6.Teil: Modell der Identitätsverwaltung

Für die Begründung des Modells der Identitätsverwaltung sollen aus den bestehenden Analysen die maßgeblichen Voraussetzungen herausgearbeitet werden. Diese stehen den bisherigen Konzepten der Identitätsverwaltung als Berechtigungsverwaltung entgegen und legen einen Paradigmenwechsel zum dynamischen Identitätsbegriff nahe. Daher sollen nach einer Einführung (A.) die Modellvoraussetzungen der Identitätsverwaltung konkretisiert werden (B.) und in ein Konzept der verhandelten personalen Identität mit einem dezentralen Zugang überführt werden (C.).

A. Einführung

Für die Identitätsverwaltung wurden die Grundlagen herausgearbeitet und die Anforderungen aus dem IKT-Recht benannt. Weiter wurde eine spieltheoretische Modellierung vorgenommen, damit die ökonomischen Wirkungen gegenüber den persönlichen Informationen in dem Lösungskonzept ebenfalls berücksichtigt werden. Dies führte zu der Begründung des technischen Mediationsagenten, der *de lege ferenda* Gegenstand einer Regelung werden oder aber im „Schatten des Rechts" wirken könnte. Insoweit wurden rechtliche und ökonomische Modellierungen für ein Identitätsverwaltungsmodell vorgenommen, die nunmehr in eine systematische Perspektive in Gestalt einer technischen Infrastruktur eingeordnet werden. Danach konnten in den Grundlagen des 2. Teils dieser Arbeit die grundrechtlichen Anforderungen an den Begriff der personalen Identität festgelegt und im 3. Teil die Anforderungen an die Identitätsverwaltung beschrieben werden. Diese Anforderungen sollten, auch wenn sie ideell sein mögen, in eine technische Infrastruktur überführt werden. Die technische Infrastruktur sollte die rechtlichen und ökonomischen Perspektiven einbeziehen und im Zusammenhang mit den Realweltphänomenen der Selbstbestimmung und Selbstdarstellung der natürlichen Person im offline-Kontext stehen. Daher sollen aus den erarbeiteten rechtlichen und ökonomischen Perspektiven übergeordnete systematische Voraussetzungen der Identitätsverwaltung im online-Kontext beschrieben werden.

B. Modellvoraussetzungen der Identitätsverwaltung

Mit der bisherigen Einordnung der Identitätsverwaltung sind die Paradigmen einer statischen und dauerhaften Dimension der personalen Identität in ihren *Idem*-Anteilen verbunden, die im IKT-Kontext über ein *Berechtigungskonzept* verwaltet werden können. Aus den herausgearbeiteten IKT-rechtlichen Phänomenen ergibt sich jedoch eine Erweiterung der personalen Identität auf den Datenzyklus in seinen dynamischen und temporären Dimensionen des Begriffs der Identität in ihrem *Ipse*-Anteil. Unter Einbeziehung der ökonomischen Auswirkungen IKT-rechtlicher Phänomene erscheint eine Schwerpunktverschiebung auf den relationalen und kommunikativen Gehalt der Identität maßgeblich, so dass die Identitätsverwaltung eine Erweiterung verlangt. Dazu gehört, dass die bisherige Perspektive einer Berechtigungsverwaltung einem Perspektivwechsel unterzogen wird und auf eine kommunikationsbezogene, dynamische und temporäre Dimension der personalen Identität abzustellen ist. Dieser Perspektivwechsel[858] soll im Folgenden anhand der herausgearbeiteten Modellvoraussetzungen aufgeführt werden, und als Zuspitzung der Ergebnisse aus den rechtlichen und ökonomischen Analysen fungieren. Für ein Identitätsverwaltungsmodell wurden die Voraussetzungen herausgearbeitet, wonach die personale Identität zugänglich sein muss (I.), verhandelbar sein soll (II.) und dezentral auszugestalten ist (III.).

I. Paradigmenwechsel zum Identitätszugang

Die Ausprägungen der personalen Identität wurzeln bereits in der Legaldefinition zu den personenbezogenen Daten gemäß Art. 4 Nr. 1 DSGVO und in den Regelungen zu den Profilen und besonderen Kategorien personenbezogener Daten, aus denen sich jeweils ein eigenständiger kontextbezogener Erkenntnisgehalt generieren lässt. Gleichwohl gehört zu den Kriterien der Identitätsverwaltung die Kontrolle über die personalen Identitäten, die mit dem Zugang realisiert wird. In Anbetracht der Kontextbezogenheit und des Kommunikationszusammenhangs von personalen Identitäten können diese nur in relativer Hinsicht der Kontrolle unterliegen, so dass für eine ausgeprägte Steuerung und Kontrolle der Zugang Voraussetzung ist.[859] Zwar unterliegt auch die Generierung der Attribute von personalen

858 *Kuhn*, Die Struktur wissenschaftlicher Revolutionen, 2003, S. 137–155.
859 3. Teil, C., II., 2.

Identitäten zu Beginn des Datenzyklus der absoluten Kontrolle, jedoch verlagert sich die Kontrolle auf die Transparenz gemäß Art. 12 DSGVO und das Auskunftsrecht als Zugangsrecht gemäß Art. 15 DSGVO.[860] Ebenso spricht der Erlaubnisvorbehalt der Identitätsverwaltung für einen Kontrollschwerpunkt bei der Einwilligung, obwohl diese faktisch an Schutzwirkung gegenüber der informationellen Selbstbestimmung des Betroffenen einbüßt.[861] Entscheidend ist der Zugang zu den personenbezogenen Daten als Kontrollgegenstand gegenüber der scheinbaren Kontrolle durch die rechtfertigende Einwilligung, wie sie in dem Konzept „myneData"[862] beschrieben wird.

Es ergibt sich daraus der Bedarf nach einer verlagerten Betrachtung auf die Rechte nach der Rechtfertigung, die mit dem Zugang zu den kontextspezifischen personalen Identitäten über ein bereits beschriebenes *Dashboard-System* erfolgen kann. Dabei wird die Ausübung der informationellen Selbstbestimmung mit einem iterativen Zugangskonzept gefördert, das den Anknüpfungspunkt für die kontextbezogene Bündelung des Zugangs zu den personalen Identitäten mit einer spezifischen Vertrauens- und Sicherheitsstufe bilden kann, sog. (online) „*Identity Ecosystem*".[863] Voraussetzung dafür wäre, dass innerhalb des Kontextes der jeweiligen Vertrauens- und Sicherheitsstufe, wie sie gemäß Art. 8 Abs. 2 eIDAS-VO abgebildet ist,[864] die Interoperabilität über die personalen Identitäten hergestellt wird. Daher wäre eine gesicherte Plattform innerhalb der Vertrauens- und Sicherheitsstufe mit einem hohen Schutzniveau für personale Identitäten denkbar, welches als plattformbasiertes „*Identity Ecosystem*" fungieren würde. In diesem stünde zunehmend die Entscheidung der natürlichen Person im Vordergrund, inwieweit in den jeweiligen Vertrauens- und Sicherheitsstufen die personalen Identitäten verwaltet werden.

Darin liegt eine Verlagerung der Informationsmacht vom Verantwortlichen auf den Betroffenen, so dass bei dem Identitätszugang von einem nutzerzentrierten Ansatz auszugehen ist. Gleichzeitig steht der nutzerzentrierte Ansatz in Relation zu dem Verantwortlichen, so dass die Zugangsgewährung aufgrund der widerstreitenden Interessenlagen zum Gegenstand der Verhandlung werden sollte. Dafür wäre es denkbar, den Zugang

860 4. Teil, B., II., D., I.
861 4. Teil, C.
862 In „myneData" ist ein Datencockpit mit der Kontrollmöglichkeit über die Einwilligung vorgesehen, *Matzutt/Müllmann/Zeissig u.a.*, in: Eibl/Geadke (Hrsg.), INFORMATIK 2017, 1073 (1081).
863 2. Teil, A., III.
864 2. Teil, B., II., 2., b).

auch vertraglich durch Einräumung von Rechten und Pflichten zu regeln, damit die Verhandlungspositionen aneinander angeglichen werden können. Gleichzeitig bleibt für die Gewährleistung des Zugangs zu personalen Identitäten aus wettbewerbsrechtlichen Gründen eine staatliche Intervention nicht ausgeschlossen. Dabei geht es darum, dem Betroffenen eine effektive Verhandlungsmöglichkeit über den *Ipse*-Anteil der personalen Identität im Rahmen des Selbstdatenschutzes einzuräumen.

Um eine Abkehr von einem Zugang zu den personenbezogenen Daten und eine Hinwendung zu einem Identitätszugang vornehmen zu können, bedarf es durch den Verantwortlichen einer Bereitstellung der personenbezogenen Daten in einer die personale Identität darstellenden Form. Damit läge eine Maßnahme zum Ausgleich der Informationsasymmetrie und erweiterten Transparenz zugunsten des Betroffenen vor. Denn mit dem Identitätszugang wird die kontextbezogene personale Identität zunächst erkennbar und kann anschließend Gegenstand der individuellen Risikobewertung und Entscheidung über die Geltendmachung von Rechten werden. Ebenso könnte in einer Bereitstellung der Datensätze als personale Identität bereits ein Teil der Begründung und Erklärung der automatisierten Datenverarbeitung im Rahmen der Informationspflichten gemäß Art. 13 Abs. 2 f) DSGVO liegen, die Bestandteil eines „*identity management by design*"-Konzeptes werden könnten.

II. Paradigmenwechsel zur verhandlungsfähigen Identität

Von der Zugangs- und Berechtigungsverwaltung aus der informationstechnischen Perspektive abgesehen, geht es bei den personalen Identitäten um die kommunikative Ausprägung. Diese stellt sich infolge des dialogischen Prozesses zwischen *Idem*- und *Ipse*-Anteil der personalen Identität als ein narratives Selbstbild dar, welches wiederum zum Gegenstand der Kommunikation wird und von dem Empfänger als Gegenbild wahrgenommen wird. Infolgedessen kann sich der kommunikative Ablauf wiederholen und sich die Relation zwischen Selbstbild und Gegenbild einer Verhandlung über die personale Identität gleichen. Demnach bedarf es der Schwerpunktverlagerung von der personalen Identität hin zu den im Rahmen der Kommunikation verhandelten Bildern personaler Identitäten. Diese Bilder der personalen Identität sind das nach außen erkennbare Ergebnis, welches innerhalb der Kommunikation in Erscheinung tritt.

Nach dem bestehenden IKT-Recht erfolgt die Vergabe von Identitäten durch staatliche oder private Institutionen (1.) und kann zur Wahrung der

informationellen Selbstbestimmung in ein kompensatorisches Konzept der verhandelten personalen Identität mit einem Mediationsagenten münden (2.).

1. Identitätsvergabe durch Institutionen

a) Öffentlich-rechtliche Identitätsvergabe

Die öffentlich-rechtliche Identitätsvergabe über das Namensrecht, Pass-, Personalausweisgesetz oder Meldewesen begründet einen öffentlichen Glauben an die Identität der natürlichen Person, so dass diese Identitätsvergabe die höchste Vertrauens- und Sicherheitsstufe bildet und der „Identitätsvergewisserung“[865] dient. Mit dieser staatlichen Identitätsvergabe wird der statische *Idem*-Anteil der personalen Identität umfasst, der nicht verhandelbar ist und sich nur unter den engen Voraussetzungen etwa des Namensrechts oder Transsexuellenrechts ändern lässt.[866] Ebenso wird mit der staatlich erteilten Identität ein Vertrauensmaß geschaffen, welches im elektronischen Rechtsverkehr etwa für Bürgerdienste über den elektronischen Identitätsnachweis gemäß § 18 PAuswG zur Identifizierung und Erteilung von Berechtigungen[867] eingesetzt werden kann. Mit niedrigerem Vertrauensniveau kann die Identitätsvergabe bei der einfachen elektronischen Signatur erfolgen und damit einem anderen Vertrauens- und Sicherheitsniveau unterliegen, EWG 48. Insofern fungiert die identitätsvergebende Institution als akkreditierte *Trusted Third Party* für die innereuropäische Interoperabilität behördlicher Identifizierungen, was die Anerkennung der Zertifikate in den Mitgliedstaaten voraussetzt, Art. 25 Abs. 3 eIDAS-VO. Damit ist für den Zertifikatnutzer der Zugang zu einem innereuropäischen Identifizierungssystem geschaffen, welches zur europaweiten behördlichen Identifizierungsmöglichkeit und Rationalisierung dokumentengeprägter Prozesse beiträgt.[868] Voraussetzung dafür ist eine personale Teilidentität, bestehend aus den Personenidentifizierungsdaten gemäß Art. 3 Nr. 3 eIDAS-VO, mit denen die eindeutige Repräsentation der natür-

865 *Eichenhofer/Gusy*, in: Hornung/Engemann (Hrsg.), Der digitale Bürger und seine Identität, 2016, 65 (67); über das „informationelle Vertrauen“ in der Identitätsverwaltung, vgl. *Warnecke*, Identitätsmanagement und Datenschutz, 2019, S. 59–63.

866 2. Teil, A., II., 1., a).

867 *Hornung/Möller*, Passgesetz, Personalausweisgesetz, 2011, § 18 PAuswG Rn. 8.

868 *Sosna*, CR 2014, 825 (828).

lichen Person möglich wird. Dieses innereuropäische Identifizierungssystem kann um autorisierte privatrechtliche Institutionen erweitert werden, wie es die eIDAS-VO in EWG 13, 17 S. 1 vorsieht. Dies könnte langfristig ein Gegengewicht zu der verbreiteten Identifizierungsmöglichkeit von Intermediären bilden, die ebenfalls identitätsstiftend wirken können und das staatliche Identitätsstiftungsmonopol ignorieren würden.[869] Insofern ist mit der eIDAS-VO für eine grenzüberschreitende Identitätsvergabe eine Stärkung der staatlichen Identitätsstiftung anzunehmen, die sich auf den privatrechtlichen Kontext ausweiten lässt und als ein Beitrag zur Steigerung des Identitätsschutzes in Europa eingeordnet werden kann.

b) Privatrechtliche Identitätsvergabe

Mit der privatrechtlichen Identitätsvergabe durch Intermediäre werden die Funktionen des dienstbezogenen und kontextübergreifenden Identitätszugangs, wie es *Facebook* und *Google* mit *Single Sign-On*-Lösungen ermöglichen, umfasst. Die gebündelte Funktionalität eines kontextübergreifenden Identitätszugangs sieht ebenfalls eine *Trusted Third Party* vor, bei der die personalen Identitäten hinterlegt sind. Als Intermediäre für den privatrechtlichen Kontext kommen ebenso staatlich zugeordnete Institutionen in Betracht, wie die Bundesdruckerei oder die Bundesrechtsanwaltskammer, die kontextspezfische personale Teilidentitäten in Gestalt des Personalausweises mit einer Personalausweisnummer und den Zugang zum elektronischen Anwaltspostfach vergeben können. Diese können über die bloße Identitätsvergabe hinaus mit zertifizierten personalen *Idem*-Teilidentitäten ausgestattet werden, so dass die Einsatzfähigkeit in Kontexten mit einem gesteigerten Vertrauens- und Sicherheitsniveau gewährleistet wird.

Denn die privatrechtliche Identitätsvergabe durch Intermediäre wirft die Frage nach der Umsetzung IT-sicherheitsrechtlicher Standards auf, gerade wenn die Niederlassung außerhalb des Regelungsregimes der Europäischen Union liegt. Insofern sollte die Wahl der Intermediäre zur privatrechtlichen Identitätsvergabe in Verbindung mit dem herrschenden Regelungsregime stehen, so dass die Entscheidung über die Nutzung eines Intermediärs zugleich eine Entscheidung über das maßgebliche rechtliche Schutzregime ist. Damit obliegt der natürlichen Person die Verantwortung, den geeigneten Intermediär zu wählen, der über die spezifischen Plattformen für das jeweilige Vertrauens- und Sicherheitsniveau verfügt

869 *Hornung/Engemann* (Hrsg.), Der digitale Bürger und seine Identität, 2016, S. 16.

und als „*Identity Ecosystem*“ dem Regelungsregime der europäischen Datenschutzgrundverordnung unterliegt.

2. Identitätsvergabe durch den Mediationsagenten

a) Mediationsagent als Software

Die Identitätsvergabe unter der Prämisse einer verhandelten personalen Identität setzt die Offenlegung der personalen *Ipse*-Identität durch den Verantwortlichen voraus, die mit dem Selbstbild der personalen Identität des Betroffenen verhandelt werden sollte. Ein dafür eingesetzter technischer Mediationsagent könnte eine weitere Identität vergeben, die der Verhandlung unterliegt und das Ergebnis eines Aushandlungsprozesses unter spezifischen *Instruktionen* darstellt. Diese verhandelte Identität würde dem Kalkül des Mediationsagenten sowie den Eingabewerten des Verantwortlichen und des Betroffenen über die personale Identität unterliegen. Dabei würde das Kalkül des Mediationsagenten aus den Eigenschaften eines Mediators bestehen, das neutrale und diskriminierungsfreie *Instruktionen* für die Bilder personaler Identitäten ermöglicht. Darüber hinaus kommen inhaltliche Verstärkungs- und Schwächungsmechanismen über Attribute in Betracht, die kontextbedingt hinsichtlich der generierbaren Erkenntnismöglichkeiten gesteuert werden müssten. Damit könnten unerwünschte Wissensgenerierungen, wie sie etwa in § 81g Abs. 2 S. 2 StPO über die Beschränkung der Erkenntnisse aus der DNA geregelt werden, vermieden werden.

Der Mediationsagent würde als Softwareprogramm eingesetzt werden können, welches mit eigener Intelligenz ausgestattet wäre und *Instruktionen* für die Generierung der Bilder personaler Identität enthielte und vollziehen könnte.[870] Dieses müsste als Finalprogramm ausgestaltet sein, bei dem das Entscheidungsergebnis offen ist und das Programm auf der Einbeziehung von Informationen basiert.[871] Insofern würde mit dem Vollzug der Regeln eines Mediationsagenten durch Software gleichzeitig eine Steuerung des Verhaltens ausgelöst werden können, so dass einem technischen Mediationsagenten aus Software eine institutionelle Dimension[872] zukommen würde, sog. „*Code as law*“. In Anbetracht der möglichen recht-

870 5. Teil, C., III.–IV.
871 *Reisinger*, Rechtsinformatik, 2016, S. 99 f.
872 *Orwat/Raabe/Buchmann u.a.*, Informatik Spektrum 2010, 626 (628).

lichen Verankerung eines technischen Mediationsagenten im MedG könnte der Mediationsagent als Legitimationsquelle gegenüber der bisherigen einseitigen Identitätsvergabe fungieren und das Legitimations- und Kontrolldefizit auf der Ebene der Rechtfertigung kompensieren.

b) Mediationsagent als „*Smart Contract*"

Für den Einsatz eines technischen Mediationsagenten könnte die Generierung einer verhandelten Identität mit einem *Smart Contract* erfolgen. Indem *Smart Contracts* eine Streitbeilegungsklausel über einen „*online dispute resolution*"-Mechanismus enthalten können,[873] erscheint eine Verbindung zum technischen Mediationsagenten naheliegend. Dabei könnte das Mikroverfahren eines technischen Mediationsagenten möglicherweise mit einem *Smart Contract* ausgeführt werden.

Grundsätzlich ist dabei die Bezeichnung des *Smart Contracts* missverständlich, denn es handelt sich im Rechtssinne gerade nicht um einen Vertrag, sondern um die automatisierte Durchführung und Durchsetzung eines vorher verhandelten Vertrages.[874] Dies setzt voraus, dass der Vertragsinhalt technisch übersetzt werden kann, was gerade bei der Übersetzung der allgemeinen Geschäftsbedingungen in ein Softwareprogamm[875] naheliegend erscheint und aus der IKT-rechtlichen Perspektive der Übersetzung von Datenschutzerklärungen entsprechen kann. Damit könne die Realisierung der Datenschutzerklärung in der Datenverarbeitung mit der automatisierten Durchführung „garantiert"[876] werden. Dieser Mechanismus des *Smart Contract* könnte etwa durch die Einwilligung ausgelöst werden und zum Vollzug der kontextspezifischen Datenverarbeitungsvorgaben führen.

Gleichwohl erscheint die Verhandlung der personalen Identität mit einem *Smart Contract* fernliegend, da mit diesem die Durchführung von Regeln unter der Prämisse erfolgt, dass es keine inhaltlichen Unbestimmtheiten über die konkrete Darstellung des Bildes personaler Identitäten geben darf. Demnach ist die Funktionalität eines *Smart Contract* für den technischen Mediationsagenten zur Verhandlung von Bildern personaler Identitäten fernliegend und steht dem Erfordernis der Ergebnisoffenheit in der

873 *Kaulartz*, DSRI 2017, 599 (605).
874 *Kaulartz/Heckmann*, CR 2016, 618.
875 *Dies.*, CR 2016, 618 (622); *Wright/Filippi*, Decentralized blockchain technology and the rise of lex cryptographia, 2015, S. 24–26.
876 *Dies.*, CR 2016, 618 (620); *Kaulartz*, DSRI 2017, 599 (601).

Mediation entgegen. Allerdings könnte ein *Smart Contract* für eine automatisierte Verweisung zu einem technischen Mediationsagenten in einem bestimmten Zeitpunkt im Datenzyklus eingesetzt werden, wie es bei der automatischen Verweisung zu einem Streitbeilegungsverfahren mit einem *Smart Contract* möglich ist.

3. Zusammenfassung

Nach den IKT-rechtlichen Vorgaben erfolgt die Identitätsvergabe öffentlich-rechtlich und privatrechtlich. Die öffentlich-rechtliche Identitätsvergabe kann aufgrund ihrer Funktionalität der Identitätsvergewisserung und des öffentlichen Glaubens im Rechtsverkehr nicht verhandelbar sein. Demgegenüber sind die vergebenen personalen Identitäten durch die privatrechtlichen Institutionen faktisch ebenfalls nicht verhandelbar, wenngleich das Interesse an der Identitätsvergewisserung bei Intermediären aufgrund des Vorrangs der Datenverarbeitungen geringer ausgeprägt sein dürfte. Indem der institutionellen Identitätsvergabe keine Identitätsvergabe durch den Betroffenen – mit Ausnahme der Einwilligung – gegenübergestellt wird, bedarf es für einen Ausgleich der Interessenlagen zwischen dem Verantwortlichen und Betroffenen der Identitätsvergabe durch einen technischen Mediationsagenten. Dieser könnte mit Software gestaltet werden, die die formalisierten Verfahrensprinzipien der Mediation enthalten würde und in inhaltlicher Hinsicht ergebnisoffen ausgestaltet wäre. Dabei müsste der technische Mediationsagent über *Instruktionen* verfügen, die eine neutrale und diskriminierungsfreie Generierung der Bilder personaler Identitäten ermöglicht. Für eine Schwerpunktverlagerung von der bloßen Identitätsvergabe hin zu einer verhandelten Identität könnte ein softwarebasierter technischer Mediationsagent für die Identitätsverwaltung im privatrechtlichen Kontext als Institution wirken.

III. Paradigmenwechsel zur dezentralen Identitätsverwaltung

Der dynamische Identitätsbegriff und das Konzept einer kontextspezifischen Identitätsverwaltung verlangen eine dezentrale Identitätsverwaltung, die es ermöglicht, zwischen verhandelbaren und nicht verhandelbaren personalen Identitäten zu differenzieren. Da es jeweils um die Darstellung des Bildes einer personalen Identität geht, führt eine *kontextspezifische Identitätsverwaltung* zu einer pluralisierten Verteilung der personalen Teilidenti-

täten, die der jeweiligen Verwaltung bedürfen. Demnach erscheint aus der Gesamtbetrachtung, die dezentrale Ausgestaltung der Identitätsverwaltung dem *Idem*- und den *Ipse*-Anteilen der personalen Identität in einem Datenzyklus gerecht zu werden. Auch kann damit der Lebenszyklus spiegelbildlich in dem Datenzyklus der personalen Identität abgebildet werden. Dies würde bei einem zentralisierten Konzept, das aus *einer* „digitalen Identität" besteht, kaum mit dem grundrechtlichen und fachübergreifenden Identitätsbegriff vereinbar sein, weil darin das differenzierte Vertrauens- und Sicherheitsniveau nicht aufgehen würde. Vielmehr liegt darin eine Zentrierung und Beschränkung auf den Namen als *Idem*-Anteil der personalen Identität, was dem hier vertretenen Identitätsbegriff nicht entspricht.

Für ein dezentrales Identitätsverwaltungsmodell spricht weiter, dass bereits im Volkszählungsurteil die Dezentralisierung von Datenspeicherungen als verfassungsrechtliches Gebot vorgetragen wurde.[877] Denn bei einem Angriff auf die Datenspeichersysteme würde das Risiko für die Datensicherheit deutlich geringer ausfallen, als wenn ein Angriff gegenüber einer *Trusted Third Party* mit sämtlichen Datensätzen einer personalen Identität erfolgt. Ferner ermöglicht die dezentrale Identitätsverwaltung die *iterative Kontrolle* personaler Teilidentitäten in ihrem *Ipse*-Anteil in systemischer Hinsicht, da die natürliche Person die Kontrolle im Laufe des Datenzyklus für den jeweiligen Kontext ausüben und das Bild der personalen Identität gestalten könnte. Mit einem dezentralen Identitätsverwaltungsmodell könnte die natürliche Person durch kontextspezifische Transparenz und damit verbundene Kontrollmöglichkeiten gestärkt werden. Für eine nähere Analyse des dezentralen Identitätsverwaltungsmodells sollen im Einzelnen das treuhänderische Konzept (1.) und die Blockchain (2.) als mögliche Lösungsmechanismen untersucht werden.

1. Treuhänderische Identitätsverwaltung

Die treuhänderische Identitätsverwaltung lässt sich zwischen einer zentralen *Trusted Third Party* und einem dezentralen System einordnen. Denn das Treuhandkonzept würde die Verwahrung der personenbezogenen Daten vorsehen, ohne ein wirtschaftliches Interesse zu verfolgen. So wird als Datentreuhand von *Kühling/Sackmann* eine Pseudonymisierungsinstanz vorgeschlagen, die als Stellvertreter der Verbraucher eingesetzt werde und die Verwaltung des Personenbezugs der Daten mit dem damit verbunde-

877 BVerfGE 65, 1 (19).

nen Risiko der Identifizierbarkeit ermögliche.[878] Die Neutralität und Unabhängigkeit des Datentreuhänders wäre dabei entscheidend, um mit dem Treuhänder keine weitere Risikoquelle über den Schutz der informationellen Selbstbestimmung zu schaffen. Weiter wird eine treuhänderische Lösung auch von *Hermstrüwer* vorgeschlagen, wonach neben der Rechtfertigung zwischen dem Verantwortlichen und Betroffenen eine Treuhandabrede darüber geschlossen werden könnte, dass die personenbezogenen Daten gewinnbringend eingesetzt werden sollen und eine entsprechende Auszahlung an den Betroffenen zu erfolgen hätte.[879] Ferner schlägt die Kommission Wettbewerbsrecht 4.0 für die betroffenen Personen einen selbstgewählten Datentreuhänder vor, mit dem die Bereitstellung der personenbezogenen Daten organisiert werden kann.[880] Ebenso wird als Treuhand ein „*Digital Clearinghouse*" von dem europäischen Datenschutzbeauftragten (EDPS) angeführt, mit dem Verbraucher- und Wettbewerbsfragen vereinigt und der natürlichen Person zur Rechtsdurchsetzung verholfen werden soll.[881] Schließlich wird von *Drexl* eine Agentenstruktur vorgebracht, die den Verbraucher mit dem Verantwortlichen bei umfangreichen und dynamischen Datensätzen zusammenbringen soll und so der Zugang zu den Datensätzen mit den Privatheitseinstellungen durch den Betroffenen kontrolliert werden könne.[882]

Auch wenn in einer treuhänderischen Konstruktion eine Alternative zur *Trusted Third Party* liegen kann, besteht dennoch eine strukturelle Parallele zu dieser. Denn bei einem Angriff auf die IT-Sicherheit der Treuhand kann der Schaden für die informationelle Selbstbestimmung erheblich sein, so dass die treuhänderische Konstruktion in Nischenbereichen naheliegender erscheint.[883] Weiter setzt eine treuhänderische Konstruktion voraus, dass der Betroffene den Zugang und die Einstellungen kontrollieren kann, womit das Risiko des Kontroll-Paradoxons seine Wirkung entfaltet und die vermeintliche Kontrolle über den kontextbezogenen Zugang zu einer bereitwilligen Offenlegung personenbezogener Daten führt.

Insgesamt würde es sich bei der treuhänderischen Konstruktion ebenfalls um einen Mediator auf der Makroebene handeln, der unabhängig und neutral zwischen dem Verantwortlichen und dem Betroffenen einge-

878 *Kühling/Sackmann*, Rechte an Daten, 20. November 2018, S. 17.
879 *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, S. 139 f.
880 *Kommission für Wettbewerbsrecht 4.0*, Bericht, S. 43 f.
881 www.edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_de (zuletzt aufgerufen 20.06.2020).
882 *Drexl*, JIPITEC 2017, 257 (275) Rn. 88; *Bernau*, FAS vom 10.02.2019, 23.
883 *Kühling/Sackmann*, Rechte an Daten, 20. November 2018, S. 18.

setzt wird. Insoweit kann das *Dashboard-System* zum Bestandteil einer treuhänderischen Konstruktion werden, damit der Zugang zu den personalen Identitäten und die Transparenz über die kontextspezifischen Bilder der Teilidentitäten gewährt werden. Dabei müsste ein Gleichgewicht zwischen einer absoluten Kontrolle in Gestalt des Zugangs und dem Kontroll-Paradoxon hergestellt werden. Ein solches *Dashboard-System* könnte den Zugang, die Bilder personaler Identitäten und den technischen Mediator umfassen, der von dem Verantwortlichen oder einem Dritten eingesetzt werden könnte. Dabei sollte der Dritte keine wirtschaftlichen Eigeninteressen verfolgen. Ebenfalls ließe sich an eine Zertifizierung eines solchen *Dashboard-Systems* mit einem technischen Mediator gemäß Art. 42 DSGVO denken, was sich auf eine positive Reputation und damit auf das Marktverhalten des Betroffenen und des Verantwortlichen auswirken könnte. Schließlich kommt die Anknüpfung an einen bestimmten Schwellenwert über den Datenverarbeitungsumfang in Betracht, der dazu verpflichten könnte, ein *Dashboard-System* einzuführen.

2. Identitätsverwaltung in der Blockchain

Für die dezentrale Identitätsverwaltung lässt sich die Blockchain einsetzen. Die Blockchain ist eine Ausprägung der „*Distributed Ledger Technologie*" und löst einen zentralen Intermediär ab, indem eine koordinierte und dezentrale Speicherung der Datensätze erfolgt. Es handelt sich dabei um eine Technologie, die aus einer Kombination von „*Peer-to-Peer-network*" und Kryptographie besteht. Daher wird der Blockchain aus ökonomischer Perspektive ein institutioneller Charakter zugeschrieben,[884] der für den Anwendungsbereich der Identitätsverwaltung maßgeblich sein könnte. Denn die Blockchain ermöglicht eine interoperable, dezentrale Datenverarbeitung und stellt gleichzeitig die Authentizitität über die Datensätze sicher, weshalb sie als Technologie für die Identitätsverwaltung in Frage kommt. Demnach soll die Funktionsweise der Blockchain (a) aufgezeigt und ihr Einsatz bei der Identitätsverwaltung (b) diskutiert werden.

884 *Davidson/Filippi/Potts*, Journal of Institutional Economics 2018, 639.

a) Funktionsweise der Blockchain[885]

Die Blockchain besteht aus „*Nodes*“[886], in denen die Eingabe des Wertes durch ein Individuum vorgenommen wird. Dieser Eingabewert wird in einem Datenblock („*Block*“) dezentral repliziert und synchronisiert, was zur allgemeinen Transparenz des Datensatzes in den jeweiligen „*Nodes*“ führt. Gleichzeitig erscheint der Datensatz als umgerechneter Hashwert, dem verschlüsselten Datensatz, der mit einem Zeitstempel versehen ist, womit sich der Hashwert in eine zeitliche Reihenfolge gegenüber anderen Hashwerten setzen lässt. Diese in einer festen Reihenfolge miteinander verbundenen Datenblöcke bilden eine Kette, sog. „*chain*“, die nur erweitert werden kann und damit irreversibel ist.[887] Die Entstehung der Kette verlangt das „*hashing*“ und „*rehashing*“, welches den „*Proof of Work*“ darstellt und eine hohe Rechenleistung verlangt.[888] Demgegenüber kann die kostenintensive hohe Rechenleistung mit einer Technologie ohne den „*Proof of Work*“ reduziert werden, indem der Vorgang des „*hashing*“ und „*rehashing*“ auf den „*Proof of Stake*“ beschränkt wird, ohne dass die vorangegangenen Eingabewerte in die Rechenoperation einbezogen werden, so dass der Rechenleistungsaufwand geringer wird.[889] Insgesamt wird mit der Blockchain die allgemeine Transparenz, verteilt auf die „*Nodes*“, gewährleistet und mit der Bildung des Hashwertes ein Schutzmechanismus gegen

885 Vgl. *Steinbrück*, in: Schweighofer/Kummer/Saarenpää (Hrsg.), Tagungsband, IRIS 2019, 2019, 283.

886 *Wattenhofer*, The science of the blockchain, 2017, S. 5, Definition: „We call a single actor in the system node“; historisch ging es darum, das byzantinische Problem zu lösen, wonach ein *Node* sich inkorrekt verhält etwa mit der Sendung eines korrumpierten Datensatzes. Wenn in einem Netzwerk durch ein Quorum aller Nodes ein Gleichlauf hergestellt wird, würde dieses byzantinische *Node* überstimmt werden können, was mit dem Paxos-Algorithmus ermöglicht wird.

887 *Peck*, IEEE Spectrum 54 (2017), 26.

888 *Ders.*, IEEE Spectrum 54 (2017), 26 (27, 32 f.); *Wattenhofer*, The science of the blockchain, 2017, S. 83. Hinsichtlich der hohen Rechenleistung und des Energieverbrauches werden daher Alternativen diskutiert, etwa „*Hashgraph*“.

889 Ein System ohne den Proof of Work bildet „*Hashgraph*“; *Luu/Teutsch/Kulkarni u.a.*, in: Ray/Li/Kruegel (Hrsg.), CCS'15, 2015, 706 (706–708): Mit dem sog. „*Verifier Dillema*“ kann die hohe Rechenleistung in Frage gestellt werden. Denn nach der bisherigen Konstellation müssen die Miner eine Transaktion verifizieren, jedoch kann diese Verifizierung ausbleiben und der Rechenaufwand wird geringer.

die Manipulation des Datensatzes geschaffen, wodurch ein Vertrauensanker gebildet wird.[890]

Die Blockchain wird in eine öffentliche und private Blockchain differenziert. Die Unterscheidung richtet sich danach, ob der Zugang zu der Blockchain für einen beschränkten Nutzerkreis besteht und einer Erlaubnis bedarf oder der Zugang für jeden eröffnet wird. Für die kontextbezogene Identitätsverwaltung erscheint eine private Blockchain mit einem beschränkten Nutzerkreis als eine potentielle technische Lösung zur Realisierung eines „*privacy by design*"-Konzeptes[891]. Indem die Blockchain auf die Sicherstellung der allgemeinen Transparenz und der Irreversibilität von Datensätzen abstellt, könnte sie für die Kontexte einer statischen personalen Identität dann eingesetzt werden, wenn der Bedarf nach dem öffentlichen Glauben besteht, wie es etwa bei Grundbucheintragungen der Fall ist. Gleichzeitig ermöglicht die Blockchain die wiederkehrende Erneuerung von Erkenntniswerten mit dem jeweiligen „*Update*" das Hashwertes, wobei die redundante Speicherung der Hashwerte erwünscht sein müsste.

b) Personale Identität in der Blockchain

Sobald die Identitätsverwaltung in der Blockchain erfolgt, bedarf es der Bestimmung eines Datensatzes, der in einen Hashwert umgewandelt werden soll. Dabei kommen die Speicherung einer personalen Identität, die Speicherung spezifischer Attribute, die Speicherung der Einwilligung oder die Speicherung eines Zugangsrechts in der Blockchain in Betracht.

Es wird für eine Identitätsverwaltung unter Einbeziehung der elektronischen Identifizierung nach der eIDAS-VO die Speicherung von Identitätsattributen („*Identifier*") mit der Einwilligung im Hashwert vorgeschlagen.[892] Diese sollte mit einer elektronischen Signatur als Hashwert verschlüsselt werden, was über die ISÆN-App erfolgen könnte. Nach dem ISÆN-Konzept wird mit dem Hashwert, in dem die Einwilligung gespeichert ist, eine gezielte Authentifikation für den privaten Sektor möglich,

---

890 *Peck*, IEEE Spectrum 54 (2017), 26 (28). Danach wird zunächst auf Bitcoin Bezug genommen mit einem Ausblick auf weitere Anwendungen etwa den Kontext *Social Media.*

891 *Bechtolf/Vogt*, ZD 2018, 66 (71).

892 *Smart Data Begleitforschung*, Sicheres Identitätsmanagement im Internet, 2017, S. 37; demgegenüber setzt das estländische e-Residency Programm die Blockchain Technologie für die Authentifizierung und Verifikation ein, vgl. *Sullivan*, CLSR 2018, 723 (727).

wobei der Hashwert aufgrund der Verschlüsselung als anonymes Datum eingeordnet wird.[893] Dagegen lässt sich einwenden, dass mit der Verschlüsselung durch den Hashwert zwar die Identifizierbarkeit deutlich erschwert wird, aber im Sinne des objektiviert-relativen Ansatzes die Identifizierbarkeit einer natürlichen Person nicht ausgeschlossen ist.[894] Dies gilt besonders, weil der „*Public Key*" für die Verschlüsselung als personenbezogene Daten zu qualifizieren ist. Um einen angemessenen Schutz für die informationelle Selbstbestimmung zu gewährleisten, wird der Annahme von anonymen Daten in der Blockchain nicht gefolgt. Sobald diese als anonyme Daten eingeordnet werden, würden die Grundsätze der Datenverarbeitung nach der DSGVO nicht mehr gelten, obwohl das Risiko der Identifizierbarkeit etwa aus den Metadaten bei der Verwendung der Blockchain besteht und der Personenbezug hergestellt werden kann.[895]

Die personenbezogenen Daten können auch in der „*off-chain*" gespeichert werden, womit der Hashwert in jedem Fall als anonym einzustufen wäre und die datenschutzrechtlichen Anforderungen für die Blockchain nicht gelten würden.[896] Demnach ist für einen datenschutzkonformen Einsatz der Blockchain diese als Dienst im Sinne eines „*Blockchain as a Service*" (BaaS) denkbar, so dass die Funktionsweise der Blockchain außerhalb des datenschutzrechtlichen Regelungsregimes erfolgen könnte.[897]

Darüber hinaus würde die Speicherung der Identitätsattribute mit der Einwilligung in der Blockchain datenschutzrechtlich fragwürdig sein, da in einem dezentralen Speicherungssystem die Datenminimierung und das Recht auf Vergessenwerden umzusetzen wären. Für die Wahrung des Grundsatzes der Datenminimierung könnte zwar argumentiert werden, dass die DSGVO auf zentrale Strukturen ausgerichtet sei und eine angepasste Auslegung auf dezentrale Strukturen verlangt, so dass die Verschlüsselung im Hashwert eine ausreichende Umsetzung der Datenminimierung darstelle, Art. 5 Abs. 1 c), 4, Nr. 5 DSGVO. Jedoch erscheint diese Ausle-

893 *Smart Data Begleitforschung*, Sicheres Identitätsmanagement im Internet, 2017, S. 34.

894 *Finck*, EDPL 2018, 17 (25).

895 *Dies.*, EDPL 2018, 17 (22). Eine Ausnahme wird dann gesehen, wenn der Hashwert sich über eine sog. Einwegfunktion bilden lässt. Für diesen Fall könne der Hashwert als anonymes Datum eingeordnet werden; als Metadaten kommen die Verkehrs- und Standortdaten, die eine eigene personale Teilidentität bilden können, in Betracht.

896 *Dies.*, EDPL 2018, 17 (22).

897 *Dies.*, EDPL 2018, 17 (27 f.); *Kulhari*, Building-blocks of a data protection revolution, 2018, S. 22.

gung der Datenminimierung zu weitgehend und es steht vielmehr eine Anpassung der DSGVO an dezentrale Technologien im Raum. Hinsichtlich des Rechts auf Vergessenwerden würde sich die Umsetzung gemäß Art. 17 Abs. 2 DSGVO auf die „Berücksichtigung der verfügbaren Technologie" beschränken und steht gemäß § 35 Abs. 1 BDSG unter dem Verhältnismäßigkeitsvorbehalt, so dass für die rechtskonforme Umsetzung das Löschen des Datensatzes nicht zwingend erforderlich ist. Folglich könnte nach der Geltendmachung des Rechts auf Vergessenwerden der Block um einen weiteren Block mit dem Inhalt erweitert werden, dass die Blockchain bis zu einem bestimmten Zeitpunkt „falsch" sei. Zwar wird damit ein eigener neuer Erkenntnisgehalt begründet, aber zumindest könnte auf diesem Weg der Neubeginn einer personalen Teilidentität ermöglicht werden. Ebenso könnte das Recht auf Berichtigung gemäß Art. 16 DSGVO durch Hinzufügung einer weiteren „*chain*" realisiert werden, so dass auch hier eine der Blockchain angepasste Lösung denkbar wäre.[898]

Insgesamt lässt sich diesen Lösungsmöglichkeiten entgegenhalten, dass die Realisierung der Identitätsverwaltung in der Blockchain mit erheblichen rechtlichen Risiken verbunden ist. Weiter konterkariert sich die Zielrichtung der Blockchain, einen hohen öffentlichen Glauben und Transparenz zu schaffen, mit dem Ziel der Identitätsverwaltung, unter Wahrung der Datenminimierung und Sicherstellung eines dynamischen Identitätsbegriffs umgesetzt zu werden. Demnach erscheint die Verbindung zwischen Identitätsverwaltung und Blockchain nach den bekannten technischen Lösungsmöglichkeiten als Konstruktion, ohne derzeit ein rechtskonformes Konzept der Blockchain als „*privacy by design*"-Lösung abbilden zu können.

Für die Blockchain spricht jedoch, dass mit ihr die Kontrolle über die Datensätze in den Hashwerten und eine grenzüberschreitende, dezentrale und interoperable Datenverarbeitung ermöglicht wird. Gleichwohl ist sie als Technologie für die privatheitsschützende Identitätsverwaltung bislang mit der DSGVO schwerlich in Einklang zu bringen, jedoch nicht vollständig abzulehnen. Etwa kommt eine private Blockchain in einem Unternehmen in Betracht, das über ein eigenständiges und separiertes Schutzregime verfügt. Weiter kommen für die spezifischen Anforderungen der Identitätsverwaltung technische Anpassungen bei der Gestaltung der Blockchain in Frage, mit denen sich die datenschutzkonforme Umsetzung vornehmen

898 *Dies.*, EDPL 2018, 17 (29 f.); ebenso den Modizierungsbedarf des Rechts auf Vergessenwerdens anerkennend, vgl., *Kulhari*, Building-blocks of a data protection revolution, 2018, S. 42–45, 52.

lässt. Ebenso ist die Anpassung der DSGVO auf dezentrale Technologien und dezentrale verantwortliche Stellen denkbar.

3. Zusammenfassung

Die Identitätsverwaltung über ein Treuhandsystem kann eine Alternative zu der Identitätsverwaltung mit einer zentralen *Trusted Third Party* darstellen, wenn die Treuhand neutral und ohne wirtschaftliche Interessen zum Einsatz käme. Denn die treuhänderische Konstruktion birgt die Chance, dass die umfangreiche Datenverarbeitung zur Auszahlung eines Geldbetrages führen und die Transparenz über die Bilder personaler Teilidentitäten hergestellt werden könnte. Insoweit wäre ein *Dashboard-System* ein Konzept, mit dem eine treuhänderische Identitätsverwaltung erfolgen könnte. Gleichwohl bündelt ein treuhänderisches Konzept ebenfalls die personalen Teilidentitäten, so dass bei einem Angriff auf die IT-Sicherheit der Treuhand ebenso ein erhebliches Risiko für den Schutz der informationellen Selbstbestimmung besteht. Demnach bedarf es der Verlagerung des Betrachtungsschwerpunktes auf eine dezentrale Identitätsverwaltung.

In technologischer Hinsicht kommt dafür die Blockchain in Betracht, dahingehend, dass mit ihr die personalen Teilidentitäten dezentral gespeichert und kontrolliert werden können. Gleichwohl konnte bei einer Identitätsverwaltung mit der Blockchain nachgewiesen werden, dass erhebliche Rechtsunsicherheiten über die Eröffnung des datenschutzrechtlichen Anwendungsbereiches und der Umsetzung der Betroffenenrechte bestehen. Daher sind technische Konzepte, in denen die Blockchain zwar eingesetzt wird, aber die Identitätsattribute und personalen Teilidentitäten in der „*off-chain*“ gespeichert werden, bislang vorzugswürdig. Weiter erscheint technologieunabhängig die Transparenz über die bestehenden Bilder personaler Identitäten notwendig, wobei die Datenverarbeitungen entsprechend zum Datenzyklus personaler Identitäten dezentral erfolgen sollten. Damit kann den kontextbezogenen IT-sicherheitsrechtlichen Anforderungen entsprochen und das gestufte Vertrauens- und Sicherheitsniveau gemäß Art. 8 Abs. 2 eIDAS-VO über die jeweiligen Teilidentitäten realisiert werden.

IV. Zwischenergebnis

Ein Modell für die Identitätsverwaltung setzt voraus, dass die Kontrolle über die personalen Identitäten mit dem Zugang zu den Identitäten sichergestellt wird. Folglich bedarf es eines Zugangskonzeptes zu den personalen Identitäten und der Verhandlungsfähigkeit von Bildern personaler Teilidentitäten in den jeweiligen Kontexten, was über ein *Dashboard-System* erfolgen sollte. Ein derartiger Identitätszugang lässt sich aus dem Transparenzgebot gemäß Art. 12 DSGVO und dem Auskunftsrecht als Zugangsrecht gemäß Art. 15 DSGVO ableiten. Eine bislang ungeregelte Voraussetzung ist, dass mit dem Zugang die Transparenz über die personale Identität durch den Verantwortlichen hergestellt werden müsste. Dafür könnte von einer Treuhand das *Dashboard-System* zur Verfügung gestellt werden, mit dem die Transparenz zu der personalen Teilidentität hergestellt wird. Dieses *Dashboard-System* würde in struktureller Hinsicht einem Mediator entsprechen, der die personale Identität in ihrer statischen *Idem*- und dynamischen *Ipse*-Dimension unterteilt und mit dem Zugang zu den personalen Identitäten die Verhandlung der Bilder personaler Identitäten ermöglicht.

Die Verhandlung würde auf der Mikroebene mit dem technischen Mediator erfolgen, der aus Software besteht und über *Instruktionen* für die ergebnisoffene Verhandlung der Bilder personaler Identitäten verfügt. Dabei würden die *Instruktionen* aus den formalisierten Verfahrensprinzipien der Mediation bestehen, damit die Generierung der Bilder personaler Identität unter rechtlichen Schutzvorgaben und nicht willkürlich erfolgt. Dies ermöglicht eine kontextbezogene Pluralität der Bilder personaler Identitäten, was zugleich der *iterativen* Identitätsverwaltung im Rahmen des Lebenszyklus dienen würde.

Insgesamt bedarf es auf der Makroebene eines dezentralen Identitätsverwaltungskonzeptes, bei dem die treuhänderische Lösung eines *Dashboard-Systems* als vorzugswürdig herausgearbeitet wurde. Daneben erscheint die Blockchain als dezentrale Technologie für die Identitätsverwaltung ebenso naheliegend, würde aber nach derzeitiger Rechtslage entweder als private Blockchain oder in der „*off-chain*" in Betracht kommen. Die dezentrale Identitätsverwaltung verlangt, dass kontextspezifische Vertrauens- und Sicherheitsanforderungen etwa nach den *drei Stufen* gemäß Art. 8 Abs. 2 eIDAS-VO umgesetzt werden, damit die *kontextuelle Integrität* der personalen Identität in ihren *Idem*- und *Ipse*-Anteilen gewährleistet wird.

C. Ergebnis: Dezentraler Zugang zur verhandelten Identität

Ein Modell der Identitätsverwaltung soll die *kontextuelle Integrität* der personalen Identität gewährleisten. Der Komplexität des realen Individuums wird in einem IKT-System entsprochen, wenn neben dem statischen *Idem*-Anteil der personalen Identität der dynamische *Ipse*-Anteil ebenso kontrollierbar wird. Voraussetzung dafür ist der Perspektivwechsel weg von einem statischen Berechtigungskonzept hin zum Zugang zur personalen Identität und zu der Verhandlungsfähigkeit der Bilder personaler Identitäten. Somit bedarf es der *iterativen Kontrollmöglichkeit* in einem Identitätsverwaltungsmodell, welches den absoluten Zugang der personalen Identität und die relative Verhandlungsfähigkeit der Bilder personaler Identitäten ermöglicht. Die Modellvoraussetzung der Iteration wurde auf der Miko- und Makroebene der mediativen Identitätsverwaltung nachvollzogen.[899]

Auf der Mikroebene bedarf es eines technischen Mediationsagenten, der die Verhandlungsfähigkeit der Bilder personaler Identitäten gewährleistet und über *Instruktionen* für die Generierung der Bilder personaler Identitäten verfügt. Diese sollten als Software ausgestaltet werden und aus den Verfahrensgrundsätzen der Mediation bestehen, damit ergebnisoffene und diskriminierungsfreie Bilder personaler Identitäten generiert werden können. Dazu gehört, dass die Erkenntnismöglichkeiten über die Bilder personaler Identitäten von den *Instruktionen* abhängen, indem allein die rechtlich zulässigen Bilder personaler Identitäten generiert werden sollen. Darin liegt eine Verschiebung des Blickwinkels auf den Schutz des dynamischen *Ipse*-Anteils einer personalen Identität, der zum Gegenstand der relativen Kontrolle des Betroffenen und Voraussetzung für das Identitätsverwaltungsmodell wird.[900]

Auf der Makroebene bedarf es der Gewährleistung eines kontextbezogenen Vertrauens- und Sicherheitsniveaus, welches dezentral und treuhänderisch mit einem *Dashboard-System* ausgestaltet sein sollte. Dieses dient dem Zugang zu den personalen Identitäten als absolute Kontrolle und der damit verbundenen Verhandlungsfähigkeit der Bilder personaler Identitäten als relative Kontrolle. Daneben kommt die dezentrale Identitätsverwaltung über die Blockchain in Betracht, die jedoch mit der derzeitigen Rechtslage der DSGVO schwerlich in Einklang zu bringen ist. Vielmehr kommt die Blockchain als Lösung in Betracht, wenn die personalen Identitäten in der „*off-chain*" gespeichert werden. Weiter verlangt der *Ipse*-Anteil einer perso-

899 6. Teil, B., I., II., 1.
900 6. Teil, B., II., 2.

nalen Identität, dass die technische Lösung eine dynamische Anwendung erlaubt. Diese lässt sich mit der Blockchain und den statischen Hashwerten kaum realisieren. Ebenso wird mit einem *Smart Contract* allein ein statisches Ergebnis generiert, was keine adäquate Lösung für die Identitätsverwaltung bilden würde. Somit kommt ein Intermediär in Frage, der die kontextbezogene Identitätsverwaltung mit spezifischen Plattformen für das jeweilige Vertrauens- und Sicherheitsniveau ermöglicht und damit ein „*Identity Ecosystem*" begründet. Folglich würde dem Individuum mit der iterativen Identitätsverwaltung über den Datenzyklus hinweg eine Kontrollmöglichkeit im Rahmen des Selbstdatenschutzes eingeräumt werden.[901]

901 6. Teil, B., III.