachlässigt.

[15] Die Differenzierung ablehnend auch *Albrecht* (Fn. 5), 157f.

[16] Bisweilen werden alle Referenzdaten (auch Volldaten) und nur leicht komprimierte Rohdaten als „Templates" bezeichnet.

struieren.[17] Letzteres ist jedoch zumindest bei einigen Merkmalen und Algorithmen möglich.[18] Können die Volldaten komplett errechnet werden, sind Templates wie diese zu behandeln. Aber auch bei einem lediglich teilweisen Rückschluss auf den Volldatensatz ergibt sich eine (Teil-)Information, die je nach Kontext und Zusatzwissen ein personenbezogenes Datum entstehen lassen kann. Nur wenn eine Rückwärtskonstruktion ausgeschlossen ist, ist das Template nicht selbst, sondern nur bei Vorliegen eines Zuordnungssystems personenbezogen.

3.3 Verarbeitung auf Chipkarten

Bei einer Speicherung der Referenzdaten auf Chipkarten ist zu unterscheiden. Werden die Daten (in Form von Volldaten wie Templates) *zum Matching aus der Karte ausgelesen*, so besteht hierbei regelmäßig Personenbezug (s.o.). Zwischen mehreren Auslesevorgängen hat die verantwortliche Stelle zwar keine Verfügungsgewalt über die Daten. Diese Zwischenräume sind aber lediglich notwendige Folge der spezifischen Art der Speicherung, die bei jedem Kontakt zwischen dem Betroffenen und der Stelle der letzteren den Zugriff auf die Daten ermöglicht. Deshalb bleiben die biometrischen Daten personenbezogen, und die verantwortliche Stelle hat auch für die Zwischenräume Sicherungsmaßnahmen zu treffen.

Findet *Matching-On-Card* statt, so sendet ein Sensor die Vergleichsdaten an die Karte, die den Abgleich vornimmt. Damit verlassen die Referenzdaten den Chip nicht. Hierdurch entfällt der Personenbezug jedoch nicht, weil immer noch außerhalb der Karte Daten erhoben werden, die im Fall einer positiven Verifikation mit einem sehr hohen Grad an Wahrscheinlichkeit mit den Referenzdaten übereinstimmen.

Verfügt die Karte dagegen über einen *Sensor*, und finden auch die Merkmalsextraktion und das Matching im Chip statt,[19] so verfügt die verantwortliche Stelle über keinen Einfluss auf die Daten und kann, anders als beim schlichten Matching-On-Card, auch nicht auf diese schließen. Zwar bleiben die Angaben, da sie fest in der Karte gespeichert sind, dem Inhaber an sich zugeordnet. Da jedoch niemand in der Lage ist, von ihrem Inhalt Kenntnis zu nehmen, handelt es sich nicht um ein personenbezogenes Datum.[20]

3.4 Templatefreie Verfahren

Bei *templatefreien Verfahren* wird mittels der Daten des Betroffenen ein „biometrischer Schlüssel“ berechnet und mit diesem aus einem Klartext ein Chiffrat erzeugt, das als Referenzdatensatz dient.[21] Zur Authentifikation wird der Vorgang wiederholt. Beim Einsatz sicherer Verschlüsselungsalgorithmen ist es der speichernden Stelle nicht möglich, aus dem Chiffrat auf den Klartext oder das biometrische Merkmal zu schließen.

Es kann jedoch *nicht gefolgert werden*, es seien „hier keine personenbezogenen Daten mehr verfügbar“,[22] entsprechende Verfahren realisierten „biometrische Anwendungen ohne Personenbezug“,[23] beziehungsweise es handele sich um „anonyme Biometrie“[24]. Zum einen kann das gespeicherte Chiffrat personenbezogen sein, beispielsweise beim Vorliegen einer Zuordnungsliste. Zum anderen werden auch bei templatefreien Verfahren bei jedem Matching zur Berechnung des biometrischen Schlüssels Volldaten erhoben, die wie erläutert in aller Regel personenbezogen sind. Im Ergebnis vermeiden templatefreie Verfahren zwar die Speicherung biometrischer Referenzdaten, nicht jedoch die Verwendung personenbezogener biometrischer Daten überhaupt.

4 Zusammenfassung

Bei der Präsentation biometrischer Merkmale entstehen in aller Regel personenbezogene Daten. Das ist beim Enrolment stets, beim Matching immer dann der Fall, wenn die Identität des Betroffenen durch die verantwortliche Stelle auf anderem Wege feststellbar ist. In diesem Fall sind auch die jeweiligen Referenzdaten personenbezogen. Gleiches gilt, wenn diese mit einem Zuordnungssystem gespeichert sind. Bei einer Speicherung auf Chipkarten, auf denen der Name des Inhabers aufgedruckt ist, handelt es sich nur dann nicht um personenbezogene Daten, wenn die Karte selbst über einen Sensor verfügt.

Für Daten außerhalb biometrischer Identifikationssysteme ist eine Analyse des jeweiligen Zusatzwissens der verantwortlichen Stelle erforderlich. Dabei kann es Unterschiede zwischen einzelnen Merkmalen geben, weil einige leichter einer Person zugeordnet werden können. Eine Verallgemeinerung dahin, dass alle oder einige biometrische Merkmale stets personenbezogen wären, verbietet sich jedoch aufgrund der Relativität des Personenbezugs. Bei Templates kommt es entscheidend auf die Möglichkeit der Rückwärtskonstruktion an. Templatefreie Verfahren vermeiden den Aufbau einer zentralen Datenbank mit personenbezogenen biometrischen Daten, lassen das Problem der Erhebung derartiger Daten zum Matching jedoch unberührt.

Auch die dezentrale Speicherung der Referenzdaten auf Chipkarten vermeidet große Datenbanken mit biometrischen Daten. Templatefreie und dezentrale Verfahren weisen deshalb datenschutzrechtliche Vorteile auf. Die von *Saeltzer* zur Vermeidung eines Personenbezugs vorgeschlagenen Maßnahmen des unscharf Stellens einer Überwachungskamera oder der Verwendung eines alten Monitors[25] mögen demgegenüber für den Sonderfall der Internetpräsentation eines Marktplatzes zu Werbezwecken tauglich sein; für den künftig zu erwartenden breiten Einsatz leistungsfähiger biometrischer Systeme ist ein derartiger „Datenschutz durch Technik“ realitätsfern.

[17] So die in der bisherigen Literatur durchweg zugrunde gelegte Prämisse, s. *AKT der DSB*, DuD 1997, 709, 713; *Albrecht* (Fn. 5), 158; *Gundermann/Probst* (Fn. 6), Rn. 48; *Gundermann/Köhntopp*, DuD 1999, 143, 150.

[18] S. *Bromba*, On the reconstruction of biometric raw data from template data, http://www.bromba.com/knowhow/temppriv.htm, 2003.

[19] Hier bestehen bislang noch erhebliche technische Probleme hinsichtlich der Rechenkapazität des Chips.

[20] Allerdings verbleiben dennoch Datensicherungspflichten der jeweiligen Stelle. Diese sind denen bei anonymen Daten vergleichbar, s. dazu *Roßnagel/Scholz*, MMR 2000, 721, 730 f.; *Roßnagel/Pfitzmann/Garstka* (Fn. 4), 108 ff.

[21] S. näher *Albrecht* (Fn. 5), 56 f.; *Gundermann/Probst* (Fn. 6), Rn. 24f.

[22] *Albrecht* (Fn. 5), 161.

[23] *Gundermann/Probst* 2003, (Fn. 6), Rn. 49.

[24] *Donnerhacke*, DuD 1999, 151ff.

[25] *Saeltzer*, DuD 2004, 218, 225.