1.Teil: Einleitung

A. Motivation

Der Schutz personenbezogener Daten aus Art. 8 der europäischen Grundrechtecharta (GRC) und in der sekundärrechtlichen Datenschutzgrundverordnung (DSGVO) ist in digitalen Kontexten allgegenwärtig. Anders verhält es sich hingegen mit zusammengefassten personenbezogenen Daten in Gestalt der personalen Identität, die ebenfalls in ihren Entwicklungsbedingungen als schutzwürdig gilt. Der titelgebende Begriff der Identität ist insofern vielschichtig. Bedingt durch die Bedeutung des Vergleichens und der Zuschreibung einer Identität, steht die inhaltliche Ausgestaltung der personalen Identität aber im Zusammenhang mit dem Individuum. Somit wird keine datenzentrierte Perspektive eingenommen, sondern die Perspektive verschiebt sich auf die entstandene personale Identität.

Als Motivation der Untersuchung wird angenommen, dass sich die personale Identität im online-Kontext anders realisiert als im offline-Kontext und sich dies auf die Wahrnehmbarkeit der Identität in der Interaktion auswirkt. Denn die gesteigerten Interaktionsmöglichkeiten im online-Kontext, die nahezu zeitgleich über die Ländergrenzen hinweg möglich sind, lassen sich im offline-Kontext kaum abbilden. Danach ist die parallele Kommunikation mit Freunden etwa in einem Browser-Fenster möglich, in dem nächsten Browser-Fenster erfolgt die Kommunikation im beruflichen Netzwerk, in einem weiteren Browser-Fenster wird die Bewertung des letzten Restaurantbesuches getätigt und parallel lässt sich in der Applikation im Mobilfunkgerät der Verbrauch des „digitalen Hausrates“[1] beim Dienstanbieter einsehen. Diese im online-Kontext parallelen Handlungsmöglichkeiten finden mit der zeitlichen Dichte und Interaktionsvielfalt schwerlich eine Entsprechung im offline-Kontext. Darin kommt eine von dem Medienwissenschaftler *Pörksen* beschriebene Annahme der *„unerträgliche(n) Gleichzeitigkeit des Seins“*[2] zum Ausdruck, die zwar auf die Sofortvergleichbarkeit eines weiten Nachrichtenspektrums zwischen voyeuristischen Nachrichten der Boulevardpresse und schrecklichen Kriegsnachrichten ab-

1 *Schallbruch*, Schwacher Staat im Netz, 2018, S. 25–38.
2 *Pörksen*, NZZ vom 12.07.2018, 37.

zielt, aber ebenso die gesteigerte Parallelität von Interaktionen und Identitätsrealisierung des Individuums verdeutlicht.

Weiter werden im online-Kontext vom Nutzer beim Aufrufen der Webseiten, dem Bewerten von Produkten oder Kommentieren von Nachrichten solche Informationsspuren hinterlassen, die Erkenntnisse über die personale Identität ermöglichen. Gleichwohl bleiben diese Informationsspuren etwa in Gestalt von Cookies und Profilen in ihrem inhaltlichen Erkenntniswert intransparent, so dass für den Nutzer eine Ungewissheit über die Folgen seines Nutzungsverhalten verbleibt. Denn einerseits können die Erkenntnisse in der Datenmenge untergehen, andererseits besteht das Risiko, dass sich Rückkoppelungswirkungen auf den Nutzer in Gestalt von zielgerichteter Werbung oder zielgerichteten Nachrichten entfalten. Dahinter stehen Algorithmen, mit denen die Profile für nutzerspezifische Einblendungen erstellt werden, die verhaltensbeeinflussenden Charakter haben können. Eine derart gezielte individuelle Ansprache der Nutzerinteressen im online-Kontext ist im offline-Kontext nicht erkennbar, was die Erforderlichkeit eines differenzierten Schutzregimes für die personale Identität im online-Kontext deutlich macht. Dabei bedarf es einer realen Kontrollmöglichkeit über die entstandenen personalen Identitäten, damit in Kenntnis dieser das Individuum seine Selbstbestimmung ausüben kann. Die Ungewissheit über die entstandenen Profile der personalen Identität im online-Kontext verlangt zunächst deren Transparenz, damit das Individuum auf die Fragen, „Wer bin ich im sozialen Netzwerk?“, „Wer wird erkennbar bei der Bewertung des Restaurants?“ und „Wer ist aus dem Benutzungsverhalten über den digitalen Hausrat erkennbar?“ auch Antworten bekommt. Erst wenn diese Fragen beantwortet werden können, besteht eine reale Selbstbestimmungsmöglichkeit. Gleichwohl ist unklar, wie sich die personale Identität im online-Kontext zusammensetzt und welchen Einfluss die Interaktionen auf die Darstellung der personalen Identität haben, was die Frage nach dem Identitätsbegriff aufwirft. Die mögliche Antwort kann in der Beschreibung aus *Alice im Wunderland* liegen, in der sich Alice fragt, ob sie am Morgen beim Aufstehen dieselbe wie immer sei und sie dabei glaubt, sich ein bisschen anders gefühlt zu haben,[3] was ein dynamisches Identitätsverständnis nahelegt.

Entsprechend lässt sich ein dynamisches Identitätsverständnis, welches sich an den verschiedenen Ausprägungen eines Individuums orientiert, für ein Identitätsverwaltungsmodell heranziehen, was sich auch in der Legal-

3 *Carroll*, Alice im Wunderland, 1993, S. 22.

definition zu personenbezogenen Daten gemäß Art. 4 Nr. 1 DSGVO[4] widerspiegelt. Danach kann etwa die online-Kennung *Ausdruck* der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen *Identitäten* einer natürlichen Person sein. Damit erkennt das Schutzregime der DSGVO neben dem Schutz der personenbezogenen Daten die Ausprägungen der Identitäten im offline- und im online-Kontext gleichermaßen an. Dazu gehört, dass die Einfluss- und Selbstbestimmungsmöglichkeit über personenbezogene Daten und die damit verbundenen personalen Identitäten gewährleistet wird. Dies umfasst auch die Kontrolle des Individuums über die personale Identität, die dem Schutzregime der informationellen Selbstbestimmung aus Art. 7, 8 GRC[5] unterliegt.

Dieses grundrechtliche Postulat der Selbstbestimmung gilt für die Identitätsverwaltung in informations- und kommunikationstechnischen (IKT)-Systemen und erwächst aus den Phänomenen der personalen Identitäten im online-Kontext in einem Zeitalter ubiquitärer Datenverarbeitungen. Neben dem rechtlichen Schutzregime wirkt das politische und wirtschaftliche *Konzept der digitalen Souveränität* zum Schutz der personalen Identität. Denn die digitale Souveränität beschreibt die selbstbestimmte Kontrolle über Daten und ihre Löschung in einer freiheitlichen Gesellschaft und funktionierenden Wirtschaft in komplexen und vernetzten Systemen.[6] Gleichzeitig kann aus dem Konzept der digitalen Souveränität der Bedarf nach rechtlichen Rahmenbedingungen für die generelle Stärkung der Entscheidungssouveränität und Transparenz über die Funktionsweise von Algorithmen gegenüber Individuen abgeleitet werden.[7]

Demnach wirkt die digitale Souveränität auf individueller Ebene als Datensouveränität über die personenbezogenen Daten und stellt zugleich das Postulat der Verwirklichung des Schutzes der informationellen Selbstbe-

4 Ebenso in Art. 2 a) der Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

5 Für das Kombinationsgrundrecht gemäß Art. 7, 8 GRC wird die Begrifflichkeit der informationellen Selbstbestimmung gewählt, um die Information als maßgebliche Anknüpfung für die Überschneidung zwischen dem Schutz der personenbezogenen Daten und dem Schutz des Privatlebens hervorzuheben. Gleichwohl wird das divergierende Schutzniveau zwischen dem europäischem Datenschutzgrundrecht und dem Recht auf informationelle Selbstbestimmung in dieser Untersuchung dargestellt.

6 *Beyerer/Müller-Quade/Reussner*, DuD 2018, 277.

7 *Dies.*, DuD 2018, 277 (278).

stimmung dar. Dies gilt verstärkt, wenn die Verarbeitung personenbezogener Daten von international agierenden Intermediären über die Ländergrenzen hinweg erfolgt und die Profile von Nutzern in sozialen oder beruflichen Netzwerken international abrufbar sind. In diesen Konstellationen drängt sich die Frage nach der Wirksamkeit des nationalen Regelungsregimes auf, wenn personale Identitäten intransparent und kaum bestimmbar sind. Neben regulatorischen Maßnahmen kommt daher die Identitätsverwaltung als ein im „Schatten des Rechts" wirkender Schutzmechanismus in Betracht.

B. Phänomene im online-Kontext

Der online-Kontext zeichnet sich, wie dargelegt, auch durch die gesteigerte Gleichzeitigkeit des Seins von Identitäten aus. Diese Identitäten sind für das Individuum mit der gleichzeitigen Nutzbarkeit zwar wahrnehmbar, die mit der Nutzung einhergehenden Erkenntnismöglichkeiten bleiben aber für das Individuum verborgen. Dieses online-Phänomen steigert sich, wenn das Nutzungsverhalten in den geschützten privaten Räumen stattfindet, aber die Eingaben etwa in einem sozialen Netzwerk einer breiten Öffentlichkeit zugänglich gemacht werden und die damit verbundenen Erkenntnismöglichkeiten kaum vorhersehbar sind. Dabei wird das Nutzungsverhalten im online-Kontext von dem Eindruck der Privatsphäre und Ortlosigkeit geprägt, was die Offenlegung privater Informationen erleichtert. Das Nutzungsverhalten ist geprägt von digital unbewussten Verhaltensweisen („*Digital unconscious*"[8]), was von den Darstellungen der Programme begünstigt wird.[9] Ebenso können im online-Kontext leichter fiktive Selbstbilder präsentiert werden, da die unmittelbaren Auswirkungen verfälschender Selbstdarstellungen im online-Kontext von der Wahrnehmbarkeit der handelnden Person zunächst ausgeschlossen sind oder die Wahrnehmbarkeit nur zeitlich verzögert erfolgt. Somit lässt sich eine Erosion der bewährten Sphäreneinteilung zwischen privater und öffentlicher Sphäre feststellen. Denn in den privaten Räumlichkeiten entsteht eine gesteigerte Offenlegungsbereitschaft über öffentlich sichtbare Äußerungen und die möglichen Folgen stehen im Widerspruch zu der empfundenen Privatsphäre.

---

8 *Hildebrandt*, Smart technologies and the end(s) of law, 2015, S. 65.
9 *Turkle*, Leben im Netz – Identität in Zeiten des Internet, 1999, S. 264 f.

Mit der Ubiquität von Datenverarbeitungsprozessen geht das *Big Data*-Phänomen einher, dass neben der Verarbeitung personenbezogener Daten die Wertschöpfung und die Innovationsmöglichkeiten aus diesen betrieben werden, was einen weitergehenden Schutzbedarf gegenüber dem Individuum auslöst.[10] Denn weitreichende Datenverarbeitungen ermöglichen das Entstehen von Datenreservoirs[11], aus denen umfangreiche Erkenntnisse ableitbar sind, die nicht nur das Risiko der Re-Identifizierbarkeit steigern, sondern aufgrund der Kombination und *Dekontextualisierung der Datensätze* den Schutz der informationellen Selbstbestimmung gefährden. Diese möglichen Erkenntnisse ergeben sich neben der Verarbeitung personenbezogener Daten aus der Einbeziehung von Metadaten, die aus den Interaktionen und dem Standortwechsel eines Individuums entstehen und zusammengeführt einen umfassenden Erkenntnisgehalt ermöglichen. Die 1983 im Volkszählungsurteil postulierten Feststellungen, dass es „unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses' Datum"[12] gäbe und die gewandelten technologischen Bedingungen umfassende und detaillierte Bilder einer Person ermöglichen[13], bleiben damit aktuell und finden in den jüngeren Entscheidungen „Recht auf Vergessen I & II"[14] eine weitere Konkretisierung für den online-Kontext.

Neben dem Phänomen der Datenverarbeitung gehört die Informations- und Wissenserlangung zum Geschäftsmodell von Intermediären, was personenbezogene Daten zu einem Rohstoff[15] macht. Den Intermediären kommt als Plattformbetreiber eine Schlüsselfunktion zu, da sie Akteure im Binnenmarkt der Datenökonomie und gleichzeitig Wärter über den Schutz der personenbezogenen Daten sind. Insofern kommt ihnen gegenüber dem Nutzer die Funktion eines Mediators[16] zu. Daher bildet das Konzept der digitalen Souveräntität zur Sicherstellung der individuellen Selbstbestimmung in seiner wirtschaftlichen Dimension ein Gegengewicht in der europäischen Datenökonomie. Dies gilt umso mehr, wenn die Trennung von Kontexten offline möglich ist, aber im online-Kontext die Grenzen der Kontexte faktisch aufgehoben sind.

---

10 *Smart Data Begleitforschung*, Smart Data - Smart Privacy?, 2015, S. 2 f.
11 *Solove*, Harv. L. R. 2013, 1880 (1889).
12 BVerfGE 65, 1 (45).
13 BVerfGE 65, 1 (17).
14 BVerfG, Urt. v. 06.11.2019 – 1 BvR 16/13, Recht auf Vergessen I; BVerfG, Urt. v. 06.11.2019 – 1 BvR 276/17, Recht auf Vergessen II.
15 *Smart Data Begleitforschung*, Smart Data - Smart Privacy?, 2015, S. 3
16 *European Data Protection Supervisor, EDPS*, Opinion 8/2016 on coherent enforcement of fundamental right in the age of big data, S. 6.

Die kontextspezifische Datenverarbeitung und Trennung der Erkenntnismöglichkeiten über die personale Identität stößt in Anbetracht der *Ubiquität von Datenverarbeitungen* auf Umsetzungsschwierigkeiten. Denn zu Beginn der Datenverarbeitung sind die hinzukommenden Kontexte und das damit verbundene Risiko erweiterter Erkenntnismöglichkeiten über die personale Identität noch unbekannt. Dies wird in der Konstellation eines smarten Arbeitsplatzes deutlich, bei dem intelligente Assistenzsysteme eingesetzt werden, die umfangreiche Erkenntnisse über das Nutzungsverhalten des Arbeitnehmers ermöglichen und aus denen sich nach einer gewissen Zeit möglicherweise gesundheitsrelevante Informationen ableiten lassen. Ebenso wird dies bei einem im Haushalt einer Familie lebenden Kindermädchen deutlich, das einer Beschäftigung nachgeht und gleichzeitig private Tätigkeiten vornimmt. Dabei ist der datenschutzrechtliche Anwendungsbereich für die private Tätigkeit gemäß Art. 2 Abs. 2 c) DSGVO ausgeschlossen und es hängt von der Erscheinung des Verhaltens ab, wann der Beschäftigtendatenschutz gilt. Weiter lassen sich in sozialen Medien persönliche Informationen austauschen, die zunächst vom Anwendungsbereich ausgeschlossen sind, aber zu einem späteren Zeitpunkt im Datenzyklus von dem Anwendungsbereich der DSGVO erfasst werden. Dies kann bei privat geteilten Informationen unter „Freunden", die in den Sozial- und Beschäftigungsbereich gelangen, erfolgen.

In diesen Konstellationen gelten unterschiedliche rechtliche Schutzregime, die aber ineinander übergehen und gemeinsam zu vielfältigen Erkenntnismöglichkeiten führen. Gesteigert wird die Aufhebung der kontextbezogenen Grenzen, wenn Endgeräte von Sprachassistenten oder gedankenlesenden Technologien mit einem sog. „*Machine-Interface*"[17] verdrängt werden und über eine Schnittstelle sämtliche Informationen aus dem Leben einer Person verarbeitet werden. Hiermit wird die Schwierigkeit einer eindeutigen Trennung der Kontexte besonders deutlich und kann kontextspezifische Schutzmechanismen erheblich erschweren. Dies gilt besonders, wenn die Erkenntnismöglichkeiten sich im Lebenszyklus einer personalen Identität von der urprünglichen Datenverarbeitung etwa im sozialen Netzwerk unvorhersehbar erweitern lassen. Demnach gilt es, das Risiko der kontextübergreifenden Erkenntniserlangung und Dekontextualisierung von personenbezogenen Daten in die grundrechtliche Selbstbestimmungsvorgabe einzubeziehen. Denn das interdependente und kontextübergreifende Gefüge von Datenverarbeitungen erfasse sämtliche Lebensbereiche, welches das spezifische Risiko der „systemischen Digitali-

17 *Budras*, FAS vom 14.10.2018, 21.

sierung“[18] darstelle und ein Schutzregime als Antwort verlangt. Dafür erscheint die Identitätsverwaltung mit der kontextbezogenen Transparenz über personale Identitäten und die Einräumung einer Kontrollmöglichkeit als eine mögliche Lösung. Folglich soll die personale Identität in IKT-Systemen eingeordnet und das IKT-Recht als Grundlage für die *Modellbildung der Identitätsverwaltung* herangezogen werden. Dafür sollen die Phänomene der personalen Identität im offline-Kontext mit dem online-Kontext verglichen werden, um daraus die spezifischen Anforderungen an die Identitätsverwaltung im online-Kontext ableiten zu können.

Mit der Transparenz kann ein Überblick über die Verantwortung des Nutzers hinsichtlich seiner personalen Identitäten im online-Kontext hergestellt werden. Die Notwendigkeit für eine gesteigerte Transparenz lässt sich aus den Speichermöglichkeiten über eine personale Identität ableiten, die im offline-Kontext in dem Maße nicht ersichtlich sind. Gleichwohl sei der Übergang zwischen personaler Identität im offline- und online-Kontext fließend und eine Trennung erscheine künstlich (sog. „*onlife*“),[19] so dass eine strikte Zuordnung der personalen Identität in den Kontexten als erschwert gilt. Dies steigert den Bedarf nach einem differenzierten Schutzmechanismus. Demnach müsste ein Identitätsverwaltungsmodell die Komplexität der personalen Identitäten im online- und offline-Kontext gleichermaßen erfassen und die Kontrollierbarkeit der personalen Identitäten fördern, was wiederum mit dem hier untersuchungsgegenständlichen Modell der Identitätsverwaltung ermöglicht werden soll.

C. Untersuchungsgegenstand

Für die Untersuchung der Rahmenbedingungen einer solchen Identitätsverwaltung in IKT-Systemen bedarf es zunächst der Einordnung in das *Konzept des Selbstdatenschutzes*. Mit dieser Einordnung geht die Annahme einher, dass das Individuum zunehmend in der Verantwortung steht, seine Schutzbedarfe und Rechte selbst zu verfolgen. Denn mit der ubiquitären Datenverarbeitung gehen neue Gefährdungen der informationellen Selbstbestimmung einher, die eines effektiven rechtlichen Schutzregimes bedürfen. Dieses Schutzregime bestand ursprünglich in dem ordnungsrechtlichen Datenschutz des BDSG a. F., der aber nur ineffektiv die neuen Phänomene ubiquitärer Datenverarbeitung lösen konnte. Damit wurde der

18 *Spiecker gen. Döhmann*, CR 2016, 698.
19 *Hildebrandt*, Smart technologies and the end(s) of law, 2015, S. 42, 50.

Bedarf eines neuen Datenschutzes formuliert, der über die Datenschutzprinzipien hinaus ein Schutzregime mit der Selbstregulierung durch Technikgestaltung ermöglicht.[20] Diese Selbstregulierung betrifft den Verantwortlichen und Betroffenen gleichermaßen, wenn es einerseits um die Implementierung von „*privacy by design*"-Lösungen geht und andererseits der Betroffene im Rahmen des Selbstdatenschutzes jederzeit seine Selbstbestimmung ausüben können soll.[21]

Diese gesteigerte Selbstbestimmung soll mit der Identitätsverwaltung umgesetzt werden und als eine technische Lösung für die Realisierung des Selbstdatenschutzes dienen (I.). Dabei bedarf es für die Eingrenzung der Identitätsverwaltung innerhalb eines Konzeptes des Selbstdatenschutzes der Bestimmung des zentralen Begriffs der Identität. Dieser soll in seinen rechtlichen Ausprägungen dargestellt werden und daneben die fachübergreifenden Perspektiven in den Untersuchungsgegenstand einbezogen werden (II.). Die konkrete Umsetzung der Identitätsverwaltung kann dabei eine dynamische Realisierung voraussetzen, um einen wirksamen und effektiven Schutz zu gewährleisten, was mit einem Regulationskonzept der mediativen Identitätsverwaltung erfolgen könnte (III.).

I. Selbstdatenschutz durch Identitätsverwaltung

Der Selbstdatenschutz als rechtliche Annahme aus der DSGVO bietet eine Lösung zur Realisierung der informationellen Selbstbestimmung und dient der Kompensation des datenschutzrechtlichen Vollzugsdefizits, mit dem der Betroffene gegen das Risiko eines „gläsernen Konsumenten" vorgehen könne.[22] Denn bei dem Phänomen der ubiquitären Datenverarbeitung wird besonders deutlich, dass die datenschutzrechtlichen Prinzipien der Transparenz, der Zweckbindung und Datenminimierung an ihre Grenzen stoßen. Die Transparenz komplexer Datenverarbeitungen und der Erkenntnismöglichkeiten lässt sich kaum für den Laien nachvollziehbar darstellen. Ferner ist eine weite Auslegung des Datenverarbeitungszwecks und eine Änderung dessen zu einem späteren Zeitpunkt der Datenverarbeitung möglich, so dass umfangreiche und unvorhersehbare Datenverarbeitungen vorgenommen werden können. Ebenso wird die Datenminimierung nur begrenzt umgesetzt, wenn Geschäftsmodelle darauf ausge-

20 *Roßnagel*, MMR 2005, 71 (74).
21 *Ders.*, MMR 2005, 71.
22 *Forum Privatheit*, White Paper – Selbstdatenschutz, 2014 S. 3 f.

richtet sind, möglichst umfassend Zugang zu personenbezogenen Daten zu erlangen. Daraus ergibt sich, dass der datenschutzrechtliche Vorfeldschutz gegenüber den Realphänomenen nur unzureichenden Schutz bietet und die Identitätsverwaltung als Konzept des Selbstdatenschutzes als Lösungsmechanismus heranzuziehen ist.

Der Lösungsmechanismus im Rahmen des Selbstdatenschutzes ist aus dem IKT-Recht in Gestalt der Transparenz, der Einwilligung, der Betroffenenrechte und dem Einsatz von technischen und organisatorischen Maßnahmen abzuleiten. Hinsichtlich der technischen Maßnahmen könnte für den Selbstdatenschutz ein Mechanismus in Frage kommen, mit dem der Nutzer sich selbst schützt. Damit würde der Selbstdatenschutz aus dem IKT-Recht mit einem technischen Konzept erweitert werden, welches über eine technische Normierung realisiert und zu einer Umsetzungsaufgabe der Hersteller werden könnte. Weiter müsste ein Konzept des Selbstdatenschutzes in einem Gesamtgefüge zum Schutz der personenbezogenen Daten stehen, welches zudem aus aufsichtsrechtlichen und strukturellen Schutzmaßnahmen bestehen kann. Mit einem in diesem Gesamtgefüge bestehenden Konzept des Selbstdatenschutzes würde die natürliche Person wieder zum Steuerungsadressaten „ihrer" Daten werden und es könnten zusätzliche Anreizmechanismen zur expliziten Steuerung der personenbezogenen Daten und der damit verbundenen personalen Identitäten eingesetzt werden.

Demnach soll ein *Modell zur Identitätsverwaltung* begründet werden, mit dem der bestehende Schutz im IKT-Recht um eine Schutzebene erweitert und als Grundlage für die Identitätsverwaltung herangezogen wird. Dabei soll der zentrale Schutzgegenstand der informationellen Selbstbestimmung über den Lebenszyklus einer personalen Identität hinweg gewahrt bleiben können und einen möglichen kompensatorischen Mechanismus enthalten, der einen Ausgleich gegenüber dem datenschutzrechtlichen Vollzugsdefizit darstellt. Für diesen Mechanismus könnte die Transparenz der Risiken von Datenverarbeitungsvorgängen über personale Identitäten erforderlich sein, um einen wirksamen Schutz der informationellen Selbstbestimmung herbeiführen zu können. Mit der Identitätsverwaltung als Möglichkeit der Selbstkontrolle könnte ein Gegengewicht zu den Phänomenen der ubiquitären Datenverarbeitung von Intermediären und der damit verbundenen Fremdkontrolle begründet werden. Sobald das „Risiko der Fremdbestimmung"[23] steige, bedarf es eines wirksamen Selbstdaten-

23 *Roßnagel*, in: Roßnagel/Abel (Hrsg.), Handbuch Datenschutzrecht, 2003, 3.4. Rn. 2.

schutzes gegen die entstandenen Informationsasymmetrien und algorithmusgesteuerten Erkenntisverfahren. Denn neben den Kräften des demokratischen Gesetzgebers wirkt der Markt auf die Phänomene in online-Kontexten und dieser Markt hat das Potential, den Bürger mit seinen Schutzmöglichkeiten zu verdrängen. Folglich könnte mit der Identitätsverwaltung und einem angemessenen regulatorischen Rahmen ein Gegengewicht geschaffen werden, welches den Selbstdatenschutz der natürlichen Person stärkt. Denn das Individuum verbleibt als „einziger plausibler Akteur“[24], der im Mittelpunkt des grundrechtlichen und IKT-rechtlichen Schutzes steht und seine Schutzwürdigkeit mit der fortschreitenden ubiquitären Datenverarbeitung beibehalten sollte.

II. Begriff der Identität

Der Begriff der Identität wird in der Rechtsordnung vielfach verwendet und es können in ihm aufgrund der rechtswissenschaftlichen Perspektive, welche als „disziplinäres Cluster“[25] verstanden werden kann, verschiedene fachliche Ausprägungen zum Ausdruck kommen. Dafür soll der Begriff zunächst überblicksartig im Recht eingeordnet (1.) und anschließend aus der philosophischen Perspektive (2.) beleuchtet werden. Mit der philosophischen Betrachtung wird die inhaltliche Grundlage für den Bedeutungsgehalt des Begriffs der personalen Identität geprägt werden. Die herausgearbeiteten Phänomene der personalen Identitäten sollen für die untersuchungsgegenständliche Modellbildung der Identitätsverwaltung herangezogen werden.

1. Identität im Recht

Unter dem Begriff der Identität wird zunächst die rechtliche Anerkennung einer staatlichen Zugehörigkeit verstanden. Diese Ausprägung der Identität entspricht einem Menschenrecht und wird von den Vereinten Nationen als solches in Ziffer 16.9 aus der „*2030 Agenda for Sustainable Develop-*

24 *Teubner*, Zeitschrift für Rechtssoziologie 2006, 5 (6).
25 *Jestaedt*, in: Kirste (Hrsg.), Interdisziplinarität in den Rechtswissenschaften, 2016, S. 110.

ment" festgeschrieben, wonach bis 2030 jeder über eine rechtliche Identität, einschließlich der Eintragung im Geburtenregister, verfügen soll.[26]

In nationaler Hinsicht lassen sich unter dem Identitätsbegriff der Name, die Eintragung im Geburtenregister und die Informationen im Personalausweis einordnen. Dahingehend wurde die „digitale Identität"[27] spiegelbildlich zur offline-Welt im elektronischen Personalausweis gemäß § 18 PAuswG anerkannt. Diese digitale Identität kann im online-Kontext eingesetzt werden, indem mit einem Passwort eine Authentifizierung ermöglicht und die digitale Identität einem Individuum zugewiesen wird. Mit der Zuweisung von Passwörtern könnte im privatrechtlichen Kontext die sog. „*Single Sign-On*"-Lösung mit nur einem Passwort als Konzept der Identitätsverwaltung umgesetzt werden, wie es bereits von Intermediären zum erleichterten Registrieren und Anmelden angeboten wird.

Neben dem Konzept der Identitätsverwaltung als Berechtigungsverwaltung mit Passwörtern,[28] soll der Begriff der personalen Identität mit seinen Ausprägungen aus Art. 4 Nr. 1 DSGVO herangezogen werden. Damit soll die Identitätsverwaltung im Sinne eines Passwortmanagers um die datenschutzrechtlich anerkannten Ausprägungen der personalen Identität erweitert werden. Dies ist der erste zentrale Beitrag, der in dieser Untersuchung geleistet werden soll, um das Schutzregime im Rahmen des Selbstdatenschutzes in der DSGVO konkretisieren zu können. Für die Veranschaulichung dieser Pluralität an Phänomenen der personalen Identitäten, die gerade in online-Kontexten sichtbar werden, soll der einfachrechtliche Bezug zur Identität über das Namensrecht hinaus einbezogen werden. Dafür werden neben den Ausprägungen der „physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität"

26 www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E (zuletzt aufgerufen 20.06.2020). Ebenso ist in der UNCITRAL, *Working Group IV – Electronic Commerce*, ein internationalisiertes Konzept der Identitätsverwaltung der Gegenstand von Konsultationen. Bei der Findung von gemeinsamen Regelungen wird die eIDAS-VO als Regelungsbeispiel mit einbezogen. Gleichwohl sind die rechtskulturellen Unterschiede der Mitgliedstaaten über den Schutz der Privatheit derart differenziert, dass ein internationales datenschutzrechtliches Identitätsverwaltungsmodell nur schwer realisierbar sein wird. Damit würde sich eine mögliche Regelung der Identitätsverwaltung auf die internationale Nutzung von Signaturen und elektronischen Identitäten beziehen (Gespräch am 04.02.2019 mit zuständigem Referat im BMWi).

27 *Hornung*, Die digitale Identität, 2005.

28 *Roßnagel*, in: Roßnagel/Abel (Hrsg.), Handbuch Datenschutzrecht, 2003, 3.4. Rn. 68.

gemäß Art. 4 Nr. 1 DSGVO die personalen Teilidentitäten im IKT-Recht für die Modellbildung herangezogen.

Aus diesen Dimensionen der personalen Identität wird ein *stipulatives Modell zur personalen Identität und der Identitätsverwaltung* begründet. Damit könnte eine Entsprechung der personalen Identität mit ihren pluralen Ausprägungen von dem offline- in den online-Kontext übertragen und ein gleichwertiger Schutzmechanismus begründet werden.

2. Identität aus der philosophischen Perspektive

a) Identität von der Ununterscheidbarkeit zum Handlungsergebnis

Der Identitätsbegriff aus der philosophischen Perspektive lässt sich zunächst mathematisch nach *G. W. Leibniz* als Prinzip der Identität des Ununterscheidbaren umschreiben.[29] Darin komme die Bedeutung der Identität als „*idem*" also Gleichheit zum Ausdruck, womit ein Zuordnungszustand von absoluter Identität beschrieben wird, der eine qualitative Differenz zweier Objekte ausschließt.[30] Dem folgend erscheint die Identität in der Natur zweifelhaft, da etwa kein Eichenblatt oder kein Lebewesen dem anderen gleichen könne.[31] Mit dem Begriff der Identität geht daher die Singularität einher, die jedoch nur dann feststellbar ist, wenn der Vergleich zweier Objekte in einem Kontext vorgenommen wird. Darin kommt zum Ausdruck, dass die Identität der Klarstellung eines absolut Gleichen dient und gleichzeitig die Beschreibung der Operation des Vergleichens ist.

Da in der Biographie eines Individuums der Lebende von Kindesbeinen an immer derselbe sei, auch wenn er das Alter erreicht habe, befinde sich das Individuum in seiner Biographie immer in einem System von Beziehungen.[32] In diesem werde sich das Individuum immer wieder in seiner Physiologie über die Haare und das Blut erneuern und in seinen Beziehungen über die Freuden, Befürchtungen, Meinungen und Gewohnheiten niemals gleich bleiben im Sinne einer mathematischen Gleichheit.[33] Folglich

29 *Brockhaus Enzyklopädie,* 2006, Bd. 13, zu „Identität".
30 *Meuter*, in: Kolmer/Wildfeuer/Krings u.a. (Hrsg.), Neues Handbuch philosophischer Grundbegriffe, 2011, Bd. 2, S. 1203; *Siegwart*, in: Sandkühler (Hrsg.), Enzyklopädie Philosophie, 2010, Bd. 2, S. 1067.
31 *Brockhaus Enzyklopädie,* 2006, Bd. 13, zu „Identität".
32 *Platon*, Symposion, 2008, 207 D.
33 *Ders.*, Symposion, 2008, 207 E.

kann die Realisierung von Identität und ihre kontextbedingte Abhängigkeit festgestellt werden, worin der Begriff der Identität eine inhaltliche Ausgestaltung erfährt.[34] Die personale Identität knüpft demnach an die Physis und das Verhalten der Person an und wird relational bestimmt.

Nach *Koorsgard* wird die Handlung als Zweck der personalen Identität beschrieben und als Ergebnis des inneren Entscheidungsprozesses, der in eine äußerlich wahrnehmbare und vorübergehende („*contingent*") Handlung münde.[35] Die personale Identität setze sich zusammen aus den inneren Entscheidungen und äußeren Handlungen, worin eine „Konzeption von praktischer Identität" als Beschreibung und Selbstdarstellung des eigenen Selbst liege.[36] Schließlich führt *Korsgaard* aus, dass eine Giraffe nur dann eine sei, wenn sie das Prinzip verfolge, sich wie eine Giraffe zu verhalten.[37] Demnach sei die Handlung als Konstituierung und Konstruktion der Persönlichkeit und Identität einzuordnen.[38] Für den Begriff der personalen Identität lässt sich daraus zum einen der Name als Gleichheit und zum anderen die Handlung als konstitutives Element über die Biographie hinweg einordnen.

b) Identität nach *Ricœur*

Aus der philosophischen Perspektive bezieht der Identitätsbegriff nach *Ricœur* drei Ebenen in das Modell ein. Diese bestehen aus der Identität im Sinne der Gleichheit, der Identität als Selbst und der Identität als Realisierung einer Handlung in einer kommunikativen Beziehung. Folglich handelt es sich bei *Ricœur* um eine zusammengesetzte Identität, die einen numerischen Teil der Gleichheit *(Idem)* umfasst, welcher auf die Frage des „*Wer?*" zugeordnet werden könne, und einem sprechenden Teil als Selbstheit *(Ipse)*, der sich über die Handlung dynamisch realisiere.[39] Beide Ausprägungen der Identität stehen dialektisch zueinander und begründen den

34 *Meuter*, in: Kolmer/Wildfeuer/Krings u.a. (Hrsg.), Neues Handbuch philosophischer Grundbegriffe, 2011, Bd. 2, S. 1202; *Luhmann*, in: Marquard/Stierle (Hrsg.), Identität, 1979, S. 322 ff.
35 *Korsgaard*, Self-Constitution, 2009, S. 12.
36 *Dies.*, Self-Constitution, 2009, S. 19 f.
37 *Dies.*, Self-Constitution, 2009, S. 35–37.
38 *Dies.*, Self-Constitution, 2009, S. 42 f.
39 *Ricœur*, Oneself as another, 1994, S. 116; ebenso auf *Ricœur* abstellend, vgl. *Hildebrandt*, Smart technologies and the end(s) of law, 2015, S. 81 f.

Charakter, der mediativ zwischen *Idem* und *Ipse* der Identität steht.[40] Mit dem dialektischen Verhältnis zwischen *Idem* und *Ipse* wird der bestehende Widerspruch zwischen statischer Gleichheit und dynamischer Selbstheit innerhalb einer personalen Identität aufgelöst.[41] Darin kommt die temporäre Dimension der personalen Identität zum Ausdruck, die sich dialektisch zwischen *Idem* und *Ipse* als Charakter bildet, und als temporäre Aktion der narrativen Identität in der kommunikativen Beziehung zur Außenwelt sichtbar wird.[42]

Mit der kommunikativen Beziehung wird ein *Agent als Bild der erscheinenden personalen Identität* begründet und für den Empfänger als eingegangenen Nachrichtengehalt erkennbar. Somit wird mit dem Agenten ein Zuschreibungsgegenstand geschaffen, der aus der Handlung und dem *Idem-Ipse*-Dialog besteht, womit im Rahmen der kommunikativen Beziehung eine Eigendynamik ausgelöst wird. Daraus können durch Zuschreibungen über die personale Identität weitere Attribute entstehen, die wiederum in das dialektische Verhältnis zwischen *Idem* und *Ipse* als Selbst und Ergebnis der reflexiven Äußerungen in Gestalt von Handlungen einfließen (Abbildung 1).[43]

Diese Annahmen dienen als philosophische Grundlage für die Modellbildung der Identitätsverwaltung, weshalb die Differenzierung zwischen dem *Idem-* und *Ipse*-Anteil einer personalen Identität im IKT-Recht eingeordnet werden soll. Denn mit einem Identitätsbegriff, der sich aus einer statischen und einer dynamischen Dimension zusammensetzt, lässt sich die Orientierung in den Regelungsbereichen zur Identität und des IKT-Rechts herstellen. Damit soll das grundrechtliche Schutzregime zur Identität herausgearbeitet und in die Modellbildung die differenzierten Ausprägungen des Identitätsbegriffs einbezogen werden.

40 *Ders.*, Oneself as another, 1994, S. 124.
41 *Ders.*, Oneself as another, 1994, S. 113 f.
42 *Ders.*, Oneself as another, 1994, S. 143.
43 *Ders.*, Oneself as another, 1994, S. 88, 122.

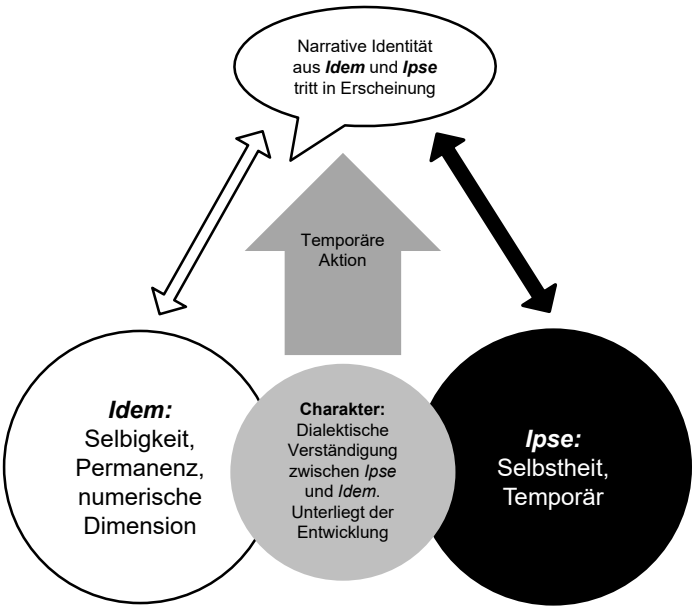

Abbildung 1: Modell zu Ricœur, „Oneself as another"[44]

III. Begründung einer regulierten mediativen Identitätsverwaltung

Die Identitätsverwaltung in IKT-Systemen könnte nach den vorgenommenen Darstellungen aus einer mediativen Identitätsverwaltung auf der Mikro- und Makroebene als ein Konzept des Selbstdatenschutzes bestehen, welches die Konzepte der *Idem*- und *Ipse*-Anteile implementiert. Mit der Prämisse eines kontextbezogenen Schutzes der personalen Identität geht es um ein ausgleichendes Schutzregime gegenüber bestehenden Informationsasymmetrien zwischen dem Verantwortlichen und Betroffenen auf der Mikro- und Makroebene.

Diese ausgleichenden Regelungsmöglichkeiten könnten auf der Mikroebene dynamisch in technischer Hinsicht ausgestaltet werden und als eine Erweiterung der bekannten informationstechnischen Berechtigungsverwaltung dienen. Die rechtlichen Anforderungen einer kontextangemessenen Identitätsverwaltung verlangen die Einbeziehung der Rechte aus dem

44 Modell orientiert an *ders.*, Oneself as another, 1994.

IKT-Recht, wozu die interoperable Ausgestaltung gehört, um die kontextübergreifende Kontrolle personaler Identitäten und die Entwicklungsbedingungen hinsichtlich des *Ipse*-Anteils zu ermöglichen. Dazu gehört ein Mechanismus, mit dem gegen diskriminierend wirkende Algorithmen auf personale Identitäten vorgegangen werden kann, was auf der rechtlichen und der technischen Ebene mit einem *„mechanism by design"* erfolgen könnte. Die Immunisierung der personalen Identität im online-Kontext würde auf der Mikroebene mit einem technischen Mediator als Vermittler erfolgen, der spieltheoretisch herzuleiten ist. Dieser würde in einem dialogischen Verfahren die Verhandlung der personalen Identitäten ermöglichen und den Schutz der *kontextuellen Integrität* gewährleisten.

Auf der Makroebene würde diese Identitätsverwaltung eine strukturelle Gewährleistung des dezentralen Identitätszugangs erfordern, mit dem die *personalen Identitäten kontrollierbar* wären. Dafür wird der Bedarf an einer erweiterten Transparenz als möglicher Lösungsmechanismus dargestellt, um strukturell einen Schutzmechanismus gegen die Intermediäre mit marktbeherrschender Stellung zu schaffen. Weiter kommt auf der Makroebene eine Plattform zur Identitätsverwaltung in Betracht, die als ein geschlossenes System zur kontextangemessenen Verwaltung personaler Identitäten fungiert. Somit ermöglicht eine mediative Identitätsverwaltung die Hinwendung zu einem differenzierten Ausgestaltungssystem für die private Datenverarbeitung als Erweiterung zur grundsätzlich bestehenden datenschutzrechtlichen Abwehrdimension. Darin lässt sich ein aktiver Gestaltungsmechanismus ausdrücken, in dem sich die Risiken der Datenverarbeitung im privaten Kontext abbilden lassen.

Mit der Förderung der Datenökonomie im europäischen Binnenmarkt bietet die europäische Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen (eIDAS-VO)[45] die Grundlage für ein europäisiertes interoperables Identitätsverwaltungsmodell. Darin kommt die Verwaltung der personalen Identitäten in Gestalt der *Idem*-Anteile zum Ausdruck, da die grenzüberschreitende Identifizierung für den elektronischen Rechtsverkehr geregelt wird. Dieses Konzept soll mit den datenschutzrechtlichen Maßgaben erweitert werden und Anhaltspunkte für eine mediative Identitätsverwaltung bieten. Damit wird ein Paradigmenwechsel in der Identitätsverwaltung nachgewiesen, der in einer Weiterentwicklung zu einer dynamischen Identitätsverwaltung über

45 Verordnung Nr. 910/2014 vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.

die *Ipse*-Anteile der personalen Identität im online-Kontext liegt. Schließlich würde darin ein konkretes Modell zur Realisierung des Selbstdatenschutzes zum Ausdruck kommen.

D. Gang der Untersuchung

Der Untersuchungsgegenstand zielt insofern auf die Modellbildung für eine soziotechnische Identitätsverwaltung ab, die als ein Konzept im Selbstdatenschutz fungiert und dem dialogisch geprägten Identitätsbegriff in seinen *Idem*- und *Ipse*-Anteilen Rechnung trägt. Für die Modellbildung bedarf es zunächst der Bestimmung grundrechtlicher Anforderungen an den Schutz der Identität als Fundament für die Ausgestaltung der Identitätsverwaltung und zur Stärkung des Selbsdatenschutzes. Die Realweltphänomene der personalen Identität sind dabei in ihren einfachrechtlichen Schutzbedarfen im offline- und online-Kontext gleichermaßen abzubilden.

Demnach werden die *Grundlagen der Identitätsverwaltung* für die Modellbildung im 2. Teil der Untersuchung aus den Grundrechten abgeleitet, die mit der Einordnung des Schutzes der personalen Identität in der europäischen Grundrechtecharta aus Art. 7, 8 GRC beginnt und bereits ein Modell für die Identitätsverwaltung aufweisen könnte. Danach wird die personale Identität in ihrer inneren Dimension mit dem Recht auf Achtung des Privatlebens etwa durch Kenntnis der Abstammung geschützt und in der äußeren Dimension wird der persönliche Reputationsschutz als Kontrollmöglichkeit über die Selbstdarstellung gemäß Art. 7, 8 GRC nachvollzogen. Daneben werden die Dimensionen zum Schutz der personalen Identität von den Grundrechten des allgemeinen Persönlichkeitsrechts und der allgemeinen Handlungsfreiheit flankiert. Damit soll die grundrechtliche Gewährleistung der Persönlichkeitsentwicklung für den online-Kontext aufgezeigt werden, was die Differenzierung der *Idem*- und *Ipse*-Anteile einer personalen Identität in dem Modell nach *Ricœur* einbezieht.

Ergänzend wird das liberal geprägte Privatheitskonzept des angloamerikanischen Rechtsraumes einbezogen, da die wellenförmige Beeinflussung

der Rechtskulturen[46] der Erweiterung des Betrachtungsspektrums dient[47] und Anhaltspunkte für ein ausgleichendes Schutzregime für die personale Identität gewonnen werden können. Gleichzeitig wird eine fachübergreifende Perspektive zur personalen Identität einbezogen, da der Identitätsbegriff in seinem konkreten Bedeutungsgehalt erheblich von der Betrachtungsperspektive abhängt. Zudem sollen in Anbetracht der Rechtswissenschaft als disziplinäres Cluster[48] die informationstechnische, die psychologische und die kommunikationspsychologische Perspektive in die Untersuchung einbezogen werden. Damit werden die Ergebnisse aus der grundrechtlichen Betrachtung um weitere Fundierungen ergänzt, um die Voraussetzungen für die Modellbildung konkretisieren zu können. Maßgeblich ist dabei der Nachweis, dass die *Instruktion* innerhalb eines Kommunikationsprozesses auf der Metaebene als Schutzmechanismus in das Modell der Identitätsverwaltung einzubeziehen ist.

Mit diesen grundlegenden Feststellungen sollen im 3. Teil der Untersuchung die Anforderungen an das Modell der Identitätsverwaltung in einfachrechtlichen Typologien aus der Realwelt konkretisiert und die Anknüpfung an den Namen für die Zuordnung der Identität in ihrem *Idem*-Anteil zum Individuum vorgenommen werden. Der Name als Identifizierungsgrundlage im elektronischen Rechtsverkehr wird dabei einbezogen und gemäß Art. 8 Abs. 2 eIDAS-VO[49] das *dreistufige Vertrauens- und Sicherheitsniveau* für eine kontextangemessene Identifizierung vorgestellt, welches als Grundlage für die Beschreibung der Modellanforderungen an eine interoperable und kontextangemessene Identitätsverwaltung dient. Neben der Identifizierung mit dem *Idem*-Anteil einer personalen Indentität wird aufgezeigt, dass im elektronischen Rechtsverkehr die vertrauliche sichere Kommunikation nach dem De-Mail-G ebenfalls geschützt ist.

Mit dieser dynamischen Dimension der Kommunikation kommt der Datenzyklus über eine personale Identität zum Ausdruck. Dieser soll eben-

---

46 *Whitman*, Yale L. J. 2004, 1151 (1158 f., 1203), der die wechselseitigen Beeinflussungen der Rechtskulturen am Schutz der Privatheit beschreibt. Weiter wird auf die Wahrnehmungen und Perspektiven aus den Rechtskulturen abgestellt, wonach etwa aus der angloamerikanischen Perspektive das deutsche Meldewesen als hochgradig freiheits- und privatheitsbeschränkend wirken kann.

47 *Kischel*, Rechtsvergleichung, 2015, § 1 Rn. 16.

48 *Jestaedt*, in: Kirste (Hrsg.), Interdisziplinarität in den Rechtswissenschaften, 2016, S. 110.

49 Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt.

falls als Kontrollgegenstand eingeordnet werden und führt zu der Darstellung des Erkenntnismodells über Daten, Informationen und Wissen. Anschließend wird die Differenzierung zwischen der relativen Kontrolle von Erkenntnissen aus der Kommunikation und der absoluten Kontrolle als Zugangsrecht zur personalen Identität vorgenommen. Weiter ist die Handlungsträgerschaft über die Bilder personaler Identitäten als Grundlage für die Modellbildung heranzuziehen. Sie wird in einer Prinzipal-Agenten-Beziehung dargestellt, in der die Agenten als Handlungsträger über die personale Identität fungieren.

Im 4. Teil wird das Identitätsverwaltungsmodell auf der Grundlage des IKT-Rechts begründet und die DSGVO einer chronologischen Betrachtung des Datenzyklus *ex ante* zur Rechtfertigung, der Rechtfertigung und *ex post* zur Rechtfertigung unterzogen. Dafür wird das begründete stipulative Identitätsverwaltungsmodell mit den *Idem*- und *Ipse*-Anteilen der Identität herangezogen, um dieses dem Regelungsregime des IKT-Rechts gegenüberzustellen und das bestehende IKT-rechtliche Identitätsverwaltungsmodell herauszuarbeiten. Dabei wird nachgewiesen, dass die erste Kontrollmöglichkeit über die Informationspflichten gemäß Art. 12, 13 DSGVO besteht und auf dieser Grundlage eine risikobewußte Entscheidung von dem Betroffenen möglich wird, was die Frage nach der Risikobewertungsmethode aufwirft.

Weiter gilt die Einwilligung gemäß Art. 6 Abs. 1 a) DSGVO als maßgebliche Kontrollmöglichkeit des Betroffenen, so dass diese einer näheren Betrachtung unterzogen und die rechtswissenschaftliche Subdisziplin der Verhaltensökonomik[50] einbezogen wird. Damit soll eine mögliche „Kluft zwischen Sein und Sollen“[51] identifiziert werden und in einen effektiven Schutzmechanismus bei der Modellbildung überführt werden. Daneben werden die bereichsspezifischen Datenschutzregeln im TMG und TKG in die Modellbildung einbezogen, solange sich die EPrivacy-VO[52] noch im Entwurfsstadium befindet. Nach den Analysen des IKT-Rechts wird ein *iteratives Verhandlungssystem* zwischen Verantwortlichem und Betroffenen be-

50 *Van Aaken*, in: Kirste (Hrsg.), Interdisziplinarität in den Rechtswissenschaften, 2016, 187 (189).

51 *Grimm*, in: Kirste (Hrsg.), Interdisziplinarität in den Rechtswissenschaften, 2016, 21 (24).

52 Vorschlag für eine Verordnung des europäischen Parlamentes und Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), COM/2017/010 final, 2017/03.

gründet, welches dem statischen *Idem*-Anteil und dynamischen *Ipse*-Anteil einer personalen Identität Rechnung trägt und übergeordnete *Instruktionen* über die personalen Identitäten ermöglicht. Dieses Verfahren lässt sich über ein technisches *Dashboard-System* abbilden, das über den gesamten Datenzyklus hinweg die IKT-rechtlichen Schutzmechnismen und einen Zugang zu den personalen Identitäten gewährleisten könnte. Die Identitätsverwaltung über ein *Dashboard-System* wird somit als ein *Metaverfahren* mit einer interoperablen Struktur über die kontextspezifischen personalen Identitäten hergeleitet.

Mit der *spieltheoretischen Perspektive* im 5. Teil soll die Identitätsverwaltung als Metaverfahren konkretisiert werden, indem die IKT-rechtlich fingierten Handlungen spieltheoretisch modelliert und die strukturellen Wirkmechanismen im IKT-Recht aufgezeigt werden. Sobald die Anreizmechanismen für die ökonomisch motivierten Entscheidungen im IKT-Recht bestimmt werden, lässt sich daraus ein Lösungsmechanismus zum Schutz der personalen Identität ableiten, was mit dem spieltheoretisch begründeten Konzept der mediativen Identitätsverwaltung vorgesehen ist. Dafür wird die Bestimmung des öffentlichen Gutes der persönlichen Informationen als Verhandlungsgegenstand zwischen Betroffenen und Verantwortlichem vorgenommen, da die personale Identität sich aus persönlichen Informationen zusammensetzt. Weiter wird die Strategiewahl, basierend auf dem IKT-Recht, in eine defektive und kooperative Handlungsmöglichkeit unterteilt, damit die Untersuchung der Handlungsauswirkungen auf das öffentliche Gut der persönlichen Informationen folgen kann. Daraus wird ein datenschutzrechtlicher „*Market for Lemons*" nachvollzogen, der in einer gesteigerten Marktpräsenz von Diensten mit einem niedrigen Datenschutzniveau besteht und sich nachteilig auf das öffentliche Gut der persönlichen Informationen auswirkt. Folglich wird die für das öffentliche Gut schonende „*TIT for TAT*"-Strategie aufgezeigt, die der Begründung eines technischen Mediationsagenten dient. Damit wird ein „*mechanism by design*" hergeleitet, der im Datenzyklus dem Schutz der persönlichen Informationen dient und eine risikomindernde Wirkung entfaltet. Ein Gesamtkonzept der mediativen Identitätsverwaltung könnte die *iterative Verhandlung* der personalen Identitäten ermöglichen und als datenschutzrechtliche Technikanforderung gemäß Art. 25 DSGVO umgesetzt werden.

Daraus wird in dem 6. Teil ein Modell der Identitätsverwaltung gebildet, welches die Vielfältigkeit der personalen Identität in den online-Kontext von IKT-Systemen überträgt und die *Idem*- und *Ipse*-Anteile der personalen Identität zu einem Kontrollgegenstand werden lässt. Demnach wird aus den beschriebenen Realphänomenen und dem IKT-Recht ein Paradigmen-

wechsel von der Berechtigungsverwaltung zur Kontrolle über den Identitätszugang aufgezeigt, der eine Abkehr von einem statischen Identitätsbegriff bedeutet und die *iterative Verhandlungsmöglichkeit* von personalen Identitäten im online-Kontext einräumt. Weiter wird nachgewiesen, dass die Voraussetzungen für ein Identitätsverwaltungsmodell kontextspezifisch, dezentral und mit einer dialogischen Verhandlungsmöglichkeit abzubilden sind, wofür ein *Dashboard-System* als geeignet erscheint. Dieses soll in seiner Funktionalität den Zugang zu den personalen Identitäten und den Zugang zu einem *iterativen Verhandlungsverfahren* über die personalen Identitäten ermöglichen. Weiter wird die Plattform für die Identitätsverwaltung dargestellt, die als ein geschlossenes System zur Verwaltung der *Idem-* und *Ipse-*Anteile einer personalen Identität im online-Kontext funktionieren würde.

Inwieweit die Modellvoraussetzungen einen eigenständigen soziotechnischen Regelungsbedarf auslösen, wird im 7. Teil vorgestellt und ist Gegenstand der abschließenden Analysen. Diese führen zu der einfachrechtlichen Anforderung, dass die „*privacy by design*"-Regelung gemäß Art. 25 DSGVO mit einer ausdrücklichen „*identity management by design*"-Anforderung erweitert werden sollte. Ferner könnte sich eine einfachrechtliche Regelung an den Hersteller richten und das Produkthaftungsrecht um den Schutz der informationellen Selbstbestimmung erweitert werden. Schließlich wird ein prinzipienbasierter Ansatz zur Implementierung eines Schutzkonzeptes der verhandlungsfähigen Identität im online-Kontext begründet, der als konsequentes Schutzregime für die personale Identität aus den Grundrechten fungiert.