SCHWEIZERISCHE BANKRECHTSTAGUNG 2019

Institut für Bankrecht, Universität Bern

Biometrische Daten im Bankkundenverkehr am Beispiel der Stimmauthentifizierung

Susan Emmenegger/Martina Reber

In: Susan Emmenegger (Hrsg.), Banken und Datenschutz, Basel 2019

ISBN 978-3-7190-4269-1

Inhaltsübersicht

Biometrische Daten im Bankkundenverkehr am Beispiel der Stimmauthentifizierung

Susan Emmenegger/Martina Reber*

* Prof. Dr. iur. Susan Emmenegger, LL.M., Direktorin des Instituts für Bankrecht, Universität Bern. Martina Reber, Rechtsanwältin, MLaw, wissenschaftliche Assistentin und Doktorandin am Institut für Bankrecht, Universität Bern.

I. Einleitung

Das Bankgeschäft ist ein Risikogeschäft. Das gilt nicht nur für die Makroperspektive, es gilt auch auf der Mikroebene und es gilt – noch kleinteiliger – für die Kommunikation und die Transaktion mit der einzelnen Bankkundin. Zu den Risiken im letztgenannten Bereich zählen die sogenannten Legitimationsmängel, bei denen ein betrügerisch handelnder Zahlungsempfänger eine Zahlung an sich selbst bewirkt, ohne dass diese Zahlung von der Kontoinhaberin autorisiert war.[1] Aber auch die Erfragung von Kontoständen oder anderen kontorelevanten Informationen steht unter dem Risiko eines Zugriffs durch vertragsfremde Dritte.

Eine mögliche Abhilfe zur Vermeidung von solchen Vorfällen sind Authentifizierungsmechanismen, die auf biometrische Erkennungsmerkmale abstellen.[2] Dabei sind allerdings die rechtlichen Rahmenbedingungen für die Verwendung von biometrischen Authentifizierungsverfahren zu beachten.

---

1 Zum Begriff des Legitimationsmangels etwa SCHALLER, Legitimationsmängel, 49 f.

2 Beispielhaft folgende Klausel: «Die Bank kann zu Sicherheitszwecken (z.B. Schutz des Kunden und der Bank vor missbräuchlichen oder deliktischen Aktivitäten) den Kunden betreffende biometrische Daten sowie Bewegungs- und Transaktionsdaten und entsprechende Profile des Kunden erheben und bearbeiten.»

II. Biometrische Daten

1. Begriff

Bestimmte Körpermerkmale sind bei jedem Menschen einzigartig. Dazu gehören etwa der Fingerabdruck oder das Irismuster, nicht aber die Körpergrösse oder die Augenfarbe.[3] Sind diese Körpermerkmale überdies messbar und nur mit erheblichem Aufwand veränderbar, handelt es sich um biometrische Merkmale.[4]

Biometrische Daten sind Angaben über biometrische Merkmale.[5] Sie dienen in der Regel der Überprüfung, ob eine Person tatsächlich diejenige ist, für die sie sich ausgibt (Verifizierung) oder dem Abgleich mit einer Gesamtdatenbank zwecks Findung der Identität einer Person (Identifizierung).[6]

2. Funktionsweise biometrischer Verfahren

Biometrische Verfahren laufen in zwei Phasen ab. Zuerst erfolgt eine Registrierungsphase (Enrollment), in der die Identität der betroffenen Person erfasst und das biometrische Merkmal mehrmals und unter veränderten Bedingungen gemessen wird.[7]

> Beispiel: Bei der Einrichtung der Fingerabdruck-Authentifikation auf dem Smartphone muss der Benutzer seinen Finger mehrmals aus unterschiedlichen Winkeln und in unterschiedlichen Positionen auf den Fingerabdrucksensor des Smartphones legen.

Anschliessend werden die relevanten Merkmale aus den Rohdaten extrahiert und als biometrisches Template zusammen mit den Angaben zur Identität des Benutzers gespeichert.[8]

Die zweite Phase wird als Erkennungsphase bezeichnet. Erneut wird das entsprechende biometrische Merkmal gemessen und daraus ein biometrisches Template erstellt, welches mit den gespeicherten Referenztemplates

---

3 HK DSG-ROSENTHAL, Art. 3 N 42.

4 BLONSKI, Biometrische Daten, 6.

5 BLONSKI, Biometrische Daten, 6.

6 BLONSKI, Biometrische Daten, 6; EDÖB, Leitfaden zu biometrischen Erkennungssystemen, 5.

7 BLONSKI, Biometrische Daten, 11, m.w.H.; EDÖB, Leitfaden zu biometrischen Erkennungssystemen, 5.

8 Vgl. EDÖB, Leitfaden zu biometrischen Erkennungssystemen, 12; BLONSKI, Biometrische Daten, 11.

verglichen wird.[9] Bei der Verifizierung findet dieser Vergleich nur mit den Referenzdaten derjenigen Person statt, als die sich eine Person ausgibt.[10] Bei der Identifizierung wird das aktuell erstellte Template hingegen mit einer Vielzahl von Referenztemplates verglichen mit dem Ziel, herauszufinden, welcher Person das biometrische Merkmal zugeordnet werden kann.[11]

3. Die Stimmerkennung im Besonderen

Bei der Stimmerkennung wird die Stimme mittels eines Mikrofons aufgenommen.[12] Dabei gibt es zwei mögliche Methoden. Bei der textabhängigen Methode muss die Kundin vorgegebene Wörter aussprechen, bei der textunabhängigen Methode kann die Software ein beliebiges Kundengespräch analysieren.[13] Anschliessend werden die charakteristischen Merkmale extrahiert und daraus ein Stimmabdruck erstellt.[14] Bei künftigen Gesprächen wird die Stimme der Kundin zwecks Authentifizierung mit diesem Stimmabdruck abgeglichen.[15]

4. Beispielfall für eine Stimmerkennung

In den AGB von Banken finden sich vermehrt Klauseln, wonach diese sich vorbehalten, zu Sicherheitszwecken biometrische Daten des Kunden zu erheben und zu bearbeiten. Dazu gehört auch die Erstellung eines Stimmabdrucks. Den jüngsten Anwendungsfall, der medial aufgegriffen wurde,[16] betrifft die PostFinance. Sie nutzt seit September 2018 ein Stimmauthentifizierungssystem der israelischen Firma NICE.[17] Ruft die Kundin das erste Mal bei PostFinance an, hört sie folgende automatische Ansage:

> «Dieses Gespräch wird zu Sicherheits- und Wiedererkennungszwecken aufgezeichnet. PostFinance erstellt aus der Aufnahme einen Stimmabdruck, um

9 BLONSKI, Biometrische Daten, 12.

10 BLONSKI, Biometrische Daten, 12 f.; EDÖB, Leitfaden zu biometrischen Erkennungssystemen, 5.

11 BLONSKI, Biometrische Daten, 13.

12 BLONSKI, Biometrische Daten, 19.

13 Vgl. BLONSKI, Biometrische Daten, 19.

14 Vgl. BLONSKI, Biometrische Daten, 19; zur Extraktion der charakteristischen Merkmale ausführlich TILLENBURG, DuD 3/2011, 198.

15 Vgl. BLONSKI, Biometrische Daten, 19.

16 So etwa in der SRF-Sendung «10vor10» vom 20. Mai 2019.

17 Inside-IT vom 2. Mai 2019 («PostFinance setzt auf Stimmerkennung zur Authentifizierung»), abrufbar unter: <www.inside-it.ch/articles/53194>.

> Ihre Identität bei jeden [recte: jedem] Anruf anhand Ihrer Stimme zu verifizieren. Wünschen Sie keinen Stimmabdruck, bitten wir Sie, dies dem Kundenbetreuer mitzuteilen.»

Alternativ zum Widerspruch am Telefon kann die Kundin die Stimmerkennung im Online-Banking-Portal der PostFinance (E-Finance) deaktivieren, woraufhin ein allfällig bereits erstellter Stimmabdruck gelöscht wird. Hat die Kundin der Stimmerkennung widersprochen, wird sie anhand von Fragen authentifiziert.[18]

Auf ihrer Website informiert die PostFinance namentlich darüber, dass der Stimmabdruck «auf Servern in der PostFinance-Sicherheitszone in der Schweiz gespeichert» werde «und zwar in Form eines Codewertes, das heisst ohne den Gesprächsinhalt.» Der Stimmabdruck werde ausschliesslich zu Authentifikationszwecken verwendet.[19]

Die PostFinance ist keinesfalls das einzige Unternehmen, welches die Stimmbiometrie zu Authentifizierungszwecken verwendet. Eingesetzt wurde das Verfahren auch bei der Swisscom, und zwar nach demselben Muster wie bei der PostFinance.[20] Allerdings hat die Swisscom das Experiment wieder abgebrochen.[21] Sodann sollen auch immer mehr Banken die Stimmbiometrie einsetzen.[22] Es handelt sich also keineswegs um ein Einzelphänomen, sondern um einen allgemeinen Trend. Der Eidgenössische Datenschutzbeauftragte sieht das gewählte Vorgehen beim Stimmabdruck kritisch, er fordert eine ausdrückliche Zustimmung.[23] Die PostFinance will Medienberichten zufolge am bestehenden Modell festhalten, bis das neue Datenschutzgesetz in Kraft ist.[24]

---

18 Zum Ganzen siehe die Informationen der PostFinance, abrufbar unter: <www.postfinance.ch/de/privat/support/persoenliche-daten/authentifizierung-stimmerkennung.html>.

19 Informationen der PostFinance, abrufbar unter: <https://www.postfinance.ch/de/privat/support/persoenliche-daten/authentifizierung-stimmerkennung.html>.

20 Tagesanzeiger vom 5. März 2019 («Wie unsere Stimme alles über uns verrät»), abrufbar unter: <https://www.tagesanzeiger.ch/digital/internet/wie-unsere-stimme-alles-ueber-uns-verraet/story/18087714>.

21 Inside-IT vom 2. Mai 2019 («Swisscom lässt Stimmerkennung sein»), abrufbar unter: <https://www.inside-it.ch/articles/54323>.

22 NZZ vom 24. April 2019 («Unsere Stimme sagt alles über uns – auch das, was wir gar nicht sagen wollen»), abrufbar unter: <https://www.nzz.ch/feuilleton/unsere-stimme-sagt-alles-ueber-uns-auch-das-was-wir-gar-nicht-sagen-wollen-ld.1380929>.

23 EDÖB, Erläuterungen zum Stimmerkennungsverfahren (Stand 17. April 2017).

24 Siehe dazu die Zusammenfassung der Sendung «10vor10» vom 20. Mai 2019 auf www.srf.ch. Offensichtlich wird diese Haltung auch dadurch, dass die PostFinance die Stimmerkennung nach wie vor einsetzt (Stand: 7. Mai 2019).

Bei dieser Ausgangslage lohnt sich ein vertiefter Blick auf die spezifische Frage der Zulässigkeit der Verwendung der Stimmbiometrie, wie es die PostFinance und möglicherweise auch zahlreiche andere Banken verwenden.

III. Datenschutzrechtliche Relevanz des Stimmabdrucks

1. Anwendbarkeit des Datenschutzgesetzes

Das DSG ist auf das Bearbeiten von Daten natürlicher und juristischer Personen durch private Personen und Bundesorgane anwendbar (Art. 2 Abs. 1 DSG).[25]

Die PostFinance ist eine privatrechtliche Aktiengesellschaft, an der die Schweizerische Post AG die Mehrheitsbeteiligung hält (vgl. Art. 14 Abs. 1 und 2 POG[26]). Sie erfüllt private Aufgaben und tritt ihren Kundinnen und Kunden gegenüber nicht hoheitlich, sondern privatrechtlich entgegen, weshalb sie nicht als Bundesorgan i.S.v. Art. 3 Bst. h DSG, sondern als Privatperson zu betrachten ist.[27] Das gilt entsprechend für die Kantonalbanken; bei den übrigen Banken stellt sich die Frage einer hoheitlichen Rechtsbeziehung zum Kunden nicht – und sie stellt sich auch nicht bei den Dienstleistern aus anderen Segmenten, die hier nicht im Fokus stehen.

Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 3 Bst. a DSG). Erfasst sind sowohl Tatsachenfeststellungen als auch Werturteile, ungeachtet ihrer Erscheinungsform (z.B. Bild, Ton, Schrift).[28] Eine Person ist bestimmt, wenn sich ihre Identität aus der konkreten Information selbst ergibt.[29] Bestimmbar ist sie dann, wenn sich ihre Identität aus dem Kontext der Information ermitteln lässt, wobei der Begriff aufgrund der heutigen technischen Möglichkeiten «äusserst weit zu fassen» ist.[30]

---

25 Zu den Ausnahmen vom Geltungsbereich siehe Art. 2 Abs. 2 DSG.

26 Bundesgesetz über die Organisation der Schweizerischen Post (Postorganisationsgesetz) vom 17. Dezember 2010, SR 783.1.

27 Die PostFinance wurde auch vom EDÖB in der Affäre E-Cockpit und Bicicletta als Privatperson betrachtet, vgl. EDÖB, Schlussbericht PostFinance, S. 6. Zur Abgrenzung zwischen Bundesorganen und Privatpersonen im Rahmen des DSG vgl. z.B. HK DSG-ROSENTHAL, Art. 3 N 99 ff.

28 BSK-DSG-BLECHTA, Art. 3 N 6.

29 BSK-DSG-BLECHTA, Art. 3 N 9.

30 BSK-DSG-BLECHTA, Art. 3 N 10 f. Siehe dazu auch BGE 138 II 346 E. 6.1 S. 353 f. (Google Street View)

Eine Bearbeitung ist jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten (Art. 3 Bst. e DSG).

Wenn die PostFinance oder ein anderer Dienstleister die Stimme ihre Kundin aufzeichnet und daraus einen Stimmabdruck erstellt, der die Identität dieser Kundin künftig verifizieren soll, bearbeitet sie deren Personendaten. Sie fällt daher in den Anwendungsbereich des DSG.

2. Bearbeitung besonders schützenswerter Personendaten

Besonders schützenswerte Personendaten sind Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe sowie administrative oder strafrechtliche Verfolgungen oder Sanktionen (Art. 3 Bst. c DSG).

Ob auch biometrische Daten zu den besonders schützenswerten Personendaten gehören, ist umstritten. Ein Teil der Lehre subsumiert biometrische Daten unter die Gesundheitsdaten i.S.v. Art. 3 Bst. c DSG.[31] Nach einer anderen Meinung gehören biometrische Daten nicht *per se* zu den besonders schützenswerten Personendaten, sondern nur, wenn sie Rückschlüsse auf solche zulassen.[32] Die blosse Möglichkeit eines solchen Rückschlusses scheint nach dieser Meinung auszureichen.[33] Weiter wird die Ansicht vertreten, dass es sich bei biometrischen Daten erst dann um besonders schützenswerte Personendaten handle, wenn sie gezielt hinsichtlich des betreffenden Merkmals ausgewertet würden.[34]

Die letzte Ansicht ist abzulehnen, weil es bei der Qualifikation eines Personendatums nicht auf den konkreten Bearbeitungsvorgang ankommen kann. Entscheidend ist der informationelle Gehalt des Personendatums an

---

31 SPRECHER, ZBJV 154/2018, 494.

32 HK DSG-ROSENTHAL, Art. 3 N 43.

33 Vgl. HK DSG-ROSENTHAL, Art. 3 N 43, der in seinem Beispiel den Konjunktiv verwendet: «wenn beim Irisscan aus der Iris auch Angaben über den Gesundheitszustand gewonnen werden könnten»; Gl.M. wohl auch BSK-DSG-BLECHTA, Art. 3 N 33: «Im Hinblick auf die Angaben über die Gesundheit i.S. des Gesetzes werden alle Informationen erfasst, die, auf welche Art auch immer, Rückschlüsse auf den körperlichen oder geistigen Gesundheitszustand einer Person erlauben.» Siehe zudem EDÖB, Leitfaden biometrische Daten, S. 17 N 3.3.4.

34 VASELLA, Stimmerkennung, *in fine*.

sich: Ist es möglich, daraus Informationen über den Gesundheitszustand oder ein sonstiges in Art. 3 Bst. c DSG genanntes Merkmal zu gewinnen, handelt es sich um ein besonders schützenswertes Personendatum. Die Diskussion dürfte sich ohnehin bald erledigt haben, da biometrische Daten sowohl nach DSGVO[35] als auch nach E-DSG[36] zu den besonders schützenswerten Personendaten zählen.

Anhand unserer Stimme erkennen Algorithmen mittlerweile nicht nur Alter, Geschlecht, Ethnie und regionale Herkunft der betroffenen Person,[37] sondern auch Erkrankungen wie ADHS, Depressionen und Parkinson.[38] Überdies können sie aus unserer Stimme auf Charaktereigenschaften schliessen und beispielsweise auswerten, wie neugierig, verträglich, risikofreudig, ausgeglichen und organisiert wir sind.[39] Auch unsere Emotionen bleiben ihnen nicht verborgen.[40]

Die Möglichkeit, Rückschlüsse auf besonders schützenswerte Personendaten wie namentlich die Gesundheit und Ethnie einer Person zu ziehen, weist die Stimme dem Kreis der besonders schützenswerten Personendaten zu. Entsprechend beinhaltet die Erstellung des Stimmabdrucks eine Bearbeitung besonders schützenswerter Personendaten.

---

35 Verordnung (EU) 2015/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. L 119 vom 4.5.2016, S. 1-88, siehe Art. 9 Abs. 1 DSGVO.

36 Entwurf zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (BBl 2017, S. 7193-7276); siehe Art. 4 Bst. c Ziff. 4 E-DSG.

37 WELT vom 6. März 2019 («Audioprofiling, Diese Stimmanalyse entlarvt all unsere Geheimnisse»), abrufbar unter: <https://www.welt.de/wissenschaft/article138138577/Diese-Stimmanalyse-entlarvt-all-unsere-Geheimnisse.html>; Tagesanzeiger vom 5. März 2019 («Wie unsere Stimme alles über uns verrät») abrufbar unter: <https://www.tagesanzeiger.ch/digital/internet/wie-unsere-stimme-alles-ueber-uns-verraet/story/18087714>.

38 Siehe z.B. DIE ZEIT Nr. 33/2016 vom 4. August 2016 (« Stimme, Wie Krankheiten aus uns sprechen»), abrufbar unter: <https://www.zeit.de/2016/33/menschliche-stimme-lunge-sprache-krankheit-mund-kehlkopf>; WELT vom 6. März 2019 («Audioprofiling, Diese Stimmanalyse entlarvt all unsere Geheimnisse»), abrufbar unter: <https://www.welt.de/wissenschaft/article138138577/Diese-Stimmanalyse-entlarvt-all-unsere-Geheimnisse.html>.

39 WOLFANGEL, digma 2019, 28.

40 WOLFANGEL, digma 2019, 30.

3. Folgen für die Untersuchung

Mit Blick auf die vorangehenden Ausführungen kann man festhalten, dass die Anfertigung eines Stimmabdrucks eine Personendatenbearbeitung im Sinne des Datenschutzgesetzes darstellt, weshalb der Vorgang in den Anwendungsbereich des Datenschutzgesetzes fällt. Entsprechend sind die allgemeinen Voraussetzungen für die Bearbeitung von Personendaten zu beachten, namentlich darf die Bearbeitung die Persönlichkeit der betroffenen Person nicht verletzen (dazu sogleich). Weil sodann die Anfertigung eines Stimmabdrucks als Bearbeitung von besonders schützenswerten Personendaten qualifiziert, sind die zusätzlichen Voraussetzungen und Rahmenbedingungen zu beachten, welche das DSG für diese Kategorie von Personendaten vorsieht.

IV. Stimmabdruck als Persönlichkeitsverletzung?

Für jede Bearbeitung von Personendaten, also auch für solche, die nicht besonders schützenswert sind, enthält das DSG die Vorschrift, dass die Bearbeitung die Persönlichkeit der betroffenen Person nicht verletzen darf.

1. Persönlichkeitsverletzung nach DSG

Gemäss Art. 12 DSG darf, wer Personendaten bearbeitet, die Persönlichkeit der betroffenen Person nicht verletzen. Der Persönlichkeitsschutz des DSG stellt gemäss Botschaft 1988 eine «Ergänzung und Konkretisierung des Persönlichkeitsschutzes des Zivilgesetzbuches» dar und folgt «den Grundsätzen des Persönlichkeitsschutzes des Zivilgesetzbuches».[41] Wie schon im System des ZGB ist eine Persönlichkeitsverletzung widerrechtlich, wenn sie nicht aufgrund des Gesetzes, des überwiegenden öffentlichen oder private Interesses oder der Einwilligung der Verletzten gerechtfertigt ist (Art. 13 Abs. 1 DSG und Art. 28 Abs. 2 ZGB).

Sowohl Art. 12 als auch Art. 13 DSG enthalten zusätzliche Konkretisierungen. Art. 12 Abs. 2 DSG hält fest, was der Datenbearbeiter «namentlich» nicht tun darf: Er darf bestimmte Datenbearbeitungsgrundsätze[42] nicht verletzen (lit. a); er darf keine Daten entgegen dem ausdrücklichen Willen der betroffenen Person bearbeiten (lit. b); er darf nicht ohne Rechtfertigungsgrund beson-

41 Botschaft DSG, BBl 1988, 458.

42 Das Gesetz nennt Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG.

ders schützenswerte Personendaten oder Persönlichkeitsprofile Dritten bekannt geben (lit. c). Art. 13 Abs. 2 DSG hält fest, wann «insbesondere» ein überwiegendes privates Interesse infrage kommt – wobei die Beispiele nicht bindend sind.[43]

Weder die persönlichkeitsverletzende Datenbearbeitung noch der Rechtfertigungsgrund des überwiegenden Interesses sind in Art. 12 Abs. 2 und 13 Abs. 2 DSG abschliessend geregelt.[44] Das ist zwar unbestritten, wird aber dennoch zuweilen übersehen. Das liegt nicht zuletzt an der kleinteiligen Regelung des Datenschutzgesetzes, das aus so vielen Bäumen besteht, dass man oft den Wald nicht mehr sieht. Das gilt insbesondere für die Datenbearbeitungsgrundsätze (Art. 12 Abs. 2 lit. a DSG). Sie konkretisieren den Tatbestand der Persönlichkeitsverletzung (Art. 12 Abs. 1 DSG) im Hinblick auf gewisse Datenbearbeitungsszenarien. Darüberhinaus bleibt aber bei jeder Datenbearbeitung die Grundnorm in Art. 12 Abs. 1 DSG (und damit letztlich Art. 28 Abs. 1 ZGB) für die Frage eines Verletzungstatbestands massgeblich.[45]

2. Die Stimme als Teil der rechtlich geschützten Persönlichkeit

Es existieren verschiedene Definitionen der Persönlichkeit. Prägend sind die Definitionen von TERCIER und JÄGGI. TERCIER definiert die Persönlichkeit als «l'ensemble des biens inhérents à chaque personne, biens qui lui appartiennent de sa naissance à sa mort de par sa seule qualité de personne physique ou morale».[46] Nach JÄGGI ist die Persönlichkeit «der Einzelne als Geistwesen und in seiner Einmaligkeit, mit der Gesamtheit seiner Anlagen und Tätigkeiten in der ihm eigenen Ausprägung.»[47] Die verschiedenen Teilgehalte der Persönlichkeit lassen sich nicht abschliessend festlegen, sondern können und müssen – auch mit Rücksicht auf neue Eingriffsszenarien – laufend weiterentwickelt werden.[48]

Ein Gut, welches jeder (gesunden) natürlichen Person inhärent ist und von der Geburt bis zum Tode zu ihr gehört, ist ihre Stimme. Sie ist «der vitalste

43 HK DSG-ROSENTHAL, Art. 13 N 33.

44 HK DSG-ROSENTHAL, Art. 12 N 14 und Art. 13 N 33.

45 Herrschende Lehre. Statt vieler BSK-DSG-RAMPINI, Art. 12 N 7; HK DSG-ROSENTHAL, Art. 12 N 3.

46 TERCIER, personnalité, N 103.

47 JÄGGI, ZSR 79 II (1960), 146a.

48 BSK-ZBG-MEILI, Art. 28 N 5, m.w.H; AEBI-MÜLLER, Persönlichkeitsschutz, § 2 N 33.

Ausdruck zwischenmenschlicher Beziehungen.»[49] Sie ist bei jedem Menschen einzigartig und daher Teil seiner Persönlichkeit.[50] Lehre und Rechtsprechung zählen sie daher zum Schutzbereich von 28 ZGB (teilweise wird von einem Recht an der eigenen Stimme gesprochen).[51] Konkret handelt es sich dabei um einen Schutz vor Eingriffen Dritter, der verbietet, dass die Stimme einer Person ohne Rechtfertigungsgrund beschafft, weiterverbreitet oder verfälscht wird.[52] Vorausgesetzt ist, dass die betroffene Person individualisierbar ist, man also weiss, zu wem die Stimme gehört.[53]

3. Der Stimmabdruck als Persönlichkeitsverletzung

Fällt bereits die blosse Aufnahme einer individualisierbaren Stimme in den Schutzbereich der Persönlichkeit,[54] muss dies erst recht für die Analyse der individuellen Stimme der Kundin zwecks biometrischer Erkennung gelten.[55] Die Stimme ist dermassen eng und dauerhaft mit der betroffenen Person verbunden, dass eine Analyse derselben zwangsläufig in ihren höchstpersönlichen Bereich eingreift. Überdies wird mit dem Stimmabdruck ein neuer Identifikator für die betroffene Person geschaffen. Es steht weder Bundesorganen noch (viel weniger) Privaten zu, beliebig biometrische Merkmale von Personen zu vermessen und daraus Identifikatoren anzufertigen. Bereits aus diesen Gründen stellt der Stimmabdruck eine Persönlichkeitsverletzung dar.

---

49 LOBE, NZZ vom 27. April 2018 («Unsere Stimme sagt alles über uns – auch das, was wir gar nicht sagen wollen»), abrufbar unter: <https://www.nzz.ch/feuilleton/unsere-stimme-sagt-alles-ueber-uns-auch-das-was-wir-gar-nicht-sagen-wollen-ld.1380929>.

50 GEISER, Persönlichkeitsverletzung, 43; AEBI-MÜLLER, Persönlichkeitsschutz, § 2 N 44.

51 BGE 110 II 411 E. 3b S. 418 f.; BARRELET/WERLY, Communication, N 1513; BSK-ZGB-MEILI, Art. 28 N 22; BRÜCKNER, Personenrecht, N 632 f.; GEISER, Persönlichkeitsverletzung, 43 ff.; PEDRAZZINI/OBERHOLZER, Personenrecht, 136; TERCIER, personnalité, N 452 ff.; WEBER/UNTERNÄHRER/ZULAUF, Filmrecht, 159 f.

52 WEBER/UNTERNÄHRER/ZULAUF, Filmrecht, 159 f.; BSK-ZGB-MEILI, Art. 28 N 22, m.w.H; TERCIER, personnalité, N 457; restriktiver hingegen GEISER, Persönlichkeitsverletzung, 45.

53 BARRELET/WERLY, Communication, N 151.; BSK-ZGB-MEILI, Art. 28 N 22, m.w.H.; PEDRAZZINI/OBERHOLZER, Personenrecht, 136; TERCIER, personnalité, N 452 ff.; WEBER/UNTERNÄHRER/ZULAUF, Filmrecht, 159 f.

54 Siehe die Ausführungen im vorangehenden Absatz. Ausdrücklich für die Aufnahme eines Bildes einer Person BGE 138 II 346 E. 8.3 S. 360 (Google Street View).

55 Beim Stimmabdruck ist die Individualisierbarkeit der Stimme ohne Weiteres gegeben. Die Kundin ist der Bank bekannt, der Stimmabdruck ist ihr mit exakt dem Zweck zugeordnet, sie anlässlich eines nächsten Anrufs zu identifizieren. Diese Voraussetzung für eine Persönlichkeitsverletzung ist also mit dem Stimmabdruck ohne Weiteres erfüllt.

Die Verletzung ist zudem schwerwiegend. Denn mit der Stimmerkennung wird ein dauerhafter Identifikator für eine Person geschaffen – für das gesamte Leben, und genau genommen darüber hinaus. Die betroffene Person kann diesen Identitifikator nicht verändern und der Identifikator kann bei einem Abhandenkommen auch nicht einfach neu eingestellt werden, wie dies etwa bei einem Passwort der Fall ist. Selbst im Vergleich zu anderen biometrischen Erkennungsverfahren ist die Stimmbiometrie einzigartig: Wer über sie verfügt, kann die betroffene Person identifizieren, ohne dass der Identifikationsprozess für diese erkennbar ist. Bei einem Irisscan oder bei einem Fingerabdruck muss demgegenüber die betroffene Person im Rahmen eines Authentifizierungsverfahrens für den Abgleich noch einmal ihre Biometrie zur Verfügung stellen – sie muss sich vor einen Irisscanner stellen oder ihren Finger auf eine Scanstelle legen. Sie ist sich also bewusst, dass ein biometrisches Kontrollverfahren stattfindet und dass ihr Gegenüber über ihre diesbezüglichen Daten verfügt.[56]

Aus dem Gesagten folgt, dass die Erstellung des Stimmabdrucks eine Persönlichkeitsverletzung i.S.v. Art. 28 ZGB darstellt. Dies gilt auch auf der Ebene des Datenschutzgesetzes (Art. 12 Abs. 1 DSG), nachdem dieser Vorgang gleichzeitig eine Bearbeitung personenbezogener Daten der Kundin beinhaltet.

Ob darüberhinaus eine Persönlichkeitsverletzung vorliegt, weil mit der Stimmerkennung die Datenbearbeitungsgrundsätze in Art. 12 Abs. 2 lit. a DSG verletzt sind, muss nicht zusätzlich geprüft werden – Fragen würden hier insbesondere der Grundsatz der Verhältnismässigkeit und der Grundsatz von Treu und Glauben aufwerfen. Denn Art. 12 Abs. 2 lit. a DSG gilt nur in eine Richtung: Der Gesetzgeber hat mit dieser Norm in Konkretisierung

[56] Vorbehalten sind Überlistungsszenarien, die allerdings auf einer anderen Ebene liegen. Dort geht es darum, dass man das Sicherheitsdispositiv, das auf einen biometrischen Identifikator beruht, austrickst: Man überlistet den Irisscanner oder man überlistet das Fingerabdruck-Kontrollsystem oder man überlistet das Stimmabdruck-System, indem man den entsprechenden Identifikator ohne Zustimmung und Wissen der betroffenen Person nachkonstruiert und sich dann als die betreffende Person ausgibt. Dies ist ein weiteres Risikoszenario bei biometrischen Daten, die alle diese Daten aber gleichermassen betrifft.

von Art. 28 ZGB und Art. 12 Abs. 1 DSG die Fiktion einer Persönlichkeitsverletzung geschaffen.[57] Wer einzelne Datenbearbeitungsgrundsätze nicht einhält, verletzt *per se* das Persönlichkeitsrecht der betroffenen Person.[58] Mit dieser Fiktion wird die Anwendung des allgemeinen Persönlichkeitsschutzes im Kontext der Datenverarbeitung im Hinblick auf einzelne Konstellationen vereinfacht. Das Umgekehrte gilt aber nicht: Die Einhaltung sämtlicher Datenbearbeitungsgrundsätze bedeutet nicht, dass *keine* Persönlichkeitsverletzung vorliegt.[59] Wie bereits erwähnt, kann eine Persönlichkeitsverletzung sogar dann vorliegen, wenn gar keiner der Tatbestände in Art. 12 Abs. 2 Bst. a-c DSG erfüllt ist.

4. Die Weitergabe des Stimmabdrucks als Persönlichkeitsverletzung

Art. 12 Abs. 2 lit. c DSG enthält eine Konkretisierung der persönlichkeitsverletzenden Datenbearbeitung: Die Weitergabe von besonders schützenswerten Personendaten erfüllt ohne Weiteres den Verletzungstatbestand gemäss Art. 12 DSG. Im Fall der Banken steht diese Konstellation allerdings nicht im Vordergrund, weil es zunächst einmal nur um die Frage geht, ob Banken und andere Dienstleister den Stimmabdruck selbst erstellen und nutzen dürfen.

V. Rechtfertigungsgründe nach DSG im Überblick

Gemäss Art. 13 Abs. 1 DSG ist eine Persönlichkeitsverletzung widerrechtlich, wenn sie nicht durch die Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist (vgl. Art. 13 Abs. 1 DSG).

Eine gesetzliche Grundlage ist für die Erstellung des Stimmabdrucks nicht ersichtlich. Gemäss Art. 179quinquies StGB ist zwar die Stimmaufnahme nicht strafbar, wenn die aufgenommenen Gespräche «Bestellungen, Aufträge, Reservationen und ähnliche Geschäftsvorfälle zum Inhalt haben». In solchen Fällen besteht auch ein zivilrechtlicher Rechtfertigungsgrund.[60] Erstens ist zweifelhaft, ob die Hotline eines Finanzdienstleisters überhaupt unter diesen

---

57 Botschaft DSG, BBl 1988, 458; BSK-DSG-RAMPINI, Art. 12 N 1, 6; HK DSG-ROSENTHAL, Art. 12 N 14.

58 Vgl. BSK-DSG-RAMPINI, Art. 12 N 6; HK DSG-ROSENTHAL, Art. 12 N 14.

59 Vgl. BSK-DSG-RAMPINI, Art. 12 N 7.

60 Vgl. EDÖB, Aufzeichnung von Telefongesprächen.

Tatbestand fällt.[61] Zweitens erstreckt sich der Rechtfertigungsgrund mit Sicherheit nicht auf die Erstellung eines Stimmabdrucks.

Öffentliche Interessen spielen bei privaten Datenbearbeitern als Rechtfertigungsgrund eine untergeordnete Rolle.[62] Sie lassen sich aufgrund ihrer zeitlichen und örtlichen Wandelbarkeit nicht abschliessend definieren.[63] Die wichtigsten Gruppen sind die polizeilichen Interessen wie z.B. die öffentliche Ordnung und Sicherheit oder Treu und Glauben im Geschäftsverkehr, planerische Interessen (z.B. Raumplanung), soziale und sozialpolitische Interessen (z.B. Arbeitnehmerschutz), und rechtsstaatliche Interessen.[64] Im Bereich des Persönlichkeitsschutzes ist insbesondere das Informationsinteresse der Öffentlichkeit an Personen des öffentlichen Lebens von Bedeutung.[65] Vorliegend ist kein öffentliches Interesse der Banken an der Verwendung von Stimmabdrücken zwecks Authentifikation ihrer Kundinnen und Kunden ersichtlich.

Näher zu prüfen ist hingegen der Rechtfertigungsgrund der Einwilligung, denn immerhin kann die Kundin anlässlich des ersten Anrufs bei der Hotline erklären, dass sie die Anfertigung eines Stimmabdrucks nicht wünscht.[66] Auch der Rechtfertigungsgrund eines überwiegenden privaten Interesses seitens der Banken bedarf einer genaueren Betrachtung, ist doch das Vorliegen eines Interesses offenkundig, was allerdings noch nicht bedeutet, dass dieses Interesse überwiegt.

VI. Rechtfertigung durch Einwilligung?

Die Anforderungen an die Einwilligung sind in Art. 4 Abs. 5 DSG festgehalten. Danach ist die Einwilligung nur gültig, wenn sie nach angemessener Information freiwillig erfolgt. Bei der Bearbeitung besonders schützenswerter Personendaten muss die Einwilligung zudem ausdrücklich erfolgen.

---

61 Wie der EDÖB unter Hinweis auf die parlamentarischen Beratungen richtig festhält, geht es um Bestell- bzw. Reservationsanrufe (z.B. in der Tourismusbranche) und nicht um Gespräche, die Reklamationen oder Vertragsverhandlungen zum Inhalt haben.

62 HK DSG-ROSENTHAL, Art. 13 N 20.

63 HÄFELIN/MÜLLER/UHLMANN, Verwaltungsrecht, § 7 N 465.

64 HÄFELIN/MÜLLER/UHLMANN, Verwaltungsrecht, § 7 N 471 ff.; BVerG A-7040/2009 vom 30. März 2011, E. 10.4.2 (Google Street View).

65 HK DSG-ROSENTHAL, Art. 13 N 22.

66 Siehe vorne III. (Eingangsparagraph).

1. Angemessene Information

a) Anforderungen

Angemessen informiert ist die betroffene Person dann, wenn sie über alle notwendigen Informationen verfügt, um die Tragweite der Einwilligung in die konkrete Datenbearbeitung zu erkennen,[67] oder kurz: «wenn die Eingriffe in die Persönlichkeitsrechte transparent werden».[68] Der betroffenen Person müssen mindestens die Datenbearbeiter, Art, Zweck und Umfang der Bearbeitung sowie gegebenenfalls deren Risiken bekanntgegeben werden.[69] Auch die Folgen einer Verweigerung der Einwilligung sind der betroffenen Person mitzuteilen.[70]

Diese Informationen müssen ihr in leicht verständlicher Art und Weise präsentiert werden.[71] Aus dem klaren Wortlaut («*nach* angemessener Information») ergibt sich, dass die Information *vor* der Erteilung der Einwilligung zu erfolgen hat.[72] Nicht erforderlich ist eine Information über Risiken, die allgemein bekannt sind oder die für die betroffene Person auch ohne Information erkennbar sind.[73] Sowohl der notwendige Umfang als auch die Form der Information richten sich nach den Umständen des Einzelfalls.[74]

b) Angemessene Information durch telefonische Ansage?

Orientiert man sich wiederum am medial verbreiteten Beispiel der PostFinance, so informiert diese ihre Kundinnen und Kunden einerseits mittels folgender telefonischer Ansage:

> «Dieses Gespräch wird zu Sicherheits- und Wiedererkennungszwecken aufgezeichnet. PostFinance erstellt aus der Aufnahme einen Stimmabdruck, um

---

67 BVerG A-3908/2008 vom 4. August 2009, E. 4.2; EPINEY, in: Belser/Epiney/Waldmann, § 9 N 17; HK DSG-ROSENTHAL, Art. 4 N 72.

68 SHK-BAERISWYL, Art. 4 N 59.

69 EPINEY, in: Belser/Epiney/Waldmann, § 9 N 17; ebenso BSK-DSG-MAURER-LAMBROU/STEINER, Art. 4 N 16f. BAERISWYL verlangt zusätzlich noch die Angabe der Kategorien der bearbeiteten Daten, SHK-BAERISWYL, Art. 4 N 59.

70 BSK-DSG-MAURER-LAMBROU/STEINER, Art. 4 N 16f.

71 EPINEY, in: Belser/Epiney/Waldmann, § 9 N 17; BSK-DSG-MAURER-LAMBROU/STEINER, Art. 4 N 16f.

72 So zu Recht auch HK DSG-ROSENTHAL, Art. 4 N 72; einschränkend WERMELINGER/SCHWERI, Jusletter 3.3.2008, Rz. 12.

73 HK DSG-ROSENTHAL, Art. 4 N 74.

74 EPINEY, in: Belser/Epiney/Waldmann, § 9 N 17.

> Ihre Identität bei jeden [recte: jedem] Anruf anhand Ihrer Stimme zu verifizieren. Wünschen Sie keinen Stimmabdruck, bitten wir Sie, dies dem Kundenbetreuer mitzuteilen.»

Die Ansage enthält Informationen über die Datenbearbeiterin (PostFinance), die Bearbeitungszwecke (Sicherheit, Wiedererkennung bei künftigen Anrufen), die Art der Datenbearbeitungen (Aufnahme des Gesprächs, Erstellung eines Stimmabdrucks und seine spätere Verwendung zwecks Verifikation) sowie eine Belehrung der Kundin über ihr Widerspruchsrecht.

Allerdings ist nicht davon auszugehen, dass die Durchschnittskundin aufgrund dieser Ansage die effektive Tragweite der geplanten Datenbearbeitung wirklich erfasst. Insbesondere kann nicht unterstellt werden, eine Durchschnittskundin wisse ohne Weiteres, was mit einem Stimmabdruck gemeint ist (nämlich die Festlegung eines unabänderlichen Identifkators), und dass sie Fremdwörter wie «Identität» und «verifizieren» versteht.

Die telefonische Information ist somit für sich alleine nicht als angemessen zu betrachten. Entsprechend kann gestützt darauf keine gültige Einwilligung erteilt werden.

c) Angemessene Information durch Website?

Die telefonische Ansage bei einer Hotline kann durch weiterführende Informationen auf der Website des Dienstleisters komplementiert werden.

Auf der Website der PostFinance[75] wird der Kundin beispielsweise erklärt, dass aus den verschiedenen Merkmalen ihrer Stimme wie Sprechtempo, Lautstärke und Frequenz ein Stimmabdruck erstellt werde, der in Form eines Codewerts ohne Gesprächsinhalt auf den Servern der PostFinance in der Schweiz gespeichert werde. Diesen Stimmabdruck benutze die PostFinance, um festzustellen, «ob die Person, die anruft, tatsächlich diejenige ist, als die sie sich ausgibt». Auch zu gewissen mit der Stimmerkennung verbundenen Herausforderungen (z.B. Heiserkeit der Kundin, ähnliche Stimme einer Verwandten) nimmt die PostFinance in verständlicher Art und Weise Stellung.[76]

Fraglich ist, ob diese zusätzlichen Informationen dazu führen, dass von einer gültigen Einwilligung ausgegangen werden kann. Das ist aus zwei Gründen zu verneinen. Erstens ist nicht sichergestellt – es ist sogar unwahr-

---

[75] Siehe unter <www.postfinance.ch/de/privat/support/persoenliche-daten/authentifizierung-stimmerkennung.html>.

[76] Zum Ganzen <www.postfinance.ch/de/privat/support/persoenliche-daten/authentifizierung-stimmerkennung.html>.

scheinlich –, dass die Kundin das Telefongespräch in Kenntnis der Informationen auf der Website vornimmt. Insofern fällt die zusätzliche Information für die Frage der rechtsgültigen Einwilligung ausser Betracht. Doch selbst wenn man die Webinformationen dem Telefongespräch ausnahmsweise «zurechnen» könnte, so würde sie – zweitens – nicht genügen, weil sie in ungenügendem Mass auf die Risiken hinweist, die mit einem solchen Vorgang verbunden sind. Die Verbindung zwischen einer Person und ihrer Stimme ist hochsensibel. Wird auf irgendeine Art und Weise bekannt, dass ein Stimmabdruck zu einer bestimmten Person gehört, so kann diese Person künftig überall allein durch ihre Stimme identifiziert werden.[77] Eine angemessene Information der Kundin würde daher voraussetzen, dass sie über dieses Risiko aufgeklärt wird und dass die Massnahmen geschildert werden, mit denen die PostFinance dieses Risiko zu verhindern sucht. Ansonsten kann die Kundin die Tragweite ihrer Entscheidung nicht überblicken. Entsprechend liegt auch in diesem Fall keine rechtsgenügende Einwilligung vor.

d) Fazit: Keine angemessene Information

Die telefonische Ansage stellt für sich alleine keine angemessene Information i.S.v. Art. 4 Abs. 5 DSG dar. Selbst wenn darin auf die weiterführenden Informationen auf der Website verwiesen würde, wäre die Information nicht angemessen, da keine genügende Risikoaufklärung stattfindet. Die fehlende Risikoaufklärung führt im Übrigen dazu, dass auch die Zustimmung zum Stimmabdruck, welche die Kundin im Online-Banking-Portal vornimmt, die Voraussetzungen für eine rechtsgültige Einwilligung nach DSG nicht erfüllt.

2. Freiwilligkeit

Die Freiwilligkeit der Einwilligung ist vorliegend relativ unproblematisch, da die Kundin die Möglichkeit hat, der Erstellung eines Stimmabdrucks zu widersprechen und stattdessen anhand von Sicherheitsfragen authentifiziert zu werden. Zu bedenken ist aber, dass sich die Kundinnen und Kunden, die bei einer Hotline, gerade der Hotline einer Bank, anrufen, häufig in einer Drucksituation befinden dürften – beispielsweise, weil ihnen das Portemonnaie abhandengekommen ist und sie ihre Kreditkarte so schnell wie möglich sperren lassen möchten. Ob sie in einer solchen Situation noch die Vor- und Nachteile

[77] Forbes 6. Oktober 2016 («Voice Recognition: Risks To Our Privacy»), abrufbar unter: <https://www.forbes.com/sites/realspin/2016/10/06/voice-recognition-every-single-day-every-word-you-say/>.

der Stimmerkennung abwägen und eine freiwillige Entscheidung treffen können, darf bezweifelt werden.

3. Ausdrücklichkeit (besonders schützenswerte Personendaten)

Wie erläutert,[78] werden bei der Erstellung des Stimmabdrucks besonders schützenswerte Personendaten bearbeitet, weshalb die Einwilligung nicht nur informiert und freiwillig, sondern darüberhinaus ausdrücklich erfolgen muss. Eine ausdrückliche Zustimmung bei Stimmerkennungsverfahren verlangt auch der EDÖB.[79] Der Begriff «ausdrücklich» ist dabei wie im Vertragsrecht gleichbedeutend mit «nicht konkludent».[80]

Wenn nun die Kundin nach Anhörung der elektronischen Ansage das Telefonat nicht beendet, sondern direkt ihr Anliegen an den Kundenberater heranträgt, willigt sie nicht ausdrücklich ein. Eine andere Situation bestünde, wenn der Kundenberater nochmals nachfragen und die Kundin erklären würde, dass sie mit dem Stimmabdruck einverstanden sei. Dann wäre die Einwilligung ausdrücklich. Allerdings wäre sie trotzdem ungültig, da die Kundin nicht angemessen informiert wurde.

4. Fazit: Keine Rechtfertigung durch Einwilligung

Bei der hier untersuchten Ausgestaltung des Zustimmungsverfahrens für die Anfertigung eines Stimmabdrucks fehlt es an der rechtsgültigen Einwilligung: Weder die telefonische noch die webbasierte Information ist von ihrem Inhalt her genügend verständlich und genügend detailliert, um die Voraussetzung einer angemessenen Information zu erfüllen. Selbst wenn man also

78 Siehe oben III.2.

79 EDÖB, Erläuterungen zu Stimmerkennungsverfahren, passim. In den Erläuterungen wird das Stimmerkennungsverfahren nicht ausdrücklich als Bearbeitung besonders schützenswerter Daten qualifiziert, diese Qualifikation ergibt sich aber aus dem geforderten Zustimmungsmodus der Ausdrücklichkeit. Richtig ist allerdings, dass nicht *jede* Bearbeitung besonders schützenswerter Personendaten eine Persönlichkeitsverletzung beeinhaltet und deshalb einer Rechtfertigung bedarf (so auch VASELLA, Stimmerkennung). Das ändert allerdings nichts daran, dass – spezifisch – die Erstellung eines Stimmabdrucks eine Persönlichkeitsverletzung ist, die ohne Rechtfertigungsgrund widerrechtlich ist.

80 Zutreffend und mit Erläuterung der verschiedenen Auslegungen der Lehre VASELLA, Jusletter 16.11.2015, Rz. 21 ff.

annehmen würde, dass es – mangels Bearbeitung von besonders schützenswerten Personendaten – keiner ausdrücklichen Zustimmung bedarf, wären die Voraussetzungen für eine rechtsgültige Einwilligung nicht erfüllt.

Allerdings wird hier vertreten, dass der Stimmabdruck als Bearbeitung von besonders schützenswerten Personendaten zu qualifizieren ist, weshalb die Einwilligung ausdrücklich zu erfolgen hat. Auch dieses weitergehende Erfordernis ist nicht erfüllt, denn die Kundin muss beim aktuellen Verfahren ausdrücklich erklären, dass sie *keinen* Stimmabdruck wünscht. Eine ausdrückliche Einwilligung beinhaltet dieser Vorgang jedenfalls nicht. Im Übrigen ist fraglich, wie die Nichtausübung der Widerspruchsmöglichkeit zu qualifizieren ist: Bei Lichte betrachtet handelt es sich um eine Vertragsänderung, die für ihre Gültigkeit der Zustimmung bedarf. Schweigen gilt im Vertragsrecht nicht als Zustimmung (vgl. Art. 6 OR).

VII. Rechtfertigung durch überwiegende private Interessen?

Falls kein Gesetz, kein überwiegendes öffentliches Interesse und keine gültige Einwilligung für den Stimmabdruck besteht, so bleibt noch zu untersuchen, ob dieser durch das überwiegende private Interesse des Bearbeiters gerechtfertigt ist. Art. 13 Abs. 2 DSG enthält eine nicht abschliessende Auflistung von Situationen, in denen ein überwiegendes privates Interesse «in Betracht» fällt. Diese Formulierung verdeutlicht, dass in den aufgezählten Fällen kein Automatismus greift, sondern stets noch eine Interessenabwägung durchgeführt werden muss, den Beispielen mithin nicht der Rang gesetzlicher Vermutungen zukommt.[81] Sie bilden aber nach der Botschaft «Gewichtssteine» für die Interessenabwägung durch das Gericht.[82] Als mögliche Interessen fallen nicht nur Interessen des Datenbearbeiters, sondern auch Interessen Dritter, insbesondere der betroffenen Person selbst, in Betracht.[83]

1. Mögliche Interessen

Vorliegend ist von den genannten Beispielen nur die Abwicklung eines Vertrages i.S.v. Art. 13 Abs. 2 Bst. a DSG einschlägig, wonach ein überwiegendes

---

81 HK DSG-ROSENTHAL, Art. 13 N 33; BSK-DSG-RAMPINI, Art. 13 N 26.

82 Botschaft DSG, BBl. 1988, 460.

83 BGE 138 II 346 E. 10.3 S. 364 f. (Google Street View).

Interesse namentlich dann in Betracht fällt, wenn in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags Personendaten des Vertragspartners bearbeitet werden. Die Norm adressiert den Datenbearbeitungsbedarf, der mit einer Vertragsbeziehung einhergeht, und schafft den notwendigen Spielraum für deren Errichtung und sachgerechte Durchführung. Die Stimmauthentifizierung steht im Zusammenhang mit der Nebenpflicht der Banken, eine Kunden-Hotline zu betreiben und die Kundinnen und Kunden im Falle eines Anrufs zuverlässig zu authentifizieren. Diese Nebenpflicht ist vorliegend zu berücksichtigen.

Aber: Ein Spielraum ist kein Freipass. Auch innerhalb eines Vertragsverhältnisses ist die Persönlichkeit der Gegenpartei zu wahren. Art. 13 Abs. 2 Bst. a DSG vermag mit anderen Worten nicht unbesehen jede Persönlichkeitsverletzung zu rechtfertigen, sondern erfordert eine Interessenabwägung im Einzelfall.[84] Da hier mildere Mittel für die Authentifizierung der Kundinnen und Kunden möglich sind (Stichwort: Sicherheitsfragen), dürfte das Interesse der Bank an der Erfüllung ihrer Nebenpflicht für sich alleine nicht ausschlaggebend sein.

Zu prüfen ist daher, welche Interessen die Banken daran haben, diese Nebenpflicht *spezifisch mittels Stimmerkennung* zu erfüllen. Medienberichten zufolge sind dies einerseits das Interesse an einer schnelleren Authentifikation der Kundinnen und Kunden und andererseits das Interesse an einer sichereren Verifizierung und insbesondere der Verhinderung von Identitätsdiebstahl.[85]

2. Effiziente Kundenauthentifizierung

Als berechtigte Interessen i.S.v. Art. 13 DSG kommen auch rein wirtschaftliche Interessen infrage, wie z.B. das Interesse an einer effizienten Gestaltung der Datenbearbeitung.[86] Das Interesse, die Kundenauthentifizierung möglichst zeit- und ressourcensparend zu gestalten ist daher ein berechtigtes Interesse.

Das Stimmerkennungsverfahren hat gegenüber den Sicherheitsfragen den Vorteil der Zeitersparnis. Textgebundene Stimmerkennungsverfahren ver-

---

84 Allgemein zur Notwendigkeit einer Interessenabwägung bei den Rechtfertigungsgründen nach Art. 13 Abs. 2 DSG siehe HK DSG-ROSENTHAL, Art. 13 N 6.

85 Inside-IT vom 18. Dezember 2018 («PostFinance setzt auf Stimmerkennung zur Authentifizierung»), abrufbar unter: <www.inside-it.ch/articles/53194>.

86 BGE 138 II 346 E. 10.3 S. 364 f. (Google Street View).

langen nur das Sprechen eines vorgegebenen Textes und nicht die Beantwortung mehrerer Fragen, textungebundene Verfahren laufen gar im Hintergrund des Kundengesprächs ab. Sie nehmen daher weniger Zeit für die Authentifikation der Kundin in Anspruch und das Gespräch kann sich stärker auf das konkrete Anliegen der Kundin konzentrieren. Überdies dauern die Kundengespräche generell weniger lange, was einerseits die Ressourcen der Bank schont und andererseits die Nerven der übrigen Kundinnen und Kunden, die weniger lange in Warteschlaufen verbringen müssen.

Beim Interesse an einer effizienten Kundenauthentifizierung handelt es sich somit nicht nur um ein Interesse der Bank, sondern auch um ein Interesse der Kundin selbst sowie der übrigen Kundinnen und Kunden.

3. Sicherere Kundenauthentifizierung

Ein weiteres Interesse liegt in der sicheren Kundenauthentifizierung. Auch dieses erfüllt die Voraussetzung eines Interesses «von allgemein anerkanntem Wert»[87] und kann daher in der Interessenabwägung berücksichtigt werden. Die sichere Kundenauthentifizierung liegt gleichzeitig im Interesse der Kundin selbst.

4. Interessenabwägung

Dass die Banken schützenswerte (wirtschaftliche und sicherheitsrelevante) Interessen an der Erstellung von Stimmabdrucken geltend machen können, bedeutet noch nicht, dass diese Interessen die Persönlichkeitsverletzung der Kundin rechtfertigen. Eine Rechtfertigung liegt nur vor, wenn man die Interessen zugunsten der Stimmauthentifizierung höher gewichtet als die Interessen der Kundin am Schutz ihrer Persönlichkeit.

a) Effiziente Kundenauthentifizierung

Anhaltspunkte für diese Interessenabwägung liefert insbesondere die bundesgerichtliche Rechtsprechung. Zwar anerkennt das Bundesgericht die grundsätzliche Eignung des wirtschaftlichen Interesses als Rechtfertigungsgrund, sie lässt dieses Interesse im Regelfall aber nicht genügen.[88] Vor diesem

---

87 BUCHER, Natürliche Personen, N 518.

88 Siehe dazu BGE 138 II 346 E. 10.4, 10.6.1, 10.6.3, S. 365 f., 367, 369 (Google Street View). So auch BSK ZGB-MEILI, Art. 28 N 49, unter Hinweis auf den soeben erwähnten BGE 138 II 346.

Hintergrund fallen die reinen Effizienzinteressen der Banken an einer Authentifizierung mittels Stimmerkennung als Rechtfertigungsgrund ausser Betracht. Das gilt umso mehr, als der Verzicht auf diese Authentifizierungsmethode für die Banken keine schwerwiegenden oder gar existenzbedrohenden Folgen hätte; die Institute verfügten bislang über Alternativen und können diese Alternativen auch für die Zukunft beibehalten und um neue Modelle ergänzen. Im konkreten Abwägungsprozess kommt dem wirtschaftlichen Interesse der Banken also von vornherein kein massgebliches Gewicht zu. Betrachtet man auf der anderen Seite den massiven Eingriff in die Persönlichkeit, der mit einem Stimmabdruck verbunden ist, führt die Interessenabwägung eindeutig dazu, dass der Persönlichkeitsschutz höher zu gewichten ist als das wirtschaftliche Interesse der Banken.

b) Sichere Kundenauthentifizierung

Für die Gesamtabwägung bleiben damit die Sicherheitsaspekte auf der einen Seite und der Persönlichkeitsschutz auf der anderen Seite. Auch hier sind die Sicherheitsinteressen in einem ersten Schritt auf das Gewicht hin zu überprüfen, das ihnen im Abwägungsprozess überhaupt zukommen soll. Hierzu ist festzuhalten, dass Stimmerkennungsverfahren zwar als zuverlässig gelten, sie aber keine vollständige Sicherheit gewähren. Ähnlich klingende Verwandte werden nicht immer herausgefiltert,[89] Systeme wurden in der Vergangenheit mehrfach überlistet.[90] Auch hier bestehen zudem Alternativen, die einen vergleichbaren Sicherheitsstandard bieten, ohne dass eine Persönlichkeitsverletzung in Kauf genommen werden muss, etwa die Ergänzung der Sicherheitsfragen um einen weiteren Überprüfungsfaktor.[91] Mithin besteht

---

89 Siehe dazu BLONSKI, Biometrische Daten, 19. Erst 2017 gelangte das Stimmerkennungssystem der HSBC in die Schlagzeilen, weil es einen BBC-Reporter fälschlicherweise als dessen Bruder authentifizierte. Siehe BBC News 19. Mai 2017 («BBC fools HSBC voice recognition security system»), abrufbar unter: <www.bbc.com/news/technology-39965545>. Die PostFinance äussert sich zu diesem Risiko auf ihrer Website nur ausweichend: <www.postfinance.ch/de/privat/support/persoenliche-daten/authentifizierung-stimmerkennung.html>.

90 So gelang es zwei Sicherheitsforschern, durch Machine Learning synthetische Stimmen zu erzeugen und damit Apples Siri sowie Microsofts Cloud-Dienst Azure Speaker Recognition zu täuschen. Siehe dazu Heise vom 13. August 2019 («Die eigene Stimme als Passwort? Besser nicht ...») abrufbar unter: <https://www.heise.de/newsticker/meldung/Die-eigene-Stimme-als-Passwort-Besser-nicht-4134163.html?view=print>.

91 Z.B. via Mobile-App (wo allfällige biometrische Erkennungsmerkmale lediglich dezentral gespeichert sind), oder mittels Abfragen eines Zugangscodes, der vom Kartenlesegerät generiert wird.

ein schützenswertes, aber kein ausserordentlich schwerwiegendes Sicherheitsinteresse an der Verwendung eines Stimmabdrucks zu Identifizierungszwecken.

Dem Interesse an einer sicheren Authentifizierung stehen der Schutz der Persönlichkeit vor tiefgreifenden und intensiven Eingriffen gegenüber. Wie bereits ausgeführt wurde, stellt ein Stimmabdruck einen massiven Eingriff in die Persönlichkeit der betroffenen Person dar.[92] Die Stimme ist einzigartig und sie ist untrennbar mit der Person verbunden. Mit der Stimmerkennung wird (bis zu einer allfälligen Löschung) ein ewiger, unveränderbarer Identifikator für eine Person geschaffen. Dieser Identifikator hebt sich von den anderen biometrischen Erkennungsmerkmalen zusätzlich ab, indem die betroffene Person ohne weiteres Zutun (also ohne nochmalige Zurverfügungstellung ihrer biometrischen Daten) identifiziert werden kann. Das macht die Verwendung der Stimmbiometrie sehr einfach, aber gleichzeitig im Hinblick auf die eigene Datenherrschaft sehr riskant.

Im Ergebnis ist die Anfertigung eines Stimmabdrucks ein massiver Eingriff in die Persönlichkeit der betroffenen Person, der in keinem Verhältnis zu den Sicherheitsinteressen der Banken beim Authentifizierungsprozess steht. Insgesamt können sich Banken weder auf ihre wirtschaftlichen noch auf ihre sicherheitsbezogenen Interessen berufen, um die persönlichkeitsverletzenden Anfertigung eines Stimmabdrucks zu rechtfertigen.

VIII. Fazit

«Sprich nur ein Wort, und ich sage Dir, wer Du bist.» Mit der Stimmauthentifizierung greifen die PostFinance und andere Banken, die ein solches Verfahren verwenden, in die höchstpersönliche Sphäre ihrer Kundinnen und Kunden ein. Sie schaffen sich aufgrund der bei jedem Menschen einzigartigen und unveränderbaren Stimme einen privaten Identifikator der jeweiligen Kundin oder des jeweiligen Kunden. Dies stellt eine Persönlichkeitsverletzung im Sinne von Art. 12 Abs. 1 DSG dar.

Diese Persönlichkeitsverletzung ist dann nicht widerrechtlich, wenn sie durch das Gesetz, ein überwiegendes öffentliches oder privates Interesse oder durch die Einwilligung seitens der verletzten Person gerechtfertigt ist. Näher in Betracht kommen nur der Rechtfertigungsgrund der Einwilligung und der

[92] Siehe zu diesen Argumenten oben V.3.

Rechtfertigungsgrund des überwiegenden privaten Interesses. Beim hier untersuchten Modellverfahren scheitert die gültige Einwilligung bereits daran, dass an der angemessenen Information fehlt, die Kundin also nicht *informiert* einwilligt. Dass zusätzlich keine ausdrückliche Einwilligung erfolgt, bestätigt nur das bereits gefundene Ergebnis. Ob man also, wie es der EDÖB vertritt, den Stimmabdruck als Bearbeitung besonders schützenswerter Personendaten einstuft, ist für das Ergebnis der fehlenden rechtsgültigen Einwilligung nicht ausschlaggebend. Dennoch verdient die Auffassung des EDÖB Zustimmung: Die Erstellung eines Stimmabdrucks beinhaltet die Bearbeitung besonders schützenswerter Personendaten, weshalb es einer ausdrücklichen Zustimmung bedarf.

Schliesslich vermögen auch die unstreitig vorhandenen Sicherheits- und Effizienzinteressen seitens der Bank die Persönlichkeitsverletzung nicht zu rechtfertigen. In der Interessenabwägung stellen sie angesichts des massiven Eingriffs in den Schutzbereich der Persönlichkeit, den ein Stimmabdruck beinhaltet, kein überwiegendes Interesse dar.

Im Ergebnis wird also mit den bestehenden Modellen der Stimmerkennung das Persönlichkeitsrecht der Kundinnen und Kunden verletzt, womit gleichzeitig gesagt ist, dass auch eine Verletzung des Datenschutzgesetzes vorliegt.

Literaturverzeichnis

Stand sämtlicher Internet-Referenzen in diesem Beitrag ist der 19. Juni 2019.

AEBI-MÜLLER REGINA E., Personenbezogene Informationen im System des zivilrechtlichen Persönlichkeitsschutzes, Unter besonderer Berücksichtigung der Rechtslage in der Schweiz und in Deutschland, Abhandlungen zum schweizerischen Recht, Heft 710, Bern 2005.

BAERISWYL BRUNO/PÄRLI KURT, Datenschutzgesetz (DSG), Stämpflis Handkommentar, Bern 2015 (zit. SHK-BEARBEITER).

BARRELET DENIS/WERLY STÉPHANE, Droit de la communication, 2. Auflage, Bern 2011.

BELSER EVA MARIA/EPINEY ASTRID/WALDMANN BERNHARD, Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011.

BLECHTA GABOR P. Art. 3 DSG, in: Urs Maurer-Lambrou / Gabor P. Blechta (Hrsg.), Basler Kommentar Datenschutzgesetz Öffentlichkeitsgesetz, 3. Auflage, Basel 2014.

BLONSKI DOMINIKA, Biometrische Daten als Gegenstand des informationellen Selbstbestimmungsrechts, ASR – Abhandlungen zum Schweizerischen Recht, Band/Nr. 816, Bern 2015.

BRÜCKNER CHRISTIAN, Das Personenrecht des ZGB (ohne Beurkundung des Personenstandes), Zürich 2000.

BUCHER ANDREAS, Natürliche Personen und Persönlichkeitsschutz, 4. Auflage, Basel 2009.

GEISER THOMAS, Die Persönlichkeitsverletzung insbesondere durch Kunstwerke, Basler Studien zur Rechtswissenschaft, Reihe A: Privatrecht, Band 21, Basel und Frankfurt am Main 1990.

GEISER THOMAS/FOUNTOULAKIS CHRISTIANA (HRSG.), Basler Kommentar Zivilgesetzbuch I, Art. 1-456, 6. Auflage, Basel 2018.

HÄFELIN ULRICH/MÜLLER GEORG/UHLMANN FELIX, Allgemeines Verwaltungsrecht, 7. Auflage, Zürich/St. Gallen 2016.

JÄGGI PETER, Fragen des privatrechtlichen Schutzes der Persönlichkeit, ZSR 1960 II, S. 133a-261a.

MAURER-LAMBROU URS/BLECHTA GABOR P. (HRSG.), Basler Kommentar Datenschutzgesetz Öffentlichkeitsgesetz, 3. Auflage, Basel 2014 (zit. BSK-DSG-BEARBEITER, Art. […] N. […]).

MAURER-LAMBROU URS/STEINER ANDREA, Art. 4 DSG; in: Urs Maurer-Lambrou/Gabor P. Blechta (Hrsg.), Basler Kommentar Datenschutzgesetz Öffentlichkeitsgesetz, 3. Auflage, Basel 2014.

MEILI ANDREAS, Art. 28 ZGB, in: Thomas Geiser/Christiana Fountoulakis (Hrsg.), Basler Kommentar Zivilgesetzbuch I, Art. 1-456, 6. Auflage, Basel 2018.

PEDRAZZINI MARIO M./OBERHOLZER NIKLAUS, Grundriss des Personenrechts, 4. Auflage, Bern 1993.

RAMPINI CORRADO, Art. 13 DSG, in: Urs Maurerl-Lambrou/Gabor P. Blechta (Hrsg.), Basler Kommentar Datenschutzgesetz Öffentlichkeitsgesetz, 3. Auflage, Basel 2014.

ROSENTHAL DAVID/JÖHRI YVONNE, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich/Basel/Genf 2008 (zit. HK-BEARBEITER, Art. […] N. […]).

SCHALLER JEAN MARC, Legitimationsmängel, in: Susan Emmenegger (Hrsg.), Bankvertragsrecht, Basel 2017, S. 45–70.

SPRECHER FRANZISKA, Datenschutz und Big Data im Allgemeinen und im Gesundheitsrecht im Besonderen, ZBJV 154/2018, 482-519.

TERCIER PIERRE, Le nouveau droit de la personnalité, Zürich 1984.

TILLENBURG GEREON, Stimmt die Stimme? Biometrielösungen im Einsatz, DuD 3/2011, S. 197-199.

VASELLA DAVID, Der EDÖB in «10vor10» zur Stimmerkennung bei PostFinance, 20. Mai 2019, abrufbar unter: < https://datenrecht.ch/der-edoeb-in-10vor10-zur-stimmerkennung-bei-postfinance/>.

– Zur Freiwilligkeit und zur Ausdrücklichkeit der Einwilligung im Datenschutzrecht, in: Jusletter 16. November 2015.

WEBER ROLF H./UNTERNÄHRER ROLAND/ZULAUF RENA, Schweizerisches Filmrecht, ZIK - Publikationen aus dem Zentrum für Informations- und Kommunikationsrecht der Universität Zürich, Band/Nr. 25, Zürich/Basel/Genf 2003.

WERMELINGER AMÉDÉO/SCHWERI DANIEL, Teilrevision des Eidgenössischen Datenschutzrechts – Es nützt nicht viel, schadet es etwas?, in: Jusletter 3. März 2008.

WOLFANGEL EVA, Unsere Stimme haben sie, digma 2019, S. 28-31.

Materialien

Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23. März 1988, BBl 1988 II, S. 413-534.

Botschaft zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 19. Februar 2003, BBl 2003, S. 2101-2155.

EDÖB, Schlussbericht vom 1. Juni 2015 betreffend Abklärung im Zusammenhang mit E-Cockpit und Bicicletta.

– Leitfaden zu biometrischen Erkennungssystemen, Version 1.0, September 2009, abrufbar unter: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/do kumentation/leitfaeden/leitfaden-zu-biometrischen-erkennungssystemen.html>

– Aufzeichnung von Telefongesprächen, abrufbar unter: <www.edoeb.admin.ch/edoeb/de/home/datenschutz/telekommunikation/telefonie/aufzeichnung-von-telefongespraechen.html>

– Erläuterungen zu Stimmerkennungsverfahren (Stand: April 2017), abrufbar unter <www.edoeb.admin.ch/edoeb/de/home/datenschutz/technologien/biometrie/erlaeuterungen-zu-stimmerkennungsverfahren.html>

Entwurf zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (BBl 2017, S. 7193-7276).