Buket Günay

Biometrische Daten aus der Perspektive der DSGVO

Biometrische Daten sind die Daten, mit denen jede natürliche Person geboren wird. Nach der Datenschutz-Grundverordnung (DS-GVO) handelt es sich um besondere Kategorien personenbezogener Daten. Daher unterliegt ihre Verarbeitung besonderen Regeln. Mit der Entwicklung der Technologie werden biometrische Daten im täglichen Leben immer häufiger verarbeitet. Der Grundgedanke des Datenschutzrechts, der auf den Schutz von Personen und nicht von Daten abzielt, sollte auch bei der Verarbeitung und dem Schutz biometrischer Daten berücksichtigt werden. Biometrische Daten nehmen unter den Arten personenbezogener Daten einen besonderen Platz und eine besondere Bedeutung ein, da personenbezogene Daten von besonderer Qualität aufgrund des mit ihnen verbundenen Risikos sensibel geschützt werden müssen. Diese Studie geht von den konzeptionellen Grundlagen der personenbezogenen Daten aus. Daher werden der Stellenwert und die Bedeutung biometrischer Daten im Recht zum Schutz personenbezogener Daten im Rahmen der Datenschutz-Grundverordnung analysiert. Darüber hinaus wird veranschaulicht, wie häufig biometrische Daten in jedem Aspekt unseres täglichen Lebens verwendet werden.

1 Konzept der personenbezogenen Daten

Gemäß Art. 4 Nr.1 DS-GVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare lebende Person beziehen. Der Begriff der personenbezogenen Daten besteht daher aus zwei grundlegenden Elementen: einer bestimmten oder bestimmbaren natürlichen Person und Informationen über diese Person.

Das erste Element des Begriffs personenbezogene Daten besteht darin, dass die Identität einer natürlichen Person bestimmt oder bestimmbar ist. Die Identifizierung der Person bedeutet, dass die Person durch Daten ohne Mittel direkt identifiziert werden kann. Beispielsweise ist der Name einer Person einer der häufigsten Identifikatoren, die verwendet werden, um sie direkt zu identifizieren. Eine direkte Identifizierung ist auch über die Identifikationsnummer oder die Sozialversicherungsnummer möglich.

Buket Günay, LL.M.

Wissenschaftliche Mitarbeiterin
Yaşar Universität
Rechtwissenschaftliche Fakultät

E-Mail: buket.gunay@yasar.edu.tr

Das erste, was eine Person auszeichnet und sie von anderen unterscheidet, kann jedoch ihr Name sein. Art.4 Nr.1 DS-GVO definiert personenbezogene Daten als „alle Informationen", die eine natürliche Person bestimmbar oder identifizierbar machen. Alle Informationen, die sich auf den Namen der Person beziehen, beispielsweise Geburtsdatum, Geburtsort, Namen der Eltern, Adresse, ein Foto des Gesichts oder andere biometrische Daten, sind weitere Elemente, die der direkten Identifizierung der Person dienen. Die Elemente, die eine Person direkt identifizierbar machen, sind auch die Elemente, die sie voneinander unterscheiden.[1] Identifizierbar zu sein bedeutet, die Identität durch Hilfsmittel preiszugeben. Beispielsweise sind der Fingerabdruck oder die IP-Adresse einer Person die Daten, die die Person identifizierbar ma-

1 *Wolff/Brink*, Datenschutzrecht in Bund und Ländern, 2013, § 3 Rn.1; *Eßer/Kramer/von Lewinski*, Datenschutz-Grundverordnung, 7. Aufl., 2020, Art. 4 Rn. 6; *Paal/Pauly*, Beck'sche Kompakt-Kommentare Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 3. Aufl., 2021, Art. 4 Rn. 4; *Gola*, Datenschutz-Grundverordnung Kommentar, 2. Aufl., 2018, Art. 4 Rn. 4; *Ehmann/Selmayr*, Datenschutz-Grundverordnung Kommentar, 2. Aufl., 2018, Art. 4 Rn. 8; *Gierschmann/Schlender/Stentzel/Veil,* Kommentar Datenschutz-Grundverordnung, 2018, Art. 4 Rn. 7; *Schwartmann/Jaspers/Thusing/Kugelmann*, Datenschutz-Grundverordnung, 2. Aufl., 2020, Art. 4 Rn. 10; *Däubler/Wedde/Weichert/Sommer*, EU-DSGVO und BDSG, 2. Aufl., 2020, Art. 4 Rn. 17; *Simitis/Hornung/Spiecker*, Datenschutzrecht Kommentar, 2019, Art. 4 Rn. 6; *Götting/Schertz/Seitz*, Handbuch Persönlichkeitsrecht, 2. Aufl., 2019, § 22 Rn. 10; *Schmidt-Holtmann*, Der Schutz der IP-Adresse im deutschen und europäischen Datenschutzrecht, 2014, S. 41; *Roßnagel*, Das neue Datenschutzrecht, 2018, § 3 Rn. 6; *Haase*, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 37.

chen?[2] An dieser Stelle erfüllen Technologien der künstlichen Intelligenz und darauf basierende Software eine wichtige Funktion bezüglich des Punktes „identifizierbar sein" und erleichtern die Identifizierbarkeit.[3]

In der Doktrin gibt es einige Auffassungen über die Bestimmung der Bestimmbarkeit der Person. Es gibt zwei Ansichten zur Bestimmbarkeit: absolute Bestimmbarkeit und relative Bestimmbarkeit. Nach der Auffassung der absoluten Identifizierbarkeit sind die Identität des für die Verarbeitung Verantwortlichen und der Zweck der Datenverarbeitung nicht von Bedeutung. Unabhängig davon, ob der für die Verarbeitung Verantwortliche Zugang zu den von Dritten gespeicherten Daten hat, wird davon ausgegangen, dass die von Dritten gespeicherten Informationen, die die Identifizierung der Person ermöglichen, ebenfalls unter der Kontrolle des für die Verarbeitung Verantwortlichen stehen.[4] Mit anderen Worten, um Daten als personenbezogene Daten zu qualifizieren, indem das Element der Identifizierbarkeit realisiert wird, wird als Kriterium verwendet, ob es möglich ist, die Daten in Kombination mit Daten eines Dritten mit einer Person zu verknüpfen. Im Hinblick auf die relative Identifizierbarkeit werden nur die Identität und Informationen der Person, die die Daten verarbeitet, zugrunde gelegt.[5] In diesem Zusammenhang ist die Qualifizierung von IP-Adressen als personenbezogene Daten im Hinblick auf eine absolute Identifizierbarkeit möglich. Denn die vom Internet-Service-Provider vergebene IP-Adresse selbst enthält keine Rückschlüsse auf die Identität der Person. Soweit die Identitätsinformationen des aufrufenden Diensteanbieters einer Person zuordenbar sind, kann die IP-Adresse im Hinblick auf eine zweifelsfreie Identifizierbarkeit als personenbezogenes Datum angesehen werden.[6]

Das Element des Begriffs „personenbezogene Daten", wonach sich die Informationen auf eine Person beziehen, bedeutet, dass sich die Informationen auf diese Person beziehen. Im allgemeinen Sinne weisen Daten über eine Person darauf hin, dass sich diese Daten auf die Person beziehen. Persönliche Informationen können in numerischer, grafischer, fotografischer, Audio- oder irgendeiner anderen Form vorliegen. Personenbezogene Daten umfassen vertrauliche und nicht vertrauliche Daten. Der Umfang der Informationen über die Person umfasst sowohl objektive Informationen als auch subjektive Informationen, die auf Gedanken, Absichten und sogar falschen Informationen über die Person beruhen.[7]

2 Grund des Schutzes besonderer Kategorien personenbezogener Daten

Ein wichtiger Punkt ist die Unterscheidung zwischen personenbezogenen Daten von besonderer Eigenschaft und personenbezogenen Daten von allgemeiner Eigenschaft. Besondere Kategorien von personenbezogenen Daten sind sensible Informationen, die sich auf eine natürliche Person beziehen. Diese Art von Daten beinhaltet Risiken, wie die Diskriminierung der betroffenen Person. Aus diesem Grund ist es wichtig, ob personenbezogene Daten als besondere Kategorien personenbezogener Daten eingestuft werden können. Eine allgemeine Definition besonderer Kategorien personenbezogener Daten findet sich in der Datenschutz-Grundverordnung nicht. Andererseits regelt Art. 9 DS-GVO die Verarbeitungsbedingungen, indem er die Arten von personenbezogenen Daten besonderer Art aufzählt. Als besondere Arten personenbezogener Daten gelten danach die rassische und ethnische Herkunft, die politische Meinung, die religiöse oder weltanschauliche Überzeugung, die Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten, Gesundheitsdaten, das Sexualleben oder die sexuelle Orientierung einer natürlichen Person.

Die Tatsache, dass besondere Kategorien personenbezogener Daten als separate Kategorie zu personenbezogenen Daten gehören und auch organisiert und geschützt werden, liegt in der Natur dieser Daten. Besondere Kategorien personenbezogener Daten bergen Risiken im Vergleich zu allgemeinen Kategorien personenbezogener Daten. Dieses Risiko ist die Gefahr von Vorurteilen in der Gesellschaft bei der Verarbeitung sensibler personenbezogener Daten. Wenn andere von den betreffenden personenbezogenen Daten erfahren, kann die Person diskriminiert oder schikaniert werden.[8] Personenbezogene Daten von besonderer Eigenschaft werden aufgrund dieses Risikofaktors auf einer höheren Ebene geschützt. Das höhere Schutzniveau für diese Daten zeigt sich am deutlichsten in dem absoluten Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten. Absolutes Verarbeitungsverbot bedeutet, dass sensible personenbezogene Daten in keiner Weise verarbeitet werden dürfen, mit Ausnahme der im Gesetz festgelegten Ausnahmen.[9]

Bei der Bestimmung des Umfangs von personenbezogenen Daten besonderer Art ist es besonders wichtig, alle Merkmale des konkreten Falls zu berücksichtigen. Beispielsweise sollte ein Foto einer Person mit Brille Informationen über ihren Gesundheitszustand enthalten oder die Tatsache, dass der Name der Person ihre religiöse Überzeugung widerspiegelt, nicht ausreichen, um jeden Text als Text mit personenbezogenen Daten von besonderer Eigenschaft zu bezeichnen. In einem solchen Fall können Fotos oder Namen solcher Personen als sensible personenbezogene Daten betrachtet werden. Aus diesem Grund sollte eine Bewertung unter Berücksichtigung aller Merkmale des konkreten Falls erfolgen. Wenn beispielsweise eine Bewertung über die Person mit Sehbehinderung oder die religiöse Überzeugung der Person vorgenommen wird, können diese als personenbezogene Daten

2 *Spindler,* Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung, 2012, S. 71; *Elixmann,* Datenschutz und Suchmaschinen neue Impulse für einen Datenschutz im Internet, 2012, S. 150.

3 *Strauß,* Privacy and Identity in a Networked Society Refining Privacy Impact Assessment, 2019, S. 16.

4 *Lindner,* Die datenschutzrechtliche Einwilligung nach §§ 4 Abs.1, 4a BDSG – ein zukunftsfähiges Institut?, 2013, S. 64.

5 *Gierschmann/Saeugling*, Systematischer Praxiskommentar Datenschutzrecht, 2014, § 3 Rn. 31.

6 *O'Doherty,* Internet Law, 2020, S. 212.

7 *Hacker*, Datenprivatrecht, 2020, S.4; *Meinecke*, Datenschutz und Data Science, 2021, S.31; *Jahnel*, Kommentar zur Datenschutz-Grundverordnung, 2021, Art. 4 Rn. 9.

8 *Jay*, Data Protection: Law and Practice, 2007, S. 272.

9 *Lloyd*, Information Technology Law, 6. Aufl., 2011, S. 41; *Plath*, Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen von TMG und TKG, 3. Aufl., 2018, Art. 9 Rn. 4; Kühling/Buchner-*Weichert*, Datenschutz-Grundverordnung BDSG-Kommentar, 3. Aufl., 2020, Art. 9 Rn. 4a; *Sydow*, Europäische Datenschutzgrundverordnung Handkommentar, 2. Aufl., 2018, Art. 9 Rn. 1; *Vicente/de Vasconcelos Casimiro*, Data Protection in the Internet, 2020, S. 461; *Wiebe/Dietrich*, Open Data Protection, 2017, S. 39.

von besonderer Eigenschaft betrachtet werden. Bei einer solchen Bewertung stellt der Name der Person, der seine/ihre religiöse Überzeugung widerspiegelt, wenn er unter Berücksichtigung dieser Eigenschaft verwendet wird, personenbezogene Daten von besonderer Eigenschaft dar, während die bloße Aufnahme in eine Datenbank nicht dazu führt, dass er als personenbezogene Daten von besonderer Eigenschaft qualifiziert wird.[10] In jenem Fall sollten solche Daten nicht als besondere Kategorien personenbezogener Daten betrachtet werden. Wenn solche Daten verarbeitet werden und demgegenüber eine Bewertung über die betroffene Person vorgenommen wird, wie in dem genannten Beispiel, wäre es ein richtiger Ansatz, sie als besondere Kategorien personenbezogener Daten zu bezeichnen.

Alle personenbezogenen Daten – mit Ausnahme der besonderen Kategorien personenbezogener Daten – sind allgemeine Kategorien personenbezogener Daten. Die Unterscheidung zwischen besonderen und allgemeinen Kategorien personenbezogenen Daten zeigt keine Rangfolge der Daten. Mit anderen Worten, die genannte Unterscheidung wurde nicht geschaffen, weil personenbezogene Daten von allgemeiner Eigenschaft weniger wichtig sind als personenbezogene Daten von besonderer Eigenschaft, sondern weil personenbezogene Daten von besonderer Eigenschaft einige Risiken, wie Diskriminierung bergen.[11]

Es sollte berücksichtigt werden, dass das Hauptziel beim Schutz personenbezogener Daten ein effektiver Schutz ist. Es ist notwendig, anwendbare und wirksame Regeln für die Verarbeitung personenbezogener Daten festzulegen, unabhängige Institutionen einzurichten, die ihre Kontrolle gewährleisten, Sanktionen für Verstöße vorzusehen und das Bewusstsein für das Thema zu schärfen sowie alle Arten von Daten zu schützen, die die Persönlichkeit beeinträchtigen, ohne Unterscheidung besonderer oder allgemeiner Art. Darüber hinaus sollten Datenschutzbehörden oder Datenschutzbeauftragte nicht nur die Unterscheidung zwischen allgemeinen und besonderen Kategorien personenbezogener Daten berücksichtigen, sondern auch die Merkmale jedes konkreten Falls, die einzigartigen Merkmale der einzelnen Daten und die Unterschiede des Datentyps.

3 Platz und Bedeutung biometrischer Daten

Art. 4 Nr.14 DS-GVO enthält eine Definition der biometrischen Daten. Biometrische Daten sind personenbezogene Daten, die sich auf physische, physiologische oder verhaltensbezogene Merkmale einer natürlichen Person beziehen und durch besondere technische Verfahren gewonnen werden, mit denen diese natürliche Person eindeutig identifiziert oder überprüft werden kann. Gesichtsbilder und daktyloskopische Daten werden in der DS-GVO Art. 4 Nr. 14 als Beispiele für biometrische Daten genannt. Mit dem besonderen Schutz dieser Informationen sollen umfassende Persönlichkeitsprofile mithilfe systematischer Zusammenführung solcher Daten verhindert werden.[12]

Biometrische Daten können in verschiedenen Arten und Methoden erzeugt werden. Die biometrische Erkennung durch biometrische Systeme zielt auf die Verwendung automatischer Messverfahren, die Menschen voneinander unterscheiden, um bestimmte Merkmale zu identifizieren. Biometrische Daten sind entweder angeborene, passive, unveränderliche Körpermerkmale (Fingerabdruck, Gesicht, Netzhaut, DNA, Handaussehen/-geometrie) oder Verhaltens- und aktive Merkmale (Signatur, Stimme, Bewegung/Gang, Tastatur/Geometrie), die durch biometrische Verfahren erfasst werden können (Tastenanschlag). Biometrische Daten sind Daten, die durch spezielle Verarbeitung und systematische Kombination von Venen-, Iris-, Stimmerkennungssystemen die Erstellung umfassender Persönlichkeitsprofile ermöglichen.[13]

Da der Identifizierungsprozess bei biometrischen Verfahren auf den physischen oder verhaltensbezogenen Merkmalen von Personen beruht, können die betreffenden Daten nicht übertragen, vergessen oder verloren werden. Mit Hilfe biometrischer Verfahren kann eine Person genau und präzise identifiziert werden. Diese Situation zeigt den Hauptvorteil biometrischer Verfahren und führt dazu, dass sie häufig bevorzugt werden.[14] Beispielsweise wird die Biometrie im täglichen Leben eingesetzt, wenn Mitarbeiter das Unternehmen mit einem Fingerabdruck-Scanner betreten oder wenn Banken bei Hochsicherheitstransaktionen die Iriserkennung nutzen. Biometrische Daten werden auch in vielen anderen Bereichen des täglichen Lebens verwendet. Beispielsweise können die Länder Gesichtserkennungs- und Fingerabdruckdaten verarbeiten, um die Ein- und Ausreise von Personen zu kontrollieren oder in einigen Ländern werden biometrische Daten, wie Gesichtserkennung oder Fingerabdrücke, verwendet, um den Zugang zu staatlichen Dienstleistungen zu verwalten und zu kontrollieren, bei der Ausstellung von Personalausweisen oder der Beantragung von Sozialleistungen.

Ein weiteres eindrucksvolles Beispiel für die Verarbeitung biometrischer Daten im Alltag hat sich unter den Bedingungen der Covid 19-Pandemie ergeben. Unter den Bedingungen der Covid-19-Pandemie, die die ganze Welt betrifft, sind biometrische Daten ein wichtiges Thema für Bildungssysteme. Denn unter den Pandemiebedingungen wurde der Unterricht über Online-Systeme durchgeführt und in der Zwischenzeit wurden persönliche Daten von Schülern, wie Name-Nachname, Stimme, Bild verarbeitet. An dieser Stelle sei betont, dass nicht alle in Online-Bildungssystemen verarbeiteten Audio- und Videodaten als biometrische Daten und damit als personenbezogene Daten besonderer Eigenschaft zu betrachten sind. Stattdessen sind sie als biometrische Daten anzusehen, wenn durch eine Auswertung mithilfe eines Gesichts- oder Augenerkennungssystems etc. auf die Identität des Schülers geschlossen wird.

Die zunehmende Verwendung biometrischer Methoden im täglichen Leben bringt einige Bedenken hinsichtlich personenbezogener Daten mit sich. Die größten Bedenken in diesem Zusammenhang sind die Zunahme der Bereiche, in denen biometrische Methoden zur Erfassung von Personen eingesetzt werden, und die damit mögliche Verletzung des Datenschutzrechts.[15] Die Sicherheit des biometrischen Verfahrens in Bezug auf die Person, die es verwendet, ist für die betroffene Person von besonderer Be-

10 *Gola/Schomerus*, Bundesdatenschutzgesetz Kommentar, 10. Aufl., 2010, § 3 Rn. 56.

11 *Kuner/Bygrave/Docksey*, The EU General Data Protection Regulation (GDPR) a Commentary, 2020, S. 369.

12 Taeger/Gabel-*Mester,* Kommentar zum DSGVO-BDSG-TTDSG, 4. Aufl., 2022, Art. 9 Rn. 14.

13 Taeger/Gabel-*Buchner,* Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 2. Aufl., 2020, § 3 Rn. 57; *Schaar,* Das Ende der Privatsphäre, 2009, S. 79.

14 *Jain/Bolle/Pankanti*, Biometrics, Personal Identification in Network Society, 2002, S. 4.

15 *Campisi*, Security and Privacy in Biometrics, 2013, S. 2.

deutung, da es sich um die Verarbeitung besonderer personenbezogener Daten handelt. Hauptbedenken gegen den weit verbreiteten Einsatz biometrischer Verfahren, biometrische Daten sind sehr private Informationen über die betreffende Person, die sie nicht an Dritte weitergeben wollen. Es sollte betont werden, dass es das natürlichste Recht des Betroffenen ist, sein Leben in Sicherheit und Freiheit zu leben und sich darauf zu verlassen, dass seine persönlichen Daten, die durch diese Methoden gewonnen wurden, geschützt sind.

Das verwendete biometrische Verfahren muss einige grundlegende Merkmale aufweisen. Bei einem biometrischen Verfahren müssen Robustheit, Unterscheidungskraft, Verwendbarkeit und Akzeptanz gegeben sein, was bedeutet, dass die Person, von der Daten genommen werden, dem nichts entgegensetzen sollte. Es gibt zwei Anwendungen im Zusammenhang mit biometrischen Verfahren, Identifizierung und Verifizierung. Bei der Verifizierung geht es um die Bestätigung oder Verleugnung der eigenen angeblichen Identität. Bei der Authentifizierungsmethode zeigen die Benutzerdaten auf eine Vorlage in der Datenbank im System, benötigen ein biometrisches Muster des Benutzers, verarbeiten dieses Muster und vergleichen es mit den im System registrierten. Bei der Identifizierung geht es darum, die Identität einer bereits bekannten Person festzustellen. Bei der Identifizierung liest das biometrische Gerät eine Probe, verarbeitet diese Probe und vergleicht sie mit jeder Aufzeichnung oder Vorlage, die in der Datenbank gespeichert ist. Diese Definitionen sind wichtig, da mit diesen Methoden und Anwendungen biometrische Daten erstellt werden. Beispiele für biometrische Datentypen sind Fingerabdruck, Stimme, Netzhautmodell, Gesichtsmodell, Unterschriftsmodell. Dabei wird als Kriterium zur Abgrenzung biometrischer Daten von anderen personenbezogenen Daten herangezogen, dass es sich um Daten handelt, die zur Unterscheidung der Person geeignet sind. Alle Audiodaten, Bilder, Fotos oder Videos sind keine biometrischen Daten, sondern gewöhnliche personenbezogene Daten. Biometrische Daten sind die Daten, die eigens für ein Erkennungssystem, wie Fingerabdruck, Netzhautregistrierung, biometrische Sprach- oder Bildaufnahme erstellt oder in diesem Erkennungssystem verarbeitet werden.

Zwischen den Arten biometrischer Daten soll nach Ansicht in der Doktrin unterschieden werden. Nach dieser Auffassung sind beispielsweise die durch den Einsatz von Sprach- und Gesichtserkennungstechnologien am Arbeitsplatz verursachten Probleme anders zu bewerten als das Führen von Fingerabdrücken und DNA-Aufzeichnungen. Die Erfassung von öffentlich sichtbaren Elementen, wie dem Gesicht einer Person im Rahmen des Arbeitsvertrags ist im Vergleich zu Fingerabdrücken ein geringerer Eingriff in das Privatleben. Bei der Entscheidung zu dieser Frage sollten jedoch alle Umstände des konkreten Falls berücksichtigt werden. Denn Informationen, die am Anfang vielleicht unbedeutend erscheinen, können mit der Veränderung der Bedingungen extrem wichtig werden.

Authentifizierung bedeutet konzeptionell den Nachweis, dass eine bestimmte Person eine bestimmte Identität besitzt oder berechtigt ist, bestimmte Tätigkeiten auszuführen. Die Authentifizierung kann auf verschiedene Arten erfolgen. Zu den Möglichkeiten der Authentifizierung gehören eine E-Mail-Adresse, die über ein in einer E-Mail-Nachricht gesendetes Passwort verifiziert wurde, Sozial-Media-Konten, die mit Sozial-Media-Anmeldeinformationen verifiziert wurden, Mobiltelefonnummern, die durch ein per SMS gesendetes Passwort verifiziert wurden, eine Fotokopie eines Ausweisdokuments, ein verifizierter Befrager. Als Beispiele können Fragen zu öffentlichen Registrierungsinformationen und biometrische Verfahren zum Scannen von Gesichtern und Handflächen, die in Gesundheitszentren verwendet werden, genannt werden. Authentifizierungsverfahren lassen sich grundsätzlich in drei Kategorien einteilen. „Einfaktor-Authentifizierung", bei der die Authentifizierung mit einem vom Benutzer festgelegten Passwort erfolgt, „biometrische Verifizierung" unter Verwendung biometrischer Informationen, die für die Person eindeutig sind, und „zweistufige Verifizierung". Die Anwendung jeder Methode bedeutet die Verarbeitung biometrischer Daten, und die aus der Anwendung dieser Methoden resultierenden Daten sind biometrische Daten. Die Methoden sind also wichtig.

4 Fazit

Mit den sich ständig weiterentwickelnden Technologien werden biometrische Daten in fast allen Aspekten des täglichen Lebens verwendet. Beispielsweise können Smartphones, die ein wichtiger Bestandteil unseres täglichen Lebens sind und von vielen Menschen genutzt werden, nicht nur mit einem Passwort, sondern auch mit einem Fingerabdruck geschützt werden. Parallel zur sich entwickelnden Technologie verwenden einige Anwendungen auch Fingerabdrücke, also biometrische Daten von Personen. Eine ähnliche Situation wie beim Fingerabdruck gilt auch für die Iriserkennungstechnologie, die in Smartphones und Anwendungen verwendet wird.

Wie ich mit verschiedenen Beispielen zu zeigen versucht habe, sind biometrische Daten die Daten, mit denen jede natürliche Person geboren wird. Darüber hinaus werden biometrische Daten auch im Alltag immer häufiger verwendet, da sich die Technologie und die Lebensverhältnisse in einem immer schwindelerregenderen Tempo entwickeln. Die Besonderheit biometrischer Daten und die strengen Regeln für ihre Verarbeitung machen biometrische Daten zu einer Spezies mit besonderer Bedeutung. Es ist besonders wichtig, die Regeln für die Verarbeitung biometrischer Daten im täglichen Leben zu beachten. Biometrische Daten sind heute fast überall in unserem täglichen Leben zu finden. Selbst bei einer sehr einfachen Handlung, wie dem Entsperren des Telefons bei Smartphones werden Technologien zur Erkennung der Iris oder des Gesichts, d. h. biometrische Daten, verarbeitet. Es scheint, dass die Bedeutung und der Stellenwert biometrischer Daten im Recht zum Schutz personenbezogener Daten von Tag zu Tag weiter zunehmen werden.