3.Teil: Anforderungen an die Identitätsverwaltung

Die grundrechtliche und fachübergreifende Verankerung der personalen Identität im Hinblick auf ein Identitätsverwaltungsmodell bedarf ebenso der einfachrechtlichen Einordnung des Begriffs der personalen Identität. Diese ist für die Begründung eines Identitätsverwaltungsmodells erforderlich, um die personale Identität in ihren dynamischen *Ipse*-Anteilen und in ihren statischen *Idem*-Anteilen abbilden zu können. Dafür müssen die einfachrechtlichen Typologien zur personalen Identität (A.) herausgearbeitet werden, da diese den unmittelbaren Anknüpfungspunkt für die Modellbildung darstellen. Weiter ist für das Identitätsverwaltungsmodell die Ebene der Erkenntniserlangung über die personale Identität einzubeziehen, was mit dem Modell über Daten-Informationen-Wissen (B.) erfolgt. Ebenso verlangt die Identitätsverwaltung die Steuerung der personalen Identitäten, die mit dem Konzept der Kontrolle über die Erkenntnismöglichkeiten der personalen Identität (C.) abgeleitet werden soll. Dabei kommt als Kontrollgegenstand in der Identitätsverwaltung der (elektronische) Agent in Betracht, der anschließend eingeführt wird (D.) und schließlich in die Grundannahmen für die Modellbildung über die kontrollierbaren Erkenntnisse zu personalen Identitäten überführt werden soll (E.).

A. Personale Identität in einfachrechtlichen Typologien

Die personale Identität in einfachrechtlichen Typologien lässt sich primär mit dem Namen einer Identität in Verbindung bringen, mit dem die Zuordnung der personalen Identität möglich wird. Dies gilt für den offline-Kontext und für den online-Kontext gleichermaßen, da etwa der elektronische Personalausweis als eine Anknüpfung für die „digitale Identität“[244] im online-Kontext gilt und der Name in einem Identitätsverwaltungsmodell als Anknüpfungspunkt heranzuziehen ist (I.). Weiter ist mit der kommunikativen Ausprägung der personalen Identität das Recht im elektronischen Rechtsverkehr einzubeziehen, welches in seinem statischen *Idem*-Anteil

244 *Hornung*, Die digitale Identität, 2005; ebenso auf die statische *Idem*-Dimension der Identität abstellend, *Warnecke*, Identitätsmanagement und Datenschutz, 2019, S. 14.

aus der elektronischen Signatur und in seinem dynamischen *Ipse*-Anteil aus der vertraulichen und sicheren Kommunikation besteht (II.). Diese einfachrechtlichen Regelungen über die elektronische Kommunikation sind Anknüpfungspunkte für das Identitätsverwaltungsmodell im online-Kontext, welches das kontextspezifische Vertrauens- und Sicherheitsniveau bei der Identifizierung der personalen Identität umfasst. Diese Ausprägungen der personalen Identität können primär der Identitifizierung und Authentifizierung mit einem *Identifizierer* und sekundär dem schutzwürdigen Vertrauen des Kommunikationspartners über die tatsächliche Identität in einem spezifischen Kontext dienen. Dabei würde der Schutzbereich der informationellen Selbstbestimmung zunächst unberührt bleiben, gleichzeitig werden aber die Schnittmengen zum Datenschutzrecht aufgezeigt (III.).

I. Personale Identität als Name

Der Name als *Idem*-Anteil der personalen Identität des Individuums bildet einen Anknüpfungspunkt für die kontextübergreifende Identitätsverwaltung. Damit ist der Name in seiner statischen *Idem*-Dimension der personalen Identität in die Modellbildung einzubeziehen und fungiert als zentraler Anker. Gleichwohl kann auch der Name Änderungen unterliegen und in direkter Verbindung zu den Ausprägungen der personalen Identität stehen, so dass die einfachrechtlichen Vorgaben aus dem Namensrecht für die einfachrechtliche Konkretisierung des Identitätsbegriffs und die Modellbildung heranzuziehen sind.

Zunächst dient der Name aus der öffentlich-rechtlichen und privatrechtlichen Perspektive der Identifizierung der natürlichen Person und wirkt sich auf die Selbstdarstellung ebenso aus wie auf das wahrnehmbare Bild der personalen Identität. Der Name gemäß § 12 BGB kann der bürgerliche Name kraft Gesetzes gemäß § 1757 BGB oder ein Wahlname etwa als Deckname oder auch ein Pseudonym sein.[245] Dabei dient der Name der Unterscheidung und der Identifizierung und gilt in diesen Funktionen als schutzwürdig.[246] Gleichzeitig gilt gemäß § 1616 BGB der Gleichlauf der Namensführung zur Gewährleistung der Kontinuität der Namensführung, worin eine staatliche Fürsorge über die Namensgebung erkennbar ist. Daher kann die Eintragung von Namen mit unzureichender Identifizierungs-

245 *Palandt*, Kommentar, BGB, 2020, § 12 BGB Rn. 4.
246 *Ders.*, Kommentar, BGB, 2020, § 12 BGB Rn. 1, 11.

und Unterscheidungsfunktion, die im Widerspruch zu einer mit dem Vornamen einhergehenden Identitätsfindung stehen, abgelehnt werden.[247]

Vom Namensrecht nicht erfasst sind akademische Grade, obgleich diese als Namenszusätze im Personalausweis stehen können, §§ 5 Abs. 2 Nr. 3, 9 Abs. 3, 18 Abs. 3 Nr. 3 PAuswG, § 4 Abs. 1 Nr. 3 PassG.[248] Ebenso wird über § 132a StGB der Missbrauch von Titeln, Berufsbezeichnungen und Abzeichen unter Strafe gestellt, denn der allgemeine Rechtsverkehr verlangt die Lauterkeit der Titelführung und das Vertrauen in die Echtheit der Titel von Berufsträgern auch für die Funktionsfähigkeit dieser Berufsgruppen.[249] Weiter kommen als Namenszusätze die Adelsprädikate als Teile des bürgerlichen Namens in Betracht, auch wenn sie nicht mehr verliehen werden dürfen.[250] Daraus wird erkennbar, dass der Name als Bestandteil der personalen Identität neben der Identifizierungsfunktion im Rechtsverkehr eine Beschreibungsfunktion der personalen Identität erfüllt. Gleichwohl bleibt festzuhalten, dass der Titel auf das Verhalten der natürlichen Person zurückzuführen ist, so dass sich im Namen und in den Titeln verhaltensunabhängige *Idem*-Anteile und verhaltensbezogene *Ipse*-Anteile widerspiegeln.

Als weiteres Identifikationsmittel kommen biometrische Daten gemäß § 18 PAuswG hinzu, womit der Schutzbereich des Rechts auf informationelle Selbstbestimmung eröffnet ist.[251] Gleichwohl wird bei der Verwendung biometrischer Daten zur alleinigen Authentifizierung kein Verstoß gegen die Menschenwürdegarantie und das Recht auf informationelle Selbstbestimmung gesehen, da Überschussinformationen etwa über gesundheitliche Merkmale technisch ausgeschlossen werden.[252] Insgesamt ist gerade im öffentlichen Recht, wie auch im Privatrecht, der zum Einsatz kommende elektronische Identitätsnachweis maßgeblich,[253] so dass für die Identifizierung eine Beschränkung der übermittelten Identifizierungsdaten

247 *Ders.*, Kommentar, BGB, 2020, Einf § 1616 BGB Rn. 10; so wurde „Waldmeister" als männlicher Vorname für unzulässig erklärt.
248 *Ders.*, Kommentar, BGB, 2020, § 12 BGB Rn. 7.
249 *Sternberg-Lieben*, in: Schönke/Schröder/Eser u.a. (Hrsg.), Strafgesetzbuch, 2019, § 132a StGB Rn. 3.
250 Art. 109 Abs. 3 S. 2 WRV i. V. m. Art. 123 GG; *Palandt*, Kommentar, BGB, 2020, § 12 BGB Rn. 6.
251 *Hornung/Möller*, Passgesetz, Personalausweisgesetz, 2011, Einf Rn. 31–33.
252 *Dies.*, Passgesetz, Personalausweisgesetz, 2011, Einf Rn. 34 f.; § 16a PassG Rn. 8 f.
253 *Dies.*, Passgesetz, Personalausweisgesetz, 2011, Einf Rn. 87.

erfolgt,[254] und damit dem Grundsatz der Datenminimierung Rechnung getragen wird. Folglich erkennt das Personalausweiswesen die personale Identität im offline- und im online-Kontext gleichermaßen an. Mit dem elektronischen Personalausweis wird die Identitätsverwaltung im online-Kontext ermöglicht, wobei sich diese auf den Namen und die zusätzlichen Informationen gemäß § 18 Abs. 3 PAuswG beschränkt, was überwiegend der personalen Identität in ihrem *Idem*-Anteil gleichkommt.

Insgesamt geht es bei den rechtlichen Schutzdimensionen um den Namen und Familiennamen selbst, seinen Zusätzen in Gestalt von akademischen Graden und Adelsprädikaten. So hat der Name in der Biographie der personalen Identität eine statische Dimension, es sei denn, er wird über das Namensänderungsrecht (NamÄndG) geändert. Weiter kann mit dem Eheschluss der Familienname eines Ehepartners geändert oder beibehalten werden, worin wieder eine dynamische Dimension im Namensrecht zum Ausdruck kommt, § 1355 Abs. 1 BGB.

Für den Begriff der personalen Identität lässt sich daraus ableiten, dass mit dem Namen und seiner Änderung sich eine Identität begründen lässt, mit der eine rechtssichere Zuordnung zu einer natürlichen Person ermöglicht wird. Schließlich kann damit für das Identitätsverwaltungsmodell der Name als maßgeblicher Anknüpfungspunkt der personalen Identität festgehalten werden, der mit Zusätzen in Gestalt von Titeln oder Adelsprädikaten versehen sein kann, die sich als dynamische Realisierungen im Rahmen der individuellen Biographie darstellen können. Gleichzeitig kann der Name im Rahmen des Identifizierungsprozesses hinter dem Authentifizierungsprozess stehen und als *Identifizierer* für einen weiteren kontextbezogenen Datensatz eingesetzt werden.

II. Personale Identität im elektronischen Rechtsverkehr

Ein Identitätsverwaltungsmodell, basierend auf den grundrechtlichen Ausprägungen der personalen Identität, verlangt einerseits den statischen *Idem*-Anteil und andererseits den dynamischen *Ipse*-Anteil auch im online-Kontext. Diese Ausprägungen sollen aus dem einfachen Recht des elektronischen Rechtsverkehrs hergeleitet werden, um daraus weitere Grundlagen für die Modellbildung ableiten zu können. Dazu werden die statische *Idem*-Dimension der personalen Identität im Recht der elektronischen Si-

254 BT-Drucks. 16/10489, S. 40: In der Gesetzesbegründung wurde ausdrücklich auf die Möglichkeit des „persönlichen Identitätsmanagements“ hingewiesen.

gnatur (1.) und bei der gestuften sicheren Identifizierung (2.) dargestellt. Beide lassen sich auf den Namen zurückführen, der für die Erteilung einer elektronischen Signatur und der Identifizierung im elektronischen Rechtsverkehr erforderlich ist, so dass sie für die Modellbildung eine direkte rechtliche Grundlage bilden. Demgegenüber ist der *Ipse*-Anteil der personalen Identität in ihrer Dynamik im Recht zum Schutz der vertraulichen Email-Kommunikation nach dem De-Mail-G abbildbar und stellt eine weitere einfachrechtliche Grundlage für die Modellbildung dar (3.).

1. Qualifizierte elektronische Signatur, §§ 11, 12 VDG

Die personale Identität in Gestalt des Namens tritt im Recht der Vertrauensdienste in verschiedenen Phasen auf. Dazu gehören die Identitätsprüfung bei dem Vertrauensdienstanbieter, die Identifizierung und die Gewährleistung der rechtssicheren Durchführung des Vertrauensdienstes, damit der Kommunikationspartner mit einer hohen Sicherheit auf die Richtigkeit der Identität vertrauen kann. Die Identitätsprüfung wird gemäß § 11 VDG als Nachfolgegesetz des SigG über die „Personenidentifizierungsdaten" gemäß Art. 3 Nr. 3 eIDAS-VO durchgeführt. Dabei können weitere Attribute, wie etwa Angaben über die Vertretungsmacht, im qualifizierten Zertifikat gemäß § 12 VDG aufgenommen werden. Mit der Identitätsprüfung erfolgt die Ausstellung eines qualifizierten Zertifikates, welches beim Inhaber gespeichert wird und mit einem Passwort zugänglich ist. Dieses ausgestellte Zertifikat stellt einen *Idem*-Anteil der personalen Identität dar, da mit ihm der Kommunikationspartner auf die statische Dimension der Identität vertrauen kann. Denn mit dem Zertifikat kann die Schriftform als Identitätsnachweis mit der Unterschrift durch die elektronische Signatur ersetzt werden, §§ 126, 126a BGB, Art. 25 Abs. 2 eIDAS-VO. Darin kommen gerade die Funktionen der Formregeln in der Abschluss-, Kontroll- und Beweisfunktion zum Ausdruck. Zwar richten sich diese an den Rechtsverkehr, jedoch kommen darin die rechtlichen Wertungen über die Gewährleistung eines hohen Sicherheits- und Vertrauensniveaus über die Identität zum Vorschein, was gleichermaßen für personale Identitäten in der Identitätsverwaltung erforderlich ist. Denn mit der qualifizierten elektronischen Signatur lässt sich für einen spezifischen Kontext ein hohes Vertrauens- und Sicherheitsniveau herstellen.

In technischer Hinsicht wird die Signatur mit dem Verfahren der asymmetrischen Kryptographie erstellt, wonach Verschlüsselung und Entschlüsselung jeweils mit zwei Schlüsseln erfolgen, einem öffentlichen und einem

privaten Schlüssel, sog. „*Public-Key-Infrastructure*“ (PKI). Dem Signieren jedes Dokuments geht ein technisches Verfahren voraus, mit dem ein Hashwert als Element für das spezifische Dokument erzeugt wird, welches mit dem privaten Schlüssel generiert wird.[255] Der Empfänger des Dokuments nutzt wiederum seinen privaten Schlüssel und anschließend erfolgt die Prüfung der Schlüssel mit dem Abgleich zu den öffentlichen Schlüsseln. Erst mit dem Zertifikat werden der private und öffentliche Schlüssel miteinander in Verbindung gebracht.[256] Damit ist in technischer Hinsicht die reale Kontrolle durch den Zertifikatinhaber mit einem hohen Sicherheits- und Vertrauensniveau gegeben. Gleichwohl können Angriffe und damit ein Identitätsmissbrauch oder Identitätsdiebstahl[257] nicht ausgeschlossen werden, jedoch besteht ein gesteigertes Sicherheitsniveau.

Insgesamt lässt sich das Kontrollkonzept über die personale Identität aus der qualifizierten elektronischen Signatur ableiten, EWG 51, 52, 53 eIDAS-VO. Denn es wird in Art. 26 c) eIDAS-VO geregelt, dass die Umgebungen zur Verwendung der elektronischen Signaturen der alleinigen Kontrolle des Unterzeichners unterliegen. Gleichzeitig kann der Einsatz eines spezifischen Zertifikates zeitlich begrenzt werden und ein neues Zertifikat als *Idem*-Anteil der personalen Identität ausgestellt werden, was einer „Beendigung von Identitäten“[258] und einer Neubegründung dieser gleichkommt.

2. Gestufte sichere Identifizierung, Art. 8 eIDAS-VO

Das Vertrauens- und Sicherheitsniveau von elektronischen Identifizierungssystemen unterliegt Abstufungen, die sich in der Regelung des Art. 8 Abs. 2 eIDAS-VO widerspiegeln. Danach sind *drei Sicherheitsstufen* in niedrig, substantiell und hoch für die Identifizierung vorgesehen, worin bereits ein eigenes Identitätsverwaltungsmodell erblickt werden kann. Bei der Identifizierung mit einem niedrigen Sicherheitsniveau genügt zur Authen-

255 *Bergfelder*, Der Beweis im elektronischen Rechtsverkehr, 2006, S. 97.

256 *Ders.*, Der Beweis im elektronischen Rechtsverkehr, 2006, S. 98 f.

257 Es kommen Angriffe auf das Trägermedium etwa den Laptop, auf das zu signierende Dokument oder eine Manipulation bei Erstellung des Hashwertes in Betracht. Ebenso kann das Verhalten der Passworteingabe über „*social engineering*“ oder Schwachstellen im Betriebssystem der Gegenstand von Angriffen werden, so dass die Unmöglichkeit einer absoluten Sicherheit und damit Kontrolle über die Signatur ausgeschlossen ist, *ders.*, Der Beweis im elektronischen Rechtsverkehr, 2006, S. 95 f., 199 f.

258 *Hornung*, in: Roßnagel (Hrsg.), Wolken über dem Rechtsstaat?, 2015, 189 (198).

tifizierung der Einsatz von Passwörtern, auf der zweiten Stufe sind für das substantielle Sicherheits- und Vertrauensniveau etwa Zertifikate vorgesehen und auf der dritten Stufe mit einem hohen Sicherheitsniveau wird der Schutz vor Duplizierungen gewährleistet, indem die Identifizierung ausschließlich von einer Person etwa über den elektronischen Personalausweis vorgenommen werden kann. Danach verlangt die Identifizierung des Bürgers gegenüber einer staatlichen Institution ein hohes Sicherheits- und Vertrauensmaß, Art. 8 Abs. 2 c) eIDAS-VO, wohingegen gegenüber einem notifizierten Dienstanbieter für die Rechtsbeziehung unter Privaten[259] die Authentifizierung über ein Passwort ausreichend sein kann, Art. 8 Abs. 2 a) eIDAS-VO. Aus diesen drei verschiedenen Sicherheitsniveaus geht der Grad der Vertrauenswürdigkeit des elektronischen Identifizierungsmittels hervor, mit dem das Vertrauensmaß zwischen festgelegter Identität und der damit zugewiesenen Identität beschrieben wird, EWG 16 S. 1. Die Anknüpfung dieses Vertrauensmaßes richtet sich nach dem Registrierungsumfang für die Ausstellung des Passwortes, Zertifikates oder etwa des elektronischen Personalausweises. Denn von der Identifizierung durch persönliches Erscheinen bei einer „*Trusted Third Party*" als notifizierten Vertrauensdienstanbieter mit den „Personenidentifizierungsdaten" gemäß Art. 3 Nr. 3 eIDAS-VO, geht eine hohe Beweiswirkung aus, die einer Identifizierung mit der bloßen Email-Adresse gegenübersteht.

Aus den gestuften Sicherheits- und Vertrauensniveaus lässt sich innerhalb des jeweiligen Niveaus eine kontextübergreifende Identifizierung abbilden, wie sie ein differenziertes Identitätsverwaltungsmodell voraussetzen würde. Erweiternd ist für ein Identitätsverwaltungsmodell die Anforderung maßgeblich, eine grenzüberschreitende Interoperabilität gemäß Art. 12 eIDAS-VO zu gewährleisten, die innerhalb eines Sicherheits- und Vertrauensniveaus gelten würde. Darin kommt die Beseitigung der Hindernisse zur grenzüberschreitenden Verwendung des gleichen elektronischen Identifizierungsmittels zur Authentifizierung bei öffentlichen Diensten zum Ausdruck, EWG 12 S. 1. Der technische Interoperabilitätsrahmen ist gemäß Art. 12 Abs. 3 a) eIDAS-VO technologieneutral und kann durch Kommunikationsschnittstellen realisiert werden. Dabei besteht der zu regelnde Interoperabilitätsrahmen aus Bezugnahmen auf die Sicherheitsniveaus nach Art. 8 eIDAS-VO, technischen Mindestanforderungen, Verfahrensregelungen und Regelun-

259 Die eIDAS-VO ist grundsätzlich für die Identifizierung und Authentifizierung gegenüber öffentlichen Diensten vorgesehen, jedoch soll gemäß EWG 57, 2 und Art. 3 Nr. 7, 30 eIDAS-VO auch der Rechtsverkehr unter Privaten einbezogen werden.

gen zur Streitbeilegung, Art. 12 Abs. 4 a, c–f) eIDAS-VO. Mit dem Interoperabilitätsrahmen für eine grenzüberschreitende Identifizierung in dem jeweiligen Sicherheitsniveau gemäß Art. 8 Abs. 2 eIDAS-VO kann jedoch einhergehen, dass das Risiko einer kontextübergreifenden Identifizierbarkeit steigt und die Trennung der Sicherheitsstufen faktisch aufgehoben wird.

Damit lässt sich die rechtliche Überschneidung zwischen dem Vertrauensdiensterecht und den datenschutzrechtlichen Vorgaben gerade an der Datenminimierung aufzeigen. Denn das Vertrauensdiensterecht soll die sichere Identifizierung ermöglichen und zugleich gemäß Art. 5 Abs. 1 eIDAS-VO datenschutzrechtliche Maßgaben einhalten. Im Rahmen des Selbstdatenschutzes können dabei Zielkonflikte mit der Sicherstellung der kontextbezogenen Identifizierung auf der einen Seite und der faktischen kontextübergreifenden Re-Identifizierbarkeit als Ausprägung des *Big Data*-Phänomens auf der anderen Seite entstehen. Insoweit erscheint die konsequente Einhaltung des kontextspezifischen Sicherheitsniveaus aus datenschutzrechtlicher Hinsicht fraglich, wenn die Identifizierung auf einem niedrigen Sicherheitsniveau gemäß Art. 8 Abs. 2 a) eIDAS-VO erfolgt und die damit verbundenen Erkenntnisse kontextübergreifend herangezogen werden können, wobei damit das höhere „substantielle" Schutzniveau gemäß Art. 8 Abs. 2 b) eIDAS-VO herangezogen werden müsste. Um gegen dieses Risiko vorgehen zu können, wäre der zeitlich beschränkte Einsatz der Identifizierungsmittel denkbar, indem etwa die Wirksamkeit einer Signatur an den Erstellungszeitpunkt anknüpft, zeitlich begrenzt ist und nach Zeitablauf automatisch gelöscht wird.

3. Vertrauliche sichere Kommunikation, § 1 De-Mail-G

Das Konzept der Kontrolle als Beherrschbarkeit kann ebenso die Kommunikation umfassen, da der Kommunikationsvorgang durch eine der Kontrolle unterliegenen Handlung ausgelöst wird. Indem die personale Identität neben dem statischen *Idem*-Anteil über einen kommunikativen und damit dynamischen *Ipse*-Anteil verfügt, kann in den einfachrechtlichen Regelungen zur vertraulichen und sicheren Kommunikation ein wesentlicher Anknüpfungspunkt für das Identitätsverwaltungsmodell liegen.

Mit dem De-Mail-G wird gerade die sichere, vertrauliche und nachweisbare Kommunikation geregelt und dabei die Vertraulichkeit der Kommunikation als Kernelement des De-Mail-G begründet, § 1 Abs. 1 De-Mail-G. Darin sollte eine Antwort auf die bislang unausgeprägten elektronischen Kommunikationsmöglichkeiten zwischen dem Bürger und staatlichen Institutionen

etwa für Bürgerdienste oder die elektronische Post liegen. Die Voraussetzung ist wiederum, parallel zum Erhalt einer qualifizierten elektronischen Signatur, die Registrierung bei einem akkreditierten Dienstanbieter unter Vorlage eines Personalausweises, wodurch wiederum ein hohes Sicherheits- und Vertrauensniveau gewährleistet wird. Dies wird im besonderen Maße sichergestellt, indem die Identitätsdaten in angemessenen zeitlichen Abständen auf ihre Richtigkeit geprüft werden, §§ 1 Abs. 2, 3 Abs. 3 Nr. 1 a), 3 Abs. 5 S. 2 De-Mail-G. Maßgeblich sind nach dem De-Mail-G der Schutz vor Manipulation der Identität des Kommunikationspartners und auch die rechtssichere inhaltliche Zustellung elektronischer Dokumente gegen unkooperative Kommunikationspartner.[260] Damit werden über die Identitäten des Senders und Empfängers hinaus die Inhalte der Kommunikation durch die verschlüsselte Kommunikation geschützt, §§ 4 Abs. 3, 5 Abs. 3 De-Mail-G, und über die inhaltliche Zustellung eine Beweiserleichterung begründet, die als Anscheinsbeweis über die Richtigkeit des Absenders und den Inhalt der Nachricht fungiert, § 371a Abs. 2 ZPO.[261]

In dieser Erweiterung der Beweisvermutung, die sich auf den Inhalt der Nachricht erstreckt, liegt ein wesentlicher Erkenntniswert für die Identitätsverwaltung. Denn nach der Wertung des Gesetzgebers kommt es im online-Kontext nicht allein auf die rechtssichere elektronische Identifizierung in Gestalt einer Signatur an, sondern auf den Schutz der rechtssicheren inhaltlichen Kommunikation gegenüber staatlichen Institutionen und zwischen Privaten. Mit dem Schutz der Identität des Kommunikationspartners auf der einen Seite und dem Schutz des Inhaltes der Kommunikation auf der anderen Seite ist für den online-Kontext aus dem De-Mail-G ein aufschlussreiches Regelungsregime für die Identitätsverwaltung ableitbar. Denn es wird neben der statischen Dimension der personalen Identität über eine Signatur die dynamische Dimension der schützenswerten Kommunikation in die gesetzgeberische Wertung einbezogen. Zwar kann die Kommunikation einem eigenständigen grundrechtlichen Schutz aus dem Fernmeldegeheimnis, Art. 10 Abs. 1 GG, und der allgemeinen Meinungsfreiheit, Art. 5 Abs. 1 GG, unterliegen, jedoch bezieht sich die vorliegende Betrachtung auf die enge Verbindung zur Identität des Kommunikationspartners. Diese strahlt unmittelbar auf das Schutzniveau der inhaltlich vertraulichen Kommunikation aus. Die personale Identität in ihrer verhaltensbezogenen Dimension findet damit im online-Kontext eine unmittelbare einfachrechtliche Abbildung, welches für ein Identitätsverwaltungsmodell zu einer Aner-

260 *Roßnagel*, CR 2011, 23 (29).
261 *Ders.*, CR 2011, 23 (29).

kennung der personalen Identität im Rahmen der Identifizierung und der damit verbundenen inhaltlichen Kommunikation führt. Damit sind die Grundlagen für ein Identitätsverwaltungsmodell im online-Kontext gelegt, weil ein einfachrechtliches Schutzkonzept für die personale Identität und ihre inhaltliche kommunikative Ausprägung besteht.

4. Bewertung

Das Recht der Vertrauensdienste und das Recht über die sichere, vertrauliche elektronische Kommunikation knüpfen an die Identifizierung der personalen Identität an, was über das Registrierungsverfahren und anschließend die Anwendung einer Signatur oder des De-Mail-Kontos erfolgt. Darin kommt die statische Dimension der personalen Identität in ihrem *Idem*-Anteil über den Namen zum Ausdruck, erfährt aber durch die Kommunikation mit diesem eine dynamische Erweiterung in ihrem *Ipse*-Anteil. Denn über die Gewährleistung des Schutzes der Identität und der inhaltlichen Kommunikation kommt im online-Kontext ein dynamisches Schutz- und Ausgleichskonzept in direkter Verbindung zur personalen Identität zum Ausdruck.

Gleichzeitig stellt sich bei der IT-sicherheitsrechtlichen Prägung die Frage nach der Gewährleistung datenschutzrechtlicher Vorgaben, um eine umfassende Überführung der Maßgaben in ein rechtlich gestütztes Identitätsverwaltungsmodell vornehmen zu können. Gemäß Art. 5 Abs. 1 eIDAS-VO wird auf die Datenschutzrichtlinie verwiesen, was nunmehr einem Verweis auf die DSGVO gleichkommt. Eine konkretisierte Regelung erfolgt in Art. 5 Abs. 2 eIDAS-VO und § 5 Abs. 2 De-Mail-G, wonach die Benutzung von Pseudonymen nicht untersagt werden darf. Darin und in § 15 De-Mail-G liegt eine Konkretisierung der Datenminimierung nach Art. 5 Abs. 1 c) DSGVO, wonach zum Schutz der personenbezogenen Daten eine Beschränkung der Datenverarbeitung auf das notwendige Maß geregelt wird. In den nur punktuellen Bezugnahmen[262] auf datenschutzrechtliche Vorgaben wie etwa „*privacy by design*“, Art. 12 Abs. 3 c) eIDAS-VO, ohne jedoch die differenzierten Interdependenzen zwischen Datenschutz und IT-Sicherheit aufzugreifen, wird ein Regelungsgefüge gesehen, welches „unterkomplex“ sei.[263] So sieht etwa Art. 8 Abs. 2 c) eIDAS-VO für die Identifizierung mit dem elektronischen Personalausweis ein hohes Schutzniveau vor, ohne jedoch in

262 Art. 12 Abs. 3 c), d), Art. 19 Abs. 2, Art. 20 Abs. 2, Art. 24 Abs. 2 b) und j) eIDAS-VO.

263 *Roßnagel*, NJW 2014, 3686 (3687).

der eIDAS-VO ein Regelungsgefüge für die Verarbeitung besonderer Kategorien personenbezoger Daten nach Art. 9 DSGVO zu enthalten. Darin kommen die noch unzureichende Verknüpfung zwischen dem Vertrauensdienste- und Datenschutzrecht und das Fehlen eines ausdifferenzierten Schutzgefüges für die informationelle Selbstbestimmung zum Ausdruck. Folglich wäre eine differenzierte Einbeziehung der Datenverarbeitungsgrundsätze gemäß Art. 5 Abs. 1 DSGVO wünschenswert und könnte einen gesteigerten Schutz für die informationelle Selbstbestimmung bedeuten.

Insgesamt lässt sich aus den bestehenden Regelungen dennoch ein Schutzgefüge zur Gewährleistung der Datenminimierung nachweisen, welches bei der Modellierung heranzuziehen ist. Dieses könnte mit einem zeitlich beschränkten Identifizierungsvorgang umgesetzt werden, damit das Risiko von Erkenntnissen zu einer personalen Identität über die jeweiligen Stufen des Sicherheits- und Vertrauensniveaus hinweg gemindert wird.

Mit der Verbindung der IT-sicherheitsrechtlichen und der datenschutzrechtlichen Regelungen würde einem Identitätsverwaltungsmodell mit statischen und dynamischen Ausprägungen entsprochen werden können. Dabei sind die Zielkonflikte, einerseits eine rechtssichere Identifikation des *Idem*-Anteils einer personalen Identität zu ermöglichen und andererseits das Risiko der Re-Identifizierbarkeit in einem anderen Kontext mit einem höheren Sicherheitsniveau zu mindern, miteinander in Einklang zu bringen. Insofern verlangt das Identitätsverwaltungsmodell eine Differenzierung des Sicherheitsniveaus bei der rechtssicheren Identifizierung und einen Schutzmechanismus für die rechtssichere Gewährleistung der Interoperabilität innerhalb des Schutzniveaus.

III. Zusammenfassung

Aus dem einfachen Recht wurden die Konkretisierungen der verfassungsrechtlichen Vorgaben zur personalen Identität für das Identitätsverwaltungsmodell abgeleitet. Dazu gehört, dass der Name als übergreifender Bezugspunkt im einfachen Recht fungiert und kontextspezifisch das Vertrauens- und Sicherheitsmaß der personalen Identität und Kommunikation variiert. Dies kommt in der zivilrechtlichen Regelung des Namensrechts in § 12 BGB zum Ausdruck und dem damit einhergehenden Schutz im Rechtsverkehr hinsichtlich der Unterscheidbarkeit und Identifizierbarkeit der natürlichen Person. Gleichzeitig erlangt der Name in der Rechtsbeziehung zwischen Bürger und Staat besonders durch das PAuswG ein hohes Vertrauens- und Sicherheitsmaß hinsichtlich der Identifizierbarkeit. Dieses wird für

den elektronischen Rechtsverkehr über die eIDAS-VO für den öffentlich-rechtlichen und privatrechtlichen Kontext gleichermaßen geregelt. Danach erfolt die Registrierung zum Erhalt eines Zertifikates für die elektronische Signatur mit den Personenidentifizierungsdaten und für den Erhalt eines De-Mail-Kontos muss der Personalausweis vorgelegt werden, §§ 3 Abs. 3 a), c), 4 Abs. 2 De-Mail-G.

Gleichzeitig wird ein gestuftes System zur Identifizierung nach Art. 8 Abs. 2 eIDAS-VO anerkannt, woraus die Grundstruktur eines Identitätsverwaltungsmodells dahingehend abzuleiten ist, dass dieses abhängig von dem jeweiligen Kontext ein niedriges, substantielles oder hohes Vertrauens- und Sicherheitsniveau enthält. Dieses richtet sich auf die statische Identifizierung und den über das De-Mail-Konto gewährleisteten Schutz der Identität und der Kommunikation gleichermaßen. Daraus ergibt sich für die personale Identität und das Identitätsverwaltungsmodell das Erfordernis von kontextbedingten Vertrauens- und Sicherheitsabstufungen. Damit werden die Identifizierung und die inhaltliche Kommunikation geschützt. Aus diesen rechtlichen Phänomenen lässt sich ein einfach- und sekundärrechtliches Grundmodell ableiten. Dabei würde sich die digitale Identität über den elektronischen Personalausweis als ein Bestandteil in dem Gesamtgefüge der personalen Identität im online-Kontext erweisen.

B. Erkenntnismodell

Die *Modellbildung der Identitätsverwaltung* verlangt darüber hinaus die Bestimmung des Gegenstands der personalen Identitäten, der sich aus dem Erkenntnismodell ableiten lässt. Danach können die Anknüpfungspunkte für die personale Identität die Daten, die Informationen und das Wissen über die Identität sein (I.). Dabei sind die vielfältigen Erkenntnismöglichkeiten über personale Identitäten kontextbezogen und flexibel, was in die Modellbildung einzubeziehen ist, um einen wirksamen Schutz- und Ausgleichsmechanismus begründen zu können. Daneben kommt der dynamische *Ipse*-Anteil einer personalen Identität über die Kommunikation im Rahmen der Datenverarbeitung und dem damit verbundenen Datenzyklus einer personalen Identität als Schutzgegenstand zum Ausdruck. Dieser kann mit einer übergeordneten Metakommunikation durch *Instruktionen* in einem Verfahren über das Wissen zu einer personalen Identität maßgeblich sein (II.). Schließlich geht es um die Konkretisierung der Gegenstände für das Identitätsverwaltungsmodell, die an die Informationen und das verfahrensbedingte Wissen über personale Identitäten anknüpfen und einen Schutz- und

Ausgleichsmechanismus über die entstandenen Bilder personaler Identitäten bilden können (III.).

I. Daten-Informationen-Wissen

Im Verfassungsrecht und im einfachen Recht sind als Schutzgegenstände zur personalen Identität die Daten und die semantischen Bedeutungsgehalte über die personale Identität erfasst. Bei einem Identitätsverwaltungsmodell stellt sich die Frage, welche dieser Erkenntnisgehalte zur personalen Identität zum Gegenstand der Kontrolle werden können. Denn es kommt nicht nur der Schutz der Signale als Daten über eine personale Identität in Betracht, sondern auch die damit verbundenen Interpretations- und Erkenntnismöglichkeiten. Daraus ergibt sich der Bedarf, den Gegenstand des Schutzes einer näheren Differenzierung zu unterziehen, damit sich der Kontrollgegenstand spezifizieren lässt.

Nach dem Erkenntnismodell wird eine Untergliederung in Daten, Informationen, Wissen und dem Vorgang der Entscheidung vorgenommen, die in einem Identitätsverwaltungsmodell jeweils zum Gegenstand der Kontrolle werden können. Diese aus Daten bestehenden Zeichenfolgen erlangen einen Bedeutungsgehalt erst durch den Vorgang der Interpretation, woraus sich aus den Daten die semantischen Informationen über die personale Identität ergeben. Mit der Interpretation werden die Daten aus der „Schattenwelt der Informationstechnik" in ein sozialwirksames Folgensystem überführt.[264] Der Interpretationsvorgang unterliegt einem bestimmten Zweck und ist damit perspektivisch, so dass es sich nicht um wertfreie, objektive Informationen handeln könne.[265] Dabei beschreibt *Steinmüller* diesen Vorgang eigens als Übermittlungsvorgang, bei dem es auch zu einem Übermittlungsirrtum kommen könne und die Informationen – vergleichbar mit einer Amöbe – dem räumlichen und zeitlichen Wandel unterliegen.[266] Wiederum können aus den Informationen und ihrer Bündelung weitere Erkenntnisebenen wirken und einen eigenständigen kontextspezifischen Bedeutungsgehalt als „konsolidiertes Wissen"[267] entfalten, wobei das kon-

264 *Steinmüller*, Information, Modell, Informationssystem, S. 48.
265 *Ders.*, Information, Modell, Informationssystem, S. 37 f.; *Albers*, Informationelle Selbstbestimmung, 2005, S. 92–94.
266 *Ders.*, Information, Modell, Informationssystem, S. 5, 32–35.
267 *Hoffmann-Riem*, in: Augsberg (Hrsg.), Ungewissheit als Chance, 2009, 17 (23); ebenso *Gasser*, Kausalität und Zurechnung von Information als Rechtsproblem, 2002, S. 74.

krete Wissen von der Wandlungsfähigkeit der Informationen abhänge (Abbildung 2).[268] Somit ist Wissen in einem System flexibel und könne nicht objektiv sein, aber einem kontextbedingten Wahrheitssystem entsprechen.[269] Sobald das Wissen aber als ableitbare Schlussfolgerung festgestellt wurde, kann dem erlangten Wissen die Eigenschaft eines Agenten zukommen,[270] so dass dem Wissen über eine personale Identität in einem spezifischen Kontext die Agenteneigenschaft zugeschrieben werden kann. Damit wird das Bild der personalen Identität in Gestalt eines Agenten zum Gegenstand der Kommunikation.

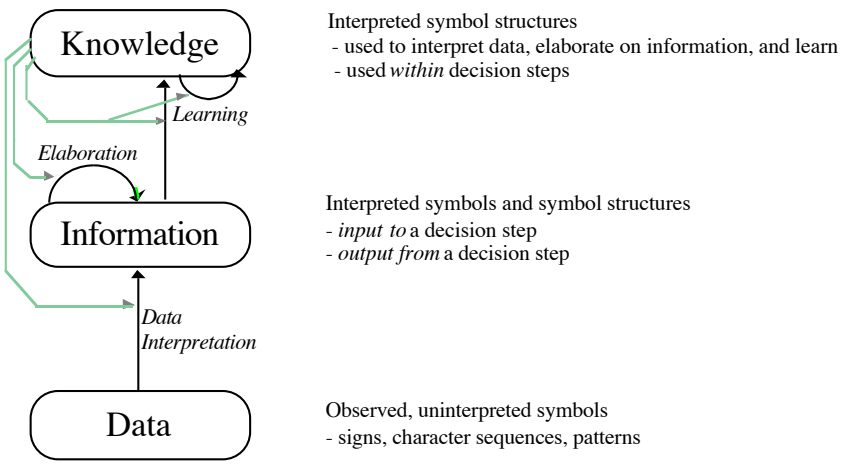

Abbildung 2: Aamodt/Nygård[271]

Dies setzt den Vorgang des Entscheidens voraus, der von *Steinmüller* als Aggregatzustand über die Informationen beschrieben wird, denn Informationen verlangen einen dynamischen Informationserzeugungsvorgang, der eines *strukturierten Entscheidungsverfahrens* etwa als „iteratives Entschei-

268 *Aamodt/Nygård*, Data & Knowledge Engineering 16 (1995), 191 (199); *Reisinger*, Rechtsinformatik, 2016, S. 75.
269 *Dies.*, Data & Knowledge Engineering 16 (1995), 191 (200); *Steinmüller*, Information, Modell, Informationssystem, S. 67; zudem hänge das Wissen von möglichem *Vorwissen* ab, *Gasser*, Kausalität und Zurechnung von Information als Rechtsproblem, 2002, S. 77.
270 *Dies.*, Data & Knowledge Engineering 16 (1995), 191 (204).
271 *Dies.*, Data & Knowledge Engineering 16 (1995), 191 (198).

dungsmodell“ bedarf.[272] Darin könnte eine Begegnung von missverständlichen, falschen oder manipulierten Informations- und Wissensergebnissen über die Bilder personaler Identitäten liegen, die gerade bei der Profilerstellung oder in Scoringverfahren in Erscheinung treten können. Demnach geht es bei dem Wissen in *Big Data*-Zeiten nicht allein um das Erlernen aus Informationen an sich, sondern um die Validierung der Informationen nach bestimmten Regeln, damit sinnlose, überholte oder widerlegte Informationen für eine wirksame Beschränkung des Wissens ausgeschlossen werden.[273] Dies setzt ein strukturiertes Entscheidungsverfahren voraus, das aus *Instruktionen* für die Entscheidungsfindung besteht und ein wesentlicher Anknüpfungspunkt für die Identitätsverwaltung sein kann, um die aus Wissen erstellten Bilder personaler Identitäten tatsächlich kontrollieren zu können.

II. Datenzyklus

Der Datenzyklus im Zusammenhang mit der personalen Identität umfasst die Datenverarbeitung der personenbezogenen Daten in ihren Ausprägungen der Erfassung, der Organisation, der Speicherung oder Veränderung, der Einschränkung, des Löschens oder der Vernichtung der personenbezogenen Daten, Art. 4 Nr. 2 DSGVO, EWG 39 S. 2. Demnach wirkt sich das Recht auf Vergessenwerden im Datenzyklus als ein entscheidendes Schutzrecht im Hinblick auf das verfassungsrechtliche Recht auf Neubeginn für die personale Identität aus. Mit einem Identitätsverwaltungsmodell sind auf der Ebene der Realphänomene die biographischen Kontexte maßgeblich, denn das Individuum steht in einer kontinuierlichen kommunikativen Beziehung zu der sozialen Umgebung.

Für den Schutz der personalen Identität innerhalb des Datenzyklus kann die Einteilung in die Phasen vor der Datenverarbeitung, der Begründung der Rechtmäßigkeit und der Phase nach der Rechtfertigung der Datenverarbeitung vorgenommen werden. An dieser Stelle sollen jedoch im Rahmen des dargestellten Erkenntnismodells die Relevanz des Datenzyklus für die personale Identität und der Identitätsverwaltung analysiert

272 *Steinmüller*, Information, Modell, Informationssystem, S. 76; ebenso zur Information als Zustand, vgl. *Gasser*, Kausalität und Zurechnung von Information als Rechtsproblem, 2002, S. 26.

273 *Weyh*, Philosophie in der digitalen Welt - DigiKant oder: Vier Fragen, frisch gestellt.

werden. Unter der Maßgabe, dass ein Identitätsverwaltungsmodell über die Verwaltung von Teilidentitäten hinaus einem Kommunikationsgefüge unterliegt und der Bedarf einer übergeordneten Kommunikationsstruktur bestehen kann, soll im Folgenden der Datenzyklus als Kommunikation (1.) und als Metakommunikation (2.) dargestellt werden.

1. Datenzyklus als Kommunikation

Der Datenzyklus unterliegt einem Kommunikationsprozess, der aus einer Vielzahl von Interpunktionen besteht. Dabei wird angenommen, dass sich die aus der Kommunikationspsychologie stammenden Erkenntnisse fragmentarisch auf die digitale Kommunikation in einem Datenzyklus übertragen lassen.[274] Denn es handelt sich um einen Datenzyklus, der personenbezogene Daten zum Gegenstand hat und bei dem in der Kommunikation neben der Informationstechnik der Mensch beteiligt ist, was sich auf die Bilder personaler Identität auswirkt. Demnach ist zwischen Sender, Empfänger, Nachricht und Vermittler als technische Umsetzer in einem Kommunikationsverhältnis zu differenzieren.[275] Ein Identitätsverwaltungsmodell verlangt diese Bestandteile eines technischen Systems, wonach es über die identitätsrelevanten Daten, Informationen und das Wissen[276] hinaus eines Senders, Empfängers und Vermittlers zum Schutz der personalen Identität bedarf. Damit sind die wesentlichen Bestandteile eines Identitätsverwaltungsmodells beschrieben, mit dem die Bilder personaler Identität als Erkenntnisse aus Daten entstehen und im räumlichen und zeitlichen Zusammenhang kontrolliert werden können.

Dahingehend wird von einer „Lebenszyklusverwaltung" über produktive, archivierte, gesperrte oder gelöschte Daten als Ausprägung des „*Infor-*

274 *Steinmüller* hat in der Begründung des Grundbegriffs der Kommunikation in der Informatik die Annahmen von *Watzlawick* einbezogen und festgestellt, dass die psychologische Facette der Kommunikation in der Begriffsfindung der informationstechnischen Kommunikation als Erkenntnisquelle für die Informatik unzureichend diskutiert werde, *Steinmüller*, Information, Modell, Informationssystem, S. 2 Fn. 6, S. 4 Fn. 32.

275 *Ders.*, Information, Modell, Informationssystem, S. 2 f.

276 Nach *Watzlawick* wird das Konzept des Wissens über die andere Partei in der menschlichen Kommunikation sogar in Frage gestellt und er geht vielmehr davon aus, dass sich Parteien vertrauen oder misstrauen können, jedoch nicht „Wissen" können; *Watzlawick/Beavin/Jackson*, Menschliche Kommunikation, 2016, S. 249 f.

mation lifecycle Management" ausgegangen, welches dem Regelungsregime der DSGVO unterliegt.[277] Daraus lässt sich für die Bilder personaler Identitäten die Annahme eines Datenzyklus über das kontextspezifisch generierte Wissen ableiten, welches dem Wandel der Zeit unterliegt. Demnach erscheint die Forderung nach regulatorischen und technischen Maßnahmen für ein Identitätsverwaltungsmodell von *Froomkin* folgerichtig, mit dem eine Kombination aus dem Verwalten, Synchronisieren, Sammeln und Verwenden von personenbezogenen Daten zur Kontrolle kontextspezifischer personaler Identitäten erfolgen würde.[278]

2. Datenzyklus als Metakommunikation

Ein Identitätsverwaltungsmodell könnte eine übergeordnete Kommunikationsebene als Metakommunikation darstellen. Dem liegt die Annahme zugrunde, dass nach dem Erkenntnismodell das Wissen nicht absolut und objektiv ist, sondern mehrere Versionen von Wissen zur Verfügung stehen können und eine Differenzierung des Wissens notwendig ist, was den rationalen Umgang mit personenbezogenen Daten voraussetze.[279] Folglich geht es um das *Wissen über das Wissen* und die damit verbundene Wissensverwaltung,[280] wie es mit den *Instruktionen* zur Generierung von Wissen über das Bild der personalen Identität erforderlich ist. Entsprechend kann das Verfahren das Wissen konsolidieren, wie es mit dem Verwaltungsverfahren, den Regeln der Beweislastverteilung und der Durchsetzung von Entscheidungen geregelt wird.[281]

In einem Datenzyklus geht es demnach um ein Verfahren, mit dem die Identitätsverwaltung erfolgen kann, welches eine weitere Ordnung über die Daten, Informationen und das Wissen zur personalen Identität begründet. Dabei geht es weniger um die Kontrolle über die Daten-, Informations- und Wissensströme, als um die Einbeziehung einer Metaebene der Kommunikation in Gestalt von *Instruktionen*. Auf dieser Metaebene kann ein Verfahren die *Instruktion* zur Steuerung über die Regeln der Informations- und Wissenserlangung von Bildern personaler Identitäten umfassen.

---

277 *Lehnert/Luther/Christoph u.a.*, Datenschutz mit SAP, 2018, S. 142; *Veil*, ZD 2015, 347 (350).
278 *Froomkin*, Building Privacy into the Infrastructure: Towards a New Identity Management Architecture, 2016, S. 8.
279 *Cohen*, JTHTL 2012, 242 (242 f.).
280 *Steinmüller*, Information, Modell, Informationssystem, S. 69.
281 *Hoffmann-Riem*, in: Augsberg (Hrsg.), Ungewissheit als Chance, 2009, 17 (24 f.).

III. Übertragung auf das Identitätsverwaltungsmodell

Das Erkenntnismodell ermöglicht die Differenzierung der Identitätsverwaltung hinsichtlich der Daten, Informationen und des Wissens über eine personale Identität. Diese Erkenntnisebenen variieren in einem Datenzyklus und hängen von dem jeweiligen Betrachtungswinkel ab. Darin kommt zum Ausdruck, dass im Laufe einer Biographie der personalen Identität kontextbedingte Änderungen entstehen, die sich im Datenzyklus widerspiegeln können und den Bedarf einer Anpassung auslösen, was in einem Identitätsverwaltungsmodell einzubeziehen ist. Dieser Datenzyklus ist nach dem Erkenntnismodell geprägt von den Daten, den Informationen und dem Wissen, wobei die Informations- und Wissenserlangung als Kommunikationsvorgänge einzuordnen sind.[282] Dem folgend wird die Bezeichnung des „Datenschutzes" als unzutreffend gesehen, denn es gehe um den Schutz vor Informationen und Wissen über natürliche Personen, damit Fehlentwicklungen von Informationen und Erkenntnissen erkannt und korrigiert werden können.[283] Demnach kann mit der Perspektive auf das datenschutzrechtliche Phänomen der Kommunikation möglicherweise ein Paradigmenwechsel mit einem Identitätsverwaltungsmodell vorgenommen werden, der in einer Verlagerung des datenbasierten Ansatzes auf ein Verfahren der Erkenntniserlangung über die personale Identität liegt.

Es kommt insgesamt nicht allein auf die mit der personalen Identität verbundenen Daten, Informationen und das Wissen an, sondern auf die damit verbundenen Kommunikationsvorgänge mit ihren Regeln und *Instruktionen* zur Erkenntniserlangung. Darin würde die für ein Identitätsverwaltungsmodell erforderliche Metaebene einbezogen werden. Dabei ginge es um *Instruktionen* zur Informations- und Wissenserlangung in einem Verfahren, welches für die Herbeiführung eines Ergebnisses als Bild der personalen Identität eingesetzt werden könnte. In dieser Metaebene in einem Identitätsverwaltungsmodell könnte eine Antwort auf die von Dataisten festgestellte Umkehrung der Erkenntnispyramide liegen, wonach die Dominanz der Daten für den menschlichen Erkenntnisprozess dem Einsatz intelligenter Algorithmen weicht, denn diese würden einen „höheren Er-

282 „Jede Information ist vielmehr Kommunikation", vgl. *Veil*, NVwZ 2018, 686 (687); *Albers*, Informationelle Selbstbestimmung, 2005, S. 88.

283 *Spiecker gen. Döhmann*, in: Vesting (Hrsg.), Der Eigenwert des Verfassungsrechts, 2011, 263 (265); *Lewinski*, Die Matrix des Datenschutzes, 2014, S. 3 mwN.; *Haft*, Einführung in die Rechtsinformatik, 1977, S. 16; ebenso den Schutz des Erkenntnisgehalts von Daten betonend, *Drexl*, JIPITEC 2017, 257 (263) Rn. 24.

kenntniswert“ generieren und die Bedeutung der Daten verdrängen.[284] Demnach können übergeordnete *Instruktionen* den algorithmusbasierten Erkenntnisprozessen entgegengehalten werden, so dass mit den *Instruktionen* eigenständige Bilder personaler Identitäten generiert können. Diese sollen als Gegenbild in die Kommunikation einbezogen werden. Mit den festgelegten Verfahrensregeln und *Instruktionen* könnte die Kontrolle über die Interpretations- und Erkenntnisprozesse zu den Bildern personaler Identitäten in einem Identitätsverwaltungsmodell implementiert werden.

IV. Zwischenergebnis

Für die Identitätsverwaltung ist das Erkenntnismodell maßgeblich, um den Kontrollgegenstand bestimmen zu können. Zunächst ließe sich annehmen, dass die Kontrolle über Daten-Informationen-Wissen zu personalen Identitäten entscheidend sei. Jedoch stehen in Anbetracht des amöbenartigen kontextspezifischen Informations- und Erkenntnisgehaltes die *Instruktionen* im Vordergrund. Mit den *Instruktionen* wird der Schutz über kontextspezifische Wahrheitsgehalte gewährleistet, da Informationen und Erkenntnisse in Systemen nicht absolut und objektiv sind. Die Identitätswaltung sollte daher den Aggregatzustand von Informationen einbeziehen und sich über den Datenzyklus erstrecken. Damit liegt ein Paradigmenwechsel insofern vor, dass sich die Identitätsverwaltung auf die Kommunikation und die Metakommunikation in Gestalt der *Instruktionen* erstrecken soll. Folglich bedarf es der Kontrolle personaler Identitäten unter Einbeziehung der Kommunikation und der *Instruktionen*.

C. Kontrolle personaler Identitäten

Das Konzept der Kontrolle über die personale Identität kann aus den Grundrechten und dem einfachen Recht abgeleitet werden (I.). Die Kontrolle soll dabei in eine absolute (II.) und relative Kontrolle (III.) unterteilt werden, wobei sich das Konzept der Kontrolle als Paradoxon (IV.) gegenüber dem Schutz der informationellen Selbstbestimmung erweist. Die Wirkungen des Kontroll-Paradoxons sollen bei der Übertragung der Kontrolle auf das Identitätsverwaltungsmodell (V.) näher untersucht werden.

---

284 *Harari*, Homo Deus, 2017, S. 498–500.

I. Einführung

Der Kontrollbegriff für ein Identitätsverwaltungsmodell lässt sich bereits aus dem Volkszählungsurteil herleiten, welches den Schutzbedarf gegen „unkontrollierbare Persönlichkeitserfassung“[285], unkontrollierbare Nebenfolgen mit der Weitergabe des Namens[286] und den Bedarf nach Kontrolle über Persönlichkeitsbilder, die aus Datensammlungen zusammengefügt wurden, beschreibt[287]. Weiter lässt sich der Kontrollbegriff direkt aus der Datenschutzgrundverordnung ableiten, indem die Kontrolle über die eigenen Daten in den Erwägungsgründen (EWG) 7 S. 2; 13, S. 1; 68 S. 1; 75 benannt wird und der Kontrollverlust über die personenbezogenen Daten als mögliche Grundlage für einen Schadensersatzanspruch nach dem EWG 85 S. 1 vorgesehen ist. Daraus lässt sich ein Verständnis über den Kontrollbegriff ableiten, wonach es um das bewusste Einwirken, Beherrschen, Gestalten und Beaufsichtigen der personenbezogenen Daten geht. Gleichzeitig realisiert sich in diesem einfachrechtlichen Kontrollbegriff das grundrechtliche Konzept der informationellen Selbstbestimmung und der Schutz, dass die Handlungen in der privaten und öffentlichen Sphäre über die Informationen und Bilder zur Identität beherrschbar sind. Gegen den Begriff der Beherrschbarkeit von Informationen führt *Marsch* auch unter Einbeziehung des Begriffs der Kontrolle jedoch die fehlende Beherrschbarkeit von Interpretationsvorgängen an.[288] Demgegenüber wird aus einer rechtskulturellen Perspektive die Kontrolle als Bestandteil des kontinentaleuropäischen Privatheitskonzepts angesehen,[289] was die Entscheidungsmöglichkeit über die Offenlegung von Informationen über die Begründung und Entwicklung des eigenen Bildes[290] umfasst. Folglich geht es bei den Begriffen der Kontrolle und Beherrschbarkeit von Informationen nicht allein um ein absolutes Verständnis, sondern es kommt ebenso die relative Be-

285 BVerfGE 65, 1 (4).
286 BVerfGE 65, 1 (18).
287 BVerfGE 65, 1 (42).
288 *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 99 f.
289 *Whitman*, Yale L. J. 2004, 1151, (1161, 1199): Insgesamt könne es nicht um ein Konzept der absoluten Kontrolle gehen, sondern immer nur um die relative Kontrolle.
290 *Dreier*, Bild und Recht, 2019, S. 60, 68, ebenso den Begriff der „Kontrolle über das eigene (Lebens)Bild“ und der „Kontrolle über das eigene Selbstbild“ verwendend; *Albers* geht von der Chance aus, das Wissen oder das „Bild“ anderer zu beeinflussen, vgl. *Albers*, Informationelle Selbstbestimmung, 2005, S. 576.

herrschbarkeit und Kontrollierbarkeit von Bildern personaler Identitäten in Frage.

Der für das Identitätsverwaltungsmodell anzuwendende Begriff der Kontrolle soll daher als Synonym für das Herrschaftsrecht über die personenbezogenen Informationen verstanden und folgend differenziert werden. Demnach wird die Kontrolle über die Entscheidung, was zum Privaten gehöre und was gegenüber einem Dritten zu eröffnen ist, angenommen.[291] In diesem absolut privaten Kontext wird gerade die „kontrollierte Unzugänglichkeit" als Kriterium des Privaten beschrieben.[292] Dazu gehört die räumliche und die informationelle Abgeschiedenheit, die den Kern der Selbstbestimmung ausmacht und die Kontrolle über private Entscheidungen und Handlungen umfasst.[293]

Gleichzeitig ist die Kontrolle nicht solipsistisch ausgestaltet, sondern die Kontrolle hat den Zugang, die Offenlegung und die Verwendung von persönlichen Informationen zum Gegenstand, so dass es sich bei der Kontrolle auch um ein Konzept der kommunikativen Privatheit handelt.[294] Mit der kommunikativen Ausprägung der Kontrolle soll von einer relativen Kontrolle ausgegangen werden. Danach kann über den Zugang und die Offenlegung persönlicher Informationen die Kontrolle ausgeübt werden, aber die Auswirkungen bei dem Kommunikationspartner liegen außerhalb des Kontrollierbaren und sind daher relativ. Dennoch unterliegt nach der Rechtsprechung des Bundesverfassungsgerichts auch dieser Bereich dem grundrechtlichen Schutz, denn es wird auch geschützt, dass das erlangte Wissen der Kommunikationspartner für das Individuum einigermaßen einschätzbar ist.[295] Darin kommt zum Ausdruck, dass die relative Kontrolle innerhalb der Kommunikation besteht und eine Vorhersehbarkeit von Gegenbildern geschützt wird. Entsprechend wird die Relativität der Kontrolle durch die rechtlichen Regelungen über den Schutz vor Beleidigungen und dem Recht am eigenen Bild etwa über das Einwilligungserforder-

---

291 *Maus*, Der grundrechtliche Schutz des Privaten im europäischen Recht, 2007, S. 21; von „Einflusschancen" und „Einflussmöglichkeiten" ausgehend, *Albers*, Informationelle Selbstbestimmung, 2005, S. 114, 122.

292 *Ders.*, Der grundrechtliche Schutz des Privaten im europäischen Recht, 2007, S. 34–37.

293 *Ders.*, Der grundrechtliche Schutz des Privaten im europäischen Recht, 2007, S. 37.

294 *Ders.*, Der grundrechtliche Schutz des Privaten im europäischen Recht, 2007, S. 162; *DeHert/Gutwirth*, in: Claes/Gutwirth/Duff (Hrsg.), Privacy and the criminal law, 2006, 61 (74 f.)

295 BVerfGE 65, 1 (43).

nis nach § 23 KUG geschützt, so dass von einem Konzept der absoluten Kontrolle über die Privatheit nicht ausgegangen werden könne.[296]

Demnach soll in das Identitätsverwaltungsmodell die Kontrolle über die personale Identität in relativer Hinsicht einbezogen werden. Denn die Informationen über die personale Identität unterliegen der relativen Kontrolle, wohingegen die Datensätze zu dieser absolut kontrollierbar sein können. Aufgrund des mit dem Phänomen *Big Data* einhergehenden Bedarfs, die Kontrollierbarkeit über Profilinhalte und Scoringwerte wiederherzustellen, erscheint die grundrechtlich begründete Beherrschbarkeit und absolute Kontrolle mit Hilfe eines Eigentumsrechts an Daten naheliegend, aber möglicherweise nicht problemlösend. Im Folgenden soll demnach ein Konzept der absoluten und relativen Kontrolle nachvollzogen werden.

II. Absolute Kontrolle

Die absolute Kontrolle über die personalen Identitäten kann sich aus einem Konzept des Dateneigentums in Gestalt eines Verfügungsrechts über die Bilder personaler Identitäten ableiten lassen (1.). Ein solches Konzept könnte zu einem rechtlichen Schutzmechanismus führen, der den *Big Data*-Phänomenen am ehesten Rechnung trägt. Gleichwohl fügt sich eine Kommerzialisierung des allgemeinen Persönlichkeitsrechts in Anbetracht der absolut wirkenden informationellen Selbstbestimmung in das bestehende Datenschutzrecht schwerlich ein, so dass sich die absolute Kontrolle in Gestalt eines Zugangsrechts zu personalen Identitäten für das Identitätsverwaltungsmodell als geeignet erweisen kann (2.).

1. Eigentumsrecht an Daten?

Der Kontrollbegriff in der DSGVO lässt sich mit einem Konzept des Eigentumsrechts an Daten in Verbindung bringen, zumal in der englischsprachigen Fassung des EWG 68 S. 7 der Begriff „*own*" verwendet wird. Gerade unter Einbeziehung der *Big Data*-Phänomene und des Internets der Dinge wird das Konzept des Dateneigentums als ein Lösungsmechanismus gegenüber bestehenden Schutzeinbußen gesehen.[297] Grundsätzlich haftet

296 *Whitman*, Yale L. J. 2004, 1151 (1169, 1199).
297 *Janeček*, CLSR 2018, 1039 (1040 f).

jedoch einem Eigentumsrecht über personenbezogene Daten ein fragwürdiger Gehalt an, da mit dem Versuch der Kommerzialisierung von Daten auch die Kommerzialisierung des allgemeinen Persönlichkeitsrechts und der Unantastbarkeit der Menschenwürde einhergeht. Gleichzeitig ist die Verfügung über absolute grundrechtliche Positionen im Zivilrecht anerkannt, so dass eine eigentumsähnlich ausgestaltete Position über Daten als sonstiges Recht nach § 823 Abs. 2 BGB angenommen wird und das praktische Bedürfnis nach einem umfassenden Schutz des Rechts auf informationelle Selbstbestimmung diese Einordnung rechtfertige.[298] Weiter wird das Dateneigentum als Konstruktion des Treuhandeigentums diskutiert, wonach über die Einwilligung hinaus eine Treuhandabrede geschlossen werden könnte und der Verantwortliche die personenbezogenen Daten als vermögenswertes Gut gewinnbringend einsetzen müsste, so dass zwischen einem effektiven Kontrollrecht über Daten aus ökonomischer Perspektive („*economic property right*") und dem rechtlich zugewiesenen Verfügungsrecht („*legal property right*") differenziert werden würde.[299] Dagegen lässt sich jedoch anführen, dass Daten nicht automatisch ein Wert zukommt, was aber die Voraussetzung für ein Konzept des Dateneigentums wäre. So lässt sich anhand eines Berechnungsbeispiels über den Wert von personenbezogenen Daten in sozialen Medien ein geringer Wert feststellen: Denn die Übernahme etwa von *Whats-App* durch *Facebook* für ca. 18 Milliarden Dollar hätte einen Datenwert von 42 Dollar pro Nutzer-Konto zur Folge und der Wert von Benutzerdaten auf dem Schwarzmarkt würde wenige Cent für ein Email-Konto betragen.[300] Nach diesem Beispiel erscheint der Auszahlungsbetrag für die Verarbeitung personenbezogener Daten nicht ansprechend genug, um damit eine Schutzsteigerung für die informationelle Selbstbestimmung der Betroffenen insgesamt herbeiführen zu können.

Weiter sieht das von *Janeček* entwickelte Konzept über ein Eigentumsrecht an Daten einen aktiven Teil, der die Kontrolle umfasst, und einen passiven Teil, der den Schutz der Daten umfasst, vor.[301] Hinsichtlich des zu kontrollierenden Gegenstandes stellt sich die Frage nach der Bestim-

298 *Wagner*, in: Säcker (Hrsg.), Münchener Kommentar – BGB, 2015, Bd. 5, § 823 BGB Rn. 294–297.

299 *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, S. 138–140. Ebenso ein Ausschließlichkeitsrecht an Daten zugunsten des wirtschaftlich verantwortlichen Datenerzeugers in Gestalt von Nutzungsrechten begründend, vgl. *Specht*, CR 2016, 288.

300 *Bernau*, FAS vom 10.02.2019, 23.

301 *Janeček*, CLSR 2018, 1039 (1042).

mung des Kontrollgegenstandes. Dies stößt bei personenbezogenen Daten jedoch deswegen auf Schwierigkeiten, weil zum einen der Übergang von Daten zu Informationen fließend und zum anderen die Personenbeziehbarkeit kontextspezifisch ist, so dass die Daten allein als Eigentumsgegenstand in Betracht kämen.[302] Daher wird eine Regelung über ein Eigentumsrecht an Daten als unzureichende Lösung gesehen und vielmehr auf ein Dateneigentumskonzept abgestellt, nach dem auf die faktische Kontrollmöglichkeit etwa über das Recht auf Datenportabilität nach Art. 20 DSGVO abgestellt werde, der sog. *Bottom up*-Ansatz.[303] Dennoch ist bei diesem Ansatz die Abbildbarkeit der Kontrolle kaum realisierbar, da bei Systemen mit einem hohen Vernetzungsgrad und redundanten Speichersystemen die faktische Kontrollmöglichkeit kaum umzusetzen und der faktisch kontrollierte Datensatz kaum zu ermitteln ist.[304] Erschwerend kommt hinzu, dass bei der Annahme eines kontrollierbaren Datensatzes die Zuordnung zu einem Eigentümer erfolgen müsste. Dieser könnte sich nach dem Grundsatz des Erstbesitzes und nach den Grundsätzen der Publizität ableiten lassen, was aber aufgrund der kaum feststellbaren Publizität und der fehlenden Haptik und Visualität von Daten kaum realisierbar sei.[305] Neben den dogmatischen Hürden, ein Eigentumsrecht an Daten zu begründen, kommt das Wesen der informationellen Selbstbestimmung hinzu, einen Kommunikationsprozess als Grundbedingung der Persönlichkeitsbildung vorauszusetzen. Denn die Anknüpfung an den Kommunikationsprozess verhindert die eindeutige Zuordnung der faktischen Kontrolle, da die Kontrolle über Informationen relativ ist. Weiter könnten Daten nicht als Partikel des Selbst an Dritte überlassen und nach Belieben wieder zurückgegeben werden.[306]

Darin kommt gerade die von *Marsch*[307] angeführte dogmatische Problematik zum Ausdruck, dass im einfachen Recht keine Unterscheidung zwischen den Datenverarbeitungen durch die öffentliche und private Stelle vorgenommen werde. Denn die Datenverarbeitung durch öffentliche Stellen kann durch eine Ermächtigungsgrundlage gerechtfertigt sein, ohne dass es eines Momentes der Kontrolle in Gestalt einer Einwilligung durch den Betroffenen bedurfte. Ferner wird festgestellt, dass Informationsord-

302 *Ders.*, CLSR 2018, 1039 (1043, 1052).
303 *Ders.*, CLSR 2018, 1039 (1051).
304 *Ders.*, CLSR 2018, 1039 (1045).
305 *Ders.*, CLSR 2018, 1039 (1048–1050); *Kühling/Sackmann*, Rechte an Daten, 20. November 2018, S. 8
306 *Masing*, NJW 2012, 2305 (2307).
307 *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 103 f.

nungen nicht eigentumsanalog ausgestaltet sein können, da die Vielschichtigkeit von Informationsströmen und ihre gesellschaftlichen und ökonomischen Wirkungen mit einem Verfügungsrecht nicht ausreichend abbildbar sind.[308] Zudem könne ein Eigentumsrecht an Daten zu einer Steigerung der Marktmacht führen, wenn Intermediäre über einen hohen Datenbestand verfügen, was gerade aus wettbewerbsrechtlicher Perspektive zu vermeiden sei.[309] Insgesamt werde die Anknüpfung an den Begriff der Kontrolle des Betroffenen über seine Daten in der DSGVO daher mehr als rechtspolitische PR gesehen als die tatsächliche rechtliche Einräumung einer Kontrollmöglichkeit.[310]

Schließlich kann die Diskussion über ein Eigentumsrecht auch auf rechtskulturelle Einflüsse aus dem angelsächsischen oder angloamerikanischen Privatheitskonzept einer „*reasonable expectation of privacy*" zurückgeführt werden,[311] wonach ein Verfügungsrecht über die Preisgabe von persönlichen Informationen nahezuliegen scheint. Es kommt daher anstelle eines Verfügungsrechts über personenbezogene Daten das Zugangsrecht in Betracht, denn auch der strafrechtliche Schutz gegen das Ausspähen von Daten nach § 202a StGB setzt einen Schutz gegen den unbefugten Zugang zu Daten voraus.[312] Ein mögliches Verfügungsrecht an Daten kann demnach mit dem Zugangsrecht abgebildet werden, so dass das Zugangsrecht der Gegenstand absoluter Kontrolle wird. Somit sieht *Kühling* gegenüber einem Dateneigentumsrecht den Steuerungsbedarf auf der Ebene der Zugänglichkeit zu Informationen, denn zu der Freiheit, die eigenen Daten weiterzugeben, gehöre spiegelbildlich, dies genau nicht zu tun und keinen Zugang zu gewähren.[313]

2. Zugang als absolute Kontrolle

Dem Konzept der absoluten Kontrolle folgend, geht es um das Bestehen eines Zugangs zu den personenbezogenen Daten und der daraus ableitba-

---

308 *Reinhardt*, AöR 142 (2017), 528 (535 f.); *Kühling/Sackmann*, Rechte an Daten, 20. November 2018, S. 9; *Roßnagel*, in: Roßnagel/Abel (Hrsg.), Handbuch Datenschutzrecht, 2003, 3.4. Rn. 40; *Graf von Westphalen*, IWRZ 2018, 9 (13 f.).

309 *Drexl*, JIPITEC 2017, 257 (266) Rn. 36; *Bundeskartellamt*, Fallbericht vom 15.02.2019, Az.: B6-22/16.

310 *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 105.

311 *Jay*, Data protection law and practice, 2012, Rn. 2.66.

312 *Kühling/Sackmann*, Rechte an Daten, 20. November 2018, S. 13 f.

313 *Dies.*, Rechte an Daten, 20. November 2018, S. 20.

ren personalen Identität. Dabei ist zu differenzieren zwischen der inneren Dimension als Kontrollentscheidung[314] über die Zugangsgewährung und der äußeren Dimension als tatsächlichen Zugang über das Wissen eines Passwortes oder den Besitz eines Schlüssels. Von der äußeren Dimension des Zugangs ist die räumliche Dimension umfasst, nach der zwischen Privatheit und Öffentlichkeit zu differenzieren ist. Es kann darum gehen, Dritte vom Zugang zu privaten Räumen in örtlicher und informationeller Hinsicht auszuschließen.[315] Die innere Dimension umfasst die Entscheidung über die informationelle Selbstbestimmung in Gestalt der Gewährung des Zugangs zu den personenbezogenen Daten und der personalen Identität durch Dritte.

Das Konzept der absoluten Kontrolle über den Zugang in seiner äußeren Dimension ist im Folgenden maßgeblich und umfasst den Zugang durch Wissen oder Besitz. Ein Zugangssystem über Wissen erfolgt etwa durch die Kenntnis eines Passwortes, wohingegen der Zugang auch mit dem Besitz eines Schlüssels möglich ist und sich auf die Kontrolle der Informationsflüsse erstrecken kann.[316] Am Beispiel des Zahlungsverkehrs wird der Zugang mit Wissen und Besitz eingeräumt, wie es beim Einsatz der Bankkarte vereint wird und beim Online-Banking über das TAN-Verfahren die Transaktion durch Wissen des Passwortes und der TAN authorisiert wird. Daraus lässt sich die jeweilige Zugangsmöglichkeit zu einem Identitätsverwaltungssystem ableiten, bei dem der Zugang durch Wissen und Besitz gemeinsam angewendet und mit den Attributen der personalen Identität in Verbindung gebracht werden kann. Als technisches Zugangssystem in einem Identitätsverwaltungsmodell kommen insbesondere der elektronische Personalausweis als Authentifizierungssystem, ein Pseudonym zur persönlichen Identifikation und die elektronische Signatur in Betracht.[317] Entsprechend wurde in Südafrika ein Identitätsverwaltungssystem implementiert, welches für öffentliche und private Einrichtungen genutzt und als Authentifizierungs-, Identifizierungs- und Zahlungsmittel eingesetzt werden könne, ohne dass der Nutzer sein Kontroll- und Korrek-

314 *Maus*, Der grundrechtliche Schutz des Privaten im europäischen Recht, 2007, S. 82

315 *Ders.*, Der grundrechtliche Schutz des Privaten im europäischen Recht, 2007, S. 33 f.

316 *Smedinghoff*, Introduction to Online Identity Management, S. 7; *Sorge/Wethoff*, DuD 2008, 337; *Eichenhofer/Gusy*, in: Hornung/Engemann (Hrsg.), Der digitale Bürger und seine Identität, 2016, 65 f.; ingesamt zum Datenzugang, *Albers*, Informationelle Selbstbestimmung, 2005, S. 112.

317 *Sorge/Wethoff*, DuD 2008, 337 (338–341).

turrecht verliere, sog. „*smart cards*".[318] In dieser Art von Identitätsverwaltungskonzepten erscheint jedoch die Einbeziehung datenschutzrechtlicher Maßgaben fraglich. Entsprechend wird aber bei dem elektronischen Personalausweis die Stärkung der informationellen Selbstbestimmung durch die Möglichkeit eines kontrollierten Umgangs mit den Attributen durch den Ausweisinhaber angenommen.[319]

Darüber hinaus sei eine sektorspezifische Realisierung von einem Zugangsrecht möglich, wobei ein entsprechender Anspruch auf Zugang zu Intermediären mit marktbeherrschender Stellung wünschenswert wäre.[320] Folglich wurde das Zugangsrecht als Kontrolle und Informationsmöglichkeit gegenüber dem Intermediär „*Facebook*" in einer jüngeren erbrechtlichen Entscheidung des Bundesgerichtshofes[321] anerkannt. Danach wurden auch nicht-vermögensrechtliche Zugangsrechte zu einem *Facebook*-Benutzerkonto für vererblich erklärt. Hervorzuheben ist dabei, dass der Zugang zu dem gesamten Inhalt, einschließlich der inhaltlichen Kommunikationsdaten des Benutzerkontos, auf die Erben übergegangen ist und ein eingeschränkter Zugang zu dem im Gedenkzustand befindlichen „Datenfriedhof" dem erbrechtlichen Grundsatz der Universalsukzession nicht entspräche.[322] Dabei wird in der Urteilsbegründung der Vergleich zu einem Girovertrag vorgenommen, der ebenfalls im Wege der Gesamtrechtsnachfolge auf die Erben übergehe.[323] Folglich können als Zugangssysteme das Wissen über das Passwort und der Besitz eines Schlüssels auf die Erben übergehen.[324] Maßgeblich sei die Vererblichkeit des Zugangsrechtes und nicht der Umstand, dass auf dem Benutzerkonto personenbezogene Daten und Kommunikationsdaten aus der Privatsphäre gespeichert sind, denn das Erbrecht erfasst nicht den Schutzgehalt der informationellen Selbstbestimmung, wie es der BGH über die nicht Vererblichkeit von Geldentschädigungsansprüchen bei der Persönlichkeitsverletzung bereits entschieden habe.[325]

Weiter berührt die absolute Kontrolle über den Zugang zu personenbezogenen Daten und damit der personalen Identität in inhaltlicher Hinsicht

---

318 *Black*, Cornell Int'l LJ 34 (2001), 397 (431).
319 *Hornung/Möller*, Passgesetz, Personalausweisgesetz, 2011, § 18 PAuswG Rn. 5.
320 *Kühling/Sackmann*, Rechte an Daten, 20. November 2018, S. 22; *Drexl*, JIPITEC 2017, 257 (276) Rn. 101.
321 BGH, Urt. v. 12.07.2018 – III ZR 183/17.
322 BGH, Urt. v. 12.07.2018 – III ZR 183/17 Rn. 17–30.
323 BGH, Urt. v. 12.07.2018 – III ZR 183/17 Rn. 36.
324 BGH, Urt. v. 12.07.2018 – III ZR 183/17 Rn. 49–50.
325 BGH, Urt. v. 23.05.2017 – VI ZR 261/16.

die grundsätzliche Frage, *ob* der Zugang von den Intermediären eingeräumt wird. Weiter wird sich die Frage stellen, *wie* im Einzelnen die Zugangsgewährung ausgestaltet sein wird, und welches Bild der personalen Identität das Individuum einsehen darf. Folglich wird die Kontrolle über personenbezogene Daten und der Zugang zu den personalen Identitäten von den wirtschaftlichen Interessen des Intermediärs geprägt sein und kann im Einzelnen durch die Interessen der Intermediäre, wie es die oben genannte *Facebook*-Entscheidung belegt, erschwert werden. Weiter lässt sich dies im Zusammenhang mit personalisierter Werbung nachweisen, da sich mit der Werbung eine Wertsteigerung der personenbezogenen Daten für den Verantwortlichen herbeiführen lässt, den Betroffenen jedoch der Zugang zu den entsprechenden Profilen oder Geschäftsmodellen verwehrt bleibt.[326] Auch hierbei lässt sich eine Diskrepanz zwischen den generierbaren Erkenntnissen aus den personenbezogenen Daten und dem tatsächlichen Zugang zu diesen konstatieren.

3. Zwischenergebnis

Die absolute Kontrolle über personenbezogene Daten kann weder aus dem bestehenden Recht noch aus dem Eigentumsrecht an Daten begründet werden. Damit können Daten als Kontrollgegenstand ausgeschlossen werden, es sei denn, sie fungieren als Schlüssel mit dem der Zugang zu personenbezogenen Daten gewährt wird. Denn die absolute Kontrolle in einem Identitätsverwaltungsmodell lässt sich hinsichtlich des Zugangs zu der personalen Identität und ihren Teilidentitäten abbilden. Danach kann die absolute Kontrolle über das Wissen und den Besitz die Zugangserlangung ermöglichen, wie es etwa bei beim Einsatz des elektronischen Personalausweises, der elektronischen Signatur oder bei Bankgeschäften mit dem Einsatz einer Karte oder eines Passwortes der Fall ist.

III. Relative Kontrolle

Die relative Kontrolle ist aus dem kommunikativen Vorgang der Interpretation und der Erkenntniserlangung aus Daten nach dem Erkenntnismodell abzuleiten. Danach besteht zwar eine absolute Kontrolle über die Da-

326 Zur Methode der Score-Bestimmung als Geschäftsgeheimnis, BGHZ 200, 39 (47) – SCHUFA.

ten, die Interpretation dieser und die Erkenntniserlangung in Gestalt von Wissen unterliegt aber der Perspektive und den *Instruktionen* des interpretierenden und lernenden Kommunikationspartners. Demnach liegt die Kontrolle in informationeller Hinsicht vor, wenn über die Erkenntnisse von Dritten und die Gegenbilder eine Einflussnahmemöglichkeit besteht. Diese Einflussnahmemöglichkeit stelle eine Ausprägung des selbstbestimmten Verhaltens über die informationelle Privatheit dar.[327]

Dennoch sind einmal offengelegte Informationen in ihren Interpretationsmöglichkeiten kaum mehr beherrschbar, denn die Offenlegung der Informationen gegenüber dem Kommunikationspartner bewirkt den Verlust der Einflussmöglichkeiten auf diese Informationen und Erkenntnisse. Vergleichbar mit einem Brief, können Nachrichten kontrolliert versendet werden, demgegenüber unterliegt nicht der Kontrolle, wer die Inhalte zur Kenntnis nimmt und seine Rückschlüsse daraus zieht. Demnach kann mit der Einwilligung nach Art. 6 Abs. 1 a) DSGVO zwar die absolute Kontrolle über die Erklärung ausgeübt werden, aber die damit einhergehende Rechtfertigung über die Verarbeitung personenbezogener Daten erlaubt zugleich die vielfältigen Interpretationsmöglichkeiten durch den Verantwortlichen. Mit der Einwilligung werden daher Informationen preisgegeben, die irreversibel in ihren Auswirkungen bis hin zur möglichen Ausübung der Betroffenenrechte sein können. Somit ist ab dem Vorliegen der Rechtfertigung über den Datenverarbeitungsvorgang der Datenzyklus über die personale Identität begründet und es können folglich für diesen Zeitraum im Rahmen der Zweckmäßigkeit die Informationen über die Person generiert werden, ohne dass eine Kontrollmöglichkeit besteht.

Im Rahmen der relativen Kontrolle über die Informationen und das Wissen bleibt die Möglichkeit der Kontrolle durch *Instruktionen* über die konkrete Ausführung des Interpretations- und Lernvorgangs. Denn nicht jedes Erlernen in einem Kontext ist zulässig, wie es die *Instruktionen* aus § 81g StPO zur DNA-Identitätsfeststellung belegen, wonach aus der DNA allein das Identifizierungsmuster und das Geschlecht als Erkenntnis generiert werden dürfen und darüber hinaus keine weiteren Erkenntnisse gerechtfertigt wären. Somit gilt für die relative Kontrolle personaler Identitäten der Schutzmechanismus über *Instruktionen*, der für das Identitätsverwaltungsmodell herangezogen werden soll.

---

327 *Maus*, Der grundrechtliche Schutz des Privaten im europäischen Recht, 2007, S. 40.

IV. Kontroll-Paradoxon

Dem Konzept der Kontrolle personaler Identitäten für das Identitätsverwaltungsmodell könnte entgegenstehen, dass die Einräumung der Kontrolle nicht zwingend zu einer Steigerung, sondern möglicherweise zu einer Gefährdung des Schutzes der informationellen Selbstbestimmung führt.

Mit verhaltensökonomischen Untersuchungen zur Kontrolle des Nutzers bei der Verarbeitung personenbezogener Daten konnte ein Paradoxon festgestellt werden, wonach die Begründung der Kontrolle über personenbezogene Daten zu einer Einbuße des Schutzes führe.[328] Es wurde mit statistischen Untersuchungen nachgewiesen, dass differenzierte Privatheitseinstellungen und die damit einhergehende Kontrolle, eine gesteigerte Bereitschaft beim Nutzer auslöse, Informationen offenzulegen.[329] Dieses Phänomen wurde besonders deutlich, wenn zuvor das Bestehen der Kontrollmöglichkeit zugesichert wurde.[330] Aufgrund dieser Untersuchungen könne eine Schutzsteigerung durch die Erweiterung oder Begründung eines Kontrollkonzeptes nicht angenommen werden, vielmehr liege ein Kontroll-Paradoxon vor.[331]

Sobald dieses Ergebnis auf die Einwilligung übertragen wird, lässt sich mit dem Vorgang der Einwilligung bereits die Gefahr einer die Privatheit einschränkenden Handlung erblicken, die zu einer Absenkung des individuellen Privatheitsniveaus führen kann. Denn nach den dargestellten Untersuchungen von *Brandimarte/Acquisti/Loewenstein* könne die Einwilligung eine gesteigerte Bereitschaft auslösen, Informationen offenzulegen oder überhaupt einzuwilligen. Folglich soll festgehalten werden, dass mit einer Steigerung des Kontrollniveaus nicht gleichzeitig die Steigerung des Schutzes der Privatheit einhergeht, vielmehr folgt mit der Kontrollmög-

328 *Brandimarte/Acquisti/Loewenstein*, Social Psychological and Personality Science 4 (2013), 340.

329 *Dies.*, Social Psychological and Personality Science 4 (2013), 340 (344, 346) mit Verweis auf einen „Post" von Marc Zuckerberg mit dem Titel „*Giving you more control of your privacy*". Es konnte festgestellt werden, dass mit der suggerierten Kontrollmöglichkeit durch die Privatheitseinstellungen tatsächlich der Eindruck von Kontrolle erweckt werden könne, dieser aber irreführend sei, da das Kontroll-Paradoxon bei der eingeräumten Schutzmöglichkeit mit Privatheitseinstellungen wirken könne.

330 *Dies.*, Social Psychological and Personality Science 4 (2013), 340 (344).

331 *Dies.*, Social Psychological and Personality Science 4 (2013), 340 (346).

lichkeit eine Überschätzung der tatsächlichen Einflussmöglichkeit.[332] Denn aufgrund der Relativität von Informationen und Wissen, kann die absolute Kontrolle allein über Daten ausgeübt werden. Die ausdrückliche Einbeziehung eines Kontrollkonzeptes lenkt folglich von dem tatsächlichen Risiko für den Schutz der personenbezogenen Daten ab. Denn es wird die Illusion über die faktische Kontrollmöglichkeit von Interpretationen und Erkenntnissen aus Datenverarbeitungen geschaffen.

V. Übertragung auf das Identitätsverwaltungsmodell

In einem Identitätsverwaltungsmodell bedarf es der Kontrolle über die Realisierung der personalen Identität und ihrer Teilidentitäten, damit das Individuum seine informationelle Selbstbestimmung ausüben kann. Dabei bedeutet ein Kontrollkonzept die Vorverlagerung des Schutzes der personalen Identität, mit dem einer Verselbstständigung des Selbstbildes durch Fremdbilder begegnet und damit dem datenschutzrechtlichen Vorfeldschutz entsprochen wird. Dem ist immanent, dass bei einem Identitätsverwaltungsmodell das Individuum im Zentrum stehen muss, sog. „*user centric identity management*“[333]. Entsprechend kommen verschiedene Ausprägungen der Identitätsverwaltung in Betracht.

Es kann um die Kontrolle von Benutzerkonten mit der Authentifizierung oder Identifizierung des Nutzers im Sinne einer *Berechtigungsverwaltung* gehen. Weiter kommt aus der Perspektive des Verantwortlichen die Verwaltung von Profilen und Kommunikationsdaten in Betracht.[334] Schließlich kann ein kontextabhängiges Rollen- und Pseudonym-Management etwa mit biometrischen Daten oder *Single Sign-On*-Lösungen als Identitätsverwaltungskonzept dienen.[335] Gleichwohl lässt sich in diesen Ausprägungen jeweils der Datensatz als Gegenstand der Kontrolle im Identitätsverwaltungssystem über das Wissen eines Passwortes als *Idem*-An-

---

332 *Dies.*, Social Psychological and Personality Science 4 (2013), 340 (346).

333 *Unabhängiges Landeszentrum für Datenschutz* (ULD), Identity Management Systems (IMS), 2004, S. 30.

334 *Schallaböck*, in: Hornung/Engemann (Hrsg.), Der digitale Bürger und seine Identität, 2016, 103 (121): Dabei wird auf die Identitäts-*Managementsysteme* der US-amerikanischen und britischen Geheimdienste verwiesen.

335 *Ders.*, in: Hornung/Engemann (Hrsg.), Der digitale Bürger und seine Identität, 2016, 103 (107–109); *Unabhängiges Landeszentrum für Datenschutz* (ULD), Identity Management Systems (IMS), 2004, S. 19; *Hornung/Engemann* (Hrsg.), Der digitale Bürger und seine Identität, 2016, S. 18.

teil einer personalen Identität feststellen, ohne die Ausprägungen einer personalen Identität in ihrem dynamischen *Ipse*-Anteil im online-Kontext einzubeziehen. Danach soll im Identitätsverwaltungsmodell die Realisierung der Interpretations- und Erkenntnisgehalte zum Gegenstand eines Kontrollkonzeptes im online-Kontext werden. Dies würde einen gesteigerten Einfluss auf die Bilder personaler Identitäten aus Profilbildungen ermöglichen. Folglich würden die generierbaren Erkenntnisse aufgrund ihrer Rück- und Auswirkungen auf das Individuum einbezogen werden und der Selbstbestimmung unterliegen.

Daraus lässt sich der Bedarf nach einer Übertragung des Kontrollgegenstandes auf den Zugang zu den Daten, Informationen und dem Wissen über eine personale Identität ableiten. Denn die Analysen über ein Eigentumskonzept an Daten haben dargelegt, dass ein Eigentumsrecht an Daten nicht zu einer Schutzsteigerung führt und rechtlich schwerlich abzubilden ist. Folglich soll ein Kontrollkonzept als ein Zugangsrecht für ein Identitätsverwaltungsmodell eingesetzt werden, um die Kontrolle über die personale Identität in absoluter und relativer Hinsicht zu ermöglichen. Damit würde die Kritik an einem Kontrollkonzept, dass aufgrund redundanter Speichermöglichkeiten *de facto* über die Datensätze keine Kontrolle ausgeübt werden könne,[336] ins Leere laufen. Denn es ginge nicht um die Kontrolle über die Daten, sondern um die Kontrolle über den Zugang zu Daten und den mit ihnen verbundenen Erkenntnissen.

Gleichwohl konnte aufgrund verhaltensökonomischer Untersuchungen belegt werden, dass die Kontrollmöglichkeit zu einer gesteigerten Bereitschaft der Offenlegung von Informationen führe und das Kontroll-Paradoxon wirke. Demnach könne bei einem ausdifferenzierten Kontrollkonzept von einem neuen Risiko ausgegangen werden, da mit der Einwilligung zwar die Kontrolle ausgeübt wird, aber damit eine gesteigerte Bereitschaft zur Offenlegung privater Informationen einhergehen kann. Danach wäre von einem „vollständigen Kontrollverlust“[337] auszugehen, der über ein differenziertes Zugangs- und Iterationskonzept kompensiert werden könnte. Damit wird dem Einzelnen die Möglichkeit eingeräumt, in einem iterativen und dialogischen Verfahren infolge des Zugangs zu den personenbezogenen Daten und personalen Identitäten, Einfluss auszuüben. Demnach würde es der informationellen Selbstbestimmung im online-Kontext entsprechen, eine erhöhte Differenzierung möglicherweise mit einem iterati-

336 *Veil*, NVwZ 2018, 686 f.; *Spindler*, in: Verhandlungen des 69. Deutschen Juristentages, 2012, S. F 20.
337 BVerfGE 120, 274 (336 f.).

ven und dialogischen Prozess vorzunehmen, welches der weitere Gegenstand dieser Untersuchung sein soll.

VI. Zwischenergebnis

Die Kontrolle personaler Identitäten erfolgt in absoluter Hinsicht über den Zugang und in relativer Hinsicht in einem dialogischen Verfahren. Dabei sollte die Kontrolle personaler Identitäten ein differenziertes Zugangs- und Iterationskonzept umfassen, um eine Schutzsteigerung herbeizuführen. Demnach ist ein dialogisches Verfahren erforderlich, was über *Instruktionen* für die Informations- und Wissenserlangung verfügt. Damit soll ein differenzierter Schutz der informationellen Selbstbestimung gewährleistet werden.

Insgesamt ist in dem Identitätsverwaltungsmodell das Kontroll-Paradoxon einzubeziehen, wonach die Kontrollmöglichkeit zu einer Überschätzung der Einflussmöglichkeit führen kann. Somit bedarf es der Differenzierung von personalen Identitäten, um Gegenstände der relativen Kontrolle und der *Instruktionen* für das Identitätsverwaltungsmodell bestimmen zu können.

D. Agenten personaler Identitäten

Zu den personalen Identitäten gehört das Verhalten des Individuums,[338] so dass sich die Frage nach der Handlungsträgerschaft im einfachen Recht stellt. Diese wirkt sich darauf aus, dass sich das Verhalten als identitätsbildend einordnen lässt und die Zurechnung des Verhaltens zu dem Individuum voraussetzt. Indem das Recht mit Fiktionen arbeitet, wird dem Individuum nach den zivilrechtlichen Vorschriften zur Rechtssubjektivität die Rechts- und Geschäftsfähigkeit gemäß §§ 1, 105 ff. BGB verliehen und das Individuum erlangt im Rechtsverkehr die Handlungsfähigkeit, was auch über Stellvertretungsregeln erfolgen kann.[339] Darin kommt eine Prinzipal- und Agentenstruktur zum Ausdruck, bei der das Individuum als Prinzipal über die rechtlich anerkannte Handlungsträgerschaft wirkt. Vorliegend sollen für ein Identitätsverwaltungsmodell die Handlungsträgerschaften herausgearbeitet werden, unter denen sich eine Übertragung der bestehen-

338 2. Teil, A., II., 2.
339 *Zippelius*, Das Wesen des Rechts, 62012, S. 27.

den Prinzipal- und Agentenstruktur auf den online-Kontext vornehmen lässt. Dabei sollen die bestehenden Prinzipal- und Agentenstrukturen aus den rechtlichen Konzepten im offline-Kontext herangezogen werden.

Für die Begründung einer graduellen Handlungsträgerschaft sind die zivilrechtlichen Stellvertretungsregeln und das Strafprozessrecht als Grundlage für einen Transfer zu einer elektronischen Handlungsträgerschaft heranzuziehen. Nach dem zivilrechtlichen Stellvertretungsrecht kann eine graduelle Steigerung der Kontroll- und Steuerungsmöglichkeit des Prinzipals ausgehend von dem Boten, dem Verrichtungsgehilfen (§ 831 BGB), dem Erfüllungsgehilfen (§ 278 BGB) hin zu dem Stellvertreter (§§ 164 ff. BGB) erfolgen, wobei für deren Einordnung das Offenkundigkeitsprinzip und die Verkehrsanschauung maßgeblich sind. Ein Bote unterliegt hinsichtlich des *Ob* und *Wie* seiner Handlung dem höchsten Kontroll- und Steuerungsmaß durch den Prinzipal. Dieses nimmt beim Verrichtungsgehilfen ab, der in seiner Erfüllung weisungsgebunden ist, aber über einen Ausführungsspielraum verfügt. Demgegenüber ist der Erfüllungsgehilfe bei der Erfüllung des Schuldverhältnisses nicht weisungsgebunden. Das Kontroll- und Steuerungsmaß ist bei der Stellvertretung wiederum geringer, wobei der Umfang im Einzelnen von der gesetzlichen oder vertraglichen Vertretungsmacht abhängt und sich ebenfalls nach der Verkehrsanschauung richtet.

In strafprozessualer Hinsicht stellen klassische Prinzipal- und Agentenstrukturen solche aus § 110a StPO dar, wonach verdeckte Ermittler mit einem sich steigernden Identitätsveränderungsgrad in Ermittlungsverfahren eingesetzt werden. Mit der qualifizierten Legende nach § 110a StPO wird etwa eine neue Identität mit den entsprechenden Ausweispapieren und dem Lebenslauf begründet, wohingegen der gelegentlich nicht offen ermittelnde Polizeibeamte situativ ohne Legende auftritt.[340] Weiter wird zum Schutz von gefährdeten Zeugen oder deren Angehörigen eine vorübergehende Tarnidentität § 5 Abs. 3 ZSHG erstellt, wobei ausdrücklich keine Identitätsänderung vorgesehen ist.[341]

Aus diesen einfachrechtlichen Regelungsstrukturen lässt sich eine Differenzierung der personalen Identität ableiten, bei der das Individuum als Prinzipal den Agenten des Bildes der personalen Identität kontrolliert und steuert. Das Bild der personalen Identität als Agent wird dem Individuum als Prinzipal zugerechnet, so dass das Identitätsverwaltungsmodell aus

340 *Meyer-Goßner/Schmitt*, Kommentar, Strafprozessordnung, 2019, § 110a StPO Rn. 7 f., 4.

341 *Soiné/Engelke*, NJW 2002, 470 (474).

mehreren Agenten in Gestalt von Bildern personaler Teilidentitäten des Individuums besteht. Demnach verlangt die Identitätsverwaltung die Annahme, dass sie von einem Prinzipal als natürliche Person durchgeführt wird, wobei der Agent in Gestalt des Bildes der Identität über keine Rechtssubjektivität verfügt und aus einem elektronischen Ausführungsmechanismus besteht. Somit liegt eine kontextspezifische Steuerungs- und Kontrollmöglichkeit gegenüber dem elektronischen Agenten als Handlungsträger vor, die entsprechend den Regeln der Handlungsträgerschaft graduell erfolgen kann.[342]

Die Eigenschaften des Agenten können dahingehend variieren, dass der elektronische Agent intelligent reaktiv oder proaktiv handeln kann. Ein *proaktiver Agent* wäre lernfähig und könnte dem Prinzipal Entscheidungen vorschlagen, wohingegen ein reaktiver Agent ausführend wäre.[343] Wobei *Aamodt/Nygård* zwischen aktiven und passiven Agenten bei der Entscheidungsunterstützung danach differenzieren, ob eine passive assistierende Funktion oder eine aktive Unterstützung in der Entscheidungsfindung wahrgenommen werde.[344] Beide Umschreibungen sind von der graduellen Autonomie und Abhängigkeit zum Prinzipal gekennzeichnet, jedoch soll der Klarheit wegen im Folgenden der aktive und passive Agent als Begriffspaar angewendet werden. Von einem elektronischen Agenten, der aktiv ausgestaltet ist und hinsichtlich des *Ob* und *Wie* über einen dem Stellvertreter entsprechenden Entscheidungsspielraum verfügt, kann ein hohes Risiko für den Prinzipal ausgehen, welches ihm zugerechnet werden würde.

Die Einheit, die aus dem Prinzipal und elektronischen Agenten besteht, wird von *Teubner* als „Hybrid" bezeichnet, dem wiederum eine Rechtssubjektivität zukommen könne, wenn diese über eine eigene Intelligenz verfüge.[345] Damit könnte die Vorstellung einbezogen werden, dass bereits Informationsströmen unter bestimmten Bedingungen eine Personalität zukommt, was eine eigenständige rechtliche Schutzwürdigkeit begründen könnte. Dabei könne der elektronische Agent auch eine fragmentierte Rechtssubjektivität als Teilrechtsfähigkeit mit begrenzter Handlungskompetenz darstellen.[346] Demnach solle die graduelle Charakteristik der Prin-

342 *Sester/Nitschke*, CR 2004, 548 (550).
343 *Dies.*, CR 2004, 548; *Hoffmann-Riem*, AöR 142 (2017), 1 (30) mwN.
344 *Aamodt/Nygård*, Data & Knowledge Engineering 16 (1995), 191 (195).
345 *Teubner*, Zeitschrift für Rechtssoziologie 2006, 5 (14).
346 *Ders.*, Zeitschrift für Rechtssoziologie 2006, 5 (10–12).

zipal- und Agenten-Beziehung und ihre Lebensdauer in eine fragmentierte Rechtssubjektivität überführt werden.[347]

Folglich lässt sich für die Ausprägungen der personalen Identität im online-Kontext und die dazugehörenden Informationsströme eine separate fragmentierte Subjektivität zusprechen, die für das Identitätsverwaltungsmodell als weiteres Element in Gestalt eines elektronischen Agenten maßgeblich sein könnte. Dabei soll die rechtstheoretische Einordnung, ob es sich um eine neu begründete Rechtssubjektivität handelt, dahinstehen, denn vorliegend soll die Differenzierung der personalen Identität in eine Prinzipal- und Agenten-Struktur mit ihren Bestandteilen im online-Kontext für die Modellbildung entscheidend sein. Demnach können sich die statischen *Idem*-Anteile und dynamischen *Ipse*-Anteile einer personalen Identität in einem elektronischen Agenten abbilden. Weiter würde die elektronische Ausgestaltung des Agenten den Bedarf nach Transparenz über die Funktionalität auslösen, was über die Wahrung der Transparenzanforderungen gemäß Art. 12 Abs. 7 S. 2 DSGVO in maschinenlesbarer elektronischer Form erbracht werden könnte. Ebenso kommt der elektronische Agent als Vermittler auf der Mikroebene in Betracht und könnte über Software oder einen „*Smart Contract*" realisiert werden. Schließlich kann ein Agent in einem Identitätsverwaltungsmodell auf der Makroebene eingesetzt werden, wenn es um mögliche kontextspezifische Realisierungen personaler Identitäten geht.

E. Ergebnis: Kontrollierbare Erkenntnisse zur personalen Identität

Die Anforderungen an die Identitätsverwaltung richten sich primär nach den verfassungsrechtlichen und einfachrechtlichen Vorgaben, aus denen sich die Eigenschaften und Kriterien für ein Identitätsverwaltungsmodell ableiten lassen. Maßgebliche Anknüpfung für die Identität im einfachen Recht ist der Name, der im Zusammenhang mit dem elektronischen Rechtsverkehr um die elektronische Signatur ergänzt wurde. Folglich stellt die einfachrechtliche Regelung zur gestuften und sicheren Identifizierung gemäß Art. 8 Abs. 2 eIDAS-VO eine statische Dimension über kontextspezifische Vertrauens- und Sicherheitsniveaus von personalen Identitäten dar. Weiter wird die *vertrauliche und sichere Kommunikation* nach dem De-Mail-G geschützt, so dass die personale Identität in ihrem dynamischen *Ipse*-Anteil im Rahmen der Kommunikation einen rechtlichen Schutz im on-

347 *Ders.*, Zeitschrift für Rechtssoziologie 2006, 5 (24).

line-Kontext erfährt.[348] Ferner umfasst das verfassungsrechtliche und einfachrechtliche Schutzregime über die personale Identität das Erkenntnismodell, welches sich auf die personale Identität innerhalb eines Datenzyklus über eine Biographie anwenden lässt. Dabei ist einem Identitätsverwaltungsmodell immanent, dass es im Rahmen der informationellen Selbstbestimmung eine Steuerungs- und Kontrollmöglichkeit über die Daten, Informationen und das Wissen zu einer personalen Identität vorsehen muss. Gleichwohl ist nach dem Erkenntnismodell eine absolute Kontrolle ausgeschlossen, denn zwischen den Kommunikationspartnern ist der Datensatz der Gegenstand von kontextspezifischen Interpretations- und Lernprozessen, da in der Kommunikation das Gegenbild über die personale Identität nur bedingt beeinflusst werden kann und damit der relativen Kontrolle unterliegt.[349] Aus dem Erkenntnismodell lässt sich der mögliche Bedarf an einer prozeduralen Konkretisierung über die Entstehung der Bilder personaler Identitäten ableiten, damit der dynamische Charakter der biographischen personalen Identität und den damit verbundenen Erkenntnissen in das Identitätsverwaltungsmodell überführt werden kann.

Als erweiternde Dimension kommt die systemische Perspektive der Kommunikation hinzu, nach der die kontextspezifische Kommunikation in einem System erfolgt und sich der Bedarf an der Beobachtung des Systems stellt. Mit der Beobachtung des Systems wird dieses mit der Metaebene über den Datenzyklus erweitert und ermöglicht die übergeordnete Bewertung der Erkenntnisse über personale Identitäten. Dazu gehört die Einbeziehung der *Instruktionen* in das Identitätsverwaltungsmodell, damit die Erkenntnisse über eine personale Identität einem eigenen Schutzregime unterliegen und nicht beliebig generiert werden können. Die Gestaltung des Identitätsverwaltungsmodells verlangt demnach ein iteratives Modell etwa mit der Erteilung mehrerer Einwilligungen in einem Datenzyklus und der Einbeziehung von *Instruktionen* über die Bildung der personalen Teilidentitäten.[350]

Schließlich ist für die Identitätsverwaltung die Handlungsträgerschaft über die personale Identität maßgeblich. Diese lässt sich entsprechend zum Stellvertretungsrecht in einen Prinzipal, dem die Handlung zugerechnet wird, und den Agenten, der als Handlungsträger fungiert, differenzieren. Weiter können sich die statischen *Idem*-Anteile und dynamischen *Ipse*-Anteile einer personalen Identität in einem elektronischen Agenten vereinen

348 3. Teil, A., II.
349 3. Teil, A., III.
350 3. Teil, B., I. – II.

und den datenschutzrechtlichen Transparenzregeln unterliegen.[351] Ferner wurde eine Differenzierung der Agentenstruktur auf der Mikro- und Makroebene vorgenommen, bei der ein Agent auf der Mikroebene aus Software oder einem *Smart Contract* besteht und auf die Bildung personaler Identitäten einwirkt und auf der Makroebene eine Vermittlungsstruktur zur Verwaltung personaler Identitäten in Betracht kommt.

351 3. Teil, D.