4.Teil: Begründung der Identitätsverwaltung im IKT-Recht

Für die Identitätsverwaltung im IKT-Recht soll eine differenzierte Analyse der maßgeblichen Rechtsregeln vorgenommen werden. Nach dem OSI-Schichtenmodell[352] ist die Anknüpfung auf der höchsten Ebene an die Dienste als Anwendungsebene vorgesehen, so dass die Datenschutzgrundverordnung, das Telemedienrecht und anschließend das Telekommunikationsrecht zum Gegenstand der Analysen werden. Zunächst sollen die Gegenstände der Identitätsverwaltung im online-Kontext aus der Datenschutzgrundverordnung abgeleitet werden, um daraus die Grundlagen für stipulative Definitionen zur Bewertung des IKT-Rechts herauszuarbeiten (A.). Dabei sollen die Schutzebenen innerhalb der Identitätsverwaltung bestimmt werden und gleichzeitig die Risiken für den Schutz der personalen Identität und der Erkenntnisse über diese nachvollzogen werden. Demnach soll sich die *Modellbildung der Identitätsverwaltung* aus der Datenschutzgrundverordnung an dem Datenzyklus und den damit verbundenen Risiken orientieren. Dies erfolgt anhand der datenschutzrechtlichen Grundidee eines phasenorientierten Datenschutzes[353] bei der Verarbeitung personenbezogener Daten. Folglich wird in den zeitlichen Dimensionen *ex ante* zur begründeten Rechtmäßigkeit der Datenverarbeitung (B.), der Rechtmäßigkeitsbegründung (C.) und *ex post* zur begründeten Rechtmäßigkeit (D.) unterschieden. Dabei werden die maßgeblichen datenschutzrechtlichen Vorschriften für die Identitätsverwaltung nachvollzogen. Diese Betrachtungen zur Datenschutzgrundverordnung werden mit den personalen Teilidentitäten aus dem Telemedien- und Telekommunikationsrecht ergänzt (E.), um die IKT-rechtlichen Ausprägungen der personalen Identität zu vervollständigen. Insgesamt sind dabei die konkreten Anforderungen an ein Identitätsverwaltungsmodell nach dem IKT-Recht herauszuarbeiten und anhand des stipulativen Identitätsverwaltungsmodells zu bewerten.

352 *Schmidt/Pruß*, in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, 2018, § 3 Rn. 62–64.

353 *Steinmüller*, RDV 2007, 158 (159).

A. Identitätsverwaltung in der Datenschutzgrundverordnung

I. Personale Identität in der Datenschutzgrundverordnung

1. Personale Identität aus personenbezogenen Daten, Art. 4 Nr. 1 DSGVO

Bereits die Bestimmung des Schutzbereiches nach Art. 8 GRC nimmt Bezug auf die sekundärrechtliche Definition der personenbezogenen Daten. Danach sind personenbezogene Daten alle Informationen über eine bestimmte oder bestimmbare natürliche Person. Eine Person ist bestimmbar, wenn diese direkt oder indirekt identifiziert werden kann über die Personalausweis-, Telefon-, Konto- oder sonstige Nummer oder durch Elemente, die *Ausdruck* der physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sonstigen Identität sind.[354] Im Gegensatz zu dem im Kommissionsentwurf der DSGVO in Art. 4 Nr. 1 enthaltenen Wortlaut, „personenbezogene Daten (sind) alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen", stellt der darauf folgende Entwurf des europäischen Rates ein Bekenntnis zum Identitätsbegriff dar und wurde auch in der Endfassung der DSGVO aufgenommen. Denn in Art. 4 Nr. 1 DSGVO werden personenbezogene Daten als Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität von natürlichen Personen beschrieben, die der Schutzbereichsbestimmung zu Art. 8 GRC entsprechen. In der Definition der personenbezogenen Daten ist keine abschließende Aufzählung über die möglichen Identitäten enthalten, sondern diese sind exemplarisch zu verstehen, wie es sich aus dem Wortlaut „Ausdruck" ergibt, dem die Bedeutung des Erscheinens gleichkommt. Ferner überschneiden sich die aufgezählten Identitätsausprägungen und können nicht unabhängig voneinander stehen, wie es bei der sozialen und kulturellen Identität augenscheinlich wird. Dies spricht insgesamt für die Annahme einer exemplarischen Aufzählung der Identitätsausprägungen in Art. 4 Nr. 1 DSGVO.

Weiter unterliegen personenbezogene Daten und die damit zum Ausdruck kommenden Identitäten einem geringeren Schutzniveau als die besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO, an deren Verarbeitung höhere Anforderungen geknüpft sind. Zu den besonderen Kategorien personenbezogener Daten gehören die rassische und eth-

354 *Jarass*, Kommentar, Charta der Grundrechte der EU, 2016, Art. 8 GRC Rn. 5.

nische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit und genetische Daten (Art. 4 Nr. 13 DSGVO), biometrische Daten (Art. 4 Nr. 14 DSGVO) und Gesundheitsdaten (Art. 4 Nr. 15 DSGVO) von natürlichen Personen. Diese besonderen Kategorien personenbezogener Daten können als Attribute[355] zu der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität in Erscheinung treten, so dass sie ungeachtet der Form der Daten als digital oder analog, Bild oder Ton[356] von dem Begriff und Schutz der personalen Identität umfasst sind. Dabei unterliegen die besonderen Kategorien personenbezogener Daten einem besonderen Risikogehalt für die Rechte und Freiheiten natürlicher Personen, wie es auch aus der Zuordnung als Risikokriterium in Art. 35 Abs. 3 b) DSGVO hervorgeht.

Ebenfalls kommen als Attribute die Standortdaten, online-Kennungen und die Telefonnummer in Betracht.[357] Daraus ergibt sich aus dem zentralen datenschutzrechtlichen Begriff der „personenbezogenen Daten" die rechtliche Annahme von verschiedenen nicht abschließend aufgezählten Identitäten, die einer natürlichen Person zugeordnet werden. Die einzelnen zum Ausdruck kommenden Identitäten sollen im Folgenden als *Teilidentitäten*, die zu einer personalen Identität gehören, bezeichnet werden und können aus dem IKT-Recht herausdifferenziert werden. Dem liegt die Annahme zugrunde, dass in IKT-Systemen verschiedene personale Teilidentitäten entstehen, die einem IKT-rechtlichen Regelungsbereich unterliegen und in diesem beschrieben werden können. Die Gesamtheit der personalen Teilidentitäten bildet die personale Identität und würde sich in ihrem Informations- und Erkenntnisgehalt der natürlichen Person annähern oder dieser entsprechen. Gleichzeitig soll die immanente Differenzierung in der DSGVO zwischen Identität und natürlicher Person dahingehend aufgegriffen werden, dass hinter der personalen Identität ein Indivi-

355 Die Zuordnung als Attribute basieren auf dem Wortlaut der Legaldefinitionen zu Art. 4 Nr. 13 DSGVO „genetische Daten": *Eigenschaften* einer natürlichen Person; Art. 4 Nr. 14 DSGVO „biometrische Daten": *Merkmalen* einer natürlichen Person; Art. 4 Nr. 15 DSGVO „Gesundheitsdaten": *Beziehen*, *Hervorgehen*.

356 *Klar/Kühling*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 4 Nr. 1 DSGVO Rn. 9.

357 Nach EWG 30 gehören zu den Online-Kennungen die IP-Adressen, Cookie-Kennungen, die das Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern und solche, die Spuren hinterlassen und die Profilerstellung ermöglichen.

duum als natürliche Person steht und der Ausdruck der personalen Identität dieser zugerechnet wird.

2. Personale Teilidentität aus Profilen, Art. 4 Nr. 4 DSGVO

Das „Profiling" als automatisierte Verarbeitung personenbezogener Daten besteht darin, bestimmte persönliche Aspekte einer Person zu bewerten, zu analysieren oder vorherzusagen, Art. 4 Nr. 4 DSGVO. Dabei werden als Bewertungsaspekte die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel in Art. 4 Nr. 4 DSGVO genannt. Aus diesen verhaltensbezogenen Bewertungsaspekten, die als personenbezogene Daten eigene profilrelevante Attribute begründen und besondere Kategorien personenbezogener Daten darstellen können, lassen sich neue Identitäten als Teilidentitäten begründen. Durch das Verfolgen („*Tracking*") und die Markierung von Datensätzen können im Laufe der Zeit unbemerkt Profilidentitäten entstehen. Diese im Datenschatten entstehenden *Konstruktionen und Dekontextualisierungen* eines Bildes der personalen Identität basieren auf Kriterien, die aus einer Kohorte begründet wurden. Demnach wird ein Kriterium durch ein erhöhtes Auftreten in einer Kohorte gebildet. Mit diesem Kriterium wird eine Korrelation verbunden, die eine Wahrscheinlichkeitsaussage über das Vorliegen bestimmter Attribute ermöglichen soll. So kann die Teilnahme an einem bestimmten Musikfestival mit der politischen Einstellung korrelieren und zu einer entsprechenden Zuschreibung führen, obwohl die Teilnahme am Musikfestival nicht mit der politischen Einstellung in einem Kausalitätsverhältnis steht.[358] Darin liegt die Lückenhaftigkeit der entstandenen Bilder personaler Identitäten aufgrund von Profilen, die das Erfordernis einer nachgelagerten Korrekturmöglichkeit für den Betroffenen auslöst. Weiter kommen beim Tracking personenbezogener Daten solche Werte zum Einsatz, mit denen Prognosen und Wahrscheinlichkeitsaussagen etwa über die Bonität, wie es im SCHUFA-Urteil[359] entschieden wurde, ermöglicht werden. In diesem Urteil wurde der Zugang zu den verarbeiteten personenbezogenen Daten durch den Be-

358 Vgl. *Lanzing*, Ethics and Information Technology 2016, 9 (12 f.); *Edwards/Veale*, Duke L. & Tech. Rev. 2017, 18 (35); *Wischmeyer*, AöR 143 (2018), 1 (13 f.); ebenso im Zusammenhang mit dem Finden und Vergessen von Bildern im Digitalen, *Dreier*, Bild und Recht, 2019, S. 44.

359 BGHZ 200, 39 – SCHUFA.

troffenen bestätigt, zugleich aber die Auskunft an den Betroffenen über die genaue Funktionsweise der Scoreformel abgelehnt.[360]

Die im SCHUFA-Urteil zum Ausdruck kommende Tendenz der Kommerzialisierung von personenbezogenen Daten zur Erlangung eines Wertes („Score") begründet eine Gefährdungslage für die informationelle Selbstbestimmung und lässt sich mit der *Mosaik*-Theorie[361] veranschaulichen, wonach mit der Zusammenführung punktueller Datenverarbeitungen ein ausdifferenziertes Bild einer Persönlichkeit ermöglicht wird. Indem diese Profilidentitäten meist auf Verbraucherdaten basieren, würden die „*Consumer*" zu „*Prosumern*"[362], da die Verbraucher die Daten „*für*" die verantwortliche Stelle zur Verfügung stellen und damit umfangreiche Profilbildungsmöglichkeiten befördert werden. Demnach sind Konzepte des Selbsttrackings in einem „*Tool*" zur Wahrung der Selbstkontrolle naheliegend und könnten in einem Identitätsverwaltungsmodell zur Gewährleistung der Einflussnahme auf die Profilbildung umgesetzt werden, was dem Selbstdatenschutz dienen würde. Dabei wäre das Zweckbindungsprinzip maßgeblich, da mit ihm der Betroffene den Rahmen der Datenverarbeitung und das Risiko von Profilbildungen unmittelbar erkennen würde. Denn jede Profilbildung außerhalb des Zweckbindungsprinzips würde ein neues Risiko schaffen und bedürfte eines eigenen Rechtfertigungsgrundes. Daneben bedarf es der technischen Sicherstellung, dass die Verarbeitung der personenbezogenen Daten zu dem jeweiligen Zweck getrennt erfolgt und die Daten nicht-verkettbar sind. Mit der Nicht-Verkettbarkeit von Datensätzen werden zugleich die Erkenntnismöglichkeiten durch den Verantwortlichen beschränkt. Insoweit würde ein Identitätsverwaltungsmodell die Nicht-Verkettbarkeit der personenbezogenen Daten und die Kontrollmöglichkeit über die Profile und Bilder personaler Identitäten voraussetzen.

Weiter müsse dem faktischen Rückbezug von Profilidentitäten auf personenbezogene Daten aus der Vergangenheit und gerade dem fehlenden Bezug auf das aktuelle und zukunftsbezogene Identitätsbild begegnet werden.[363] Denn die Profilidentitäten setzen sich aus Attributen zusammen, die in der Vergangenheit liegen. Dabei wird die natürliche Person diesem

360 BGHZ 200, 39 (47) – SCHUFA.
361 2. Teil, A., III.; ebenso das Phänomen des Mosaiks beschreibend, *Reisinger*, Rechtsinformatik, 2016, S. 282.
362 *Lanzing*, Ethics and Information Technology 2016, 9 (12).
363 *Hildebrandt*, in: Claes/Gutwirth/Duff (Hrsg.), Privacy and the criminal law, 2006, 43 (51 f.).

„neuen" Profil ausgesetzt und mit ihm rückgekoppelt, worin eine Beeinflussung zurück zu den vergangenen Attributen und Bildern personaler Identität erfolgen könne.[364] Dahingehend lässt sich parallel zu der Meinungsenklave im online-Kontext eine Identitätsenklave über Profilidentitäten konstatieren, welche einen eigenen Schutzbedarf über die informationelle Selbstbestimmung auslöst. Dabei könnte als Schutzmechanismus einerseits ein Identitätsverwaltungsmodell und andererseits die Begründung von Transparenzanforderungen über die hinter der Profilbildung stehenden Algorithmen in der „*Black Box*"[365] in Frage kommen, wie sie bereits für die automatisierte Einzelentscheidung gemäß Art. 13 Abs. 2 f) DSGVO vorgesehen sind. Denn insgesamt geht es bei einem Schutzmechanismus gegen die Profilbildung um die Einbeziehung von Diskriminierungsverboten gegenüber willkürlichen Zuschreibungen innerhalb des Profilings und damit verbundenen verfälschten Bildern personaler Identitäten. Dies gilt besonders in Anbetracht von bestimmten Merkmalen in einer Kohorte, die als Vergleichsmaßstab für die Bildung einzelner Profilidentitäten eingesetzt werden und zu einer Beeinflussung der Bilder personaler Identitäten nach den Kriterien des mehrheitlichen Verhaltens in einer Kohorte führen, ohne dabei den aus der Menschenwürde erwachsenden Individual- und Minderheitenschutz zu gewähren. Demnach kann in dem Profil ebenfalls der kontextspezifische Ausdruck einer personalen Identität angenommen werden, der jedoch in seiner Eigenschaft als Profil einen eigenständigen Schutzbedarf auslöst und zum Gegenstand der Identitätsverwaltung werden sollte.

3. Personale Teilidentität aus Pseudonymen, Art. 4 Nr. 5 DSGVO

Die Pseudonymisierung nach Art. 4 Nr. 5 DSGVO sieht eine Verarbeitung personenbezogener Daten in der Weise vor, dass der Personenbezug der Daten nicht ohne Hinzuziehung zusätzlicher Informationen möglich ist, weil diese zusätzlichen Informationen gesondert aufbewahrt werden. Erst mit dem Einsatz der Kennung ist die Zuweisung zu den personenbezogenen Daten möglich, wobei die Kennung zur Identifizierbarkeit eingesetzt wird und ebenfalls als personenbezogenes Datum gilt, Art. 4 Nr. 1

364 *Dies.*, in: Rannenberg/Royer/Deuker (Hrsg.), The Future of Identity in the Information Society, 2009, 274 (293 f.).

365 *Hoffmann-Riem*, AöR 142 (2017), 1 (29); *Schallbruch*, Schwacher Staat im Netz, 2018, S. 49 f.

DSGVO. Grundsätzlich sollen durch das Pseudonym die personenbezogenen Daten ersetzt werden und die Zuordnung zwischen Pseudonym und Betroffenen erfolgt über eine Zuordnungsregel, die mit einem Passwort ausgelöst werden kann. Dahingehend war der Wortlaut „ersetzen durch" des § 3 Abs. 6a BDSG-alt eindeutig und im Gegensatz zu dem neuen Wortlaut in der Datenschutzgrundverordnung „in einer Weise (…) betroffenen Person nicht mehr zugeordnet werden können" enger. Denn mit dem neuen Wortlaut aus Art. 4 Nr. 5 DSGVO kann man zu dem Ergebnis kommen, dass zur Pseudonymisierung auch die Verschlüsselung gehört. Gemein ist der Verschlüsselung und Pseudonymisierung, dass sie der Datenminimierung und Datensicherheit dienen, wodurch sie als *Maßnahmen der Risikominimierung* fungieren, Art. 32 Abs. 2 DSGVO.[366] Als Erweiterung der Risikominimierung kommen die „Vermischung der Datensätze" und die „Umverteilung" dieser in Betracht, was zu einem Rauschen mit extrahierten Informationen führen und eine Irrtumswahrscheinlichkeit herbeiführen kann.[367] Diese Methoden sind zwischen Pseudonymisierung und Anonymisierung einzuordnen, weshalb sie für ein Identitätsverwaltungsmodell herangezogen werden sollten. Ebenso kommt zur Risikominimierung die Entfernung von Datensätzen als „Kontrolle von Intransparenz"[368] in Betracht, das sog. *„Information Hiding"*.[369]

Mit der Zuordnung eines spezifischen Pseudonyms kann weiter die Zuordnung einer Rolle einhergehen. Als Rolle gilt der Verbund von Handlungsmöglichkeiten und Berechtigungen, die für den Handelnden in einem bestimmten Kontext gelten.[370] Diese kontextbezogene Limitierung kann mit einem spezifischen Schutzniveau in Verbindung gebracht werden, so dass sich mit der Rolle die maßgebliche technische Vorgabe für das Pseudonym graduell bestimmen lässt. Hierin kommt bereits die Ausprägung eines Identitätsverwaltungsmodells zum Vorschein. Denn es bedarf eines Treuhänders, der über die Zuordnungsregel zwischen Kennung und dem pseudonymisierten Datensatz verfügt und den Dienst eines (rollen-

366 *Pfitzmann/Köhntopp*, in: Federrath (Hrsg.), Designing Privacy Enhancing Technologies, 2001, 1 (7 f.); *Laue/Nink/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis, 2019, § 1 Rn. 28.

367 *Buchmann*, DuD 2015, 510 (512 f.).

368 *Luhmann*, in: Baecker (Hrsg.), Die Kontrolle von Intransparenz, 2017, 96.

369 *Buchmann*, DuD 2015, 510 (511); *Pfitzmann*, Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management-A Consolidated Proposal for Terminology, 2006, S. 10 Fn. 25.

370 *Pfitzmann*, Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management-A Consolidated Proposal for Terminology, 2006, S. 23.

spezifischen) Schutzes personenbezogener Daten erbringt. Dies lässt sich am Beschäftigtendatenschutz illustrieren, wonach dem Arbeitnehmer die zusätzlichen Rollen als Betriebsrat oder leitender Angestellter (§§ 5 Abs. 3, 9 ff. BetrVG) zukommen können und diese Rollen temporär im IT-System eingerichtet werden müssen.

Insgesamt fungiert die Identifizierung als ein Anknüpfungspunkt für die Identitätsverwaltung, da mit ihr die Kontrolle über die Passworteingabe ausgeübt wird.[371] Wann die Kennung auch die Funktion als *Identifizierer* für den Zugang zu einem pseudonymisierten Datensatz erfüllt, ist eine Frage des Schutzniveaus und kann graduell abhängig vom Kontext und der Rolle des Betroffenen variieren. Dabei kann die Kennung als *Identifizierer* aus Attributen der personalen Identität bestehen, mit denen der Zugang zu einem informationstechnischen System ermöglicht wird. So können Pseudonyme dauerhaft oder temporär ausgestaltet sein und aufgrund eines hohen Schutzniveaus ein nur einmaliger *Identifizierer* eingesetzt werden, wie es bei *Single Sign-On*-Lösungen vorgenommen wird. Abhängig vom Schutzniveau kann das Passwort für den *Identifizierer* bei der verantwortlichen Stelle oder bei der betroffenen Person hinterlegt werden. In einem derartigen Identitätsverwaltungsmodell ginge es primär um den Datensatz als Gegenstand der Kontrolle für die Identifikation und den Zugang, ohne dass die Erkenntnismöglichkeiten zum Gegenstand der Identitätsverwaltung werden. Somit sind Pseudonyme als Kennungen ebenfalls der Ausdruck einer personalen Identität und können aus Attributen der personalen Identität bestehen.

4. Zwischenergebnis

Die DSGVO regelt ausdrücklich in der Definition zu den personenbezogenen Daten den Schutz der Identität in ihren Ausdrucksformen als physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Identität. Demnach ist die Anknüpfung an die personenbezogenen Daten für die Bestimmung der personalen Identität notwendig, auch für die Beschreibung des Gegenstandes der Identitätsverwaltung. Weiter kommt als Ausprägung der personalen Identität die Profilidentität nach Art. 4 Nr. 4 DSGVO hinzu, die gerade keine Ausprägung des grundrechtlichen Rechts auf Selbstdarstellung ist, sondern algorithmischen De-

371 *Hammer/Knopp*, DuD 2015, 503 (504).

konstruktionen und Kombinationen von Attributen der personalen Identität unterliegt.

Schließlich sieht die DSGVO die Pseudonymisierung vor, die ebenfalls eine Ausprägung der personalen Identität ist. Danach wird eine Kennung über eine Zuordnungsregel mit einem Betroffenen in Verbindung gebracht. Daraus ergibt sich ein eigenes Identitätsverwaltungskonzept, in dem die personale Identität eine Kennung erhält, mit der ein kontextspezifischer Zugang begründet werden kann. Dabei fungiert die Kennung selbst als ein Bild der personalen Identität. Folglich können die für Dritte sichtbaren Kennungen aus Attributen der personalen Identität bestehen und den Zugang zu besonders schützenswerten und risikobehafteten Datenverarbeitungen von besonderen Kategorien personenbezogener Daten gewähren. Gleichzeitig kann in solch einem Identitätsverwaltungskonzept eine Beschränkung des Gegenstands auf diese Datensätze gesehen werden und Konzepte der Kontrolle durch Intransparenz umfassen. Die Kontrolle durch Intransparenz würde sich zunächst auf die Datensätze beziehen und sich zugleich auf den Informations- und Erkenntnisgehalt über eine personale Identität auswirken können. Denn bei einem Identitätsverwaltungsmodell geht es einerseits um die Schutzebenen und andererseits um die jeweiligen Risiken für den Schutz der personalen Identität und die Erkenntnisse über diese.

II. Kontextuelle personale Identitäten

Aus der Feststellung des Bundesverfassungsgerichts im Volkszählungsurteil, dass es „kein ‚belangloses' Datum" gäbe, geht hervor, dass Daten abhängig von ihrem Verwendungskontext an Bedeutung erlangen und diese Bedeutgunsgehalte variieren können.[372] Demnach ergibt sich aus der informationellen Selbstbestimmung ein kontextspezifisches Schutzbedürfnis, welches sich aus den Phasen der Datenverarbeitung im Datenzyklus ergibt und in unterschiedlicher Intensität ausgeprägt sein kann. Entsprechend sind nach dem Erkenntnismodell die Informationen zu einer personalen Identität perspektivisch einzuordnen, so dass die Erkenntnisgehalte variabel sind. Dieser Phänomenologie lässt sich entnehmen, dass die Informationen und Erkenntnisse über eine personale Identität in einer sozialen,

372 BVerfGE 65, 1 (45).

zeitlichen und räumlichen Beziehung stehen.[373] Entsprechend soll mit dieser Kontextbezogenheit eine systemtheoretische Perspektive einbezogen werden. Denn es kann sich bei der Datenverarbeitung zu einer personalen Identität im Kontext um ein autopoietisches Kommunikationssystem ohne eine Intervention der Umwelt handeln.[374] In diesem System ist die Verstärkung von Informationen möglich und kann dazu führen, dass der Erkenntnisgehalt gegenüber anderen Systemen im Widerspruch steht.[375] Dabei können als Kommunikationssystem in einem IKT-Kontext Datenbanken, Informationssysteme und intelligente wissensbasierte Systeme fungieren, wonach verschiedene kontextbezogene Datensätze in einen neuen Kontext überführt und eingeordnet werden können. Gleichzeitig ist das Kommunikationssystem aus systemtheoretischer Hinsicht in der Unterscheidung zwischen der Wahrheit und dem Irrtum indifferent, aber es unterscheidet zwischen System und Umwelt, so dass das Konzept der Beobachtung von Kommunikationssystemen eine Kontrollierbarkeit ermöglichen kann.[376] Denn die Beobachtung und Beobachtungsinstruktionen können als „unsichtbare Hand" wirken, wie es etwa bei Verfahren und Handlungsanweisungen als *Instruktionen* in einem Unternehmen der Fall sein kann.[377]

Für die Identitätsverwaltung kommt die Beobachtung mit *Instruktionen* in Betracht, die übergeordnet als Metakommunikation in Gestalt eines Verfahrens in den Systemen wirkt. Indem diese systembezogenen *Instruktionen* in einem datenschutzrechtlichen Kontext wirken würden, ist zunächst die Kontextbezogenheit der personalen Identität herauszuarbeiten. Folglich werden die Kontexte innerhalb der Datenschutzgrundverordnung (1.) im Hinblick auf eine kontextübergreifende Datenverarbeitung (2.) und das Konzept einer kontextuellen Integrität (3.) und ihre Auswirkung auf ein Identitätsverwaltungsmodell (4.) nachvollzogen.

373 *Solove*, Harv. L. R. 2013, 1880 (1890); *Bender*, in: Hornung/Engemann (Hrsg.), Der digitale Bürger und seine Identität, 2016, 187 (190); *Albers*, Informationelle Selbstbestimmung, 2005, S. 120.
374 *Luhmann*, in: Baecker (Hrsg.), Die Kontrolle von Intransparenz, 2017, 9 (10 f.).
375 *Ders.*, in: Baecker (Hrsg.), Die Kontrolle von Intransparenz, 2017, 9 (10 f.); *Steinmüller*, Information, Modell, Informationssystem, S. 8.
376 *Luhmann*, in: Baecker (Hrsg.), Die Kontrolle von Intransparenz, 2017, 9 (15–17).
377 *Hoffmann-Riem*, AöR 142 (2017), 1 (31) Fn. 119.

1. Kontexte in der Datenschutzgrundverordnung

a) Persönliche oder familiäre Tätigkeiten, Art. 2 Abs. 2 c) DSGVO

In der Datenschutzgrundverordnung wird die Datenverarbeitung in dem Kontext der ausschließlich persönlichen oder familiären Tätigkeit nach Art. 2 Abs. 2 c) DSGVO aus dem Anwendungsbereich ausgeschlossen. Die Auslegung, was sich als persönliche oder familiäre Tätigkeit einordnen lässt, hat aufgrund des Ausnahmecharakters der Regelung und dem geringeren Schutzniveau über die informationelle Selbstbestimmung restriktiv zu erfolgen. Für die Einordnung in den privaten und geschäftlichen Kontext der Datenverarbeitung ist die Verkehrsanschauung einzubeziehen, wie es bei der eindeutigen Zuordnung eines in der Familie lebenden Kindermädchens in die datenschutzrechtlichen Kontexte besonders deutlich wird. Denn hinsichtlich des Beschäftigungsverhältnisses ist Art. 88 DSGVO maßgeblich, gleichzeitig übt ein Kindermädchen, das in der Familie lebt, auch private Tätigkeiten aus, was vom datenschutzrechtlichen Anwendungsbereich ausgeschlossen wäre. Sobald eine eindeutig private Tätigkeit ausgeübt wird, kommt der zivilrechtliche Schutz des allgemeinen Persönlichkeitsrechts in Betracht (§ 823 Abs. 1 BGB). Damit wird der gesetzlichen Wertung Rechnung getragen, dass die datenschutzrechtliche Abwehrdimension bei informellen Konfliktlagen im persönlichen oder familiären Bereich ungeeignet ist.[378] Gleichwohl wird durch die technischen Überwachungs- und Kontrollmöglichkeiten der Familienmitglieder eine gleichwertige Konfliktlage angenommen, die einen datenschutzrechtlichen Schutzmechanismus auslösen könne.[379] Die Annahme einer Ausweitung des datenschutzrechtlichen Anwendungsbereichs auf private Kontexte erscheint für die datenschutzrechtliche Risikolage im online-Kontext vorzugswürdig, da die Graubereiche zwischen privaten und sozialen Kontexten gerade in sozialen Medien damit unerheblich wären und beide dem Anwendungsbereich der DSGVO unterliegen würden. Dagegen spricht jedoch, dass im privaten Kontext die Pflichten des Verantwortlichen umzusetzen wären, was in Anbetracht der fehlenden fachspezifischen Kenntnisse des privaten Verantwortlichen kaum realisierbar wäre. Damit können zwar die Gefährdungslagen im privaten Kontext der datenschutzrechtlichen Gefährdungslage entsprechen, jedoch sind die zivilrechtlichen Schutzmechanismen dabei als ausreichend einzuordnen.

---

378 *Lewinski*, Die Matrix des Datenschutzes, 2014, S. 10.
379 *Raabe/Lorenz/Pallas u.a.*, CR 2011, 831 (837).

Insgesamt ist der Ausschlussgrund nach Art. 2 Abs. 2 c) DSGVO eng auszulegen, wie es in der Linquist-Entscheidung[380] des EuGHs deutlich wurde. Darin wurde die Rechtsauffassung, dass private Informationen in einer leicht humorigen Weise auf einer Webseite vom datenschutzrechtlichen Anwendungsbereich auszuschließen sind, als unvereinbar mit der Datenschutzrichtlinie angesehen. Demnach liegt es nahe, in Grenzfällen eine Schwerpunktbetrachtung dahingehend vorzunehmen, wo der Schwerpunkt des Verhaltens liegt und welche Gefährdungen für den Schutz personenbezogener Daten bestehen. Das festgestellte Risiko für den Schutz personenbezogener Daten gibt dabei Anhaltspunkte für den Schutzbedarf und die Zuordnung in den datenschutzrechtlichen Anwendungsbereich.

b) Beschäftigungskontext, Art. 88 DSGVO i.V.m. § 26 BDSG

Weiter kommt der Beschäftigungskontext für gesonderte Regelungen über die Datenverarbeitung in Betracht, Art. 88 DSGVO i.V.m. § 26 BDSG. Von dem Beschäftigtendatenschutz sind die Phasen der Bewerbung, der Einstellung, der Durchführung und die Beendigung des Arbeitsverhältnisses mit ihren jeweiligen Zwecken der Datenverarbeitung erfasst.[381] Ebenso kommen die spezifischen technischen und organisatorischen Maßnahmen des Arbeitgebers, der Verantwortlicher in den Phasen des Arbeitsverhältnisses ist, entsprechend zu den Risikolagen der Datenverarbeitung hinzu und verlangen einen gesonderten Schutz der personenbezogenen Daten. Die im Kontext des Beschäftigtendatenschutzrechts geltende Besonderheit von konkretisierenden Regelungen durch Kollektivvereinbarungen können ein differenziertes Regelungsgefüge zur Verfügung stellen, mit dem die Unterkontexte im Beschäftigungskontext geregelt werden und unter einem angepassten Datensicherheitsniveau die personenbezogenen Daten verarbeitet werden können.[382]

Die für die Begründung des Arbeitsverhältnisses erforderlichen Datensätze, etwa die Krankenversicherungsnummer (§ 291 Abs. 2 SGB V), Steueridentifikationsnummer (§ 139b Abs. 1 AO) und Sozialversicherungsnummer (§ 147 Asb. 2 SGB VI) gehören zu der anfänglichen Phase der Einstel-

380 EuGH, Urt. v. 06.11.2003 – C-101/01, Linquist, Rn. 47.
381 *Maschmann*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 88 DSGVO Rn. 14–16.
382 *Ders.*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 88 DSGVO Rn. 24–27.

lung im Beschäftigtendatenschutz und beziehen jeweils die personale Teilidentität in ihrem *Idem*-Anteil im datenschutzrechtlichen Kontext der Beschäftigung ein. In der weiteren Phase der Durchführung des Beschäftigungsverhältnisses können die Identifizierungs- und Zeiterfassungsdaten zu einer personalen Teilidentität gehören. Ebenso kommen rollenspezifische Teilidentitäten des Beschäftigten in Betracht, die aus Zugangsrechten zu bestimmten Datenbanken und aus gesonderten Befugnissen bestehen können. Die Zugangsrechte in Gestalt von Benutzernamen und Passwörtern würden den *Idem*-Anteil einer personalen Identität darstellen und die verhaltensbezogene Ausübung der Befugnisse den *Ipse*-Anteil der personalen Identität.

2. Kontextübergreifende Datenverarbeitung

Neben den kontextspezifischen Datenverarbeitungen in der DSGVO ist die kontextübergreifende Datenverarbeitung als Gegenstand der Identitätsverwaltung einzubeziehen. Dabei geht es um die Datenverarbeitung in zwei zunächst voneinander unabhängigen Kontexten, die miteinander in Verbindung gebracht werden. Dem oben erwähnten Beispiel des im Haushalt einer Familie lebenden Kindermädchens folgend, geht es um die Überschneidung der Datensätze aus der privaten Tätigkeit mit der Tätigkeit im Beschäftigungskontext und der Kontrolle über die jeweiligen personalen Identitäten. Weiter kann bei einem „*smarten*“ Arbeitsplatz der Datensatz aus dem „*Smart Home*“ von Interesse sein und dem Beschäftigten die Option eingeräumt werden, die aus der privaten Tätigkeit stammenden Datensätze als *Ipse*-Anteil in den Beschäftigungskontext einzubeziehen. Demnach geht es über die Bestimmung des Kontextes hinaus um die Schnittstellen und Interoperabilität von personalen Identitäten zwischen den Kontexten.

Indem beide Konstellationen unterschiedlichen rechtlichen Schutzregimen unterliegen, zugleich aber der Bedarf an der Zusammenführung der Datensätze bestehen kann, stellt sich die Frage nach einer der informationellen Selbstbestimmung gerecht werdenden kontextübergreifenden Kontrolle der Datensätze. So sieht der EWG 54 S. 4 für den *Ipse*-Anteil der personalen Identität vor, dass verarbeitete Gesundheitsdaten aus einem öffentlichen Interesse heraus nicht zu einem anderen Zweck in einem anderen Kontext verarbeitet werden dürfen. Dies macht eine grundsätzliche Nicht-Verkettbarkeit der Datensätze und personalen Identitäten deutlich.

Ebenso führt die Nutzung von sozialen Medien innerhalb eines privaten und familiären Kreises zunächst zu dem Ausschluss des datenschutzrechtlichen Anwendungsbereiches. Gleichzeitig kann die Abrufbarkeit eines Nutzungsprofils unter sog. „Freunden" über den privaten Bereich hinaus dem Regelungsregime der DSGVO unterliegen, so dass Graubereiche bei der Kontextabgrenzung entstehen können.[383]

In Betracht kommt ein steuerbarer Zugriff auf die jeweiligen Datensätze durch erneute Einwilligungen der natürlichen Person. Indem spezifische Risikolagen mit der kontextspezifischen Datenverarbeitung einhergehen, kann sich das Erfordernis einer erneuten Einwilligung für die kontextübergreifende Datenverarbeitung ergeben. Demnach muss im Rahmen der Informationspflichten auf den spezifischen Zweck der kontextübergreifenden Datenverarbeitung hingewiesen werden, Art. 12–14 DSGVO, EWG 32, 39 S. 5, um eine erneute Rechtfertigung einzuholen, Art. 6, 7 DSGVO. Dabei kommt als Rechtfertigung insbesondere die Einwilligung mit der Voraussetzung einer wissensbasierten Entscheidung in Betracht. Maßgeblich ist dabei die Gewährleistung der informationellen Selbstbestimmung in den Kontexten und bei der kontextübergreifenden Datenverarbeitung, so dass die kontextspezifischen *Ipse*-Anteile der personalen Identität über den Datenzyklus hinweg solange separiert bleiben, bis eine kontrollierte kontextübergreifende Zusammenführung gerechtfertigt wird.

3. Kontextuelle Integrität

Aus der angloamerikanischen Perspektive wird von *Nissenbaum* zum Schutz der Privatheit das Konzept der „*kontextuellen Integrität*" vorgeschlagen.[384] In diesem geht es um die kontextbezogenen „Sphären der Gerechtigkeit", die in dem jeweiligen Kontext der behördlichen, der beruflichen und der privaten Kommunikation zu realisieren seien. Dem liegt die Annahme zugrunde, dass Informationen nicht kontextarm sind, sondern aus dem Kontext entstehen. Entsprechend bedarf es eines Schutzregimes, in dem die Kontexte in den Vordergrund treten. Denn bereits die Bestimmung des Kontextes und seiner Grenzen unterliegt der eingenommenen Betrachtungsperspektive, so dass Kontextüberschneidungen ein einheitli-

383 *Spindler*, in: Verhandlungen des 69. Deutschen Juristentages, 2012, S. F 76.
384 *Nissenbaum*, Wash. L. Rev. 2004, 119.

ches Schutzniveau erschweren.[385] Folglich besteht die *kontextuelle Integrität* aus vier Prinzipien, die als integraler Bestandteil gelten: Die Abwehrdimension des Schutzes der Privatsphäre, der eingeschränkte Zugang zu sensiblen und vertraulichen Kontexten, die Kontrolle der Informationen als Autonomie und die Sicherstellung von vertraulichen Informationen.[386]

In diesem Konzept der *kontextuellen Integrität* kommt die Beobachtungsdimension von Kommunikationssystemen zum Ausdruck. Dabei wird zwischen dem feststellbaren Öffentlichkeitsgrad der Informationen mit dem jeweiligen Schutzniveau und dem Zugangsniveau unterschieden.[387] Folglich ist in einem Identitätsverwaltungsmodell unter der Wahrung einer *kontextuellen Integrität* zwischen sensiblen und nicht sensiblen, öffentlichen und privaten Informationen zu unterscheiden. Aufgrund der Überschneidungen von Kontexten ist eine Separierung der Informationen nicht immer möglich, so dass die *kontextuelle Integrität* eine kontextuelle Interoperabilität verlangt. Danach geht es um ein gestuftes Sicherheitsniveau, wie es gemäß Art. 8 Abs. 2 eIDAS-VO nachgewiesen wurde, und die Beschränkung der Datensätze auf ein notwendiges Maß für den jeweiligen Kontext. Diese kontextübergreifende Datenverarbeitung mit einem kontextspezifischen Sicherheits- und Risikoniveau würde einem „*Identity Ecosystem*" entsprechen.[388]

Insgesamt lässt sich diesem Konzept der *kontextuellen Integrität* unterstellen, dass es idealistisch sei und dem *Big Data*-Phänomen mit den einhergehenden Informationsasymmetrien unzureichend Rechnung trage. Gleichwohl geht es bei der *kontextuellen Integrität* darum, dass ein gesteigerter Schutz für die personale (Teil-) Identität in dem jeweiligen Kontext begründet wird, und damit der *Selbstdatenschutz* unter verbesserten Bedingungen ausgeübt werden kann. Demnach kommt für den Schutz der *kontextuellen Integrität* ein mediierendes Verfahren zum Ausgleich der bestehenden Informationsasymmetrien in Betracht, welches von den Erfordernissen der Transparenz, Offenheit, Teilhabe und Mitteilungen[389] geprägt ist.

---

385 *Dies.*, Wash. L. Rev. 2004, 119 (122); *Hoffmann-Riem*, AöR 142 (2017), 1 (26 f.); *Steinmüller*, Information, Modell, Informationssystem, S. 45.
386 *Dies.*, Wash. L. Rev. 2004, 119 (131).
387 *Dies.*, Wash. L. Rev. 2004, 119 (151 f.).
388 *White House*, National Strategy for Trusted Identities in Cyberspace, 2011, S. 29 f.
389 *Nissenbaum*, Wash. L. Rev. 2004, 119 (130) mwN.

4. Übertragung auf das Identitätsverwaltungsmodell

In einem Identitätsverwaltungsmodell bedarf es für die personale Identität und ihren Teilidentitäten eines *kontextspezifischen Schutzregimes*, in dem die Phänomene der Kontexte als separiert und zugleich ineinander übergreifend einbezogen werden. Indem die *(kontextuelle) Integrität* als Bestandteil des Schutzes der Privatheit grundrechtlich anerkannt wurde,[390] soll diese in einem Identitätsverwaltungsmodell einbezogen werden. Dafür kommt ein Treuhandmodell in Frage, wonach die Datensätze zur personalen Identität treuhänderisch hinterlegt werden und kontextspezifisch der Zugang gewährt wird. Dabei würde für einen ineinandergreifenden Kontext die Kombination von mehreren Teilidentitäten erfolgen, wie es bei der Zusammenführung der Teilidentitäten über die Steuernummer, Sozialversicherungsnummer und Krankenversicherungsnummer eines Beschäftigten der Fall wäre.

Mit dieser kontextspezifischen Begründung der personalen Identität aus den Teilidentitäten kann dem Verständnis der statischen *Idem*-Identität begegnet werden, indem die personale Identität in einem Kommunikationssystem der Dynamik des Kontextes und seiner Beobachtung unterliegt. Weiter erlaubt das Konzept der kontextspezifischen Integrität eine iterativ, dem Datenzyklus gerecht werdende Neubildung der personalen Identität in ihrem *Ipse*-Anteil. Diese kann von der natürlichen Person im Rahmen der informationellen Selbstbestimmung ausgestaltet werden. Mit diesem *kontextspezifischen Schutz* der personalen Identität würde eine Entwicklungsoffenheit der personalen Identität im online-Kontext gewährleistet werden.

Entsprechend wurde vom Weißen Haus im Jahr 2011 ein „*Identity Ecosystem*“ auf internationaler Ebene vorgeschlagen, in dem das Sicherheitsniveau der Kontexte für die Kontrolle der Datensätze maßgeblich sei. Danach würden etwa die Bankdaten dem gleichen Sicherheitsniveau wie die Gesundheitsdaten unterliegen. In einem kontextübergreifenden interoperablen System würde der Zugang zu den personalen Identitäten entsprechend dem Sicherheitsniveau geregelt werden, wie es in Art. 8 Abs. 2 eIDAS-VO vorgesehen ist.[391]

Diesen Identitätsverwaltungsmodellen ist gemein, dass über die Einwilligung eine *iterative Kontrolle* der Zugangsgewährung ermöglicht wird. Gleichzeitig liegt darin eine Schutzmöglichkeit im Rahmen des *Selbstda-*

390 2. Teil, A., II., 1., b) – c).

391 *White House*, National Strategy for Trusted Identities in Cyberspace, 2011, S. 17 f., 31–35.

tenschutzes, die gegenüber *Big Data*-Phänomenen und den damit einhergehenden Informationsasymmetrien wirken könnte und ein kompensatorisches Verfahren darstellen könnte. Dafür kommt ein mediierendes Verfahren zum Ausgleich der bestehenden Informationsasymmetrien in Betracht, welches von den Erfordernissen der Transparenz, Offenheit, Teilhabe und Mitteilungen[392] geprägt ist.

5. Zwischenergebnis

Die Datenschutzgrundverordnung regelt ausdrücklich die Kontexte der persönlichen und familiären Tätigkeit und der Beschäftigung. Der kontextspezifische Schutz personaler Identitäten verlangt demnach eine *kontextuelle Integrität,* die als Bestandteil der informationellen Selbstbestimmung fungiert. Diese lässt sich mit dem gestuften Vertrauens- und Sicherheitsniveau gemäß Art. 8 Abs. 2 eIDAS-VO abbilden. Für das Identitätsverwaltungsmodell ist folglich ein „*Identity Ecosystem*" aufschlussreich, wonach der Zugang zu dem jeweiligen Sicherheits- und Risikoniveau gewährleistet wird. Damit könnte der *Selbstdatenschutz* wirksam ausgeübt werden und die kontextspezifische iterative Kontrolle der Informationen und Erkenntnisse über personale Identitäten ermöglicht werden. Dies könnte mit einem mediierenden Verfahren erfolgen, das von Teilhabe und Transparenz geprägt ist.

III. Stipulatives Identitätsverwaltungsmodell

Der Identitätsbegriff beschreibt zunächst den Zustand der Gleichheit und könnte demnach auch als undefinierbar gelten. Mit der Beziehung des Begriffs zur Person als personale Identität erlangt der Identitätsbegriff über den Vorgang des Vergleichens hinaus einen inhaltlichen Gehalt, der zum Gegenstand einer stipulativen Definition werden soll. Dennoch verbleibt die Frage nach der definitorischen Ebene, da die personale Identität auf einer niedrigen Stufe ihre individuelle Subjektivität mit den jeweiligen Attributen zum Definitionsgegenstand haben müsste.

Die definitorische Macht für den offline-Kontext ist in den grundrechtlichen und einfachrechtlichen Regelungen verwurzelt, so dass die darin enthaltene reale Essenz in stipulative Definitionen[393] für den online-Kontext

392 *Nissenbaum*, Wash. L. Rev. 2004, 119 (130) mwN.
393 *Pap*, Philosophy of science 1964, 49 (51 f.).

überführt werden soll. Dabei kommen für die Definition der personalen Identität solche Kriterien aus dem offline-Kontext in Betracht, bei denen die Physis, die Sozialisation und die Charakteristik der Person den Anknüpfungspunkt bilden können.[394] Demgegenüber stehen Anknüpfungen an die Attribute einer personalen Identität wie etwa die Email-Adresse bei *Single Sign-On*-Lösungen oder die digitale Identität beim elektronischen Personalausweis, die den Begriff der personalen Identität prägen können.[395]

Insgesamt soll der Begriff der personalen Identität aus den beschriebenen grundrechtlichen und einfachrechtlichen Ausprägungen heraus definiert und damit ein Abstraktionsniveau gewährleistet werden, dass dem offline- und online-Kontext gleichermaßen Rechnung trägt. Zudem sollen die Definitionen dem pluralistischen Verständnis von Individuen gerecht werden und demnach gegenüber verschiedenen Attributen offen sein. Dabei stehen die Definitionen in dem Verhältnis zueinander, wie es in dem Modell zwischen offline- und online-Kontext dargestellt ist (Abbildung 3).

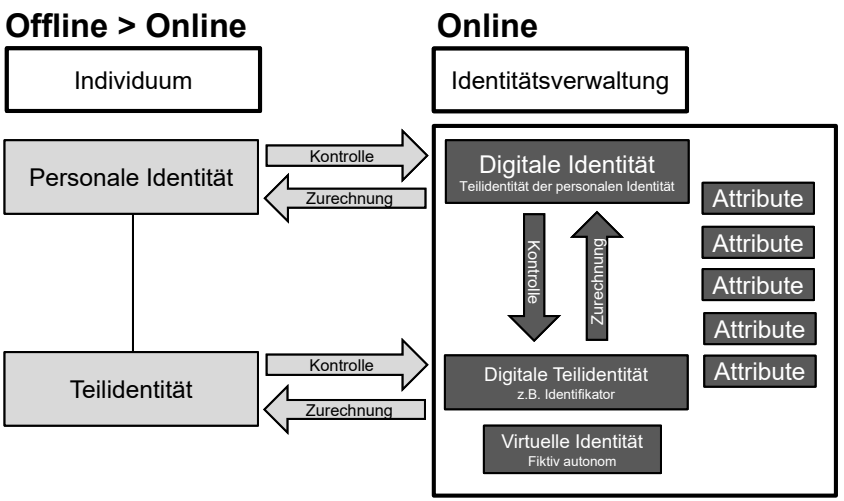

Abbildung 3: System der Definitionen zur personalen Identität

394 *Unabhängiges Landeszentrum für Datenschutz* (ULD), Identity Management Systems (IMS), 2004, S. 1.

395 *Froomkin*, Building Privacy into the Infrastructure: Towards a New Identity Management Architecture, 2016, S. 6.

1. Definitionen zur personalen Identität

- Die *personale Identität* einer natürlichen Person realisiert sich über die Selbstdarstellung und Darstellung von dynamischen (*Ipse*) und statischen *personalen Teilidentitäten* (*Idem*) als Ausdruck der inneren Selbstbestimmung und Selbstbewahrung innerhalb von IKT-Systemen durch Informationen in interpretierbaren Symbolstrukturen, aus denen Wissen generiert wird.
- Die *personale Teilidentität* einer natürlichen Person ist der personalen Identität zurechenbar und realisiert sich statisch (*Idem*) oder dynamisch (*Ipse*) innerhalb von IKT-Systemen durch kontextspezifische Informationen in interpretierbaren Symbolstrukturen, aus denen Kontextwissen generiert und aus dem Verhalten sichtbar wird.
- Die *digitale Identität* ist einer natürlichen Person über einen Identifikator zurechenbar und realisiert sich innerhalb eines IKT-Systems über ein Zuordnungsobjekt, das aus Teilidentitäten besteht.
- Die *digitale Teilidentität* einer natürlichen Person ist über einen Identifikator zurechenbar und realisiert sich innerhalb eines IKT-Systems über ein Zuordnungsobjekt, das aus Attributen als Datensätze besteht, die zu Informationen und Kontextwissen werden, sowie aus möglichen Zuschreibungen durch Dritte.
- Die *virtuelle (Teil)-Identität* wird durch eine natürliche Person oder künstliche Intelligenz als ein Zuordnungsobjekt in einem IKT-System begründet, ohne dass ein reales Äquivalent mit einem hohen Gleichwertigkeitsgehalt existiert.

2. Definitionen zur Identitätsverwaltung

- Die *Identitätsverwaltung* in einem IKT-System ist die Kontrolle einer natürlichen Person über die Begründung und Annahme von personalen Teilidentitäten, bestehend aus kontextbezogenen Daten, Informationen und generiertem Wissen, sowie die Kontrolle über die Verkettbarkeit von kontextübergreifenden Teilidentitäten.
- Ein *Agent* handelt dauerhaft oder vorübergehend für eine personale Identität durch die Übermittlung von Daten (Bote), durch Tätigwerden für einen Prinzipal (Erfüllungsgehilfe, Verrichtungsgehilfe, Stellvertretung) oder durch autonomes Auftreten mit einer anderen Bezeichnung (Legende).

- *Attribute* sind einer TeiIidentität zugeordnete und zurechenbare Eigenschaften.
- *Kontrolle* ist das bewusste Einwirken, Beaufsichtigen, Steuern und Gestalten.
- *Zurechenbarkeit* bezüglich eines Akteurs ist gegeben, wenn Vorgänge den Beteiligten Instanzen gegenüber dem Akteur zugeordnet werden können.[396]
- *Identifikator* ist ein Datensatz, mit dem eine eindeutige Identifizierung der natürlichen Person möglich ist.

B. Ex ante Rechtfertigung personaler Identitäten in der DSGVO

Der Zeitraum vor der Rechtfertigung einer Datenverarbeitung über die personale Identität unterliegt den Grundsätzen gemäß Art. 5 Abs. 1 DSGVO und verlangt entsprechende Maßnahmen durch den Verantwortlichen. Demnach soll für die Begründung des Identitätsverwaltungsmodells die Betrachtung chronologisch mit der Bestimmung der personenbezogenen Daten beginnen (I.) und mit den Anforderungen an die Transparenz fortgesetzt werden (II.). Anschließend sollen die Voraussetzungen, die der Verantwortliche gemäß Art. 5 Abs. 1 DSGVO zu erfüllen hat, konkretisiert werden (III.). Dafür sollen die Verpflichtungen hinsichtlich der Zweckbindung, der Datenminimierung, der Datensicherheit und der datenschutzkonformen Technikgestaltung ausgeführt werden. Daraus sollen die Anhaltspunkte für ein Identitätsverwaltungsmodell abgeleitet und zugleich die rechtlichen Anforderungen an die Identitätsverwaltung konkretisiert werden.

I. Bestimmung personenbezogener Daten

Die Identitätsverwaltung umfasst personenbezogene Daten als Bestandteile der personalen Identität und verlangt die Bestimmung dieser zur Eröffnung des datenschutzrechtlichen Anwendungsbereiches. Entscheidend für die Eingrenzung des Gegenstandes der Identitätsverwaltung ist daher die trennscharfe Differenzierung zwischen anonymen und personenbezogenen Daten. Indem anonyme Daten bei einer Kontextänderung zu personenbezogenen Daten werden können, stellt sich die Frage nach der Einbe-

396 *KASTEL-Kompetenzzentrum*, Begriffsdefinitionen in KASTEL S. 5.

ziehung dieser Sachlage in das Identitätsverwaltungsmodell. Aus der Perspektive der natürlichen Person, die ihre personalen Identitäten verwaltet, ist gemäß dem EWG 39 S. 5 eine Risikobetrachtung naheliegend, nach der die betroffene Person über die Risiken der Verarbeitung personenbezogener Daten informiert und aufgeklärt werden soll. Damit soll die betroffene Person von ihrem Entscheidungsspielraum über die Erteilung einer Einwilligung wirksam Gebrauch machen können. Weil bei anonymen Daten in einem Datenzyklus das Risiko der Identifizierbarkeit einer natürlichen Person (1.) besteht, wird gerade im *Big Data*-Zusammenhang der Bedarf nach einem Schutz vor der Identifizierung einer natürlichen Person deutlich. Weiter geht aus der DSGVO neben dem Schutz personenbezogener Daten der Schutz vor erlernbaren Erkenntnissen über personale Identitäten hervor, so dass die Informationen und das Wissen über eine personale Identität entsprechend zum Erkenntnismodell von der DSGVO geschützt werden. Folglich soll das Risiko der Erkenntnisse aus personenbezogenen Daten dargestellt werden (2.).

1. Risiko der Identifizierbarkeit

Das Risiko der Identifizierbarkeit einer natürlichen Person richtet sich nach den rechtlichen Bestimmungen, wann ein personenbezogenes Datum gegeben ist. Denn der datenschutzrechtliche Vorfeldschutz gebietet bei der Bewertung des Risikos der Identifizierbarkeit die Einbeziehung der kontextspezifischen Gefährdungslage,[397] was eine flexible Zuordnung zwischen anonymen und personenbezogenen Daten mit dem unbestimmten Rechtsbegriff der „Identifizierbarkeit" ermöglicht. Gemäß der Legaldefinition nach Art. 4 Nr. 1 DSGVO und dem EWG 26 S. 3–4 liegt die Identifizierbarkeit vor, wenn mit den Mitteln des Verantwortlichen die Person identifiziert werden kann, und wenn unter Einbeziehung von Informationen Dritter mit angemessenem Aufwand die Identifizierung ermöglicht wird.[398] Damit können anonymisierte Daten aus dem „digitalen Schattendasein" mit den Informationen des Verantwortlichen und des Dritten an das Licht der Identifizierbarkeit geführt werden, womit sie dem Anwendungsbereich der DSGVO unterliegen.

397 *Kühling/Klar*, NJW 2013, 3611 (3613).
398 *Klar/Kühling*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 4 Nr. 1 DSGVO Rn. 19.

In der Entscheidung *Breyer*[399] hat der EuGH dynamische IP-Adressen aufgrund ihrer dauerhaften Verfügbarkeit im Netz und die Möglichkeit der indirekten Identifizierbarkeit als personenbezogene Daten eingeordnet. Folglich wird aus der Entscheidung des EuGHs ein gemischt objektiv-relativer Ansatz angenommen,[400] wonach neben der subjektiven Perspektive des Verantwortlichen auch die objektive Perspektive für die Frage der Identifizierbarkeit maßgeblich ist. Dieser objektiv- relative Ansatz verlangt bei der Prüfung der Identifizierbarkeit die Einbeziehung der Abwägungskriterien, welche Kosten und welcher Zeitaufwand unter Einsatz der verfügbaren Technologie erforderlich sind. Dies entspricht den Wertungen aus dem EWG 26 S. 4, so dass sich die Entscheidung *Breyer* auf die DSGVO übertragen lässt, auch wenn die Entscheidung des EuGHs noch an die Rechtslage der Datenschutzrichtlinie 95/45/EG anknüpft. Für den Theorienstreit über die Identifizierbarkeit ist daher maßgeblich, wer über das Zusatzwissen zur Identifizierung verfügt, so dass es auf die Kenntnis des Verantwortlichen und eines *realistischen Dritten* ankommt. Nach dem relativen Ansatz[401] geht es um das Zusatzwissen des Verantwortlichen und nach dem objektiven Ansatz um das abstrakte Zusatzwissen eines Dritten.[402] Sobald sich mit einem Merkmal, einer Merkmalskombination oder dem Kontextwissen als Zusatzwissen auf eine natürliche Person rückschließen lässt, liegt ein identifizierendes Merkmal vor. Dieses Zusatzwissen kann aus Attributen oder Anmeldedaten bestehen und in seiner Verlässlichkeit über die Authentizität einem eigenen Risikogehalt unterliegen.

Weiter lässt sich dieses Zusatzwissen aufteilen in extrinsisch, außerhalb der natürlichen Person liegend, und intrinsisch, in der natürlichen Person liegend.[403] Darin lässt sich eine entscheidende Differenzierung erblicken, um das Zusatzwissen und das Verhalten des Betroffenen mit einem eigenen Anteil zu versehen, welches sich auf das Risiko der Identifizierbarkeit auswirkt. Damit hängt das Risiko der Identifizierbarkeit von dem Maß des potentiell einbeziehbaren Zusatzwissens ab, welches ein Verantwortlicher oder ein Dritter möglicherweise von dem Betroffenen erlangt. Folglich können viele verschiedene Attribute in sozialen Medien zu einem Namen

399 EuGH, Urt. v. 19.10.2016 – C-582/14, Breyer ./. BRD, Rn. 31, 36, 40.
400 *Karg*, DuD 2015, 520 (525), „objektiviert, relativer Ansatz"; *Kühling/Sackmann*, Rechte an Daten, 20. November 2018, S. 11, relativer Ansatz mit risikobasierten objektiven Elementen.
401 Vertreten von *Eckhardt*, CR 2016, 786 (790).
402 *Klar/Kühling*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 4 Nr. 1 DSGVO Rn. 23.
403 *Janeček*, CLSR 2018, 1039 (1044).

existieren, der als Pseudonym erscheint, aber durch die Anzahl der Attribute wird dennoch die Identifizierung der natürlichen Person möglich. Demnach erlaubt die Differenzierung zwischen extrinsischem und intrinsischem Zusatzwissen eine Aussage darüber, ob eine natürliche Person selbst zu einem gesteigerten Identifizierungsrisiko beigetragen hat.

Nach dem EuGH kann auch das Zusatzwissen eines Dritten einbezogen werden, wenn es dem Verantwortlichen zurechenbar ist und es sich um einen verhältnismäßigen Aufwand handelt, mit dem die natürliche Person identifiziert werden kann. Hinzu kommt die Frage, ob ein verhältnismäßiger und unverhältnismäßiger Aufwand anzunehmen ist, wenn ein rechtmäßiges Akteneinsichtsrecht besteht oder ob dieses ebenfalls einen unverhältnismäßigen Aufwand mit sich bringen würde.[404] Entscheidend bei der Bewertung ist, dass das einbezogene Zusatzwissen nach herrschender Meinung auf rechtmäßigem Weg[405] erlangt werden muss, da dies auch im Einklang mit dem Wortlaut des EWG 47 S. 1 „vernünftige Erwartung" steht. Dagegen lässt sich jedoch kritisch anführen, dass bei der Erlangung besonders sensibler Daten auf rechtswidrigem Weg die Schutzmechanismen der DSGVO ausgeschlossen wären und der Betroffene bei einem besonders weitreichenden Eingriff in die informationelle Selbstbestimmung schutzlos wäre. Dies wirkt sich in Anbetracht von *Big Data*-Phänomenen, die einen erleichterten Zugang zu Zusatzwissen auf rechtmäßigem und unrechtmäßigem Wege ermöglichen, als ein unbefriedigendes Ergebnis aus.[406] Daher muss im Ergebnis jede Identifizierung zu einem Schutz der personenbezogenen Daten und damit der personalen Identität führen, was mit der Identitätsverwaltung erleichtert erfolgen kann.

Aus den Verknüpfungsmöglichkeiten zwischen mehreren Daten- und Informationsbeständen geht das Risiko über die Beeinträchtigung des Schutzes der informationellen Selbstbestimmung hervor, welches für den Betroffenen und Verantwortlichen den Bedarf nach einer risikobasierten Prognoseentscheidung auslöst.[407] Demnach besteht das Risiko, dass anonymisierte Daten in einem Datenzyklus zu personenbezogenen Daten werden, wobei der Übergang von anonymen Daten zu personenbezogenen

404 Schlussanträge des Generalanwalts Manuel Campos Sanchez-Bordona, EuGH, C-582/14, 12. Mai 2016, Breyer ./. BRD, Rn. 61; *Kring/Marosi*, K&R 2016, 773 (774).

405 EuGH, Urt. v. 19.10.2016 – C-582/14, Breyer ./. BRD, Rn. 47.

406 *Klar/Kühling*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 4 DSGVO Rn. 29; *Bergt*, ZD 2015, 365 (370).

407 *Kühling/Sackmann*, Rechte an Daten, 20. November 2018, S. 12.

Daten in einer rechtlichen Grauzone[408] stattfinde, bei der für einen bestimmten Zeitabschnitt eine eindeutige Zuordnung erschwert ist. Um der Phänomenologie eines kontextspezifischen Wechsels von anonymen zu personenbezogenen Daten in einem Datenzyklus gerecht zu werden, könnte die zweischrittige Prüfung aus der Entscheidung des englischen „*Court of Appeal*" in *Vidal-Hall v Google*[409] einbezogen werden. Danach erfolgt erst eine kontextunabhängige Einordnung der Daten, und anschließend wird der Kontext in seinen Ausprägungen mit dem Risiko der Identifizierbarkeit einbezogen. Zwar begründet diese Prüfungsfolge eine gewisse Eindeutigkeit bei der Bestimmung der Daten und des Kontextes, jedoch bleibt die Ungewissheit über die Begrenzung des Kontextes und seiner Bedingungen, so dass mit der zweischrittigen Prüfung nicht zwingend eine gesteigerte Rechtssicherheit einhergeht.

Insgesamt wird aufgrund der exponentiell steigenden Datenverarbeitungen und der zügigen Identifizierungsmöglichkeit als *Big Data*-Phänomen angenommen, dass der Theorienstreit über die Identifizierbarkeit dahinstehen könne.[410] Gleichwohl erscheint für die Identitätsverwaltung ein objektiviert-relativer Ansatz naheliegend, wonach es für die Feststellung der Identifizierbarkeit auf das Zusatzwissen des Verantwortlichen und Dritten ankommt. Dabei sind das Risiko von Zusatzwissen eines Dritten und die Frage nach dem verhältnismäßigen Aufwand, dass dieses Zusatzwissen einbezogen wird, maßgeblich. Für die Identitätsverwaltung ist damit entscheidend, wann ein Datensatz in einem Datenzyklus als personenbezogen gilt und damit zum Gegenstand des Identitätsverwaltungsmodells werden muss. Ebenso lässt sich das Bewusstsein über das Bestehen von rechtlichen und technischen Grauzonen zwischen anonymen und personenbezogenen Daten als ein Risiko für den Schutz der Rechte und Freiheiten natürlicher Personen in das Identitätsverwaltungsmodell einbeziehen, indem darauf etwa ausdrücklich im Rahmen der Informationspflichten hingewiesen wird.

408 *Janeček*, CLSR 2018, 1039 (1043).
409 Vidal-Hall v Google [2015] EWCA 311, para. 111 ff.
410 *Spindler*, in: Verhandlungen des 69. Deutschen Juristentages, 2012, S. F 73; *Reinhardt*, AöR 142 (2017), 528 (532).

2. Risiko der Erkenntnisse aus personenbezogenen Daten

Das Risiko der Erkenntnisse aus personenbezogenen Daten folgt aus der Verarbeitung personenbezogener Daten im Datenzyklus und der Einbeziehung von Zusatzwissen des Verantwortlichen und Dritten. Da personenbezogene Daten aus einer Kennung, Standortdaten oder einem Identifizierungsmerkmal und zudem aus Merkmalen als Ausdruck der personalen Identität gemäß Art. 4 Nr. 1 DSGVO bestehen können, schützt die DSGVO neben den personenbezogenen Daten auch die Informationen über natürliche Personen. Demnach ist der Informationsgehalt aus den Daten ausdrücklich als Schutzgegenstand benannt, wie es sich aus den Legaldefinitionen des Profiling (Art. 4 Nr. 4 DSGVO), der biometrischen Daten (Art. 4 Nr. 14 DSGVO) und der Gesundheitsdaten (Art. 4 Nr. 15 DSGVO) ergibt. Dabei handelt es sich um Informationen aus den Daten und der Möglichkeit des Erlernens von Wissen über die personale Identität. Vom Schutz besonderer Kategorien personenbezogener Daten gemäß Art. 9 DSGVO sind folglich auch solche Daten erfasst, aus denen mittelbare Rückschlüsse oder indirekte Hinweise auf sensible Daten möglich sind.[411] Denn aus den Nutzungsdaten bei dem Einsatz des Internets der Dinge etwa in einem „*Smart Home*" können Daten generiert werden, die zunächst Erkenntnisse über das Nutzungsverhalten geben, aber zugleich aus „unbewusst erzeugten Daten"[412] als Metadaten mittelbare Rückschlüsse über die personale Identität einer natürlichen Person erlauben.

Folglich besteht mit der Verarbeitung personenbezogener Daten das Risiko, dass aus einem anfänglich im Datenzyklus unbekannten Erkenntnisgehalt zu einem späteren Zeitpunkt im Datenzyklus ein besonders sensibler Erkenntnisgehalt erwächst, der dem Schutzniveau gemäß Art. 9 DSGVO unterliegt. Dieses gesteigerte Risiko einbeziehend, schlägt *Hoffmann-Riem* die Erweiterung des begrifflichen Schutzes auf Eigenschaften vor, die sich aus einem personenbezogenen Datensatz erlernen lassen.[413] Denn innerhalb eines Datenzyklus kann das „Nochnichtwissen, Nochnichtwissenkönnen, Nichtwissenkönnen"[414] in Erkenntnisse münden, die ursprünglich unvorhersehbar waren. Folglich bedarf es *Instruktio-*

411 *Weichert*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 9 DSGVO Rn. 37.
412 *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 224; *Hildebrandt*, Smart technologies and the end(s) of law, 2015, S. 67–69.
413 *Hoffmann-Riem*, AöR 142 (2017), 1 (38 f.)
414 *Ders.*, in: Augsberg (Hrsg.), Ungewissheit als Chance, 2009, 17 (28).

nen über den Wissenserwerb und die Kanalisierung dessen, welches etwa über die Befristung und Sperrung von Datensätzen erfolgt. Für die Befristung der Speicherung spricht, dass das Risiko der Erkenntnismöglichkeit über einen Datenzyklus hinweg gemindert wird. Gleichwohl könnten auch kurzfristig generierte Erkenntnisse in die informationelle Selbstbestimmung eingreifen oder über eine redundante Speicherung perpetuiert werden, so dass die befristete Speicherung nicht zwingend zu einer Schutzsteigerung führt. Demnach erscheint für die wirksame Identitätsverwaltung der Bedarf nach Informationen über das Risiko der Erkenntnismöglichkeiten aus dem Datenverarbeitungsvorgang wünschenswert. Dazu gehört neben der Transparenz des Risikos die Einräumung der Kontrolle über die Chancen und Risiken von Erkenntnissen im Laufe des Datenzyklus.

3. Ergebnis

Die Bestimmung der personenbezogenen Daten ist für die Abgrenzung des Gegenstandes der Identitätsverwaltung und den Anwendungsbereich der DSGVO maßgeblich. Der Vorgang der Identifizierbarkeit ist allerdings mit rechtlichen und tatsächlichen Risiken verbunden, die sich auf das erlangte Zusatzwissen, die Qualität des Zusatzwissens und den möglichen Erkenntnisgehalt beziehen. Die Prüfung der Identifizierbarkeit ist ein wertender Vorgang, so dass für ein Identitätsverwaltungsmodell die natürliche Person über die rechtlichen und technischen Grauzonen zwischen anonymen und personenbezogenen Daten in Kenntnis gesetzt werden sollte. Weiter lassen sich bei der Verarbeitung personenbezogener Daten innerhalb eines Datenzyklus mittelbar Erkenntnisse ableiten, die zu einem Risiko für die informationelle Selbstbestimmung führen können.

Insgesamt wird in der DSGVO ein Paradigmenwechsel weg von dem Fokus auf die personenbezogenen Daten hin zu den Schutzzielen angenommen, was zu einer Verschiebung der Schutzmechanismen auf der Ebene der Grundsätze der Datenverarbeitung gemäß Art. 5 DSGVO und dem Risiko der Datenverarbeitung gemäß Art. 32 DSGVO führe.[415] Dies erscheint in Anbetracht der hohen Wahrscheinlichkeit einer Identifizierbarkeit im Laufe des Datenzyklus als *Big Data*-Phänomen naheliegend, zumal bei einem Fokus auf die Grundsätze der Datenverarbeitung für die kon-

415 *Veil*, ZD 2015, 347 (348 f.); *Quelle*, European Journal of Risk Regulation 2018, 502 (504).

textspezifische Risikolage geeignete Kompensationsmechanismen gemäß Art. 5 Abs. 1 DSGVO geschaffen werden können und sich so das Risiko von Erkenntnissen mindern lässt.

II. Transparenz zur Identitätsverwaltung, Art. 5 Abs. 1 a) DSGVO

Die Transparenz ist die tragende Voraussetzung für die Identitätsverwaltung. Denn die Transparenz ermöglicht eine bewusste Entscheidung des Betroffenen über die Einwilligung und eine Risikoabwägung, ob die mit einer Datenverarbeitung verbundenen Risiken von dem Betroffenen eingegangen werden sollen. Dies setzt voraus, dass die transparenten Angaben über das Risiko der Datenverarbeitung den Betroffenen zu einer risikobewussten Entscheidung befähigen. Folglich ist für die Transparenz zur Identitätsverwaltung maßgeblich, dass vorher eine Risikobewertung über die Datenverarbeitung durch den Verantwortlichen vorgenommen wurde und die Risikoinformationen anschließend dem Betroffenen in einer verständlichen Form mitgeteilt wurden. Erst mit diesen Informationen kann der Betroffene eine risikobewusste Entscheidung über die Einwilligungserteilung vornehmen.

Weiter muss der Betroffene über die konkreten Umstände der Verarbeitung personenbezogener Daten informiert werden, um auf die Teilidentitäten und Attribute der personalen Identität kontrollierend einwirken zu können. Darin spiegelt sich die informationelle Selbstbestimmung wider. Die Selbstbestimmung kann nur mit Kenntnis über die konkreten Datenverarbeitungen ausgeübt werden. Nur durch diese Kenntnis wird dem Betroffenen dazu verholfen, von seiner Selbstbestimmung risikobewusst Gebrauch zu machen.

Damit sind die Informationen über das Risiko der Datenverarbeitung im Datenzyklus zu Beginn der Identitätsverwaltung erforderlich und können sich auf die rechtfertigende Einwilligung und die Nutzung des Dienstes auswirken. Demnach sollen die Informationen über die Datenverarbeitung als Entscheidungsgrundlage des Betroffenen (1.) und die Informationen über das Risiko (2.) dargestellt werden. Anschließend soll der Frage nachgegangen werden, ob sich mit der Transparenz die Kontrolle über die Teilidentitäten ausüben lässt (3.), um dann eine Bewertung der Transparenz für die Identitätsverwaltung (4.) vornehmen zu können.

1. Informationen als Entscheidungsgrundlage

Die Transparenzpflichten nach Art. 5 Abs. 1 a), Art. 12–14 DSGVO sehen die Informationsgrundlage für die Entscheidungsprozesse durch den Betroffenen vor. Die Informationsgrundlage stellt sich aus der Perspektive des Betroffenen und somit zu Beginn des Datenzyklus dar. Danach sind solche Informationspflichten erfasst, mit denen der Betroffene Kenntnis über die Umstände und Risiken der Datenverarbeitung als Grundlage für eine rationale Entscheidung erlangen kann. Dazu gehören die Kontaktdaten der verantwortlichen Stelle, die Kontaktdaten des Datenschutzbeauftragten, die Zwecke der Datenverarbeitung, ein möglicher Empfänger dieser Daten, die Dauer der Speicherung, die bestehenden Rechte des Betroffenen, die Grundlage der Datenverarbeitung, die technische Möglichkeit der Profilbildung und ihre potentiellen Auswirkungen sowie das Risiko der gesamten Datenverarbeitung, Art. 13 Abs. 1, 2 c) DSGVO, EWG 39 S. 5. Damit soll der Betroffene zur Antizipation der Risiken über die Datenverarbeitung und möglichen Profilerstellungen befähigt werden. Bei der Informationsmitteilung besteht jedoch ein Spannungsverhältnis zwischen einerseits detaillierten Informationen für den Betroffenen zur wirksamen Ausübung der Rechte und andererseits dem Bedarf, den Betroffenen vor einer Informationsflut zu bewahren. Maßgeblich ist jeweils, dass die Informationen gut lesbar sind und leicht verständlich etwa mit Piktogrammen versehen werden. Auch können die Informationspflichten in einem maschinenlesbaren Format zur Verfügung gestellt werden, Art. 12 Abs. 7 DSGVO. Dies ermöglicht ein ausgewogenes Verhältnis zwischen einerseits rechtskonformer Informationsmitteilung über die Datenverarbeitung und andererseits einer gut verständlichen Darstellung der Informationspflichten.

Gleichwohl richtet sich die Effektivität der Informationen in einer Datenschutzerklärung danach, ob die Datenschutzerklärung gelesen wird und zur Entscheidungsfindung beiträgt. Ebenso wird bei Betroffenen ein Transparenzirrtum dahingehend angenommen, dass bei komplexen Datenverarbeitungsvorgängen gerade keine umfangreiche Kenntnis über die tatsächliche Datenverarbeitung bestehen könne.[416] Dazu gehört besonders der gesonderte Informationsbedarf bei der kontextübergreifenden Datenverarbeitung im Rahmen eines Zweckes, Art. 5 Abs. 1 b) DSGVO. Entsprechend wird ein Recht auf Begründung zugunsten der betroffenen Person abgeleitet, welches dem Recht auf Informationen über die involvierte Lo-

416 *Edwards/Veale*, Duke L. & Tech. Rev. 2017, 18 (23).

gik beim Einsatz algorithmusbasierter Einzelentscheidungen in einer Blackbox entspricht, Art. 13 Abs. 2 f) DSGVO.[417] Ein Recht auf Begründung der Einzelheiten über die Datenverarbeitung könnte dem Phänomen der betroffenen Person als „Sklaven des Algorithmus"[418] entgegenwirken und mögliche diskriminierende Wirkungen von Algorithmen aufdecken. Dieses Konzept greift zwar das Phänomen der fehlenden Kenntnis über die Folgen der Datenverarbeitung als Transparenzirrtum auf, führt jedoch nicht zu einem neuen Schutzmechanismus. Denn die Informationspflichten aus Art. 13 Abs. 2 DSGVO umfassen die Besonderheiten der jeweiligen Datenverarbeitung, so dass ein eigenes Recht auf Begründung nicht erforderlich ist. Gleichzeitig kommt in einem selbständigen Recht auf Begründung die Verantwortungsverteilung zum Ausdruck, die dem Verantwortlichen eine Begründungslast auferlegt.

Indem die Informationen für den Betroffenen als Grundlage der Entscheidungsfindung fungieren, wird die Verantwortung durch die Informationspflichten auf den Betroffenen übertragen, und mit einem Recht auf Begründung wird eine erweiterte Kenntnis über die Datenverarbeitung und damit eine weitere effektive Kontrollmöglichkeit eingeräumt.[419] Sobald die Datenschutzerklärung gelesen und auf ihrer Grundlage die Einwilligung erteilt wird, findet eine Verantwortungsverschiebung mit der Einräumung einer Kontrollmöglichkeit zum Betroffenen statt. Denn diese löst mit der Informationsgrundlage im Rahmen der informationellen Selbstbestimmung den nächsten Schritt im Datenzyklus aus, so dass die Transparenz in Gestalt eines *„notice and choice"*[420] auch als Grundlage der Kontrolle in einem Identitätsverwaltungsmodell fungieren kann.

2. Informationen über das Risiko

Der risikobasierte Ansatz gemäß Art. 32 DSGVO ist Bestandteil der Datenschutz-Folgenabschätzung, die allein bei einem hohen Risiko erforderlich ist. Gleichzeitig ist der risikobasierte Ansatz bereits in der Datenschutz-

417 Wahrnehmungsgegenstand bei der Blackbox können allein die Input- und Outputwerte sein, *Reisinger*, Rechtsinformatik, 2016, S. 64; *Hornung/Engemann* (Hrsg.), Der digitale Bürger und seine Identität, 2016, S. 18.

418 *Edwards/Veale*, Duke L. & Tech. Rev. 2017, 18.

419 *Dies.*, Duke L. & Tech. Rev. 2017, 18 (41 f.); *Wischmeyer*, AöR 143 (2018), 1 (48–54).

420 *Solove*, Harv. L. R. 2013, 1880 (1883 f.).

richtlinie 45/95 verwurzelt[421] und kann als grundlegender Ansatz bei der Rechtfertigung eines Datenverarbeitungsvorgangs angesehen werden. Denn in jeder Datenverarbeitung innerhalb eines Datenzyklus der personalen Identität sei ein immanentes Grundrisiko gegenüber dem Schutzgut der Rechte und Freiheiten natürlicher Personen vorhanden (Art. 35 Abs. 1 S. 1 DSGVO), welches sich auf die Wahl des Rechtfertigungsgrundes auswirkt. Demnach verlangt die Entscheidung über den geeigneten Rechtfertigungsgrund durch den Verantwortlichen eine immanente Risikobewertung der bevorstehenden Datenverarbeitung. Diese Risikobewertung durch den Verantwortlichen wirkt sich zum einen auf der Rechtfertigungsebene und zum anderen auf der Ebene der Informationspflichten aus.

Zwar ist in Art. 12, 13 DSGVO nicht vorgesehen, das Risiko ausdrücklich zu benennen, aber in der Gesamtschau der Informationspflichten lässt sich der Informationsbedarf über die Risiken der Datenverarbeitung aus den ausdrücklich aufgezählten Informationspflichten entnehmen. Dazu gehört das Risikokriterium des Zwecks der Datenverarbeitung gemäß Art. 13 Abs. 1 c) und der entsprechend gewählte Begriff für die Zweckbestimmung, Art. 13 Abs. 3 DSGVO. Weiter enthalten Informationen über das Bestehen der Absicht, für einen weiteren Zweck eine Datenverarbeitung vornehmen zu wollen, ebenso eine Aussage über das bevorstehende Risiko. Denn aus dem Zweck werden der Kontext und der mögliche Umfang der Datenverarbeitung erkennbar, was die Bestimmung von Risikokriterien für die Rechte und Freiheiten natürlicher Personen ermöglicht. Weiter kann aus dem zur Verfügung stehenden Rechtfertigungsgrund etwa der Einwilligung gemäß Art. 6 Abs 1 a) DSGVO das Bestehen eines höheren Risikos der Datenverarbeitung entnommen werden, welches von dem legitimen Interesse gemäß Art. 6 Abs. 1 f) DSGVO nicht gedeckt wäre. Ebenso kann als Risikokriterium die Dauer der bevorstehenden Datenverarbeitung gemäß Art. 13 Abs. 2 b) DSGVO herangezogen werden. Denn je länger die Datenverarbeitung andauert, umso höher ist das Risiko für den Schutz der Rechte und Freiheiten natürlicher Personen. Demnach kann der Bedarf bei einer langfristigen Datenverarbeitung steigen, von den Betroffenenrechten Gebrauch zu machen. Schließlich sieht der EWG 39 S. 5 der DSGVO vor, dass der Betroffene über die Risiken im Zusammenhang mit der Verarbeitung der personenbezogenen Daten informiert werden soll, weshalb die ausdrücklichen Informationspflichten aus Art. 13, 14

421 Art. 7 f); 13 Abs. 2; 17; 20 Datenschutzrichtlinie 95/45; *Veil*, ZD 2015, 347 (351); *Kuner/Kate/Millard u.a.*, IDPL 2015, 95.

DSGVO um die Informationspflichten zum Risiko der Datenverarbeitung erweitert werden sollten.

Aus dieser Gesamtschau der Risikokriterien in den Informationspflichten wird immanent die Grundlage für eine Risikoentscheidung über die Einwilligung und die Nutzung des Dienstes durch den Betroffenen geschaffen und findet seine Bestärkung im EWG 39 S. 5 der DSGVO. Demnach besteht mit den Informationen über das Risiko der Datenverarbeitung der gleichzeitige Bedarf einer vorangegangenen Risikobewertung über die Datenverarbeitung durch den Verantwortlichen (a), was wiederum eine Risikobewertungsmethode voraussetzt. Die Anforderungen an eine Risikobewertungsmethode sollen daher im Folgenden umrissen werden. Infolge dieser Darstellung könnten die Risiken gegenüber den Rechten und Freiheiten der natürlichen Person zum Gegenstand der Informationspflichten für die Risikoentscheidung des Betroffenen gemacht werden (b).

a) Risikobewertung durch den Verantwortlichen

aa) Methode zur Risikobewertung

Die Bewertung des Risikos muss gemäß dem EWG 76 S. 2 DSGVO durch den Verantwortlichen objektiv erfolgen und setzt eine Prognose[422] über die „Informationsverwendungsfolgen“[423] mit der Datenverarbeitung als ein unsicheres Ereignis in der Zukunft voraus. Danach bedarf es der Bestimmung von Risikokriterien zur Unterscheidung der Anknüpfungspunkte möglicher Maßnahmen. Es bedarf demnach einer Kalibrierung[424] zwischen dem tatsächlichen Risiko der bevorstehenden Datenverarbeitung und den Datenschutzprinzipien, damit die Pflichten und Rechte des Ver-

422 *Kahneman*, Schnelles Denken, langsames Denken, 2012, S. 181–189; *Kahneman/Tversky*, Econometrica 1979, 263 (273–277): Auf der Ebene der individuellen Prognoseentscheidung sind verhaltensökonomische Verzerrungen bei Wahrscheinlichkeitsbewertungen einzubeziehen, da scheinbar repräsentative Kriterien für die Entscheidungsfindung begründet werden und zu kognitiven Hürden führen können.

423 *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 64.

424 *Ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 57; *Quelle*, European Journal of Risk Regulation 2018, 502 (509); *Kuner/Kate/Millard u.a.*, IDPL 2015, 95.

antwortlichen konkretisiert werden können.[425] So wird die Risikobewertung mit einer Verhältnismäßigkeitsprüfung verglichen, wobei die Risikobewertung als ein Meta-regulatorisches Konzept näherliegend erscheint, da es um die übergeordnete Bewertung der Risiken einer Datenverarbeitung geht, die sich auf die Verhältnismäßigkeitsprüfung im Einzelnen auswirken könne.[426] Denn es geht um singuläre Risikobewertungen anknüpfend an die jeweiligen Risikokriterien, die in eine übergeordnete Gesamtbetrachtung über das Risiko der Datenverarbeitung münden. Damit wird eine konstatierte Skalierbarkeit der datenschutzrechtlichen Pflichten ermöglicht und die Risikobewertung in ein Konzept der „*Compliance 2.0*" überführt, welches über eine bloße binäre Struktur aus Zulässigkeit oder Unzulässigkeit einer Datenverarbeitungsmaßnahme hinaus eine wertende Betrachtung und Anpassung der Maßnahmen ermögliche, EWG 84 S. 2, 78 S 1.[427]

Als Methode zur Risikobewertung kommt eine semiquantitative Methode[428] in Betracht. In quantitativer Hinsicht wären die Zahlenwerte als Annäherungswerte einzubeziehen.[429] In qualitativer Hinsicht sind die Risikokriterien anhand der Rechtsbegriffe zu identifizieren. Gleichwohl fehle es bislang an einer Risikosystematik,[430] so dass die bestehenden Risikokriterien gemäß Art. 35 Abs. 3 a) – c) DSGVO für die Datenschutz-Folgenabschätzung und die Liste der Verarbeitungsvorgänge, die gemäß Art. 35

425 *Kuner/Kate/Millard u.a.*, IDPL 2015, 95 (97).

426 *Veil*, ZD 2015, 347 (351); *Quelle*, European Journal of Risk Regulation 2018, 502 (511).

427 *Ders.*, ZD 2015, 347 (351); *Quelle*, European Journal of Risk Regulation 2018, 502 (507); *Gellert*, CLSR 2018, 279 (284 f.)

428 *Raabe*, in: Beyerer/Winzer (Hrsg.), Beiträge zu einer Systemtheorie Sicherheit (acatech DISKUSSION), 2018, 97 (112); ebenso die quantitative und qualitative Methode befürwortend, vgl. *Quelle*, European Journal of Risk Regulation 2018, 502. Gegen einen rein quantitativen Ansatz spricht, dass die Quantifizierbarkeit der Menschenwürdegefährdung unmöglich erscheint und sich nicht mit der Verknüpfung zu Rechtsbegriffen vereinbaren ließe. Demgegenüber wäre der qualitative Ansatz geeignet, um die Auslegungsspielräume der Rechtsbegriffe angemessen zu berücksichtigen. Gleichzeitig birgt der qualitative Ansatz bei dem etwa Einstufungen in niedriges, mittleres und hohes Risiko vorgenommen werden, vgl. *Bieker/Bremert/Hansen*, DuD 2018, 492 (493), die Gefahr einer willkürlichen Entscheidung. Entsprechend wird ein semiquantitativer Ansatz befürwortet, für den aus der Empirie und Schadensersatzsummen die Zahlenwerte eingesetzt werden könnten.

429 *Ritter*, in: Schwartmann/Jaspers/Thüsing u.a. (Hrsg.), DS-GVO/BDSG, Kommentar, 2018, Art. 32 DSGVO Rn. 79 f.

430 *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 8 f.

Abs. 4 DSGVO eine Datenschutz-Folgenabschätzung voraussetzen, einbezogen werden sollten. Diese Risikokriterien fungieren bei einer Risikobewertung als *„entry points"*[431] und dienen als Anknüpfungspunkte für einen prognostischen Blickwinkel der Kausalverläufe. Denn die Risikobewertung verlangt die Analyse von hypothetischen Kausalverläufen unter Einbeziehung der Datenverarbeitungskontexte und der Datenverarbeitungszwecke, die zu einer potentiellen Gefahr oder einem Schaden für die Rechte und Freiheiten natürlicher Personen führen können. Die entscheidende Aufgabe bei der Risikobewertung wird darin liegen, die mit den Risikokriterien verbundenen hypothetischen Kausalverläufe in ihren Wirkungen anhand spezifischer *Instruktionen* zu koppeln und entkoppeln[432], um die Risikokriterien für die konkrete Datenverarbeitung in quantitative Werte zu überführen. Damit soll der möglichen Willkür von Momentaufnahmen Rechnung getragen werden, so dass im Rahmen des Datenzyklus das Risiko in den jeweiligen Phasen der Datenverarbeitung der quantitativen Bewertung unterliegen sollte.

Insgesamt sind dafür die Risikokriterien aus Art. 5 Abs. 1 DSGVO und Art. 35 DSGVO abzuleiten, so dass für den Kontext der Datenverarbeitung die Risikokriterien des angewendeten Rechtfertigungsgrundes (Art. 5 Abs. 1 a) DSGVO), der Zweckbindung (Art. 5 Abs. 1 b) DSGVO),[433] des angewendeten Standes der Technik (Art. 5 Abs. 1 c) – f) DSGVO) und der Dauer mit dem Umfang der Datenverarbeitung einzubeziehen sind. Neben den Risikokriterien aus den Datenschutzprinzipien sind die Risikokriterien gemäß Art. 35 DSGVO zu konkretisieren. Jedes dieser Risikokriterien sollte mit quantitativen Werten versehen werden, die aus einer mathematischen Gesamtschau bereits bekannt gewordener Rechtsverstöße mit verhängten Bußgeldern oder aus fiktiven Zahlenwerten bestehen können.[434] Weiter sollten die Risikokriterien im Hinblick auf die hypothetischen Kausalverläufe möglicher Schadensfälle untersucht werden, was einer qualitativen Betrachtung unterliegen würde. Dafür wäre eine Eintei-

431 *Luhmann*, in: Baecker (Hrsg.), Die Kontrolle von Intransparenz, 2017, 46 (48).

432 *Ders.*, in: Baecker (Hrsg.), Die Kontrolle von Intransparenz, 2017, 46 (58–60).

433 In der Risikobewertung ist zwischen allgemeinen Zwecken und privilegierten Zwecken etwa dem wissenschaftlichen, historischen und statistischen Zweck zu differenzieren, EWG 89 S. 3.

434 Die Quantifizierbarkeit von Risikokriterien in einer spezifischen Datenverarbeitung ist ein noch zu erforschender Gegenstand. Zunächst bestehen Unsicherheiten über die Verlässlichkeit der Informationen zu bekannt gewordenen Bußgeldern und weiter besteht Forschungsbedarf über die Bestimmung fiktiver Zahlenwerte.

lung in die Phasen der Datenverarbeitung erforderlich, die in hypothetische Schäden („potentiellen Einzelschaden“[435]) innerhalb einer Phase eingeteilt und mit einem spezifischen Zahlenwert für das Risikokriterium in der Datenverarbeitungsphase versehen werden könnten. Infolgedessen wäre eine Addition der Zahlenwerte aller Risikokriterien vorzunehmen, deren Ergebnis zwischen dem Minimal- und Maximalwert einzuordnen wäre und als semiquantitative Risikobewertung gelten könnte. Dabei geht es um eine deutlich differenziertere Darstellung des Risikos der Datenverarbeitung als es die Einordnung in eine Systematik zwischen hohem, mittlerem und niedrigem Risiko vorsehen würde, damit die Objektivität der Risikobewertungsmethode gewährleistet wird.

Insgesamt handelt es sich dabei um eine Prozeduralisierung der Datenschutzprinzipien, da diese über ein (Risikobewertungs-) Verfahren eine stufenweise Modifizierung erfahren und auf den Anwendungskontext in Gestalt der technischen und organisatorischen Maßnahmen gemäß Art. 25 Abs. 2 DSGVO übertragen werden. Denn die Prognose über die Risiken in einem Datenzyklus umfasst das Unwissen über die Wahrscheinlichkeit eines Schadenseintritts, welches prozedural „eingefangen“ werden könne.[436]

Im Hinblick auf ein Identitätsverwaltungsmodell stellt sich die Frage nach dem Umfang dieser Risikobewertung und den subjektiven Einflüssen bei der Entscheidung[437] des Betroffenen über die Verwaltung personaler Identitäten. Denn die Risikobewertung des Verantwortlichen muss zugleich die Perspektive des Betroffenen einbeziehen, welche Risiken dieser eingeht. Erst mit dieser Bewertung kann die Gesamtbetrachtung über das Risiko der Datenverarbeitung und eine Kalibrierung der geeigneten technischen und organisatorischen Maßnahmen zur Realisierung der Datenschutzprinzipien vorgenommen werden. Demnach bedarf es aus der Perspektive des Betroffenen der Transparenz über die Risiken der Datenverarbeitung, um auf dieser Grundlage eine Risikoentscheidung treffen zu können.

435 *Ritter*, in: Schwartmann/Jaspers/Thüsing u.a. (Hrsg.), DS-GVO/BDSG, Kommentar, 2018, Art. 32 DSGVO Rn. 81.

436 *Hoffmann-Riem*, in: Augsberg (Hrsg.), Ungewissheit als Chance, 2009, 17 (21).

437 *Kahneman*, Schnelles Denken, langsames Denken, 2012, S. 178 f.

bb) Risikokriterien nach Art. 35 DSGVO als Bewertungsgrundlage

Die Risikokriterien sind zunächst aus den Datenschutzprinzipien gemäß Art. 5 Abs. 1 DSGVO abzuleiten und ermöglichen die Anpassung des Standes der Technik für die spezifische Datenverarbeitung. Daneben sind die Risikokriterien zur Bestimmung der Datenverarbeitung mit einem hohen Risiko gemäß Art. 35 DSGVO einzubeziehen. Dafür ist die Datenschutz-Folgenabschätzung vorzunehmen und die in Art. 35 Abs. 1 und in Absatz 3 DSGVO indizierend aufgezählten Risikokriterien heranzuziehen, um die semiquantitative Risikobewertungsmethode für Datenverarbeitungen mit einem hohen Risiko anwenden zu können. Gemäß Art. 35 Abs. 1 DSGVO wird ein Risikokriterium in der Verarbeitung mit neuen Technologien angenommen. Durch die neuen Technologien besteht etwa das Risiko der Informationspermanenz, wonach verarbeitete Informationen eigenständig im Raum stünden und systematisch zusammengetragen werden können.[438] Folglich ergibt sich mit den neuen Technologien eine Steigerung der Speicherungsmöglichkeiten, von denen ein eigenes Risiko für die informationelle Selbstbestimmung ausgehen kann. Daraus lässt sich das weitere Risikokriterium der systematischen Bewertung persönlicher Aspekte ableiten, wonach ein hohes Risiko bei der automatisierten Verarbeitung und dem Profiling angenommen werden kann, Art. 35 Abs. 3 a) DSGVO. Aufgrund von algorithmusbasierten automatisierten Zuordnungen können Profile erstellt werden, mit denen die Wahrscheinlichkeit über die Zugehörigkeit zu einer bestimmten Kohorte (Korrelation) bestimmt werden kann, wozu die Aussage über die Teilnahmewahrscheinlichkeit an einem Musikfestival oder die Bonität gehören kann.[439] Diese Auswirkungen lassen sich als Risiko eines Publizitätsschadens oder Reputationsverlusts[440] einordnen und können als eine Enttäuschung der berechtigten Vertraulichkeits- und Privatheitserwartung gesehen werden.

Weiter kommen die von *Drackert* beschriebenen Risiken der Informationspermanenz und Informationsemergenz zum Ausdruck, in denen jeweils die Häufigkeit der Datenspeicherung zu einer Perpetuierung des Risikos führt.[441] Die Informationspermanenz kann sich bei der Speicherung unbewusst verarbeiteter Verkehrsdaten ergeben, womit das Risiko eines

438 *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 69.
439 4. Teil, A., I., 2.
440 *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 69, 193.
441 *Ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 193.

„gläsernen Bürgers“[442] bestünde und Überwachungsdruck ausgelöst werden könne.[443] Bei der Informationsemergenz werden die Daten fixiert und in unkontrollierbare, entkontextualisierte Informationen zusammengeführt, die zu Erkenntnissen und einer „verwaltungstechnischen Entpersönlichung“[444] führen können. Damit wird eine weitere Risikodimension begründet, die sich in dem gesteigerten Preisgabeverhalten des Einzelnen aufgrund eines „Kontrollgefühls“[445] niederschlagen kann. Die Risikokonzeption erfährt damit eine Subjektivierung, indem etwa psychischer Druck ausgelöst werden und dies freiheitshemmende Wirkung in Gestalt eines „Konformismusrisikos“ haben könne, was sich individuell und gesamtgesellschaftlich auswirke.[446]

Ein weiteres Risikokriterium liegt gemäß Art. 35 Abs. 3 b) in der Verarbeitung besonderer Kategorien personenbezogener Daten, wodurch aufgrund der Sensibilität von Daten das Risiko des umfassenden Erkenntnisgewinns bestehen kann. Das Risikokriterium über die systematische Überwachung öffentlich zugänglicher Bereiche gemäß Art. 35 Abs. 3 c) DSGVO erscheint dagegen als eines, welches neben dem individuellen Gefühl des Überwachtwerdens sich gesamtgesellschaftlich auswirken kann. Von diesem Risikokriterium sind besondere Kontexte im Verhältnis zwischen Staat und Bürger erfasst, so dass die „Instrumente staatlicher und privater Machtbildung“ gleichermaßen zum Risiko der Informationsmacht werden.[447] Dies gilt gerade bei dem Phänomen der im Auftrag des Staates agierenden privaten Sicherheitsunternehmen, so dass das Risiko für die Rechte und Freiheiten natürlicher Personen auch von den Akteuren und der Anzahl dieser abhängt.

Ebenso kommt bei der internationalisierten Datenverarbeitung eine weitere Dimension des Datenverarbeitungsrisikos hinzu, denn aufgrund des modifizierten Schutzregimes etwa mit dem „*EU-US-Privacy Shield*“[448]

---

442 Schlussanträge der Generalanwältin Kokott, EuGH, 18.07.2017, C-275–06, Promisucae, Rn. 97.

443 *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 104 f.; EuGH, Urt. v. 08.04.2014 – C-293/12 und C-594/12, Digital Rights Ireland, Rn. 27.

444 *Ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 183.

445 3. Teil, C., IV; *ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 291.

446 *Ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 188–190.

447 *Ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 280.

448 Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016, Az. C (2016) 4176.

gemäß Art. 45 DSGVO wirkt bei diesen grenzüberschreitenden Datenverarbeitungen ein gegenüber der DSGVO parallel wirkendes Schutzregime. Weiter kann der effektive Rechtsschutz für den Betroffenen in Frage stehen, wenn die Rechtsstreitigkeiten gemäß 2.1. (20) *EU-US-Privacy Shield* über alternative Streitbeilegungsmethoden beigelegt werden sollen. Gleichwohl bleibt anzumerken, dass mit Art. 3 Abs. 2 DSGVO auch das Beobachten des Nutzungsverhaltens und das Anbieten von Diensten und Waren an Betroffene in der Europäischen Union vom Schutzregime der DSGVO erfasst ist (Marktortprinzip) und dieses damit eine weitreichende Wirkung über die Ländergrenzen hinweg entfaltet.

In der Gesamtbetrachtung bestehe das Risiko der Überwachungskumulation etwa durch das Zusammenführen vieler einzelner Datensätze mit Bewegungsdaten, so dass sich das Risiko des Überwachungsdruckes durch *De- und Rekontextualisierung* potenzieren könne.[449] Ebenso kommt das Risiko durch ein Kontextdefizit in Betracht, bei dem bestimmte Informationen nicht übernommen werden und nur Teilaspekte einer personalen Identität transparent werden, so dass die Erkenntnis verzerrt möglich ist.[450] Darin zeigen sich die Überschneidungen zu den bereits erwähnten Risiken der Informationspermanenz und Informationsemergenz, die sich ebenso aus den Überwachungsdaten ergeben. Somit kann Art. 35 Abs. 3 c) DSGVO als Konkretisierung zu den neuen Technologien gemäß Art. 35 Abs. 1 DSGVO angesehen werden. Als weiteres Risikokriterium kommt der materielle oder immaterielle Schaden gemäß Art. 82 Abs. 1 DSGVO hinzu, der aus der Verletzung des Schutzes personenbezogener Daten entstehen kann. Ein Schaden wird gemäß dem EWG 85 S. 1 DSGVO angenommen, wenn ein Verlust über die Kontrolle personenbezogener Daten, eine Diskriminierung bei der Verarbeitung, ein Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Verlust der Vertraulichkeit von dem Berufsgeheimnis, Rufschädigung vorliegen oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile, die dem Betroffenen drohen. Diese Schadensgruppen lassen sich übergeordnet in dem von *Drackert* beschriebenen Risiko informationeller Machtverschiebung und den Selektivitätsschäden einordnen.[451] Die

449 *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 219 f.

450 *Ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 302 f.; zum Konzept der „Kontrolle durch Intransparenz" nach *Luhmann*, vgl. 2. Teil, A., II., 1., c), bb).

451 *Ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 280 f.; *Herfurth*, ZD 2018, 514 (518).

informationelle Machtverschiebung tritt bei dem Kontrollverlust etwa durch Identitätsdiebstahl oder Aufhebung der Pseudonymisierung auf. Demgegenüber sind Selektivitätsschäden bei Diskriminierungen aufgrund eines spezifischen Merkmals gegeben, die zu einer Stigmatisierung führen können.

Schließlich kann die Wahrscheinlichkeit des Schadenseintritts variieren, welches auch von dem angewendeten Stand der Technik und der technischen organisatorischen Maßnahmen abhängig ist. Denn gerade in der technischen Realisierung der Datenverarbeitung können der Kostendruck oder begrenzte Anreize zur Steigerung des Sicherheitsniveaus ebenfalls zu einer Steigerung des Risikos für die Rechte und Freiheiten natürlicher Personen führen und ein eigenes Risikokriterium begründen.

Insgesamt sind die Maßnahmen der Risikobewertung zu dokumentieren und können als Bestandteil der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO eingeordnet werden, welches die Berichtsphase vor der Datenverarbeitung und die Einzelheiten zu der Datenschutz-Folgenabschätzung gemäß Art. 35 Abs. 7 DSGVO umfassen müsste.

b) Risikoinformationen an den Betroffenen

Nach der objektivierten Ermittlung des Risikos mit einer semiquantitativen Risikobewertungsmethode für die Rechte und Freiheiten natürlicher Personen bedarf es der Informationsmitteilung an den Betroffenen. Danach sind die Risiken der Datenverarbeitung gemäß Art. 12, 13 DSGVO, EWG 39 Gegenstand der Informationspflichten und sollten möglichst ausdrücklich benannt werden, damit die natürliche Person eine risikobewusste Entscheidung treffen kann. Die Entscheidung des Betroffenen soll die Möglichkeit einer Folgenabschätzung über die Eintrittswahrscheinlichkeit von materiellen und immateriellen Schäden umfassen können, für die der Verantwortliche mit den Informationspflichten unterstützend tätig wird. Damit sind die Informationen über die Risiken der Datenverarbeitung eine notwendige Voraussetzung für die effektive Identitätsverwaltung. Denn nur mit der Kenntnis über die mit der Einwilligung oder der Nutzung eines Dienstes verbundenen Risiken, kann die informationelle Selbstbestimmung wirksam wahrgenommen werden und Schutzmaßnahmen bei einem antizipierten Kontrollverlust über die Erkenntnisse zur personalen Identität eingeleitet werden.

Voraussetzung für die Realisierung der Informationspflichten ist die Einbeziehung der Risikobewertungsergebnisse in die Informationspflich-

ten, damit dem datenschutzrechtlichen Vorfeldschutz Rechnung getragen wird. Dazu kann die Benennung des Zahlenwertes nach der semiquantitativen Risikobewertungsmethode gehören und zusätzlich könnten die Risikokriterien mit einem hohen Risikowert in die Informationen aufgenommen werden, damit der Betroffene das kontextspezifische Risiko für die personale Identität in seine Entscheidungsfindung einbeziehen kann. Demnach besteht für die Identitätsverwaltung hinsichtlich der kontextspezifischen Datenverarbeitung ebenfalls ein Transparenzbedürfnis über das Risiko, um die Grundrisiken und hohen Risiken innerhalb eines Datenzyklus in unterschiedlichen Zeitabschnitten für den Betroffenen einschätzbar zu machen.

Ebenso können die kompensatorischen Schutzmaßnahmen zur Risikominderung gemäß Art. 32 Abs. 1 a) – c), 5 Abs. 1 d) – f) DSGVO durch den Verantwortlichen zum Gegenstand der Informationspflichten werden.[452] Damit und mit der Einbeziehung der Risikobewertungsergebnisse in den Informationspflichten erfolgt *quasi* eine Begründung über die Datenverarbeitung, die dem Ausgleich bestehender Asymmetrien zwischen Verantwortlichem und Betroffenen dient. Demnach werde der betroffenen Person zu einem frühen Zeitpunkt des Datenzyklus ermöglicht,[453] die informationelle Selbstbestimmung durch Kenntnis potentieller Schäden von Anfang an wahrzunehmen.

c) Bewertung

Die Risiken der Datenverarbeitung werden von *Drackert* in eine Mikro- und Makroebene eingeteilt, wonach diese sich auf die natürliche Person auswirken können oder in gesellschaftlich-politischen Zusammenhängen wirken.[454] Beide Risikoauswirkungen können ineinander übergehen, so dass die Ergebnisse einer semiquantitativen Risikobewertung in die Infor-

452 Gemäß Art. 32 DSGVO sind Maßnahmen angeführt, wozu die Pseudonymisierung, Verschlüsselung, Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme gehören und zum Gegenstand der Informationspflichten werden können. Sofern Zertifizierungen etwa über eine behördliche Prüfung des Verfahrens der Risikobewertung erfolgen würde, könnten diese ebenfalls in die Informationen einbezogen werden.

453 Über die frühzeitige Ausübung des „*Privacy Self Management*“, *Solove*, Harv. L. R. 2013, 1880 (1891).

454 *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 278 ff.

mationspflichten aufgenommen werden sollten. Dabei könnten Risikokriterien mit hohen Zahlenwerten zum Gegenstand der Informationspflichten werden, was *de lege lata* nur aus einer Gesamtschau der Informationspflichten gemäß Art. 13 DSGVO abzuleiten ist, *de lege ferenda* wäre aber eine konkretisierte Informationpflicht über das spezifische Risiko wünschenswert.

Ebenso könnte die Einteilung gentechnischer Arbeiten in vier Sicherheitsstufen gemäß § 7 GentG für datenschutzrechtliche Risikokategorien herangezogen werden.[455] Dabei könnte für die Einteilung in die Sicherheitsstufen ein Rückgriff auf die Risikobewertung in ihrer Gesamtheit erfolgen. Die damit verbundenen Erkenntnisse könnten zum Gegenstand der Informationspflichten in den Sicherheitsstufen werden. Dies würde sich auf die Identitätsverwaltung positiv auswirken können, da das Bestehen von Sicherheits- und Risikostufen zu einer Übersichtlichkeit und gesteigerten Transparenz beitragen würde. Gleichwohl kann auch bei einer umfassenden Risikobewertung ein Risiko bestehen, welches unbekannt ist und damit in der Bewertung unberücksichtigt bliebe, sog. „*unknown unknown*“[456].

In einem Identitätsverwaltungsmodell sollte auch ein unbekanntes Risiko bei der umfangreichen Datenverarbeitung durch einen Intermediär als Plattformbetreiber über mehrere Kontexte hinweg einbezogen werden. Denn es können mehrere Identitäten in ihren *Ipse*- und *Idem*-Anteilen auf einer Plattform zu unterschiedlichen Zeitpunkten gespeichert werden und ein eigenes „*Ökosystem für personale Identitäten*“ bilden, welches erst im Laufe des Datenzyklus zu einem eigenen Risiko für die Rechte und Freiheiten natürlicher Personen führt. Dieses erweiterte Risiko über bislang unbekannte Risiken verlangt ein ausdifferenziertes Schutzregime, welches mit den Anonymisierungsmethoden umsetzbar ist. Dabei kann die Transparenz über den Schutz mit geeigneten Anonymisierungsmethoden zu einer so ausgeprägten Reputation des Plattformbetreibers führen, dass das Risiko eines Schadens für die Rechte und Freiheiten der natürlichen Person überschaubar bleibt. Weiter wäre die ausgeprägte Reputation über ein hohes Schutzniveau für personale Identitäten mit dem Geschäfsmodell unmittelbar verbunden, was zu umfassenden Schutzmaßnahmen durch den Verantwortlichen führen würde.

455 *Hoffmann-Riem*, in: Augsberg (Hrsg.), Ungewissheit als Chance, 2009, 17 (30).
456 *Spina*, EJRR 2014, 248.

Insgesamt müsse dennoch einer überzogenen Risikobewertung („*Riskifikation*“[457]) begegnet werden und die Unbekanntheit mancher Risiken anerkannt werden. Entsprechend ist neben der ausdrücklichen Einbeziehung des Risikos in die Informationspflichten gemäß Art. 13 DSGVO das Vorliegen von zertifizierten Verfahren (Art. 42 DSGVO) zur Risikobewertung wünschenswert und könnte zu einer wirksamen Risikoallokation beitragen.

3. Kontrolle durch Transparenz

Mit den Informationspflichten wird zu Beginn des Datenzyklus dem Betroffenen eine Kontrollmöglichkeit eingeräumt, da die Informationen als Entscheidungsgrundlage des Betroffenen für die Einwilligung dienen. Diese Kontrolle lässt sich mit dem Zugang zu den Informationen in der Datenschutzerklärung und der Entscheidungsmöglichkeit begründen, so dass es sich um eine absolute Kontrolle über die Entscheidung auf Grundlage der Informationspflichten handelt. Eine Steigerung der Kontrollmöglichkeit beim Betroffenen kann durch gestufte Datenschutzerklärungen erfolgen, indem bei geringen Änderungen des Kontextes die Informationspflichten iterativ und gestuft als Kaskade wahrnehmbar werden, sog. „*layered approach*“.[458] Damit können umfangreiche Informationspflichten über ein gestuftes Modell differenziert werden, so dass auf der ersten Stufe die abstrakten Informationen über die Datenverarbeitung erfolgen, auf der zweiten Stufe die kontextbezogene Konkretisierung der Informationen und auf der dritten Stufe die Beschreibung der kontextspezifisch maßgeblichen Informationen für den besonders interessierten Betroffenen. Damit würde ein dialogischer Austausch über die Informationen als ein Wechselspiel zwischen dem Betroffenen und Verantwortlichen entstehen.

Ein derartiges Konzept steht im Gleichlauf zu der in Art. 12 Abs. 1 DSGVO und im EWG 58 S. 1 DSGVO geforderten „leicht zugänglichen Form“, wonach der iterative Zugang zu den Informationen eine effiziente-

457 *Quelle*, European Journal of Risk Regulation 2018, 502 (517 f.).

458 Dessen Rechtmäßigkeit anzweifelnd, vgl. *Spindler*, in: Verhandlungen des 69. Deutschen Juristentages, 2012, S. F 78; *Art. 29 Data Protection Working Party*, WP 260, Leitlinien für Transparenz gemäß der Verordnung 2016/679 (11. April 2018), S. 17; Vorschlag einer Teil-Einwilligung von *Kremer*, CR 2012, 438 (446); www.ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/ (zuletzt aufgerufen 20.06.2020).

re Nachvollziehbarkeit und kontextspezifische Antizipation der Risikolage ermöglicht. Entsprechend gehöre es zu den Transparenzanforderungen, dass beim Besuch von *Facebook*-„*Fanpages*" auf den Zweck und die Art der verarbeiteten Daten hingewiesen wird, welches in der Verantwortlichkeit der Betreiber von „*Fanpages*" liege.[459] Damit räumt der EuGH eine gesteigerte Kontrollmöglichkeit durch die Erweiterung der Transparenzpflichten ein, die für die Betroffenen absolut wirkt und das Spektrum der Kontrolle über die personalen Identitäten erweitert.

Insgesamt wird sogar die Einbeziehung von ausdrücklichen Warnungen über den Schutz der Privatheit, vergleichbar mit den Warnungen über die Gefahren des Rauchens, vorgeschlagen, die in den kontextspezifischen iterativen Einwilligungsprozess einbezogen werden und als Bildgebote ihre Wirkung entfalten könnten.[460] Damit würde die Kontrolle für den Betroffenen durch eindeutige Informationen erleichtert werden. Ebenso könnten sog. „*sticky policies*" eingesetzt werden, die den verarbeiteten Datensätzen über den Datenzyklus hinweg anhaften und die Kontrolle über die zweckgebundene Datenverarbeitung mit maschinenlesbaren Verarbeitungsbedingungen ermöglichen.[461] Damit könne die garantierte Umsetzung der Datenverarbeitungsbedingungen aus den Datenschutzerklärungen umgesetzt werden.

Mit diesen technischen Unterstützungen können die Kontrollmöglichkeiten sichergestellt werden, ohne dass eine regelmäßige und bewusste Entscheidung des Betroffenen herbeigeführt werden muss. Folglich sind die Informationspflichten für den Betroffenen dazu geeignet, zu Beginn des Datenzyklus über die Risiken der Datenverarbeitung und der mit ihr verbundenen personalen Identitäten Kontrolle auszuüben.

4. Bewertung

Die Transparenz als Grundlage der Informationspflichten dient im Sinne einer „juristischen Glaskultur"[462] der Schaffung von Sichtbarkeit über Vorgänge, die nicht im Verantwortungsbereich des Betroffenen liegen. Viel-

459 EuGH, Urt. v. 05.06.2018 – Az.: C-210/16, Rn. 40, 44.
460 *Solove*, Harv. L. R. 2013, 1880 (1885); zu Bildgeboten und zum zwangsweise vor Augen führen von Risiken am Beispiel der Zigarettenschachteln, vgl. *Dreier*, Bild und Recht, 2019, S. 246.
461 *Pearson/Casassa-Mont*, Computer 2011, 60.
462 *Damler*, Rechtsästhetik, 2016, S. 303–305.

mehr sind zwischen Verantwortlichem und Betroffenen asymmetrische Informationslagen festzustellen, so dass die Informationspflichten zur Kompensation dieser beitragen können. Dazu gehört die Einbeziehung der Informationen aus der Risikobewertung in die Datenschutzerklärung. Denn in Kenntnis der konkreten mit der Datenverarbeitung verbundenen Risiken ist die umfassende Einschätzung möglich und kann die Grundlage für eine wirksame Identitätsverwaltung bilden.

Folglich kann sich der Bedarf nach einer fortgesetzten Informationspflicht im Rahmen von gestuften Datenschutzerklärungen als *„layered approach"* auch nach der Rechtmäßigkeit ergeben und würde in einem Identitätsverwaltungsmodell der Kontrollausübung dienen. Weiter wird aus dem Treu und Glauben-Grundsatz über die Datenverarbeitung gemäß Art. 5 Abs. 1 a) DSGVO eine Hinwendung zum Abbau bestehender Informationsasymmetrien durch Transparenz über die Datenverarbeitung und ihre Risiken angenommen.[463] Demnach wären gestufte Datenschutzerklärungen für ein Identitätsverwaltungsmodell nicht nur eine Anforderung aus den Informationspflichten gemäß Art. 12 ff. DSGVO, sondern auch aus dem Gebot der Verarbeitung nach Treu und Glauben gemäß Art. 5 Abs. 1 a) DSGVO abzuleiten und würden dem Ausgleich bestehender Informationsasymmetrien dienen.

Da Intransparenz zu Unsicherheit und Vermeidungsverhalten führen kann, wird eine eigene Informationspflicht über das Bestehen der Informationsasymmetrie und den mit ihr verbundenen Risiken befürwortet.[464] Danach sind die maßvollen Informationspflichten über die Datenverarbeitung und die Rechtsbeziehung zum Verantwortlichen eine Voraussetzung für das Identitätsverwaltungsmodell, wenn der Betroffene zu Beginn des Datenzyklus eine wirksame Kontrollmöglichkeit erhalten soll. Diese Kontrollmöglichkeit sollte jedoch beschränkt sein, um die Wirkungen des Kontroll-Paradoxons,[465] dass mit einer ausgeprägten Kontrollmöglichkeit eine höhere Offenlegungsbereitschaft besteht, einzudämmen. Entsprechend sollte der Umfang der Informationen maßvoll gestaltet werden und in inhaltlicher Hinsicht sollten aufklärende und zugleich warnende Informationen gewählt werden. Damit können die Informationen über den Datenzyklus und seine Risiken für die personale Identität langfristig zu einem gesteigerten Schutz der informationellen Selbstbestimmung beitragen.

---

463 *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 173.
464 *Di Fabio*, Grundrechtsgeltung in digitalen Systemen, 2016, S. 52.
465 3. Teil, C., IV.

III. Konkretisierte Datenschutzgrundsätze für die Identitätsverwaltung, Art. 5 Abs. 1 b) – f) DSGVO

Der Verantwortliche muss für die Erstellung der Datenschutzerklärung zunächst die Grundsätze der bevorstehenden Datenverarbeitung festgelegt haben. Insoweit ist eine umfassende Kenntnis über die inhaltliche und organisatorische Ausgestaltung der Datenverarbeitung mit der technischen Umsetzung vor der Erstellung einer Datenschutzerklärung notwendig, was die Risikobewertung einschließt. Dafür müssen die Grundsätze der Datenverarbeitung gemäß Art. 5 Abs. 1 b) – f) DSGVO mit den Anforderungen an die Identitätsverwaltung zusammengeführt und konkretisiert werden, um die Schutzmöglichkeiten für die personalen Identitäten aufzeigen zu können. Demnach wirken sich diese Anforderungen *ex ante* zur Rechtfertigung dahingehend aus, inwieweit aus der Perspektive des Betroffenen die Kontrolle über die personalen Identitäten im Rahmen der Zweckbindung gemäß Art. 5 Abs. 1 b) DSGVO ausgeübt werden kann (1.). Weiter muss bei der Datenverarbeitung der Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 c) DSGVO umgesetzt werden, so dass die Datenverarbeitungen und Erkenntnismöglichkeiten über personale Identitäten auf ein minimales Niveau zu beschränken oder sogar zu vermeiden sind (2.). Davon ist die Gewährleistung der Richtigkeit, Integrität und Vertraulichkeit der personenbezogenen Daten durch den Verantwortlichen erfasst, was eine wesentliche Anforderung zum Schutz der personalen Identitäten im Identitätsverwaltungsmodell darstellt und über die Datensicherheitsanforderung gemäß Art. 5 Abs. 1 d), f) DSGVO nachvollzogen werden soll (3.). Schließlich könnte mit einem „*identity management by design*"-Konzept als Ausprägung des Standes der Technik gemäß Art. 25 DSGVO (4.) die Identitätsverwaltung als ein eigenständiges „*privacy by design*"-Konzept ausgestaltet werden. Dieses würde als wirksamer Schutzmechanismus für die Identitätsverwaltung dienen und zum Gegenstand einer abschließenden Bewertung werden (5.).

1. Zweckgebundene Identitätsverwaltung, Art. 5 Abs. 1 b) DSGVO

Die Informationspflichten umfassen den Zweck der Datenverarbeitung, Art. 13 Abs. 1 c), Art. 5 Abs. 1 b), Art. 6 Abs. 4 DSGVO, EWG 50. Danach kann die Entscheidung des Betroffenen zur Einwilligungserteilung von den Informationen über den Zweck der Datenverarbeitung abhängig sein. Mit der Zweckbestimmung des Verantwortlichen lässt sich zudem die

Grundlage für eine „freiwillige Kooperation“[466] mit der natürlichen Person schaffen, indem der transparente Zweck die Aufmerksamkeit auf die Datenverarbeitung richtet und das Interesse an dem Dienst steigern kann. Gleichzeitig ist mit der Zweckfestlegung des Verantwortlichen das inhaltliche und zeitliche Spektrum der rechtmäßigen Datenverarbeitung festgelegt, so dass überflüssige Datenverarbeitungen identifiziert und ausgenommen werden müssen.[467] Dabei hat der Verantwortliche einen Einschätzungsspielraum über die Zweckfestlegung, der seine Grenze in der Rechtmäßigkeit des Zweckes finden würde, womit die Zweckfestlegung eine Selbstbindung des Verantwortlichen zur Einhaltung des Zwecks im Laufe des Datenzyklus auslöst. Dazu gehört das Gebot, dass die Datenverarbeitung befristet wird und nach der Zweckerreichung die Sperrung oder Löschung der Daten, wenn kein normativer Aufbewahrungsgrund besteht, vorgenommen wird, Art. 5 Abs. 1 e) DSGVO, EWG 39.[468] Damit findet das Verhältnismäßigkeitsprinzip eine einfachrechtliche Realisierung zum Schutz der informationellen Selbstbestimmung vor unvorhersehbaren Datenerhebungen und Datensammlungen in dem Zweckbindungsgrundsatz.[469]

Ebenso kommt innerhalb eines Datenzyklus des Betroffenen nach der DSGVO eine Änderung des Zweckes ohne erneute Rechtfertigung gemäß Art. 6 Abs. 1 DSGVO durch die verantwortliche Stelle in Betracht, wenn der neue Zweck mit dem ursprünglichen Zweck „vereinbar“ ist, Art. 6 Abs. 4 DSGVO, EWG 50 S. 6.[470] Die Bestimmung, wann der Zweck mit dem ursprünglichen Zweck vereinbar ist, unterliegt der rechtlichen Unsicherheit, wann zwischen beiden Zwecken ein „Zusammenhang“ angenommen werden kann und der neue Zweck von den „vernünftigen Erwartungen“ der betroffenen Person gedeckt wäre, Art. 6 Abs. 4 a)–e) DSGVO, EWG 50 S. 6. Somit besteht eine rechtliche Unsicherheit, mit welchen Datenverarbeitungen der Betroffene über die ursprüngliche Datenverarbeitung hinaus zu rechnen hat. Folglich ergibt sich aus der Zweckänderung ein konkretes Risiko für den Schutz der informationellen Selbstbestimmung, denn der ursprüngliche Umfang der Datenverarbeitung dient als Grundlage für die Erkenntniserlangung und kann unvorhersehbar zu Las-

466 *Grimm*, JZ 2013, 585 (588).
467 *Kühling/Klar/Sackmann*, Datenschutzrecht, 2018, Rn. 286, 338 f.
468 *Lehnert/Luther/Christoph u.a.*, Datenschutz mit SAP, 2018, S. 142–145; *Herbst*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 5 DSGVO Rn. 64–68.
469 BVerfGE 65, 1 (46, 63).
470 EWG 50 S. 1 und 2.

ten des Betroffenen erweitert werden. Dies läuft dem Gebot zuwider, dass mit der Zweckbindung als Minimalprinzip[471] die Datenverarbeitung eingegrenzt werden soll und als *Instruktion* für das mögliche Erkenntnisspektrum über eine personale Identität dient. Daher geht mit der Zweckfestlegung und der Zweckänderung das Risiko einher, dass der erweiterte Datensatz zu einer Erkenntniserweiterung über die personale Identität in unvorhersehbarem Maß für den Betroffenen führt.[472] Demnach wird in praktischer Hinsicht die regelmäßige Bereinigung des Datenzyklus auch für die Datenrichtigkeit als notwendiger Bestandteil der Zweckbindung angesehen.[473]

Die Zweckgebundenheit verlangt für die Identitätsverwaltung, dass eine verfahrensrechtliche Sicherung durch kanalisierte Datenverarbeitung zur Beschränkung der Erkenntnismöglichkeiten führt und damit die Risiken gegenüber den Rechten und Freiheiten natürlicher Personen minimiert werden. Mit der Zweckfestlegung durch den Verantwortlichen und der Information über den Zweck an den Betroffenen wird eine Kontrollmöglichkeit eingeräumt, die es dem Betroffenen ermöglicht, die Datenverarbeitung über die personale Identität einschätzen zu können. Gleichwohl erfährt die Einschätzungsmöglichkeit mit der Änderung des Zweckes gemäß Art. 6 Abs. 4 DSGVO eine Einschränkung, da es aus der Perspektive des Betroffenen keine erneute Kontrollmöglichkeit gibt, mit der die ursprüngliche Einschätzung korrigiert werden kann. In Anbetracht der fehlenden Möglichkeit für den Betroffenen bei der Zweckänderung durch eine erneute Einwilligung mitentscheiden zu können, kann eine Einbuße der Kontrolle des Betroffenen und damit des *Selbstdatenschutzes* angenommen werden. Daher bleibt für die Identitätsverwaltung die Transparenz des Zweckes über die Datenverarbeitung der maßgebliche Anknüpfungspunkt für die Kontrolle der personalen Identitäten und der Erkenntnismöglichkeiten über diese.

2. Datenminimierte Identitätsverwaltung, Art. 5 Abs. 1 c) DSGVO

Die Datenminimierung als Prämisse für die Identitätsverwaltung erwächst aus dem Vorsorgeprinzip und wird aus dem Verhältnismäßigkeitsgrundsatz abgeleitet. Danach wird bei der Datenverarbeitung das Gebot verfolgt,

471 *Lehnert/Luther/Christoph u.a.*, Datenschutz mit SAP, 2018, S. 254.
472 *Grafenstein*, DSRI 2016, 233 (240 f.).
473 *Lehnert/Luther/Christoph u.a.*, Datenschutz mit SAP, 2018, S. 125.

die Datenerhebung und Datenverarbeitung auf einem minimalen Niveau zu halten, wonach die Datenverarbeitung grundsätzlich vermieden und bei Erforderlichkeit eine schonende Form der Datenverarbeitung in Gestalt von frühzeitiger Löschung, Sperrung oder Pseudonymisierung gewählt werden soll.[474] Damit liegt ein Schutzregime gegenüber den möglichen Erkenntnissen über eine personale Identität vor, indem die Datenverarbeitung von Anfang an auf die wesentlichen personenbezogenen Daten beschränkt und die Vielfalt an Lernmöglichkeiten aus den Informationen eingedämmt wird. Der Grundsatz zur Datenminimierung stellt somit Anforderungen an die technischen und organisatorischen Maßnahmen für die Datenverarbeitung und ist nach neuer Rechtslage gemäß Art. 83 Abs. 5 a) DSGVO bußgeldbewährt, so dass ein wirksamer Anreizmechanismus zur Umsetzung für den Verantwortlichen geschaffen wurde, Art. 25 Abs. 1, 32 DSGVO, EWG 156.

Zu der Datenminimierung gehört die Pseudonymisierung der Daten, womit über die Kennung ein gesteigertes Schutzniveau eingeführt wird und die Zuordnungsregel allein bei der verantwortlichen Stelle liegt, Art. 4 Nr. 5 DSGVO.[475] Die Kennung ermöglicht den Zugang zu einer Teilidentität, so dass diese Ausprägung für die Identitätsverwaltung und die Steigerung des Schutzniveaus von Teilidentitäten eingesetzt werden kann. Demnach setzt die Datenminimierung voraus, dass die Datensätze pseudonymisiert, verschlüsselt oder anonymisiert werden sollten, um die Personenbeziehbarkeit zu mindern. Von der Datenminimierung erfasst ist die Anonymisierung der Datensätze, auch wenn anonyme Informationen aus dem sachlichen Anwendungsbereich der DSGVO ausgeschlossen sind, EWG 26 S. 5. Dies erklärt sich damit, dass der ausgeprägteste Schutz für die informationelle Selbstbestimmung mit der Anonymisierung erfolgt und die eindeutige Zuordnung zwischen anonymen und personenbezogenen Daten fließend erfolgt und einem Graubereich unterliegt. Damit ist die technisch-methodische Abgrenzung zwischen anonymen und personenbezogenen Daten als graduell einzuordnen.

Anonyme Daten sind gegeben, wenn die Verknüpfung zu einer natürlichen Person direkt oder in einer Kohorte faktisch aufgrund des hohen Aufwandes an Zeit, Kosten und Arbeitskraft ausgeschlossen ist, was in Übereinstimmung mit der vom Bundesverfassungsgericht geforderten ab-

474 *Herbst*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 5 DSGVO Rn. 57 f.

475 4. Teil, A., I., 3.

soluten und mathematischen Anonymität steht.[476] Indem mehrere Datenverarbeitungen zusammengefasst werden und als Daten einer Kohorte erscheinen, kann dies zu einer faktischen Anonymisierung führen, so dass Methoden mit der Zuordnung von Daten in Kohorten naheliegend für die Anonymisierung erscheinen. Dies kann mit den Anonymisierungsmethoden „*differential privacy*" und „*pufferfish framework*" erfolgen, die eine methodische Annäherung an die dauerhafte Unlesbarkeit und Unverfälschbarkeit von Daten ermöglichen. Nach dem Konzept der „*differential privacy*" werden die personenbezogenen Daten in einer Datenbank modifiziert und strukturiert, so dass die Authentizität gewährleistet wird, aber keine Rückschlüsse auf die natürliche Person möglich sind.[477] Diese Datenbanken sind mehrrelational und verfügen über Zufallsverteilungen der Datensätze, so dass für einen neugierigen Angreifer keine personenbezogenen Daten festzustellen sind.[478] Die Angriffsperspektive richtet sich dabei auf die verwendbaren Daten zur Erkenntniserlangung und die Möglichkeit der Re-Identifikation einer natürlichen Person. Dabei können etwa mit der Einordnung von Kohorten zu Gehältern die Durchschnittsgehälter gebildet werden, Erkenntnisse über die Gehaltsverteilung erlangt und Tendenzaussagen getroffen werden, ohne dass dabei die natürlichen Personen identifizierbar sind.[479] Gegenüber der Methode „*differential privacy*" geht „*pufferfish framework*" einen Schritt weiter, weil über einen Datensatz hinaus beliebige Paare von Datensätzen gebildet werden, so dass aufgrund dieser Datenpaare keine eindeutigen Erkenntnisse möglich sind und eine Intransparenz hergestellt wird.[480] Bei diesen Methoden geht es um das Risiko der Identifizierbarkeit und Erkenntniserlangung, welches mit den Me-

476 BVerfGE 65, 1 (16 f.); BVerfGE 27, 1; *Kühling/Klar/Sackmann*, Datenschutzrecht, 2018, Rn. 262 f.; *Unabhängiges Landeszentrum für Datenschutz* (ULD), Identity Management Systems (IMS), 2004, S. 37; *Pfitzmann*, Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management-A Consolidated Proposal for Terminology, 2006, S. 24.

477 *Spiecker gen. Döhmann/Tambou/Bernal u.a.*, EDPL 2016, 535 (539).

478 *Buchmann*, DuD 2015, 510 (514).

479 *Lehnert/Luther/Christoph u.a.*, Datenschutz mit SAP, 2018, S. 103; *Klar/Kühling*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 4 DSGVO Rn. 15 f.; *Gola*, in: Gola/Eichler/Franck u.a. (Hrsg.), Kommentar, Datenschutz-Grundverordnung, 2018, Art. 4 DSGVO Rn. 9. Etwa die Informationen über die Kohorte der Einwohner eines Stadtteils und das dort erreichte Wahlergebnis bestimmter Parteien. Die Rückschlüsse und inhaltlichen Aussagen über das Wahlverhalten hängen dann von dem Zusatzwissen und den Interpretationsregeln (*Instruktionen*) ab.

480 *Buchmann*, DuD 2015, 510 (513).

thoden „*differential privacy*“ und „*pufferfish framework*“ *quasi* ausgeschlossen wird. Damit ist die Anonymisierung von personenbezogenen Daten und personalen Identitäten in Kohorten in technischer Hinsicht möglich.[481]

Dem Grundsatz der Datenminimierung folgend, geht es nicht allein um die Verringerung des Umfangs der Datenverarbeitung, sondern auch um die Minimierung der Erkenntnismöglichkeiten, so dass die Anonymisierungsmethoden entscheidend für die Gewährleistung der Datenminimierung und des Identitätsschutzes sind. Mit der Datenminimierung werden Beschränkungen der Erkenntnisse ermöglicht und zugleich wird das Risiko für die Rechte und Freiheiten natürlicher Personen verringert. Dabei kann mit den Anonymisierungsmethoden der Eindruck erweckt werden, dass diese eine Garantie über den Schutz vor Erkenntnismöglichkeiten darstellen, wobei in Anbetracht ubiquitärer Datenverarbeitungen als *Big Data*-Phänomen lediglich eine Garantie über den Schutz vor Erkenntnismöglichkeiten für einen bestimmten Kontext ausgesprochen werden kann. Im Sinne eines umfassenden Schutzes vor Erkenntnissen im online-Kontext fungiert die Anonymisierung als Prämisse, kann aber zugleich nicht als Garant für den kontextübergreifenden Schutz vor Datenmacht und Informationsasymmetrien verstanden werden.[482] Insofern können Plattformen mit einem ausdifferenzierten Schutzmechanismus von Anonymisierungsmethoden ein *Ökosystem für personale Identitäten* bilden, in dem die *Ipse*- und *Idem*-Anteile aus verschiedenen Kontexten gespeichert und interoperabel ausgestaltet werden. Der Grundsatz der Datenminimierung kann darin den notwendigen Schutz vor Erkenntnismöglichkeiten bieten, die innerhalb des Ökosystems entstehen können und dem *Konzept des Selbstdatenschutzes* dienen würden.

Mit der Pseudonymisierung kann ein Schutz annähernd zu der Anonymisierung erreicht werden, wenn eine Kombination von mehreren Pseudonymen zu einer Erschwerung der Zuordnung zur natürlichen Person führt und die Erkenntnismöglichkeiten über personale Identitäten einschränkt. Indem es bei dem Identitätsverwaltungsmodell um den Schutz vor der Erkenntniserlangung in den Kontexten und bei Kontextüberschneidungen geht, liegt in den Methoden der Datenminimierung (Verschlüsselung, Pseudonymisierung, Anonymisierung) ein entsprechender

481 Die Möglichkeit der Anonymität innerhalb einer Gruppe wird bei drei oder fünf Personen angenommen, vgl. *Weichert*, DuD 2007, 17 (19).

482 *Becker*, JZ 2017, 170 (172); *Laue/Nink/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis, 2019, § 1 Rn. 20–22.

Schutzmechanismus. Folglich muss das Identitätsverwaltungsmodell an die Methoden der Datenminimierung und die *Instruktionen* anknüpfen, um das Risiko für die informationelle Selbstbestimmung antizipierbar zu machen und den Informations- und Wissensgehalt über eine personale Identität einzuschränken. Dabei könnte Bestandteil der Datenminimierung in einem Identitätsverwaltungsmodell sein, dass ein spezifischer Datensatz mehrfach in verschiedenen Kontexten verwendbar wird. Dies würde in einem Datenzyklus den kontextübergreifenden Einsatz von bestimmten *Idem*-Anteilen einer personalen Identität ermöglichen. Darin kommt das Spannungsverhältnis der Datenminimierung zum Ausdruck, wonach die Authentizität und Verfügbarkeit der Daten etwa über mehrfache Speicherung sichergestellt werden muss, was zum Bedarf an redundanten Datenverarbeitungsprozessen führt, zugleich aber im Wertungswiderspruch mit der Datenminimierung steht.

Demnach könnte die Speicherung mehrfach einsetzbarer Datensätze über die *Idem*-Anteile einer personalen Identität zu einer Umsetzung der Datenminimierung in ein Identitätsverwaltungsmodell führen, so dass die Verwaltung der personalen Teilidentitäten eine übergeordnete Maßnahme im Einklang mit der Datenminimierung sein kann. Insofern würde die Identitätsverwaltung dem kontextspezifischen Einsatz von Pseudonymisierungs- und Anonymisierungsmethoden übergeordnet sein und als Maßnahme der „Meta-Datenminimierung" fungieren können. Damit würde die Identitätsverwaltung eine Kontrollmöglichkeit mit Hilfe der Methoden zur Datenminimierung schaffen und die Beschränkung der Erkenntnismöglichkeiten fördern. Daher lassen sich der Grundsatz der Transparenz und die Datenminimierung als Mittel der Kontrolle in der Identitätsverwaltung einsetzen, so dass eine kontextspezifische Realisierung der Datenminimierung von der natürlichen Person kontrolliert werden kann. Darin liegt ein wesentlicher Bestandteil des *Selbstdatenschutzes*, da die Vorzüge des Grundsatzes der Datenminmierung gerade in der Pseudonymisierung bei der kontextübergreifenden Identitätsverwaltung zum Ausdruck kämen.[483]

483 *Roßnagel*, in: Roßnagel/Abel (Hrsg.), Handbuch Datenschutzrecht, 2003, 3.4. Rn. 56.

3. Datensicherheit in der Identitätsverwaltung, Art. 5 Abs. 1 d), f), Art. 32 DSGVO

Die Voraussetzung für die Identitätsverwaltung ist ein Modell, in dem die Verwaltung der personalen Teilidentitäten unter den Vorgaben der Datensicherheit erfolgt, wobei die Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit der Daten und der personalen Identität gewährleistet werden müssen. Bei einem Verstoß besteht nach Art. 33 DSGVO die Meldepflicht der verantwortlichen Stelle innerhalb von 72 Stunden, so dass auch mit der Bußgeldbewährtheit gemäß Art. 83 Abs. 5 a) DSGVO ein effektiver Schutzmechanismus besteht. Zudem unterliegt die Realisierung der Datensicherheit dem risikobasierten Ansatz nach Art. 32 Abs. 1 DSGVO, wonach sich die angemessene Maßnahme zur Datensicherung nach der Eintrittswahrscheinlichkeit eines Schadens und dem Maßnahmenkatalog aus Art. 32 Abs. 1 a) – d) DSGVO richtet. Demnach bedarf es einer Kalibrierung der Datensicherheitsmaßnahme spiegelbildlich zur Risikobewertung, die sich in dem Stand der Technik und den technischen und organisatorischen Maßnahmen abbildet.

Zu den funktionalen Anforderungen an ein Identitätsverwaltungsmodell gehören die Richtigkeit, die Speicherbegrenzung, die Integrität und die Vertraulichkeit der Daten sowie die Belastbarkeit des technischen Systems, womit die Widerstandsfähigkeit und Ausgleichsfähigkeit eines Systems gegenüber Störungen umfasst ist, sog. Resilienz gemäß Art. 32 Abs. 1 b) DSGVO.[484] Weiter ist die Gewährleistung der Richtigkeit der personenbezogenen Daten gemäß Art. 5 Abs. 1 d) DSGVO maßgeblich für die Datensicherheit der personalen Identitäten. Die Richtigket der Daten sieht die sachliche Richtigkeit als objektives Kriterium vor, so dass eine enge Verbindung von der inhaltlichen Richtigkeit der Daten zu dem Zweck der Datenverarbeitung besteht.[485] Denn würde der Zweck der Datenverarbeitung in der Identifizierung der natürlichen Person liegen, wäre die Speicherung eines fiktiven Namens als Pseudonym unrichtig.

Weiter erfordert die sachliche Richtigkeit der Daten auch die Gewährleistung der Nicht-Verkettbarkeit von Datensätzen, damit die objektive Richtigkeit separater Datensätze nicht durch die kontextübergreifende Verbindung gefährdet wird. Dabei ist zwischen absoluter und relativer

484 *Gonscherowski/Hansen/Rost*, DuD 2018, 442 (446); *Jandt*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 32 DSGVO Rn. 26, Fn. 55, 56.

485 *Herbst*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 5 DSGVO Rn. 60–62.

Nicht-Verkettbarkeit zu unterscheiden. Die absolute Nicht-Verkettbarkeit gewährleistet, dass keinerlei Verbindung zwischen den jeweiligen Datensätzen hergestellt werden darf und die relative Nicht-Verkettbarkeit verlangt, dass sich der Informationsgehalt durch die Verbindung der Datensätze nicht verändert.[486] Diese Differenzierung ist für ein Identitätsverwaltungsmodell entscheidend, da mit der Datensicherheit die Anforderung erfasst ist, dass neben der kontextübergreifenden Verbindung von Datensätzen keine kontextübergreifenden Erkenntnisse generierbar sein dürfen. Damit stellt der Grundsatz der Datensicherheit die kontextspezifische Trennung der Datensätze zu den personalen Teilidentitäten sicher und gewährleistet, dass keine kontextübergreifende Erkenntniserlangung erfolgt.

Weiter umfasst die Datensicherheit den Schutz vor unbefugtem Zugang und den Schutz der Daten vor Zerstörung und Verlust, was den technischen und organisatorischen Maßnahmen aus der Anlage des § 9 BDSG a. F. entspricht.[487] Danach verlangt die Datensicherheit die dynamische Sicherstellung von Zutritts-, Zugangs- und Zugriffskontrolle und etwa der Weitergabekontrolle durch den Verantwortlichen. Aus der Zugangskontrolle lässt sich die Identitätsverwaltung unmittelbar ableiten, so dass verhältnismäßige technische und organisatorische Maßnahmen hierzu getroffen werden sollten. Sobald eine physische Zugangskontrolle etwa über das Wissen eines Passwortes oder den Besitz eines Schlüssels implementiert wurde, muss sichergestellt werden, dass diese Einrichtung über den Datenzyklus hinweg die Datensicherheit gewährleistet. Hier kommen Software-Lösungen in Betracht, die aus regelmäßigen Aktualisierungen und Fehlerbehebungen bestehen.[488] Für die Gewährleistung der Datensicherheit eines Datenzyklus bei der Identitätsverwaltung bedarf es demnach der regelmäßigen Sicherstellung, dass mit dem Stand der Technik und den technischen und organisatorischen Maßnahmen die aktuellen Risiken der Datenverarbeitung einbezogen werden.

---

486 *Unabhängiges Landeszentrum für Datenschutz* (ULD), Identity Management Systems (IMS), 2004, S. 8.

487 *Herbst*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 5 DSGVO Rn. 74–76.

488 *Faber/Sedlacek*, DuD 2017, 440 (443). Indem sich das Problem bei Softwareschwachstellen manifestieren und perpetuieren kann, soll vergleichbar mit einem Sicherheitssystem in Zügen (Lockführer betätigt Knopf alle dreißig Sekunden, damit er wach bleibt) auch bei Software in bestimmten Sicherheitsstufen integriert werden, sogenanntes „Life – Sign – Controll" mit dem nur regelmäßig gepflegte Geräte am Netz bleiben sollen, „Mindesthaltbarkeit".

Für die Gewährleistung der kontextspezifischen Datensicherheit von Teilidentitäten kommen solche technischen Lösungen in Betracht, mit denen die personalen Teilidentitäten aktiviert und deaktiviert werden oder personale Teilidentitäten in Übereinstimmung mit der Zweckerreichung einer Mindesthaltbarkeit[489] unterliegen können. Darin liegen geeignete Maßnahmen für die Datensicherheit in einem Identitätsverwaltungsmodell, die von dem Verantwortlichen zunächst vor der Datenverarbeitung und nach Beginn der Datenverarbeitung im Rahmen der Sicherstellungspflichten umgesetzt werden müssten.

4. Identitätsverwaltung durch Technikgestaltung, Art. 25 DSGVO

Die Identitätsverwaltung kann Gegenstand der Technikgestaltung sein und über die Berücksichtigung des Standes der Technik gemäß Art. 25 DSGVO bestimmt werden. Es kommt neben der datenschutzkonformen Technikgestaltung der Identitätsverwaltung als „*privacy by design*" und „*privacy by default*", EWG 78 S. 2, die Konkretisierung als „*identity management by design*" in Betracht, so dass der Feststellungsvorgang über den geeigneten Stand der Technik untersucht werden soll. Gemäß Art. 25 Abs. 1 DSGVO soll durch den Verantwortlichen der Stand der Technik „berücksichtigt" werden. Der Stand der Technik wird nach der Drei Stufen-Theorie oberhalb der ersten Stufe über die allgemein anerkannten Regeln der Technik und unterhalb der dritten Stufe, dem Stand von Wissenschaft und Technik, eingeordnet.[490] Der Stand der Technik gilt in diesem Gefüge als ein unbestimmter Rechtsbegriff mit Verweisungsgehalt, wodurch der Einbeziehungsbedarf des aktuellen technischen Entwicklungsstands mit dem im Markt verfügbaren Fortschritt sichergestellt wird.[491] Damit soll über diesen unbestimmten Rechtsbegriff die Front der technischen Entwicklungen durch den Verantwortlichen angewendet und eine justiziable Lösung aus dem Spannungsverhältnis zwischen Recht und Technik ermöglicht werden.[492] Die Bestimmung der konkreten technischen Maßnahme richtet sich nach dem Öffnungsprädikat der „Berücksichtigung" des Standes der

489 *Dies.*, DuD 2017, 440 (444 f.).
490 BVerfG, NJW 1979, 359 – Kalkar-Entscheidung.
491 *Breuer*, AöR 101 (1976), 46 (50); *Seibel*, NJW 2013, 3000; *Bartels/Backer*, DuD 2018, 214 f.
492 BVerfG, NJW 1979, 359 (362) – Kalkar-Entscheidung; *Breuer*, AöR 101 (1976), 46 (68).

Technik und erlaubt die Einbeziehung subjektiver Fähigkeiten der verantwortlichen Stelle, etwa das technisch Mögliche und wirtschaftlich Zumutbare.[493]

Für die Bestimmung der potentiellen technischen Maßnahmen zur Realisierung der Identitätsverwaltung ist die Bildung eines Maßnahmenbündels für die abschließende Identifizierung der Bestleistung notwendig.[494] Der Festlegungsvorgang aus dem Maßnahmenbündel unterliegt einer iterativen individuellen Machbarkeits- und Verhältnismäßigkeitsprüfung und entspricht einer eigenständigen Risikobewertung, da es bei dem jeweiligen Stand der Technik um die Bewertung der Eintrittswahrscheinlichkeit eines potentiellen Schadens nach dem EWG 85 S. 1 geht.[495] Hierbei werden prognostische Elemente einbezogen, wenn die Datenschutzrisiken aus der technischen Gestaltung der Datenverarbeitung, der Zweck der Datenverarbeitung und die Kategorien personenbezogener Daten miteinander in Einklang zu bringen sind, EWG 83 S. 3.

Aus dem Öffnungsprädikat der Berücksichtigung kommt der prozedurale Charakter zum Ausdruck, wonach es sich um einen dynamischen Prozess zur Bestimmung des geeigneten Standes der Technik handelt.[496] Aufgrund der Bestimmung des Standes der Technik durch den Verantwortlichen aus seiner subjektiven Perspektive kann dies zu Divergenzen des Schutzniveaus innerhalb einer Produktgruppe führen, da jeder Verantwortliche über andere subjektive Kriterien verfügt, mit denen eine Maßnahme aus dem Maßnahmenbündel bestimmbar wird.[497] Zwar kann sich dies aus Gründen des Wettbewerbs positiv auf das Marktverhalten der Ver-

493 *Baumgartner*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2018, Art. 25 DSGVO Rn. 15; *Seibel*, NJW 2013, 3000 (3003); zum Öffnungsprädikat *Raabe/Schallbruch/Steinbrück*, CR 2018, 706 (708): Im Gegensatz zu dem Öffnungsprädikat der „Berücksichtigung" müssen gemäß §§ 30a Abs. 2, 36 Abs. 5 Nr. 2 StVG Maßnahmen nach dem Stand der Technik „getroffen" werden, in §§ 71 Abs. 1 S. 2, 64 Abs. 1 S. 1, 22 Abs. 2 S. 2 BDSG soll die „Berücksichtigung gewährleistet" werden, in § 18 Abs. 2 De-Mail-G soll der Stand der Technik „erfüllt" werden und in § 8a Abs. 1 S. 2 BSIG soll der Stand der Technik „eingehalten" werden. In diesen mit dem Stand der Technik verbundenen Prädikaten kann ein „mehr" oder „weniger" an Prüfungsintensität enthalten sein.

494 *Knopp*, DuD 2017, 663 (664); *Teletrust*, Handreichung zum „Stand der Technik", 2018, S. 8.

495 *Martini*, in: Paal/Pauly/Ernst (Hrsg.), Kommentar, DS-GVO, 2018, Art. 24 DSGVO Rn. 41 f.; *Bartels/Backer*, DuD 2018, 214 (216).

496 *Martini*, in: Paal/Pauly/Ernst (Hrsg.), Kommentar, DS-GVO, 2018, Art. 24 DSGVO Rn. 41–43; *Jandt*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 32 DSGVO Rn. 9.

497 *Schallbruch*, CR 2016, 663 (668 f.).

antwortlichen auswirken, jedoch liegt darin das Risiko eines eingesetzten Standes der Technik, der sich für das Schutzniveau des Betroffenen als Verbraucher nachteilig auswirkt. Ferner kann die Reputation des Verantwortlichen mit dem eingesetzten Stand der Technik erweitert werden, um im Wettbewerb über ein hohes Privatheitsniveau chancenreich zu sein. Folglich kommt dem Stand der Technik in Verbindung mit dem Öffnungsprädikat eine prinzipielle Funktion zu, indem bereichsübergreifend ein prozedurales Schema zur justiziablen Technikbestimmung angewendet wird.[498]

Sobald die geeignete technische Maßnahme zur Realisierung eines „*identity management by design*" identifiziert werden konnte, kann dies zu einer Schutzsteigerung der informationellen Selbstbestimmung führen. Wobei als Voraussetzung dafür gewährleistet sein müsste, dass den kontextabhängigen technischen Präferenzen der natürlichen Person Rechnung getragen und eine Kontrollmöglichkeit über den „*digitalen Hausrat*"[499] eingeräumt wird. Dies müsste mit entsprechenden Investitionen in die technische Gestaltung erfolgen, denn ohne ein differenziertes „*privacy by design*" wird in der Technik eine neue Risikoquelle gesetzt. Dabei sind neben den Verantwortlichen faktisch eher die Hersteller gefragt, die gemäß EWG 78 S. 4 zur Berücksichtigung des Standes der Technik bei der Produktentwicklung „ermutigt" werden sollen. Nicht selten werden Hersteller und Verantwortlicher in Personalunion auftreten, so dass *de lege ferenda* die Haftung des Herstellers wegen eines fehlerhaften Produktes nach § 3 ProdHG bei Nichteinhaltung der „*privacy enhancing technology*"-Vorgabe denkbar wäre. Dies würde ein übergeordnetes Prinzip „*privacy by design*" voraussetzen, welches die Schutzgegenstände des ProdHG mit dem Schutz der persönlichen Informationen in § 1 ProdHG erweitern könnte. Damit könnte auch ein Anreiz zur Herstellung datenerhebungsfreier Produkte, die etwa mit einem Heimlichkeitsmodus „*Stealth Modus*" versehen werden könnten, geschaffen werden.[500]

5. Zusammenfassung

Insgesamt richtet sich die inhaltliche und organisatorische Ausgestaltung der Identitätsverwaltung nach den Datenschutzgrundsätzen aus Art. 5 Abs. 1 b) – f) DSGVO. Demnach wurden die Grundsätze der Datenverar-

498 *Raabe/Schallbruch/Steinbrück*, CR 2018, 706 (714).
499 *Schallbruch*, Schwacher Staat im Netz, 2018, S. 25 ff.
500 *Becker*, JZ 2017, 170 (178); *Schallbruch*, CR 2016, 663 (669).

beitung für die Identitätsverwaltung konkretisiert. Dafür wurden die Zweckfestlegung, Datenminimierung, Datensicherheit und entsprechende Technikgestaltung hinsichtlich der Identitätsverwaltung untersucht. Dabei stellt die Zweckfestlegung einen zentralen Grundsatz dar, weil mit ihm die Dauer und der Umfang der Datenverarbeitung und die Erkenntnismöglichkeiten über die personalen Identitäten beschränkt werden. Demgegenüber sieht Art. 6 Abs. 4 DSGVO die Möglichkeit vor, im Laufe des Datenzyklus den Zweck zu ändern, was eine besondere Aufgabe an ein Identitätsverwaltungsmodell darstellt. Denn mit der Zweckänderung wird ein weiteres Risiko über die Erkenntnismöglichkeiten geschaffen, welches nicht mit der vorangegangenen Kontrollmöglichkeit des Betroffenen über den ersten Zweck der Datenverarbeitung übereinstimmt.

Weiter kann der Verantwortliche über den Grundsatz der Datenminimierung die Identitätsverwaltung gestalten, indem umfassende Pseudonymisierungsmethoden eingesetzt werden und gegebenenfalls über die Anonymisierungsmethoden Datensätze zu personalen Teilidentitäten aus dem Anwendungsbereich der DSGVO ausgenommen werden können. Dazu gehört, dass ein Identitätsverwaltungsmodell die Nicht-Verkettbarkeit der Datensätze gewährleisten muss, wonach der Informationsgehalt durch Verknüpfung von Daten unverändert bleiben soll. Demnach kommt eine Infrastruktur in Betracht, nach der die kontextübergreifende Verbindung von Datensätzen und personalen Identitäten in Gestalt einer Mehrfachverwendung ermöglicht wird. Entsprechend kann ein Plattformbetreiber für die Identitätsverwaltung ein Ökosystem (sog. „*Identity Ecosystem*“) begründen, welches die rechtlichen Anforderungen gerade in technischer Hinsicht umfassend umsetzt und eine Reputation über den Schutz personaler Identitäten im Markt erlangt. Folglich ist die Technikgestaltung durch den Verantwortlichen für die Realisierung der Identitätsverwaltung eine entscheidende Grundlage, zumal auf diesem Weg die Datensicherheit gewährleistet wird.

Für diese bedarf es der Sicherstellung kontextbeschränkter Datenverarbeitungsvorgänge und der Sicherheit über die Datensätze selbst. Demnach kann mit dem Stand der Technik ein Konzept begründet werden, welches einer eigenständigen technischen Gestaltung als „*identity management by design*“ unterliegen könnte. Damit würden neben dem Schutz der informationellen Selbstbestimmung die technische Anforderung des Standes der Technik gewährleistet werden. Der Betroffene wird demnach dazu befähigt, die personalen Identitäten mit einer angepassten Technologie kontrollieren zu können. Ein solches Konzept des „*identity management by design*“ müsste primär durch den Verantwortlichen umgesetzt werden,

gleichwohl erscheint die Realisierung durch den Hersteller ebenso naheliegend und wünschenswert. Dahingehend könnte *de lege ferenda* das Regelungsregime im Produkthaftungsrecht um den Schutz der informationellen Selbstbestimmung bei der Produktherstellung erweitert werden.

IV. Ergebnis

Die Identitätsverwaltung setzt bei den personenbezogenen Daten an und verlangt eine informierte Entscheidung über die Verwaltung personaler Identitäten. Demnach ist *ex ante* zur Rechtfertigung der Datenverarbeitung zu bestimmen, wann personenbezogene Daten vorliegen und wann der sachliche Anwendungsbereich der DSGVO eröffnet ist. Dabei befindet sich die Differenzierung in einer rechtlichen und tatsächlichen Grauzone, so dass in Anbetracht ubiquitärer Datenverarbeitungen innerhalb eines Datenzyklus die Identifizierungswahrscheinlichkeit hoch ist und der Theorienstreit über die Identifizierbarkeit an Bedeutung verliert.

Weiter kann mit den verarbeiteten personenbezogenen Daten das Risiko von Erkenntnissen einhergehen, so dass es gegenüber der natürlichen Person um die Transparenz über die mit der Verarbeitung verbundenen Erkenntnisrisiken geht. Diese transparent mitgeteilten Risiken sind das Ergebnis einer Risikobewertung durch den Verantwortlichen, wobei die Frage nach der geeigneten Methodik zur Risikobewertung noch offen ist, aber nach den bisherigen Untersuchungen in einer semiquantitativen Methodik liegen sollte. Folglich bedarf es über die Informationspflichten nach Art. 12, 13 DSGVO hinaus der Benennung von Risiken, damit die natürliche Person risikobewusste Entscheidungen bei der Verwaltung der personalen Identitäten treffen kann. Davon umfasst sind das Risiko der Identifizierung und das Risiko von Erkenntnissen über die natürliche Person. Bereits auf der zeitlichen Ebene vor Beginn des Datenzyklus und der Rechtfertigung erlangt die natürliche Person somit eine Kontrollmöglichkeit mit den Informationen über die Datenverarbeitung. Diese Kontrolle kann sogar als absolute Kontrolle eingeordnet werden, da diese sich in dem Lesen der Datenschutzerklärung und dem damit verbundenen Prozess der Entscheidungsfindung abbildet. Somit schließt die Identitätsverwaltung an die Transparenz der Verarbeitung personenbezogener Daten an.

Für die inhaltliche und organisatorische Ausgestaltung der Identitätsverwaltung muss der Verantwortliche die Grundsätze der Datenverarbeitung gemäß Art. 5 b) – f) DSGVO und den Stand der Technik gemäß Art. 25 DSGVO einbeziehen. Dabei dient die Zweckbindung der Beschränkung

der Datenverarbeitung und der damit verbundenen Erkenntnismöglichkeiten im Rahmen der *Instruktionen* durch den vorher festgelegten Zweck. Damit besteht eine Kontrollmöglichkeit über die Kenntnis des Zwecks, die aber mit einer späteren Zweckänderung aufgelöst werden kann. Weiter besteht nach dem Grundsatz der Datenminimierung mit den Pseudonymisierungs- und Anonymisierungsmethoden ein Schutzmechanismus gegenüber Erkenntnismöglichkeiten über personale Identitäten. Dieser Schutzmechanismus kann in einem Identitätsverwaltungsmodell dahingehend erweitert werden, dass Datensätze über personale Identitäten in einer interoperablen Struktur mehrfach verwendbar werden, sog. „*Identity Ecosystem*". Dies könnte mit einer spezifischen Konkretisierung des Standes der Technik über die Anforderung eines „*identity management by design*" umgesetzt werden.

C. *Rechtfertigung der personalen Identität, Art. 6 DSGVO*

Die Identitätsverwaltung bedarf der Kontrolle von personalen Teilidentitäten durch die natürliche Person, was die Rechtmäßigkeit der Datenverarbeitung zu den personalen Teilidentitäten voraussetzt. Das datenschutzrechtliche Verbot mit Erlaubnisvorbehalt steht dem zunächst entgegen, so dass die Identitätsverwaltung das Vorliegen eines Erlaubnistatbestandes gemäß Art. 6, 5 Abs. 1 a) DSGVO voraussetzt. Basierend auf dem Phänomen ubiquitärer Datenverarbeitungen und den sich daraus ergebenden personalen Teilidentitäten, soll die Identitätsverwaltung unter dem Erlaubnisvorbehalt (I.) untersucht werden. Dabei wird die schwerpunktmäßige Kontrollmöglichkeit über die Identitätsverwaltung bei der Einwilligung (II.) liegen, so dass diese differenziert betrachtet werden soll. Denn der Einwilligung kommt eine weichenstellende Funktion zu, da mit ihr der Datenzyklus beginnt. Von der Einwilligung geht eine Serie von Erkenntnismöglichkeiten über eine personale Identität aus, die zum Gegenstand der Risikoentscheidung des Betroffenen gehören sollten.

Weiter soll die Rechtfertigung allein durch den Verantwortlichen ohne das Zutun des Betroffenen gemäß Art. 6 Abs. 1 b) – f) DSGVO der rechtfertigenden Einwilligung gegenübergestellt werden (III.) und mit einem zusammenfassenden Ausblick (IV.) auf die Identitätsverwaltung *ex post* zur Rechtfertigung abgeschlossen werden.

I. Identitätsverwaltung unter Erlaubnisvorbehalt

Die Identitätsverwaltung wurde in dem bisherigen Gang der Untersuchung als grundsätzlich umsetzbar angenommen und dem Regelungsgefüge des IKT-Rechts zugeordnet. Gleichwohl gilt im Datenschutzrecht das Verbotsprinzip mit Erlaubnisvorbehalt, welches gegen die grundsätzliche Umsetzbarkeit der Identitätsverwaltung sprechen könnte. Das Verbotsprinzip wird als „Fundamentalprinzip“[501] des Datenschutzrechts angesehen und aus dem grundrechtlichen Schutz personenbezogener Daten abgeleitet, Art. 8 Abs. 2 S. 1 GRC. Danach wird zunächst keine Differenzierung vorgenommen, ob die Datenverarbeitung im öffentlich-rechtlichen oder privatrechtlichen Kontext erfolgt. In der Anwendung der Rechtfertigungsgründe wird im öffentlich-rechtlichen Kontext das öffentliche Interesse (Art. 6 Abs. 1 e) DSGVO) maßgeblich sein. Demgegenüber werden im privatrechtlichen Kontext die Einwilligung (Art. 6 Abs. 1 a) DSGVO), das berechtigte Interesse (Art. 6 Abs. 1 f) DSGVO) und die Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 c) DSGVO) durch den Verantwortlichen als Rechtfertigungsgrundlage herangezogen, wobei die Rechtfertigung aufgrund einer rechtlichen Verpflichtung ebenso im öffentlich-rechtlichen Kontext in Betracht kommt.

Im privatrechtlichen Kontext kann jedoch durch das Verbotsprinzip ein „überschießender Schutz“[502] entstehen, da jede Datenverarbeitung mit einer Einwilligung oder dem berechtigten Interesse gerechtfertigt werden müsse und dies nach der tatsächlichen Risikolage unverhältnismäßig sei. Demnach ist die Identitätsverwaltung allein in denjenigen Kontexten realisierbar, in denen eine aktive Handlung zur Rechtfertigung und *ex post* zur Rechtfertigung vorgenommen werden kann. Gleichzeitig umfasst die Identitätsverwaltung die Bewertung des mit der Datenverarbeitung verbundenen Risikos der Identifizierbarkeit und der Erkenntnismöglichkeiten, so dass sich auch auf der Ebene der Rechtfertigung die Frage nach dem Wirkungsgrad des risikobasierten Ansatzes stellt. Indem die Entscheidung über die Begründung der Rechtfertigungsgrundlage durch den Verantwortlichen erfolgt, muss dieser auch die kontextspezifische Risikobewertung über die Datenverarbeitung vornehmen, so dass der risikobasierte Ansatz auch auf der Rechtfertigungsebene seine Wirkung entfaltet.

---

501 *Spiecker gen. Döhmann*, in: Vesting (Hrsg.), Der Eigenwert des Verfassungsrechts, 2011, 263 (271).

502 *Lewinski*, Die Matrix des Datenschutzes, 2014, S. 84.

Im Rahmen der Bestimmung des Rechtfertigungsgrundes für den Datenverarbeitungsprozess werden der verfolgte Zweck und die Risiken der Datenverarbeitung gegenübergestellt. Dabei geht es im privatrechtlichen Kontext um den Rechtfertigungsgrund der Einwilligung und dem berechtigten Interesse. In diesem Vorgang kann ein Paradigmenwechsel gesehen werden, der sich von einem „rigiden Verbotsprinzip“[503] abwendet und dem risikobasierten Ansatz zuwendet, damit sich die prohibitive Wirkung des Verbotsvorbehalts in der Bestimmung des Rechtfertigungsgrundes verwirkliche. Darin kann eine Prozeduralisierung des Verbotsprinzips in Gestalt einer risikobasierten Bewertung gesehen werden, worin die datenschutzrechtlichen Regelungen ihre Vereinigung im Vorgang der Maßnahmen- und Rechtfertigungsbestimmung fänden.[504] Dieser prozedurale Anteil des Verbotsprinzips soll als ein wesentlicher Bestandteil für das Identitätsverwaltungsmodell herangezogen werden, um den Schwerpunkt auf die prozedurale Dimension der Identitätsverwaltung zu setzen und den dynamischen *Ipse*-Anteil personaler Identitäten zu gewährleisten.

Mit der Geltung des Verbotsprinzips für den privatrechtlichen Kontext werde zudem das strukturelle Ungleichgewicht zwischen dem Betroffenen und dem Verantwortlichen nicht ausgeglichen, sondern vielmehr werde die bestehende Marktmacht des Verantwortlichen zementiert.[505] Entsprechend schlägt *Masing* für die Datenverarbeitung im privatrechtlichen Kontext die Umkehr des Verbotsvorbehalts in die Begründung von Ausgestaltungsspielräumen vor.[506] Folglich erscheint der Gleichlauf des grundrechtlichen Schutzumfangs mit dem Verbotsvorbehalt für den privatrechtlichen und öffentlich-rechtlichen Kontext in Anbetracht des geringeren Schutzumfanges über die mittelbare Drittwirkung der Grundrechte als fragwürdig. Demnach ist die risikobasierte Rechtfertigung im privatrechtlichen Kontext als konsequente Anpassung an die grundrechtliche Differenzierung zwischen der Abwehrdimension gegenüber dem Staat und der mittelbaren Drittwirkung anzusehen. Mit einer Abkehr vom rigiden Verbots-

503 *Quelle*, European Journal of Risk Regulation 2018, 502 (517); *Veil*, ZD 2015, 347.

504 *Dies.*, European Journal of Risk Regulation 2018, 502 (521 f.).

505 *Lewinski*, Die Matrix des Datenschutzes, 2014, S. 85; *Roßnagel*, NJW 2019, 1 (5); *DeHert/Gutwirth*, in: Claes/Gutwirth/Duff (Hrsg.), Privacy and the criminal law, 2006, 61 (77 f.)

506 *Masing*, NJW 2012, 2305 (2307 f.); *Buchner/Petri*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 6 DSGVO Rn. 14; zur kritischen Betrachtung der Legitimationswirkung, *Kühling/Klar/Sackmann*, Datenschutzrecht, 2018, Rn. 495.

prinzip kann auch dem Eindruck begegnet werden, dass mit der rechtfertigenden Einwilligung im privatrechtlichen Kontext eine Kontrollmöglichkeit über die *Ipse-* und *Idem-*Anteile einer personalen Identität besteht. Damit ist eine risikobasierte Öffnung für Gestaltungsspielräume zur Identitätsverwaltung denkbar, in der der Schutz vor Erkenntnismöglichkeiten einbezogen wird. Demnach ist im privatrechtlichen Kontext eine Abkehr von einem rigiden Verbotsprinzip und eine Hinwendung zu einer differenzierten Ausgestaltung der Kontrollmöglichkeiten des Betroffenen im Datenzyklus wünschenswert und kann mit der Identitätsverwaltung erfolgen.

Für die Identitätsverwaltung unter dem Erlaubnisvorbehalt erstreckt sich das Schutzkonzept auf die Verwaltung der Risiken aus den Datenverarbeitungen. Dabei ist für den privatrechtlichen Kontext der Rechtfertigungsgrund der Einwilligung hervorzuheben. Mit ihm gehen das Konzept der Kontrolle über die (risiko-) bewusste Entscheidung zur Einwilligung in die Datenverarbeitung und das Risiko von Erkenntnissen über personale Identitäten einher. Weiter kann in der Einwilligung der Schlüssel zur Identitätsverwaltung gesehen werden, mit dem die personalen Identitäten zu Beginn des Datenzyklus begründet werden und sich im Verlauf des Datenzyklus vielfältige Erkenntnismöglichkeiten ergeben. Gleichwohl wird im privatrechtlichen Kontext die Rechtfertigung mit dem berechtigten Interesse erfolgen können, so dass auch ohne aktive Handlung der Datenzyklus von personalen Identitäten ausgelöst werden kann und eine Kontrollmöglichkeit erst *ex post* zur Rechtfertigung besteht.

II. Identitätsverwaltung durch Einwilligung, Art. 6 Abs. 1 a), 7 DSGVO

Die Entscheidung zur Einwilligungserteilung mit der Folge, dass personale Teilidentitäten in ihren *Idem-* und *Ipse-*Anteilen begründet und verwendet werden, stellt einen zentralen Bestandteil der Identitätsverwaltung und des Selbstdatenschutzes dar. Die Einwilligung unterliegt primärrechtlichem Schutz gemäß Art. 8 Abs. 2 S. 1 GRC und ist zentral in der Grundrechtsausübung, so dass deren Vorliegen an strenge Voraussetzungen gebunden ist. Danach bedarf es einer informierten freiwilligen Entscheidung durch den Betroffenen, in der die individuellen Präferenzen etwa über die Risikobereitschaft zu der Verarbeitung personenbezogener Daten einfließen können. Die Rechtsnatur der Einwilligung gleicht einer rechtsgeschäftlichen Erklärung und unterliegt Bestimmtheitsanforderungen, die sich auf

die Informationen und den Zweck der Datenverarbeitung beziehen.[507] Somit liegt in der Einwilligung zu einem frühen Zeitpunkt des Datenzyklus eine weichenstellende Funktion vor, da sich in ihr vielfältige Erkenntnismöglichkeiten über die personale Identität innerhalb eines Datenzyklus bündeln können und diese Gegenstand der Risikoabwägungen des Betroffenen werden sollten.

Sobald die Einwilligung erfolgt ist, wird die Datenverarbeitung durch den Verantwortlichen gerechtfertigt, so dass in der Einwilligung zunächst die absolute Kontrolle zum Ausdruck kommt und diese in eine relative Kontrolle gegenüber dem Verantwortlichen durch das begründete Kommunikationsverhältnis übergeht. Dies umfasst die Entscheidung des Betroffenen über die Verarbeitung der personenbezogenen Daten und die bevorstehenden Erkenntnismöglichkeiten des Verantwortlichen über die personale Identität infolge der Datenverarbeitung. Weiter geht mit der Einwilligung eine relative Kontrolle einher, in der auch ein „Verzicht über die Herrschaft und Kontrolle der Daten"[508] gesehen wird und diese mit der Einwilligung legitimiert werde. Dabei ist der „Herrschaftsverzicht" mit der Einwilligung in rechtsdogmatischer Hinsicht jedoch dahingehend umstritten, ob es sich bei der Einwilligung um eine Rechtfertigung des Eingriffs handelt oder ob schon gar kein Eingriff vorliege.[509] Gleichwohl bleibt aus der weitreichenden Wirkung der Einwilligung das Fortbestehen eines Schutzbedarfs nach Einwilligungserteilung festzustellen.

Gerade im privatrechtlichen Kontext fungiert die Einwilligung als Primat[510] für umfangreiche Datenverarbeitungsprozesse, indem sie einen ausgeprägten Wirkmechanismus für den Datenzyklus der personalen Identität entfaltet. Folglich sollen für das Identitätsverwaltungsmodell die informierte freiwillige Einwilligung (1.), sowie das Verhältnis des AGB-Rechts zur Einwilligung (2.) analysiert werden und eine prozedural geprägte Betrachtung der Einwilligung (3.) vorgenommen werden. Anschließend soll

507 Der Streit über die Rechtsnatur der Einwilligung als rechtsgeschäftliche Willenserklärung oder als geschäftsähnliche Handlung ist für die Identitätsverwaltung nicht maßgebend, sondern allein die Feststellung, dass der Datenzyklus zu einer personalen Identität mit der Einwilligung beginnt. Demnach erscheint das Konzept der antizipierten Erlaubnis als rechtserhebliche Handlung *sui generis* für das Identitätsverwaltungsmodell naheliegend zu sein *Buchner/Kühling*, in: dies. (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 7 DSGVO Rn. 1a, 61.

508 *Spindler*, in: Verhandlungen des 69. Deutschen Juristentages, 2012, S. F 77.

509 *Knecht*, in: Schwarze/Becker/Hatje u.a. (Hrsg.), EU-Kommentar, 2019, Art. 8 GRC Rn. 3.

510 *Veil*, NVwZ 2018, 686 (688).

der Frage nach dem Bedarf einer paternalistischen Intervention (4.) nachgegangen werden.

1. Informierte freiwillige Einwilligung, Art. 7 DSGVO

Die informierte freiwillige Einwilligung lässt sich nunmehr unter erleichterten Bedingungen erteilen. Gemäß Art. 4 Nr. 11 DSGVO setzt die Einwilligung eine in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung voraus, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Im Gegensatz zur alten Rechtslage gemäß § 4a BDSG a.F. BDSG, die ein Schriftformgebot[511] voraussetzte, sind nunmehr die mündliche Einwilligung und die Einwilligung durch schlüssiges Verhalten für die Rechtfertigung der Datenverarbeitung ausreichend, Art. 6 Abs. 1 a), 7 DSGVO, EWG 43, 42 S. 5. Dies hatte zur Folge, dass mit dem Schriftformgebot der Bedarf nach einer schriftlichen Einwilligung in manueller oder technischer Gestalt einherging und dies zu einem Medienbruch führen konnte. Nach der DSGVO lässt sich jedoch die Einbeziehung einer ausdrücklichen Einwilligungsabfrage aufgrund der niedrigeren Einwilligungsanforderungen vermeiden. Gleichwohl bedarf es einer „unmissverständlich abgegebene(n) Willensbekundung" gemäß Art. 4 Nr. 11 DSGVO in einer Erklärung, die von dem Verantwortlichen gemäß Art. 5 Abs. 2 DSGVO dokumentiert wird.[512]

Demgegenüber wird bei der Verarbeitung besonderer Kategorien personenbezogener Daten aufgrund des gesteigerten Risikos für die Rechte und Freiheiten natürlicher Personen eine explizite Einwilligung gemäß Art. 9 Abs. 1 DSGVO verlangt, da aufgrund der „informationellen Diskriminie-

511 Das Schriftformgebot ist nunmehr in § 26 Abs. 2 S. 3 BDSG für eine spezifische Anhebung des Schutzniveaus im Beschäftigendatenschutzrecht geregelt. Jedoch wird darin ein Widerspruch zu Art. 7, 4 Nr. 11 DSGVO gesehen. Denn der Zweck der DSGVO, das Schutzniveau in den Mitgliedstaaten zu harmonisieren, könne nur entsprochen werden, wenn die nationale Regelung in § 26 Abs. 2 S. 2 BDSG teleologisch reduziert werde, vgl. *Maschmann*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, § 26 BDSG Rn. 64.

512 *DSK*, Datenschutzkonferenz, Kurzpapier Nr. 20, Einwilligung nach der DS-GVO, 22.02.2019, S. 2.

rungsverbote“[513] ein gesteigertes Risiko für den Schutz der personalen Identitäten besteht. Mit dem Erfordernis einer expliziten Einwilligung wird ein gesteigertes Bewusstsein für die Einwilligung vorausgesetzt, damit der Betroffene über die potentiell diskriminierenden Auswirkungen und die Erkenntnismöglichkeiten entscheiden kann. Entsprechend könnten die Anforderungen an die Einwilligung erweitert werden mit einer vorherigen fachkundigen Beratung, einer bestimmten Bedenkzeit oder den Formerfordernissen,[514] die sich in einem Identitätsverwaltungsmodell verwirklichen können. Insbesondere kommt für die Identitätsverwaltung die Einrichtung eines elektronischen Substituts der Einwilligung in Betracht, welches über eine elektronische Signatur oder PIN-Eingabe für die Einwilligungserklärung erfolgen könnte.[515] Diese elektronische Einwilligung hätte den Vorteil, dass die Dokumentations- und Rechenschaftspflichten nach Art. 5 Abs. 2 DSGVO automatisiert gewährleistet werden könnten, indem mit einem Zeitstempel die Erteilung der Einwilligung und der Zeitpunkt eindeutig feststellbar wären und zu einer erleichterten Beweisführung beitragen könnten.

Die Einwilligung stellt eine omnipräsente Rechtfertigungsmöglichkeit dar und zugleich ist eine hohe Bereitschaft bei den Betroffenen erkennbar, die Einwilligung schnell zu erteilen, so dass „die Bürger, matt vom Nicken, zu allem Ja sagen(d)“[516] die Einwilligung erteilen.[517] Somit liegt in dem Phänomen der faktisch bereitwilligen Einwilligungserteilung des Betroffenen eine Freigabe der personalen Identitäten in ihren *Idem*- und *Ipse*-Anteilen an den Verantwortlichen, dem ein effektives und wirksames Sanktionssystem gegenüberstehen müsste. Denn die Einwilligung als zentrales Instrument der informationellen Selbstbestimmung muss den rechtlichen Anforderungen gerecht werden, was mit dem Sanktionssystem gemäß Art. 83 DSGVO möglich ist.

Neben dem Sanktionssystem zur Gewährleistung der informierten freiwilligen Einwilligung könnte die interdisziplinäre Analyse der Einwilligung erhellend sein, um weitere Anhaltspunkte für einen effektiven Me-

513 *Weichert*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 9 DSGVO Rn. 1, 13.

514 *Ders.*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 9 DSGVO Rn. 47 f.

515 *Raabe/Lorenz*, DuD 2011, 279 (283).

516 *Wieduwilt*, FAZ vom 20.10.2018, 17.

517 *Spindler*, in: Verhandlungen des 69. Deutschen Juristentages, 2012, F 99; *Hoffmann-Riem*, AöR 142 (2017), 1 (22); *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 2016, S. 79.

chanismus in einem Identitätsverwaltungsmodell erlangen zu können. Denn mit der bereitwilligen Erteilung einer rechtfertigenden Einwilligung könnte ein legitimatorisches Defizit einhergehen, welches in einem unzureichenden Bewusstsein zum Zeitpunkt der Einwilligungserteilung über die personalen Identitäten und die Erkenntnismöglichkeiten im Rahmen des Datenzyklus liegt. Für eine nähere Analyse dieser Sachlage soll die *verhaltensökonomische Perspektive* herangezogen werden, um die Annahme einer rationalen Kosten-Nutzen-Analyse bei der Einwilligungserteilung näher untersuchen zu können. Denn es kann die Ansicht vertreten werden, dass neben der Kosten-Nutzen-Analyse aufgrund der Informationspflichten gemäß Art. 12–14 DSGVO die Entscheidung des Betroffenen von weiteren inneren und äußeren Entscheidungsfaktoren geprägt ist und Verzerrungen unterliegt. Diese möglichen Verzerrungen in der Entscheidungsfindung sollen für den Schutz der informationellen Selbstbestimmung in das Identitätsverwaltungsmodell einbezogen werden. Dafür soll zunächst die verhaltensökonomische Betrachtung motiviert (a), sowie die Einwilligung in ihren endogenen (b) und exogenen (c) Faktoren der Entscheidungsfindung in Frage gestellt werden, um anschließend die Ergebnisse auf das „*Privacy Paradox*" (d) und die Identitätsverwaltung (e) zu übertragen.

a) Motivation

Die Phänomenologie der Einwilligung als tatsächliche Verhaltensweise soll in der weiteren Untersuchung vertieft analysiert werden. Denn es könnte der rechtlichen Intention einer informierten freiwilligen Einwilligung, den Maßgaben gemäß Art. 6, 7 DSGVO folgend, eine Realität gegenüberstehen, die gerade keine bewusste informierte Entscheidung darstellt. Die beschriebenen Phänomene einer hohen Einwilligungsbereitschaft können als Indiz gewertet werden, dass eine umfassende oder nur minimale Kosten-Nutzen-Analyse durch den Betroffenen nicht immer erfolgt. Damit erscheint die tatbestandlich vorausgesetzte bewusste und rationale Einwilligung zumindest fragwürdig. Denn aufgrund von direkten Netzwerkeffekten und der Omnipräsenz von Einwilligungsabfragen kann die bewusste und freiwillige Entscheidungsfindung in hohem Maß von äußeren Faktoren beeinflusst werden. Hinzu kommt, dass die Verhandlungsmacht zwischen dem Verantwortlichen und der betroffenen Person ungleich verteilt ist, so dass die Einwilligung im B2C-Kontext besondere Aufmerksamkeit für die Identitätsverwaltung verlangt.

In dem Identitätsverwaltungsmodell bedarf es der Gewährleistung einer freiwilligen Kontrolle personaler Identitäten gerade bei bestehenden Verhandlungsungleichgewichten, EWG 43 S. 1. Denn die Identitätsverwaltung verwirklicht den Schutz der personalen Identität in ihren *Idem-* und *Ipse*-Anteilen, wenn die Entscheidungsfindung von den Anforderungen an die Freiwilligkeit gedeckt ist und die Einwilligung effektiv realisiert werden kann, da nur mit einer tatsächlich freiwilligen Entscheidung der *Selbstdatenschutz* verwirklicht wird. Für die Analyse der Voraussetzungen eines wirksamen *Selbstdatenschutzes* mit der Einwilligung bedarf es daher der Einbeziehung verhaltensökonomischer Betrachtungen, um einen umfassenden Schutzmechanismus ableiten zu können.

b) Endogene Faktoren der Entscheidungsfindung

Die Einwilligung wird durch Faktoren beeinflusst, die im Inneren des Betroffenen liegen und auf individuellen Präferenzen und Überlegungen beruhen. Zu diesen endogenen Entscheidungsfaktoren gehört der „*Rational Choice*"-Ansatz (aa), der als theoretische Grundlage für die Willensbildung fungiert und anschließend mit der Darstellung der neuen Erwartungstheorie („*Prospect-Theory*") ergänzt werden soll (bb). Mit der „*Prospect-Theory*" erfährt der „*Rational Choice*"-Ansatz eine Erweiterung, so dass abschließend beide Theorien für das Identitätsverwaltungsmodell ausgewertet werden sollen (cc).

aa) „Rational Choice"-Ansatz

Die Entscheidungsfindung bei der Einwilligung stellt eine freiwillige und bewusste dem „*Rational Choice*"-Ansatz („*Utility Theory*"[518]) unterliegende Handlung dar. Dabei verfolge die Entscheidungsfindung ein bestimmtes Ziel, welches dem Kosten-Nutzen-Kalkül eines wirtschaftlich handelnden „*homo oeconomicus*" entspricht.[519] Demnach müsste sich der Betroffene mit dem Nutzen und damit einem Zustand der Vorteile und Nachteile seiner Entscheidung auseinandersetzen. Weiter müsste der Betroffene über die

518 *Kahneman/Tversky*, Econometrica 1979, 263.

519 *Eidenmüller*, JZ 2011, 814 (816 f.); von einer „approximativen Rationalität" ausgehend, vgl. *Glöckner*, in: Funke/Schmolke (Hrsg.), Menschenbilder im Recht, 2019, 79 (81).

Risiken seiner Entscheidung eine bewusste Kosten-Nutzen-Abwägung vornehmen, die zur Grundlage der bewussten freiwilligen Einwilligung wird. Von dieser Entscheidungsfindung müssten die Erkenntnismöglichkeiten über eine personale Identität erfasst sein, die der Verantwortliche infolge der Datenverarbeitung erlangen kann. Auch könnten individuelle Präferenzen des Betroffenen zum Schutz der informationellen Selbstbestimmung in die Kosten-Nutzen-Analyse einfließen, was sie zu einer zeit- und kontextbezogenen Entscheidung und Prognose über die Folgen der Einwilligung macht. Denn die individuellen Präferenzen über den Schutz der personenbezogenen Daten sind situativ und neigen dazu, unvollständig zu sein, so dass eine abschließende Abwägung über die Risiken gegenüber der informationellen Selbstbestimmung ausgeschlossen werden könne und ein rationales Kosten-Nutzen-Kalkül in Frage gestellt werden müsse.[520]

Für eine abschließende Abwägung des Betroffenen kommt hinzu, dass der Entscheidungsgegenstand der informationellen Selbstbestimmung einer hohen Komplexität unterliegt und daher eine umfassende Kosten-Nutzen-Analyse und rationale Entscheidung kaum erwartet werden könne.[521] Vielmehr können endogene Faktoren zu *kognitiven Verzerrungen* der individuellen Präferenzen führen und die Entscheidung über die Einwilligung beeinflussen. Dazu gehöre, dass der Betroffene risikoaffin oder risikoavers sein könne, welches sich über den „*Rational Choice*"-Ansatz durch die fehlende Auswirkung auf das Abwägungsergebnis nicht abbilden ließe.[522] Damit kann in dem „*Rational Choice*"-Ansatz eine Vermutung über das Entscheidungsverhalten gesehen werden, so dass sich die Frage nach der Einbeziehung der durchgeführten psychologischen und empirischen Untersuchungen in der Verhaltensökonomie stellt.[523]

Es lässt sich aufgrund des *Big Data*-Phänomens mit der bereitwilligen Erteilung von Einwilligungen und den damit einhergehenden Risiken über die vielfachen Erkenntnismöglichkeiten die Frage nach den Ursachen dafür stellen. Folglich seien die Untersuchungen von *Acquisti* angeführt, nach denen sich die „*Rational Choice*"-Entscheidungen im Zusammenhang mit der informationellen Selbstbestimmung anzweifeln und mit Modellen zu den psychologischen Verzerrungen präziser beschreiben lassen.[524] Dem-

520 *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, S. 130 f.
521 *Solove*, Harv. L. R. 2013, 1880 (1897).
522 *Kahneman/Tversky*, Econometrica 1979, 263 (285).
523 *Van Aaken*, in: Kirste (Hrsg.), Interdisziplinarität in den Rechtswissenschaften, 2016, 187 (189 f).
524 *Acquisti*, ACM 2004, 21.

nach konnte nachgewiesen werden, dass die rationale Entscheidung von einer kontextbezogenen sog. „*Privatheitskurzsichtigkeit*" geprägt sei und den umfassenden Schutz der Privatheit nicht gewährleisten könne.[525] Somit bedarf es für das Identitätsverwaltungsmodell der Einbeziehung kontextspezifischer Entscheidungsfaktoren, um einen umfassenden Schutz der personalen Identität und der damit verbundenen Erkenntnismöglichkeiten im Datenzyklus gewährleisten zu können. Dabei geht es um die Bestimmung derjenigen Faktoren, die die Entscheidungsfindung endogen beeinflussen können und zu einer möglichst umfassenden Entscheidung über die Einwilligungserteilung führen. Dafür können die maßgeblichen Faktoren nach der neuen Erwartungstheorie aufschlussreich sein.

bb) „Prospect Theory"- Neue Erwartungstheorie[526]

In der Verhaltensökonomie wird der „*Rational Choice*"-Ansatz mit der „*Prospect Theory*" als neue Erwartungstheorie erweitert und damit ein der Realität näherkommendes Modell über die individuelle Entscheidungsfindung dargelegt. Dieses unterscheidet zwischen der rationalen Motivation und dem tatsächlichen Verhalten des Betroffenen.[527] Demnach geht es nicht mehr um den Nutzen, sondern um die Erwartungen des Betroffenen.[528] Die maßgebliche Frage liege vielmehr darin, was sich mit der Entscheidung verändern würde und weniger in dem statischen Nutzen.[529]

Dabei wird von *Kahnemann* zwischen System 1 und System 2 differenziert: Das System 1, welches mühelos und ohne willentliche Steuerung als erinnerndes Selbst im Unterbewusstsein arbeitet und unwillkürlich über die vermeintlich rationalen Entscheidungen von System 2 herrscht. Demgegenüber geht das System 2 davon aus, dass es eine „*Rational Choice*"- Entscheidung treffe, ohne die tatsächlichen Wirkungen von System 1 wahrzunehmen.[530] Dies könne dazu führen, dass der Betroffene gegenüber dem Offensichtlichen blind sei und kein Bewusstsein über die Blindheit bestünde, auch wenn eine hohe Aufmerksamkeit aufgebracht werde.[531] Demnach

525 *Ders.*, ACM 2004, 21 (22).
526 *Kahneman/Tversky*, Econometrica 1979, 263.
527 *Van Aaken*, in: Kirste (Hrsg.), Interdisziplinarität in den Rechtswissenschaften, 2016, 187 (191).
528 *Kahneman*, Schnelles Denken, langsames Denken, 2012, S. 348.
529 *Ders.*, Schnelles Denken, langsames Denken, 2012, S. 344.
530 *Ders.*, Schnelles Denken, langsames Denken, 2012, S. 33.
531 *Ders.*, Schnelles Denken, langsames Denken, 2012, S. 37.

könne in der rationalen Entscheidungsfindung bei hoher Auslastung des bewusstseinsgesteuerten Systems 2, die Entscheidung faktisch durch unwillkürliche Faktoren von System 1 getroffen werden, so dass „*to pay attention*" sprichwörtlich verstanden werden müsse.[532] Damit wird die Aufmerksamkeit aus System 2 von unwillkürlichen Faktoren des Systems 1 verdrängt. Daraus schließt *Kahnemann* sogar eine „Tyrannei des erinnernden Selbst" von System 1 und beschreibt das erinnernde Selbst als „Fremden".[533] Folglich ergibt sich der Differenzierungsbedarf des Entscheidungsprozesses, der auf den Erinnerungen und vergangenheitsgeprägten Erfahrungen basiert und zum Gegenstand der Aufmerksamkeit wird.

Für die Einwilligung stellt sich demnach die Frage, ob sich die Aufmerksamkeit bei der Einwilligungserteilung tatsächlich auf die Abwägung der Kosten und Nutzen für die informationelle Selbstbestimmung richtet oder die Aufmerksamkeit von der Darstellung und den mit einer bevorstehenden Datenverarbeitung verbundenen Gratifikationen absorbiert wird. Denn die ursprüngliche Anforderung des Schriftformgebots an die Einwilligung gemäß § 4a Abs. 1 S. 3 BDSG a. F. hatte für den Betroffenen die Warn-, Beweis- und Kontrollfunktion, so dass der Betroffene auf mehreren Ebenen eine Abwägung und damit eine von System 2 getragene Entscheidung treffen konnte. Nunmehr sieht Art. 6 Abs. 1 a), Art. 4 Nr. 11 DSGVO vor, dass die Einwilligung ohne Formerfordernis als „unmissverständlich abgegebene Willensbekundung" erkennbar sein muss und somit konkludent erteilt werden kann. Diese Abschwächung der Einwilligungsanforderungen wirkt sich auf die Ausübung der Einwilligung dahingehend aus, dass bereits mit der Nutzung eines Dienstes die Einwilligung konkludent erteilt und diese Entscheidung möglicherweise weniger von System 2 als von System 1 getragen wird. Der Anreiz, den Dienst unmittelbar nutzen zu können, wird von System 1 ausgelöst und weniger von einer Kosten-Nutzen-Analyse des Systems 2 getragen. Demnach erleichtern die Einwilliguganforderungen nach der DSGVO eine von System 1 getragene Entscheidung. Gleichwohl ist nicht auszuschließen, dass Rahmenbedingungen und die Darstellung der Informationspflichten derart ausgestaltet werden, dass ein Anreiz für eine von System 2 getragene Entscheidung über die Datenverarbeitung geschaffen wird.

Im Einzelnen können insbesondere „*Priming*"-Effekte, „*Framing*"- und *Ankereffekte* die Entscheidungsfindung beeinflussen und zum Gegenstand der Rahmenbedingungen und der Darstellung von Informationspflichten

532 *Ders.*, Schnelles Denken, langsames Denken, 2012, S. 58.
533 *Ders.*, Schnelles Denken, langsames Denken, 2012, S. 470–480.

für die Einwilligungserteilung werden. Durch „*Priming*"-Effekte erfolgt etwa mit dem ersten Wort, dem ersten Verhalten oder der technischen Einstellung die Bahnung der Aufmerksamkeit in die Richtung einer bestimmten Assoziationskette, was über System 1 erfolge.[534] Durch „*Priming*"-Effekte wird eine Überbewertung des ersten Informationsgegenstandes gegenüber den darauf folgenden Informationen ausgelöst, so dass Chancen und Risiken fehlinterpretiert werden können.[535] Ebenso kann die Entscheidungsfindung durch *Ankereffekte* beeinflusst werden, die dem „*Priming*"-*Effekt* sehr nahe sind. Danach lösen die Ankereffekte bei System 1 und System 2 einen Anknüpfungspunkt aus, an den sich alle folgenden Einschätzungen richten. Folglich wird bei der Verhandlung eines Preises das erste Angebot die weiteren Preisvorschläge maßgeblich beeinflussen. Daraus ergibt sich, dass die Unabhängigkeit der Folgeverhandlung von dem ersten Gebot überschätzt und die intuitive Wirkung des ersten Angebotes auf die Folgeverhandlung unterschätzt werde.[536] Mit „*Framing*"-*Effekten* wird entsprechend der Begrifflichkeit ein Rahmen für die folgenden Assoziationen und Vorstellungen erweckt.[537] Demnach beeinflusst die Begriffswahl den Rahmen der Assoziationen bei der Entscheidungsfindung, so dass der Gestaltung der Informationspflichten und der damit auslösbaren Assoziationsketten bei dem Betroffenen eine entscheidende Bedeutung in der Einwilligungserteilung zukommt.

Für die Identitätsverwaltung können sich diese Befunde auf die Gestaltung der Informationspflichten durch den Verantwortlichen auswirken. Danach können Ankereffekte über die wahrnehmbaren Informationen in dem Sinne wirken, dass „*What you see is all there is*" – „WYSIATI" – Entscheidungen zu voreiligen Schlussfolgerungen und Urteilssprüngen verleiten können.[538] Denn die „WYSIATI"-Regel führe zu der Gewichtung von Faktoren, die Wahrnehmungsgegenstand sind und blenden weniger offensichtliche Faktoren aus, so dass eine kontextabhängige Fokussierungsillusion entstehen könne.[539] Demnach kann bei der Entscheidungsfindung im Rahmen der informationellen Selbstbestimmung das Risiko eines Schadenseintritts oder ein Risikokriterium außerhalb der Wahrnehmung des Betroffenen liegen, obwohl diese Faktoren in der Entscheidungsfindung

534 *Ders.*, Schnelles Denken, langsames Denken, 2012, S. 72 f.
535 *Kahneman/Tversky*, Econometrica 1979, 263.
536 *Kahneman*, Schnelles Denken, langsames Denken, 2012, S. 152–163.
537 *Ders.*, Schnelles Denken, langsames Denken, 2012, S. 447–450.
538 *Ders.*, Schnelles Denken, langsames Denken, 2012, S. 112 f.
539 *Ders.*, Schnelles Denken, langsames Denken, 2012, S. 497.

relevant sein müssten. Ebenso können Faktoren bei der Entscheidungsfindung einbezogen werden, die irrelevant sind und sich auf die Risikobewertung nicht auswirken können. Damit beruhen Entscheidungen nach der „*Prospect Theory*" auf der Illusion der umfassenden Gültigkeit einer Entscheidung, obwohl sie faktisch allein kontextbezogene Gültigkeit haben und auf irrelevanten Faktoren oder Bewertungen beruhen können.[540] Diese Problematik könne aufgelöst werden, wenn subjektive Risikobewertungen mit einem Verfahren derart modifiziert würden, dass diese nicht den „*Priming*"-, Anker-[541] und den „*Framing*"-Effekten unterliegen. Ein solches Verfahren könnte als ein gestuftes Verfahren ausgestaltet werden, in dem einzelne Merkmale separat bewertet werden und anschließend in eine Gesamtbewertung überführt werden können.[542]

Indem die erste datenschutzrechtliche Phase zwischen dem Betroffenen und Verantwortlichen über die Informationspflichten in der Datenschutzerklärung für die Entscheidungsfindung maßgeblich ist, müsste diese in dem Identitätsverwaltungsmodell differenziert einbezogen werden. Denn die Einwilligungsentscheidung ist von der Mühelosigkeit des Systems 1 geprägt, so dass die Generierung von personalen Identitäten nur einer eingeschränkten Rationalität unterliegt. Dieses Phänomen könnte zu der Annahme eines legitimatorischen Defizits bei der Einwilligung führen und eines eigenen Verfahrens zur Kompensation der eingeschränkt rationalen Entscheidung bedürfen. Weiter kann sich das Entscheidungsergebnis auf den gesamten Datenzyklus der personalen Identität auswirken, so dass der Einwilligungsvorgang im Identitätsverwaltungsmodell in einem separaten Verfahren aufgegliedert werden sollte. Mit einer Prozeduralisierung der Einwilligung in ein gestuftes Verfahren würde ein weitergehender Schutz für die personale Identität gewährleistet werden können.

cc) Bewertung

Die endogenen Faktoren wirken sich auf die Entscheidungsfindung und damit die Einwilligung aus, so dass die Annahme der rein rationalen Entscheidung für ein Identitätsverwaltungsmodell modifiziert werden muss. Dazu könnte die Differenzierung der Phase *ax ante* zur Rechtfertigung und der rechtfertigenden Einwilligung in weitere Iterationen gehören, mit

---

540 *Ders.*, Schnelles Denken, langsames Denken, 2012, S. 262.
541 *Tversky/Kahneman*, Science 1974, 1124 (1129).
542 *Kahneman*, Schnelles Denken, langsames Denken, 2012, S. 287.

der die Datenschutzerklärung in den Fokus rückt. Es kommt das Konzept einer iterativen und geschichteten Einwilligung, sog. „*layered approach*" in Betracht, bei der eine konkretisierte Einwilligung etwa auf kontextspezifische Risikofaktoren abgegeben werden könnte. Dem steht gegenüber, dass das empirisch nachgewiesene Interesse an unmittelbaren Gratifikationen zu einem „Abnicken" der einzelnen Einwilligungsabfragen führen könnte. Gleichwohl könnten die „*Priming*"-, Anker- und „*Framing*"-Effekte dazu eingesetzt werden, eine kontextspezifische bewusste Entscheidung über die Risiken für die personale Identität zu fördern. Demnach ist eine informierte freiwillige Einwilligung als „*layered approach*" unter Einbeziehung der verhaltensökonomischen Erkenntnisse dazu geeignet, das Legitimationsdefizit der Einwilligung zu kompensieren und in einem Identitätsverwaltungsmodell eingesetzt zu werden.

Insgesamt kommt der Datenschutzerklärung in ihrer inhaltlichen Ausrichtung und Darstellung besonderes Gewicht zu, denn mit ihr könnte der inhaltliche Hinweis auf die verhaltensökonomischen Verzerrungsfaktoren vorgenommen werden. Zwar ist dies an sich Gegenstand der Warn-, Beweis- und Kontrollfunktion des Schriftformgebotes, wie es gemäß § 4a Abs. 1 S. 3 BDSG a. F. vorausgesetzt wurde, aber nunmehr unterliegt die Einwilligungserteilung gemäß Art. 6 Abs. 1 a), 4 Nr. 11 DSGVO erleichterten Bedingungen, was eine Verschiebung zu einer Entscheidungsdominanz durch System 1 zur Folge haben kann. Folglich sollten die verhaltensökonomischen Verzerrungsfaktoren in die Informationspflichten und in die Rahmenbedingung der Entscheidungsfindung aufgenommen werden. Diese Konzeption hätte den Vorteil, dass die endogenen Entscheidungsfaktoren in die bewusste Entscheidungsfindung einbezogen und die Wahrnehmungsverzerrungen minimiert werden könnten. Eine derartige Wirkung ist in manchen Kontexten denkbar, gleichzeitig wurde festgestellt, dass Datenschutzerklärungen nicht immer zur Kenntnis genommen werden, so dass eine paternalistische Intervention in Betracht kommt. Hierbei erscheint im Rahmen der Gestaltung des Identitätsverwaltungsmodells ein weiches paternalistisches Konzept[543] auf der technischen Gestaltungsebene für die Förderung der Entscheidungsfindung naheliegend. Damit könnte eine kontextspezifische Bewusstseinsförderung über die Risiken für die personalen Identitäten und die Erkenntnismöglichkeiten über diese gestaltet werden. Zudem würde dem legitimatorischen Defizit infolge einer fehlenden, überwiegend rationalen Entscheidung in einem Identi-

543 *Brandimarte/Acquisti*, in: Peitz/Waldfogel (Hrsg.), The Oxford Handbook of the Digital Economy, 2012, S. 564.

tätsverwaltungsmodell mit einer gestuften Prozeduralisierung der Einwilligung Rechnung getragen werden können.

c) Exogene Faktoren der Entscheidungsfindung

Ebenso kann die Einwilligung durch äußere Faktoren beeinflusst werden, die in dem Verantwortungsbereich des Verantwortlichen oder in dem Verhalten mehrerer Nutzer liegen. Zunächst kommt als exogener Faktor der Entscheidungsbeeinflussung die Verbindung der datenschutzrechtlichen Einwilligung mit einer vertraglichen Angebotsannahme über das Koppelungsverbot (aa) in Frage und anschließend die Beeinflussung des Betroffenen durch Algorithmen und Netzwerkeffekte (bb).

aa) Koppelungstatbestand, Art. 7 Abs. 4 DSGVO

Die freiwillige Erteilung der Einwilligung kann in direkter Verbindung zu einem verfolgten Vertragszweck stehen, so dass dieser als exogener Faktor die Erteilung der Einwilligung beeinflusst. Durch den Koppelungstatbestand gemäß Art. 7 Abs. 4 DSGVO[544] soll bei der Beurteilung der Freiwilligkeit dem Umstand der Abhängigkeit von einem Vertragsschluss Rechnung getragen werden. Indem die Einwilligung bei einem gleichzeitigen Vertragsabschluss zu einem bloßen Formalismus verkommen und die Grundrechtsausübung mit der Einwilligung faktisch unterlaufen werden kann, kommt dem Koppelungstatbestand eine besondere Bedeutung zu.

Gemäß Art. 7 Abs. 4 DSGVO würde es an einer freiwilligen Einwilligung fehlen, wenn die Monopolstellung ausgenutzt und die Einwilligung allein aufgrund der ausgeprägten Abhängigkeit erteilt werde.[545] Dabei kann die Rechtsbeziehung derart ausgestaltet sein, dass die Einwilligung faktisch als Bedingung des Vertragsschlusses fungiert, so dass eine echte Wahlmöglichkeit ausgeschlossen ist und die Verweigerung der Einwilligung mit dem Nachteil verbunden wäre, keinen Vertrag abschliessen zu

544 Entsprechend im Telekommunikationsrecht ist der Koppelungstatbestand in § 95 Abs. 5 TKG geregelt.

545 *Laue/Nink/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis, 2019, § 2 Rn. 19 f.; *Kühling/Schall/Biendl*, Telekommunikationsrecht, 2014, Rn. 637; *Schmitz*, in: Spindler/Schmitz (Hrsg.), Kommentar, TMG, 2018, § 12 TMG Rn. 28–31.

können, EWG 42 S. 5 DSGVO.[546] Schließlich wird ein Verstoß gegen den Koppelungstatbestand angenommen, wenn die Einwilligung eine „sachfremde Begleiterscheinung zum Vertrag" darstellt, wobei die Feststellung im Einzelnen eine wertende Betrachtung verlange.[547]

Für die Identitätsverwaltung wirkt sich dies auf den Schutz des Entschließungsspielraums über die Einwilligung und die Begründung des Datenzyklus zur personalen Identität aus, indem durch den Verantwortlichen eine echte noch so granulare Wahlmöglichkeit im Rahmen der Freiwilligkeit[548] gewährleistet werden muss. Dem ist besondere Aufmerksamkeit beizumessen, wenn die Verhandlungsposition der Parteien ungleich ist, da das Verhandlungsungleichgewicht zwischen Intermediären und Betroffenen erheblich sein kann, was in die Freiwilligkeitsbewertung einzubeziehen ist. Diese ökonomische Dimension der freiwilligen Einwilligung in Gestalt von „Machtproblemen" wird im traditionellen Datenschutzrecht als noch unzureichend eingebettet angesehen.[549] Mit dem Machtungleichgewicht gelange der Betroffene in die Situation, die einer „*take it or leave it*"-Situation gleiche, bei der gerade keine Verhandlungsmöglichkeit bestünde und schnell ein „Häkchen" als mechanischer Prozeduralismus gesetzt werde.[550] Dem steht das beschriebene Erfordernis einer bewussten Entscheidung mit einer echten Wahlmöglichkeit ohne drohende Nachteile gegenüber, Art. 7 Abs. 4 i.V.m. 43 DSGVO. Dies erscheint bei einem Verhandlungsungleichgewicht nur eingeschränkt möglich, so dass die Freiwilligkeit kaum realisiert werden kann. Dies hat zur Folge, dass die Risikobewertung des Betroffenen als echte Wahlmöglichkeit im Hinblick auf die personale Identität unzureichend erfolgt oder gänzlich ausfällt. Demnach kann die enge Verbindung der Einwilligung zu einem Vertrag oder eine ungünstige Verhandlungsposition eine exogene Einschränkung der Freiwilligkeit mit sich bringen, die sich auf den tatsächlichen Rechtfertigungsgrad der kontextspezifischen personalen Identität auswirkt.

546 *Maschmann*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, § 26 BDSG, Rn. 62.
547 *Schulz*, in: Gola/Eichler/Franck u.a. (Hrsg.), Kommentar, Datenschutz-Grundverordnung, 2018, Art. 7 DSGVO Rn. 28.
548 *DSK*, Datenschutzkonferenz, Kurzpapier Nr. 20, Einwilligung nach der DS-GVO, 22.02.2019, S. 1.
549 *Hoffmann-Riem*, AöR 142 (2017), 1 (7) Fn. 20.
550 *Veil*, NVwZ 2018, 686 (688); *Hoffmann-Riem*, AöR 142 (2017), 1 (22 f.); *Becker*, JZ 2017, 170 (174).

bb) Netzwerkeffekte und Algorithmen

Die Entscheidungsbeeinflussung des Betroffenen kann durch exogene, außerrechtliche Faktoren erfolgen und im unmittelbaren Zusammenhang mit dem Kontext der Einwilligung stehen. Die exogenen Faktoren der Verhaltensbeeinflussung können unbewusst erfolgen und in den Algorithmen und dem Verhalten anderer Nutzer liegen. Dieses Phänomen der Verhaltensbeeinflussung geschieht dahingehend beiläufig, dass das Verhalten im online-Kontext unmittelbar algorithmisch verarbeitet wird, ohne mehrdeutige Interpretationen des Verhaltens zuzulassen. Sobald dies in einem großen Umfang geschieht, erlangt das unbewusste Verhalten in der algorithmischen Verarbeitung das gleiche Gewicht wie bewusste Verhaltensweisen.

Die Netzwerkeffekte können sich bei einer großen Nutzerzahl auf die Entscheidungsfindung des Einzelnen auswirken, indem die sozialen „Kosten", sich nicht dem Netzwerk anzuschließen, zu hoch erscheinen und der Nutzer zur Vermeidung des sozialen Ausschlusses die Einwilligung erteilt. Damit fungiert die Einwilligung nicht mehr als solipsistische Entscheidung, sondern unterliegt dem Eindruck des Verhaltens weiterer Nutzer, was wiederum Einwilligungsdruck auslösen und zu nachteiligen Netzwerkeffekten für den Verbraucher führen kann.[551] Dabei können die individuellen Präferenzen über den Schutz personaler Identitäten zurücktreten und die exogenen Faktoren die Entscheidungsfindung maßgeblich beeinflussen, so dass die Entscheidungsfindung als formbar angesehen wird.[552] Damit zeichnet sich die Grenze vom „*Nudging*", Gängeln hin zu einer manipulativen Herbeiführung der konsumorientierten Einwilligung ab, die durch das deutliche Ansprechen bestimmter Motivationsfaktoren in einer kaum durchschaubaren Form gekennzeichnet sei.[553] Dabei wird bereits die Motivation des Betroffenen zu einer bestimmten Handlung und das Ablenken der Aufmerksamkeit, ohne dass dies durchschaubar ist, als eine manipulative Beeinflussung eingeordnet,[554] was zu einer suggerierten freiwilligen Einwilligung führen kann. Dies kann mit einem Korridor von „zugelassenen" Verhaltensweisen erfolgen und zu einer Verhaltenssteuerung führen, mit der ein Vorhersageimperativ durch den verantwortlichen

551 *Bundeskartellamt*, Fallbericht vom 15.02.2019, Az.: B6-22/16, S. 7 f.; *Kühling/Sackmann*, Rechte an Daten, 20. November 2018, S. 19 f.
552 *Acquisti*, IEEE Security & Privacy Magazine 2009, 72 (73 f.).
553 *Zuboff*, FAZ vom 24.09.2018, 12.
554 *Glasl*, Konfliktmanagement, 2020, S. 331.

Intermediär über das künftige Verhalten geschaffen wird.[555] Damit findet eine Paternalisierung durch den verantwortlichen Intermediär statt, die sich weniger auf den Schutz der informationellen Selbstbestimmung und der personalen Identitäten richtet, sondern vielmehr auf die bereitwillige Erteilung der Einwilligung in die Datenverarbeitung.

Gegenüber diesen Phänomenen kann das Recht in seiner verhaltenssteuernden Funktion wirken, indem eine freiwillige Einwilligung gemäß Art. 6 Abs. 1 a), 7 DSGVO stipuliert und gewährleistet wird. Demnach kann die Verhaltenssteuerung durch das Recht mit der Verhaltenssteuerung durch die Technik ergänzt werden. Denn das Wirken der technischen Gestaltung im „Schatten der Einwilligung" führt zu einer Beeinflussung der Entscheidungsfindung des Betroffenen, so dass der Technologie *quasi* eine normative Dimension zukomme[556]. Somit können die algorithmusbasierten Wirkmechanismen eine Quelle der sozialen Ordnung sein,[557] wenn sie für den Betroffenen dahingehend dienlich sein können, dass sie den rechtlichen Schutz der informationellen Selbstbestimmung mit einer algorithmusbasierten Unterstützung ausweiten.

Erschwerend kommt hinzu, dass die Verhaltensbeeinflussungen auf Korrelationen beruhen[558] und die Eigenschaften eines Betroffenen in ihrer Korrelation zu künftigem Verhalten führen können, so dass der Verhaltenskorridor davon geprägt sein kann, was bei Kohorten als Korrelationsmaßstab bestimmt wurde. Dabei kann die Bildung des Verhaltenskorridors blind gegenüber Kausalitätsketten sein, die für ein bestimmtes Verhalten ursächlich sind und den Verhaltenskorridor erweitern würden. Somit könnte etwa eine häufig auftretende Suchanfrage des Betroffenen über bestimmte Buchtitel bei einem online-Händler zu einem algorithmisch festgelegten Buchgeschmack führen, ohne dabei die situative Ursächlichkeit einzubeziehen, die der tatsächlich suchenden personalen Identität in ihrem *Ipse*-Anteil am ehesten entspräche. Die Buchempfehlungen aufgrund des festgestellten Buchgeschmacks verstärken somit den vorangegangenen Verhaltenskorridor und lassen den *Ipse*-Anteil einer personalen Identität als vorübergehendes Verhalten außen vor. In diesen Verhaltenskorridoren liegt für ein Identitätsverwaltungsmodell eine Beschränkung

555 *Di Fabio*, Grundrechtsgeltung in digitalen Systemen, 2016, S. 13; *Hoffmann-Riem*, AöR 142 (2017), 1 (8); *Graf von Westphalen*, IWRZ 2018, 9 (10 f.).
556 *Hoffmann-Riem*, AöR 142 (2017), 1 (35); *Steinmüller*, Information, Modell, Informationssystem, S. 47.
557 *Ders.*, AöR 142 (2017), 1 (5 f.).
558 4. Teil, A., I., 2.

der potentiellen Verhaltensmöglichkeiten des Betroffenen, so dass eine Erweiterung und Verhandlungsfähigkeit des Verhaltenskorridors dem Schutz der informationellen Selbstbestimmung dienen könnte. Damit würde der dynamischen Ausprägung einer personalen Identität in ihrem *Ipse*-Anteil Rechnung getragen werden.

Gleichwohl bieten Algorithmen die Chance, dass eine Vorauswahl und Steuerung in die rechtlich und individuell gewünschte Richtung ermöglicht wird, so dass die rechtlichen Maßgaben etwa des Diskriminierungsschutzes effektiver verwirklicht werden und zu einer Entlastung in Überforderungssituationen führen können.[559] Damit kann für die Identitätsverwaltung ein wesentlicher Schutz durch Algorithmen erfolgen, indem die Risiken für die personale Identität hinsichtlich eines bevorstehenden Kontrollverlustes oder eines erhöhten Diskriminierungsrisikos antizipiert werden und Gegenstand von Warnungen werden könnten. In Anknüpfung an das von *Hildebrandt* beschriebene Phänomen des „*digital unconscious*" erscheint im online-Kontext das Spektrum an intransparenten Beeinflussungsmöglichkeiten deutlich weitgehender als im offline-Kontext, so dass ein eigenständiges Risiko von der subtilen technischen Beeinflussungsmöglichkeit ausgeht, welches für eine effektive Identitätsverwaltung in die Modellbildung einbezogen werden sollte. Folglich sollten die Netzwerkeffekte und Algorithmen als exogene Faktoren der Entscheidungsbeeinflussung spiegelbildlich zum Schutz der informationellen Selbstbestimmung in die Identitätsverwaltung einbezogen werden.

cc) Zwischenergebnis

Der Entscheidungsprozess über die Einwilligung hängt von exogenen Faktoren ab, die aus der Einwilligung im Zusammenhang mit dem Vertragsschluss, den Netzwerkeffekten und Algorithmen bestehen. Im online-Kontext können diese exogenen Faktoren bei der Entscheidungsfindung unbewusst wirken, so dass von dem Verantwortlichen ein gewisser Paternalismus gegenüber dem Betroffenen ausgeübt wird. Dies kann zu einer Kanalisierung der Entscheidungsfindung beim Betroffenen führen, die eine Einwilligungserteilung nahelegt. Dabei wird die echte Wahlmöglichkeit durch einen parallelen Vertragsschluss oder algorithmusbasierten Verhaltenskorridor eingeschränkt.

---

559 *Hoffmann-Riem*, AöR 142 (2017), 1 (36).

Wegen der ungünstigen Verhandlungsposition des Betroffenen gegenüber marktbeherrschenden Verantwortlichen führt eine Kanalisierung zur Einwilligungserteilung etwa durch „*Nudging*" zu einer Verstärkung der Verhandlungsungleichheit. Somit kann festgestellt werden, dass der verantwortliche Intermediär ein Interesse an der Einwilligung hat und eine dahingehende Strategie zur Herbeiführung der Einwilligung verfolgt, was zu einer *Erosion der freiwilligen Entscheidung* im Rahmen der informationellen Selbstbestimmung und einem legitimatorischen Defizit der rechtfertigenden Einwilligung führen kann. Folglich könnten die exogenen Faktoren der Entscheidungsbeeinflussung für ein Identitätsverwaltungsmodell spiegelbildlich eingesetzt werden, indem die Förderung der informationellen Selbstbestimmung mit technischer Unterstützung erfolgt. Dies könnte durch die Einbeziehung der verhaltensökonomischen Erkenntnisse des „*Framings*" und „*Primings*" erfolgen. Ebenso kommt der Einsatz von Algorithmen in Betracht, mit denen automatisiert das Bewusstsein für eine risikobewusste Identitätsverwaltung gesteigert wird. Dies könnte mit einem iterativen Verfahren erfolgen, und damit der personalen Identität in ihrem dynamischen *Ipse*-Anteil entsprochen werden.

d) „Privacy Paradox"?

Den endogenen und exogenen Faktoren der Entscheidungsfindung ist gemein, dass diese den Entscheidungsprozess zur Einwilligungserteilung beeinflussen und zu einem legitimatorischen Defizit führen können. Zu dem *Big Data*-Phänomen lässt sich die Bereitwilligkeit der Verbraucher zählen, die Einwilligung in die Datenverarbeitung vorzunehmen, ohne das Risiko der Erkenntnismöglichkeiten über den Datenzyklus einer personalen Identität umfassend antizipieren zu können. Mit diesem als „Exzess der Privatheit" bezeichneten Phänomen[560] geht der Kontrollverlust des Betroffenen über die Datenverarbeitung und mit ihr verbundenen Erkenntnisse über die personalen Identitäten einher. Gleichzeitig kann ein ausgeprägtes Interesse am Privatheitsschutz bestehen, welches im Widerspruch zur hohen Einwilligungs- und Nutzungsbereitschaft steht.

Demnach wird von einem „*Privacy Paradox*" ausgegangen, wonach die Bereitschaft zur Informationspreisgabe hoch ist, obwohl ein ausgeprägtes

560 *Froomkin*, Building Privacy into the Infrastructure: Towards a New Identity Management Architecture, 2016, S. 41–47

Schutzinteresse an der Privatheit beim Betroffenen besteht.[561] Aufgrund des Komforts oder der unmittelbaren Gratifikation, die mit der Nutzungsmöglichkeit eines Dienstes einhergingen, würden die Privatheitsinteressen kontextbedingt zurücktreten, so dass im „*Privacy Paradox*" die Einstellung des Betroffenen und das tatsächliche Verhalten auseinanderfallen.[562] Dabei konnte nachgewiesen werden, dass selbst bei geringwertigen Gratifikationen, aus Komfortgründen die Bereitschaft zur Informationspreisgabe ausgeprägt sei, da ein scheinbares Wohlwollen des Verantwortlichen durch die Bereitstellung von Gratifikationen angenommen werde und dies Vertrauen beim Betroffenen auslöse.[563] Denn der Betroffene würde sofortige Gratifikation gegenüber langen Phasen ohne Gratifikationen vorziehen,[564] was die Bereitwilligkeit der Einwilligungserteilung fördere. Weiter wurde eine Verlustaversion festgestellt, aus der ein erhöhtes Interesse an Gratifikationen hervorgehe und die Bereitschaft zurücktrete, für die Privatheit schützende Dienste zu bezahlen.[565]

Somit wird die Entscheidung über die Einwilligung von endogenen Faktoren der „*Priming*"-, Anker- und „*Framing*"-Effekte[566] sowie von exogenen Faktoren und damit bestehenden Anpassungsdruck geleitet. Wenn die Entscheidungsgrundlage auf endogene und exogene Faktoren, aber nicht auf das Schutzinteresse der Privatheit zurückzuführen ist, erscheint die bereitwillige Erteilung von Einwilligungen als logische Konsequenz und nicht als Widerspruch, so dass das „*Privacy Paradox*" in Frage gestellt werden könne.[567]

Die Einbeziehung der Phänomene des „*Privacy Paradox*" in das Identitätsverwaltungsmodell könnte durch eine weiche paternalistische Regelung erfolgen. Als ein paternalistisches Konzept kommt auf der inhaltlichen Ebene die Datenschutzerklärung mit einem Hinweis auf die möglichen Wahrnehmungsverzerrungen durch Gratifikationen in Betracht, wobei die ausbleibende Kenntnisnahme der Datenschutzerklärung der Wirksamkeit dieser Maßnahme entgegenstehen könnte. Auf der Einwilligungs-

561 *Engels/Grundwald*, Das Privacy Paradox: Digitalisierung versus Privatsphäre, No. 57.2017, S. 1; *Solove*, Harv. L. R. 2013, 1880 (1886).
562 *Dies.*, Das Privacy Paradox: Digitalisierung versus Privatsphäre, No. 57.2017, S. 2; *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, S. 231–233.
563 *Brandimarte/Acquisti*, in: Peitz/Waldfogel (Hrsg.), The Oxford Handbook of the Digital Economy, 2012, S. 561–263.
564 *Acquisti*, ACM 2004, 21 (25) Fn. 27.
565 *Hermstrüwer*, JIPITEC 2017, 9 (19) Rn. 40.
566 4. Teil, C., II., b), bb).
567 *Hermstrüwer/Dickert*, Tearing the Veil of Privacy Law, 2013, S. 24.

ebene kommt ein paternalistischer Ansatz mit einem kontextspezifischen „*layered approach*" für die Datenschutzerklärungen in Betracht, der für kontextspezifische Entscheidungen mit einer beschränkten Informationslage geeignet ist und damit eine freiwillige und bewusste Entscheidungsfindung begünstigt.

e) Übertragung auf die Identitätsverwaltung

Die informierte freiwillige Einwilligung lässt sich nicht als solipsistische Entscheidung abbilden, sondern unterliegt exogenen Faktoren der Entscheidungsbeeinflussung durch das Verhalten anderer im Entscheidungskontext. Auch auf der Ebene der endogenen Entscheidungsfaktoren wird die Annahme einer rationalen Entscheidung über die Einwilligung als Kern der informationellen Selbstbestimmung als „Mythologie"[568] oder als unrealistisch eingeordnet[569]. Damit ist der Grat einer rationalen freiwilligen Einwilligung schmal und könnte für das Identitätsverwaltungsmodell einem Modifizierungsbedarf unterliegen. Wenn weder durch exogene noch durch endogene Faktoren eine rein rationale Entscheidung gewährleistet werden kann und der Markt alleine den Schutz der informationellen Selbstbestimmung nicht regelt, bedarf es der Schutzmaßnahme über die Identitätsverwaltung.

Es könnte der Annahme nachgegangen werden, dass die rechtfertigende Einwilligung einem Legitimationsdefizit unterliege, wobei die Einwilligung im Außenverhältnis ihre vollständige Rechtfertigungswirkung beibehält. Und dies obwohl die Einwilligung das Ergebnis von Netzwerkeffekten sein kann und eine echte Auseinandersetzung mit den Verantwortlichen in Gestalt einer echten Wahlmöglichkeit ausgeblieben ist. Denn die Einwilligung sei geprägt von dem Interesse an der Nutzung und knüpft weniger an die bestehende Datenschutzqualität an, wodurch eine von dem Nutzungsvertrag unabhängige Einwilligung zur Datenverarbeitung ausbleibe.[570] Demnach wirkt sich die Einwilligung mit einem Legitimationsdefizit auf das Schutzniveau der generierten personalen Teilidentität in ihrem *Ipse*-Anteil aus. Denn nur mit einer vollständig bewussten Entscheidung über die Generierung neuer personaler Teilidentitäten, aus denen

568 *Veil*, NVwZ 2018, 686 (688).
569 *Cohen*, JTHTL 2012, 242 (249); *Solove*, Harv. L. R. 2013, 1880 (1888); *Graf von Westphalen*, IWRZ 2018, 9 (11).
570 *Becker*, JZ 2017, 170 (174 f.).

möglicherweise kontextübergreifend Erkenntnisse im Rahmen des Datenzyklus erlangt werden können, ist von ihrer Rechtfertigung und damit von ihrer Legitimität auszugehen.

Die Einwilligung mit einem Legitimationsdefizit könnte daher mit der Rechtsfigur der mutmaßlichen Einwilligung verglichen werden, die aber in der DSGVO nicht vorgesehen ist. Zugleich sieht Art. 4 Nr. 11 DSGVO die konkludente Einwilligung vor, deren Vorliegen sich auch nach der allgemeinen Verkehrsanschauung richtet. Gleichzeitig wurde von der Rechtsprechung die Konstruktion einer mutmaßlichen Einwilligung bei einem Suchmaschinenzugriff auf gespeicherte Fotos bei einer Plattform angenommen,[571] was jedoch als „dogmatische Krücke“[572] eingeordnet wird. Ob damit eine Kompensation des dogmatischen Defizits erfolgen kann, ist zweifelhaft, zumal die endogenen und exogenen Entscheidungsfaktoren nicht in die Einwilligungsdogmatik einbezogen werden. Demnach kann nach der bisherigen Rechtslage in der DSGVO zur Einwilligung das Legitimationsdefizit nicht kompensiert werden und es besteht weiterhin ein rechtlicher und tatsächlicher Ausgleichsbedarf.

Das Legitimationsdefizit könnte mit einem Konzept der Einwilligung ausgeglichen werden, welches eine Erweiterung in wenigstens granulare Wahlmöglichkeiten vorsieht. So könnte die Einwilligung in ein kompensatorisches Modell einer iterativen Identitätsverwaltung überführt werden. Mit diesem wäre die Einbuße des Schutzes über die personalen Identitäten in einem Datenzyklus auszugleichen, wenn dem Betroffenen über die datenschutzrechtliche Einwilligung hinaus ein Schutzmechanismus zur Verfügung gestellt wird. Dieser Schutzmechanismus würde in der iterativen Identitätsverwaltung liegen und weitere Einfluss- und Kontrollmöglichkeiten des Betroffenen vorsehen. Damit könnte das festgestellte Legitimationsdefizit über die Einwilligung auf der technischen Ebene mit einem *„layered approach“* kompensiert werden, was eine innovative und effektive technische Gestaltungsmöglichkeit darstellen würde.

In struktureller Hinsicht geht es bei der Identitätsverwaltung um die Einbeziehung der endogenen und exogenen Entscheidungsfaktoren bei der Einwilligungserteilung, da ein erweiterter Schutzbedarf besteht. Dieser Schutzbedarf kann aber nicht mit der Annäherung an ein eigentumsähnliches Verständnis über Daten und Informationen gelöst werden, wie bereits

571 OLG Köln, MMR 2011, 323.
572 *Spindler*, in: Verhandlungen des 69. Deutschen Juristentages, 2012, S. F 67.

nachgewiesen wurde.[573] Folglich erscheint die Identitätsverwaltung mit einer kontinuierlichen und dynamischen Kontrollmöglichkeit als eine geeignete Lösung. Dabei wären die endogenen und exogenen Entscheidungsfaktoren einzubeziehen, so dass die „*Priming*"-*Effekte* und die WYSIATI-Regel derart eingesetzt werden könnten, dass ein direkter Einblick in die generierten personalen *Ipse*- und *Idem*-Identitäten ermöglicht und die Risikobewertung für den Betroffenen damit erleichtert wird. Weiter könnten Markt- und Netzwerkeffekte zum Gegenstand von Informationspflichten werden oder in regelmäßigen Zeitabschnitten eine reaktivierende Warnung[574] über die Übermittlung von Daten, die Generierung neuer personaler Identitäten und Erkenntnisse erfolgen. Demnach könnte mit den iterativ erneuerbaren Einwilligungen[575] über den Datenzyklus einer personalen Identität das Legitimationsdefizit sukzessive kompensiert werden, was mit der Identitätsverwaltung erfolgen könnte.

In der Identitätsverwaltung kommt damit eine Steigerung der Kontrollmöglichkeit durch den Betroffenen zum Ausdruck. Gleichzeitig kann mit einer iterativ ausgestalteten Einwilligung in regelmäßigen Zeitabschnitten das Kontroll-Paradoxon wirken und langfristig zu einer Einbuße der informationellen Selbstbestimmung führen. Folglich könnte sich das iterative Identitätsverwaltungsmodell auf die Einwilligung und die personalen Identitäten direkt beziehen, die irreversibel aber im Datenzyklus erweiter- und veränderbar sind, da ein hohes Maß an Wahlmöglichkeiten[576] über die Einwilligung eingeräumt werden würde. Somit stellt die Einwilligung in normativer Hinsicht eine Öffnung für den Verhaltensspielraum durch

573 3. Teil, C, II., 1. Die ökonomische Perspektive spiegelt sich auch im angloamerikanischen System des „*contracting over privacy*" wider, in dem die Einwilligung einer Willenserklärung entspräche und eine Vereinbarung über die Datenverarbeitung geschlossen werde. In diesem Ansatz kommt das Verständnis von Daten als Tauschgegenstand zum Ausdruck, der negative Externalitäten gegenüber dem Schutz des öffentlichen Gutes der persönlichen Informationen zur Folge haben könnte, *Ben-Shahar/Strahilevitz*, The Journal of Legal Studies 2016, S1–S11.

574 *Faber/Sedlacek*, DuD 2017, 440 (443). Im Zusammenhang mit Standortdaten *Art. 29 Data Protection Working Party*, WP 185, Stellungnahme zu Geolokalisierungsdiensten von intelligenten mobilen Endgeräten (16. Mai 2011), S. 15.

575 *Spindler*, in: Verhandlungen des 69. Deutschen Juristentages, 2012, S. F 105–109; *Brandimarte/Acquisti/Loewenstein*, Social Psychological and Personality Science 4 (2013), 340; Zum Vorschlag eines *Double Opt-in*, *Hermstrüwer*, JIPITEC 2017, 9 (23) Rn. 55.

576 *Jay*, Data protection law and practice, 2012, Rn. 4–41, beschreibt das Phänomen als „*Degree of Choice*".

den Betroffenen dar. Gleichzeitig ist die Einwilligung begrenzt auf das kontextbezogene Wissen und Nichtwissen über die personalen Identitäten. Demnach führt eine uninformierte Entscheidung ebenso zu einer wirksamen Einwilligung über die Generierung personaler Identitäten.

Die Entscheidung über die Erteilung der Einwilligung ist folglich davon geprägt, dass der Betroffene die Informationen über die Datenverarbeitung einbezieht und dabei zugleich *kognitiven Verzerrungen* unterliegt, so dass die Legitimation der rechtfertigenden Einwilligung in der Vorstellung des Betroffenen, rational zu handeln, zu liegen scheint. Die Einwilligung kehrt sich von einer ursprünglich intendierten Bestätigung der informationellen Selbstbestimmung in eine „riskante Aktivität“[577] um.

f) Zwischenergebnis

Die rechtfertigende Einwilligung unterliegt der bereitwilligen Einwilligungserteilung aufgrund endogener und exogener Entscheidungsfindungsfaktoren. Daher lässt sich hinsichtlich der freiwilligen Entscheidungsfindung bei der Einwilligungserteilung ein Legitimationsdefizit feststellen. Gleichwohl entfaltet die Einwilligung im Außenverhältnis ihre vollständige Rechtfertigungswirkung. Folglich sind die verhaltensökonomischen Verzerrungsfaktoren bei der Entscheidungsfindung einzubeziehen und das Wirken der „*Priming*“-Effekte, „*Framing*“- und *Ankereffekte* sollte für die Identitätsverwaltung nutzbar gemacht werden.

Aufgrund der verbreiteten Einwilligungsbereitschaft und dem Schutzinteresse an der informationellen Selbstbestimmung lässt sich bei genauer Betrachtung nachweisen, dass sich die Einwilligung primär an Gratifikationen orientiert und nicht an dem Schutzinteresse der Privatheit, so dass das „*Privacy Paradox*“ in Frage steht. Folglich dient die Einwilligung im Außenverhältnis der informationellen Selbstbestimmung und im Innenverhältnis wirken kurzfristige Gratifikationsinteressen („Myopia“). Demnach könnte es eines differenzierten Schutzregimes bedürfen, um das Legitimationsdefizit der freiwilligen Einwilligung zu kompensieren. Dabei lässt sich an das Recht der allgemeinen Geschäftsbedingungen (AGB) denken. Denn im Recht der AGB trifft der Verbraucher mit dem Akzeptieren der AGBs eine riskante Entscheidung, die aber durch die Schutzvorschriften der §§ 305 ff. BGB kompensiert wird. Folglich könnte das AGB-Recht

577 *Hermstrüwer/Dickert*, Tearing the Veil of Privacy Law, 2013, S. 2.

für die Einwilligung in einem Identitätsverwaltungsmodell ebenfalls aufschlussreich sein.

2. AGB-Recht und Einwilligung

Das AGB-Recht kann durch das Nebeneinanderstehen von Nutzungsbedingungen eines Dienstes und datenschutzrechtlicher Einwilligung im engen Zusammenhang mit dem Datenschutzrecht stehen.[578] Der Vergleich zwischen der Einwilligung in die Datenschutzerklärung und der Zustimmung in die allgemeinen Geschäftsbestimmungen wird in der Literatur vielfach aufgegriffen.[579] In Anbetracht des Phänomens ungleicher Verhandlungspositionen im datenschutzrechtlichen Kontext, lässt sich das gleiche Phänomen als Regelungsgegenstand der §§ 305 ff. BGB feststellen. In beiden Kontexten stehen sich Verbraucher und Unternehmer mit einer ungleich verteilten Informationslage gegenüber, die über Transparenzregeln zu Beginn der Rechtsbeziehung kompensiert werden soll, indem der Verbraucher umfassend informiert wird, Art. 12, 13 DSGVO, § 305 Abs. 2 BGB.

Unter der Annahme, dass der Verbraucher die AGBs liest, müsste dieser nach der Interpretation und dem Verstehen des Inhaltes die Konsequenzen der AGB und seine fehlende Verhandlungsmacht feststellen können.[580] Gleichzeitig erscheint die Annahme einer rationalen Entscheidung, die AGB nicht zu lesen, ebenso naheliegend. Für das AGB-Recht wurde „der

578 LG Nürnberg-Fürth, Urt. v. 17.04.2018 – Az.: 7 O 6829/17: Nach diesem Urteil wurde die Datenschutzerklärung beanstandet, da aufgrund der akzeptierten AGB, die Nutzungsdaten an Dritte freigegeben wurden. In den AGB hieß es standardmäßig: „Ich möchte gefunden werden (...) von Personen, die nicht bei StayFriends sind bei Portalen mit Ehemaligenverzeichnissen bei öffentlichen Suchmaschinen (…) Wir zeigen Ihr Profilbild außerhalb von StayFriends und Sie können mit diesem Profilbild bei Suchmaschinen, wie z.B. Google, gefunden werden." Die allgemeine Einwilligung in die Datenschutzerklärung könne nicht zugleich die Zustimmung zur Veröffentlichung personenbezoger Daten sein.

579 *Becker*, JZ 2017, 170; *Hoffmann-Riem*, AöR 142 (2017), 1 (21 f.); *Hermstrüwer*, JIPITEC 2017, 9. Eine missbräuchliche Leistungsbeschreibung bei Unvereinbarkeit mit *privacy by design*-Grundsätzen wird als Verstoß gegen AGB-Recht anerkannt, vgl. *Wendehorst/Graf von Westphalen*, NJW 2016, 3745 (3749).

580 *Edwards/Veale*, Duke L. & Tech. Rev. 2017, 18 (67); *Solove*, Harv. L. R. 2013, 1880 (1886).

Mythos von der Möglichkeit zu lesen“[581] begründet, der sich auf die Datenschutzerklärungen übertragen lässt.[582] Damit wurde nachgewiesen, dass nur „exotische Individuen“[583] die AGB lesen würden und es insgesamt rationaler sei, die AGB nicht zu lesen. Dieses Phänomen wird vorliegend auch bei den Datenschutzerklärungen angenommen, denn das Lesen der Datenschutzerklärung würde keine signifikante Änderung mit sich bringen.[584] Lediglich würde der Betroffene nach dem Lesen feststellen können, dass es Änderungsbedarf oder Unklarheiten bei den Informationen in der Datenschutzerklärung gibt, um dann aber das Fehlen einer Verhandlungsposition festzustellen. Folglich könne die Lücke zwischen dem „Ideal der autonomen informierten Entscheidungswahl“ und der „Realität von Uninformiertheit“ durch Mechanismen des „*Ratings*“ und „*Labelns*“ von AGB eingesetzt werden,[585] die sich auch auf Datenschutzerklärungen übertragen ließen.

Im Recht der allgemeinen Geschäftsbedingungen wird über die *contra proferentem*-Regel nach § 305c Abs. 2 BGB die inhaltliche Kontrolle der AGB eröffnet, die zu einer teilweisen Unwirksamkeit gemäß § 306 BGB führen kann. Die datenschutzrechtlichen Informationspflichten sehen eine derartige Kontrolle nicht vor, obwohl die Verhandlungsmacht und die Informationen über die Datenverarbeitung ungleich verteilt sind, wie es bei dem Recht der AGB der Fall ist. Demnach hält *Hermstrüwer* eine *contra proferentem*-Regel im Datenschutzrecht für wünschenswert.[586] Ebenso könnten nach *Hoffmann-Riem* die im Recht der allgemeinen Geschäftsbeziehungen vorgesehenen Rechtsfolgen im Datenschutzrecht einbezogen werden, wonach rechtlich indizierte inhaltliche Restriktionen für Datenschutzerklärungen in Frage kämen.[587] Dabei könnten Datenschutzerklärungen in einem für den Betroffenen unvorteilhaften Kontext einer besonders kritischen Prüfung im Hinblick auf ihre Bestimmtheit unterliegen,[588] die ein mit §§ 307–309 BGB vergleichbares Regelungsregime umfassen würden. Eine weitergehende Differenzierung könnte den Regeln II 9:402–9:405 DCFR (*Draft Common Frame of Reference*) entnommen werden, in denen

581 *Ben-Shahar*, ERCL 2009, 1. Das fehlende Erklärungsbewusstsein bei der Einwilligung anerkennend, *Wendehorst/Graf von Westphalen*, NJW 2016, 3745 (3746 f.).
582 4. Teil, C., II., 1.
583 *Ben-Shahar*, ERCL 2009, 1.
584 *Veil*, ZD 2018, 9; *Veil*, NVwZ 2018, 686 (688).
585 *Ben-Shahar*, ERCL 2009, 1 (9).
586 *Hermstrüwer*, JIPITEC 2017, 9 (23) Rn. 53.
587 *Hoffmann-Riem*, AöR 142 (2017), 1 (21 f.).
588 *Kühling/Sackmann*, Rechte an Daten, 20. November 2018, S. 29 f.

der Rechtsbegriff „unfair" differenzierend zwischen B2C-, C2C- und B2B-Vertragsbeziehungen definiert wird. Eine entsprechende Differenzierung könnte im Datenschutzrecht für die kontextspezifische Wirksamkeit der Einwilligung herangezogen werden. Sofern das Recht der allgemeinen Geschäftsbedingungen als staatlicher Paternalismus eingeordnet wird, könnte nach einer Übertragung entsprechender Schutzmechanismen auf das Datenschutzrecht gefragt werden. Zudem wird festgestellt, dass das private Wirtschafts- und Verbraucherrecht von einer Diskussion über staatlichen Paternalismus geprägt und dies entsprechend im Datenschutzrecht kaum erkennbar sei.[589]

Neben einer dem AGB-Recht vergleichbaren rechtlichen Konkretisierung der Art. 12, 13 DSGVO kommen technische Gestaltungsmechanismen in Betracht. Diese können als „*reading agents*"[590] eingesetzt werden, mit denen die Entscheidungsfindung des Betroffenen durch einen Assistenten erleichtert wird. Ebenso kommen „*rating*"-Systeme in Betracht, bei denen die Datenschutzerklärungen vergleichbar zu Produktbewertungsportalen überprüft und bewertet werden können.[591]

3. Prozeduralisierte Einwilligung

Die Einwilligung stellt eine Prozeduralisierung der Rechtfertigung dar, denn mit ihr wird eine informierte Entscheidung vorgenommen und gleichzeitig wird mit der Einwilligung die informationelle Selbstbestimmung für die kontextbezogene Datenverarbeitung beschränkt.[592] Denn mit der Einwilligung wird die informationelle Selbstbestimmung ausgeübt, gleichzeitig wirkt diese für den Zeitpunkt der Einwilligung und für die personalen Identitäten mit den Erkenntnismöglichkeiten im Datenzyklus, ohne jedoch eine weitere Kontrollmöglichkeit vorzusehen. Daraus wurde ein legitimatorisches Defizit für die informationelle Selbstbestimmung begründet, welches mit einer erweiterten Prozeduralisierung durch die Identitätsverwaltung kompensiert und die Kontrolle über die personalen Identitäten wiederhergestellt werden könnte. Diese Prozeduralisierung

589 *Spiecker gen. Döhmann*, in: Vesting (Hrsg.), Der Eigenwert des Verfassungsrechts, 2011, 263 (278) mwN.
590 *Ben-Shahar*, ERCL 2009, 1 (19).
591 *Ders.*, ERCL 2009, 1 (22 f.).
592 2. Teil, A., I., 2., b).

könne in einer *iterativen Verhandlung*[593] bestehen, indem mit der Einwilligung des Betroffenen die Rechtsbeziehung zum Verantwortlichen nachverhandelt[594] wird. Dahingehend könnte einerseits die Verhandlung der Datenschutzerklärungen und andererseits die Einwilligungen über den *Ipse*-Anteil der personalen Identität umfasst sein.

Auf der Ebene der Datenschutzerklärung wird ein Austausch der Vorgaben einer Datenschutzerklärung auf syntaktischer Ebene zwischen dem Verantwortlichen und Betroffenen vorgeschlagen. Dabei erfolgt eine Prüfung, anschließend wird in einer weiteren Iteration eine Modifizierung ermöglicht, die in einer abschließenden Autorisierung der Datenschutzerklärung über statische Protokolle mündet.[595] Auf der Ebene der Einwilligung kommt für einen bestimmten Zeitraum der personalen Identität eine kontextspezifisch wirkende Einwilligung in Betracht, die mit dem „*layered approach*" erteilt werden könnte. Für den Betroffenen könnte die Nutzung über ein „*Dashboard*" erfolgen, in dem die Informationen über die personalen Identitäten und die dazugehörigen kontextspezifischen Transaktionen enthalten sind und zu denen dem Betroffenen der Zugang eingeräumt werden müsste. Das Konzept eines *Dashboard-Systems* wurde von *Raschke/Küpper/Drozd/Kirrane*[596] vorgeschlagen. Es soll die Betroffenenrechte zur Verfügung stellen, die Verwaltung der Rechte ermöglichen und unter der Prämisse der „*Usability*" gestaltet werden. Entsprechend würde die Einbeziehung von Transparenzmethoden für die Informationspflichten und die anschließenden Betroffenenrechte, insbesondere das Auskunftsrecht, dazu gehören. Nach dem vorgeschlagenen Konzept bedarf es eines Zugangs für alle Betroffenen und der Visualisierung von Datenflüssen mit ihren jeweiligen Datenverarbeitungszwecken, damit die Betroffenenrechte ausgeübt werden können. In diesem Konzept werden die Datenschutzprinzipien mit den Rechten des Betroffenen vereint, so dass das Schutzregime über ein technisches Verfahren erfolgen würde.[597]

Für die Identitätsverwaltung erscheint ein *Dashboard-System* als ein geeignetes technisches Verfahrenssystem, da gerade auf der Visualisierungsebene neben den Datenflüssen die personalen Identitäten transparent ge-

---

593 2. Teil, A., II., 1., d).

594 *Jay*, Data protection law and practice, 2012, Rn. 6–39, „renegotiate the terms of that relationship".

595 *Birnstill/Beyerer*, in: ACM-PETRA 2018, 292.

596 *Raschke/Küpper/Drozd u.a.*, in: Hansen/Kosta/Nai-Fovino u.a. (Hrsg.), Privacy and Identity Management, 2017, 221.

597 *Dies.*, in: Hansen/Kosta/Nai-Fovino u.a. (Hrsg.), Privacy and Identity Management, 2017, 221 (226).

macht werden können und damit der absoluten Kontrolle für die weitere Datenverarbeitung unterliegen würden. Dieses *Dashboard-System* würde zunächst an den Zeitpunkt *ex ante* zur Rechtfertigung anknüpfen und zugleich die Möglichkeit der kontextbezogenen rechtfertigenden Einwilligung umfassen. Insgesamt könnte der Betroffene im Sinne einer „*guided tour*"[598] mit einem *Dashboard-System* durch seine personalen Identitäten und Rechte nach der DSGVO geführt werden, womit ein Verfahren zur iterativen Realisierung der rechtfertigenden Einwilligung vorliegen würde.

4. Paternalistische Intervention?

Es kommt für die Kompensation des Legitimationsdefizits personaler Identitäten die paternalistische Intervention als „*opacity tool*" zum Schutz des Betroffenen in Betracht. Unter der Annahme, dass die rationale Zielverfolgung der natürlichen Person mit der neuen Erwartungstheorie unhaltbar scheint, ließe sich eine paternalistische Regelung vergleichbar mit der Verpflichtung, sich anzuschnallen gemäß § 21a StVO,[599] zum Schutz des Betroffenen vor irrationalen Entscheidungen bei der Entschließung für die Einwilligung in Erwägung ziehen. Es kommt eine Regelung in Betracht, die vor den Verzerrungsfaktoren bei der Entscheidungsfindung mit den spezifischen Risikolagen aufgrund der fehlenden Haptik von Datenverarbeitungsprozessen schützt und die Verhandlungsmacht des Verantwortlichen durch normative Intervention beschränkt.

Eine solche Regelung würde den Betroffenen vor sich selbst schützen können, zugleich aber eine tiefgreifende und mit den Annahmen einer freiheitlichen Entscheidungsfindung kaum zu vereinbarende Intervention darstellen.[600] Damit kommt ein Kompensationsmechanismus auf der Gestaltungsebene in Betracht, wonach mit Hilfe von „*Interface Design*" die bewußte Entscheidung im Rahmen der informationellen Selbstbestimmung gefördert wird. Hierbei wäre eine Kanalisierung und Beschränkung der Wahlmöglichkeiten denkbar, so dass damit der anvisierte Effekt herbeigeführt wird, einen besseren Schutz für die informationelle Selbstbestimmung zu generieren.[601] Infolgedessen könnte durch das Richten der Aufmerksamkeit auf die Veröffentlichungsrisiken eine Steigerung des Schut-

598 *Spindler*, in: Verhandlungen des 69. Deutschen Juristentages, 2012, S. F 108.
599 *Eidenmüller*, JZ 2011, 814 (815).
600 *Ders.*, JZ 2011, 814 (815) Fn. 13.
601 *Schneider/Weinmann/Vom Brocke*, Communications of the ACM 2018, 67 (71).

zes bewirkt und damit die Einwilligungsbereitschaft minimiert werden.[602] Der Betroffene könnte auch zu entsprechenden Vorsichtsmaßnahmen nach der Einwilligung animiert werden.

Für das Identitätsverwaltungsmodell erscheint die Abstufung der Einwilligungen über die personalen Identitäten in dem jeweiligen Kontext vorzugswürdig. Dabei könnte durch „*Nudging*" die Aufmerksamkeit auf endogene Verzerrungsfaktoren gelenkt werden und eine risikobewusste Entscheidung des Betroffenen für die Einwilligung zu einer bestimmten personalen Teilidentität erleichtert werden. Folglich könnte die iterative Identitätsverwaltung derart ausgestaltet sein, dass sie die Aufmerksamkeit auf die Kontrollierbarkeit der generierten personalen Identitäten richtet. Hierfür kann das *Dashboard-System* eingesetzt werden, welches eine Gesamtschau über die personalen Identitäten und zugleich die Ausübung der Rechte des Betroffenen ermöglicht. In diesem *Dashboard-System* können die Informationen über die Datenverarbeitungen und die entstandenen personalen Identitäten derart ausgestaltet sein, dass der Betroffene einen Anstoß zu möglichst risikobewussten Entscheidungen erfährt. Demnach würde das „*Nudging*" sich auf der technischen Gestaltungsebene vollziehen, da auf der rechtlichen Ebene eine paternalistische Intervention in einer Differenzierung der Einwilligungsregeln gemäß Art. 6 Abs. 1 a), 4 Nr. 11 DSGVO liegen und die Anforderung einer „risikobewussten Einwilligung" voraussetzen würde. In Anbetracht des Abstraktionsgrades von Rechtsnormen und dem bereits bestehenden Erfordernis, dass die Einwilligung eine informierte freiwillige Entscheidung voraussetzt, wirkt eine solche Regelungserweiterung wenig zielführend für die Steigerung des Schutzniveaus der informationellen Selbstbestimmung.

Somit erscheint ein Kompensationsmechanismus mit Anreizen und „*Nudging*" auf der technischen Gestaltungsebene naheliegend, wenn diese derart ausgestaltet werden, dass sie unterstützend wirken und nicht zum Schaden der Rechte und Freiheiten des Betroffenen führen. Demnach kann das *Dashboard-System* als ein *ex ante*-Kompensationsmechanismus eingesetzt werden, welcher der technischen Gestaltung des Verantwortlichen oder Herstellers unterliegt. Gleichwohl müsste ein rechtlicher Anreizmechanismus geschaffen werden, damit der Verantwortliche und der Hersteller dazu gehalten werden, die technische Gestaltung über ein *Dashboard-System* vorzunehmen. Dies könnte mit einer Regelung im Produkthaf-

602 *Acquisti*, IEEE Security & Privacy Magazine 2009, 72 (74).

tungsrecht und einer Erweiterung des Art. 25 DSGVO mit einem „*identity management by design*"-Konzept erfolgen.[603]

Insgesamt müsste bei der Implementierung eines *Dashboard-Systems* das Kontroll-Paradoxon einbezogen werden, da die Steigerung der Einflussmöglichkeiten des Betroffenen langfristig zu einem Absenken des Schutzes der informationellen Selbstbestimmung führen kann. Folglich erscheint bei einer Identitätsverwaltung über ein *Dashboard-System* eine ausgeglichene Einbeziehung von Kontrollmöglichkeiten, „*Nudging*" und automatisierten Darstellungen erforderlich, um übermäßige Kontrollmöglichkeiten zu vermeiden. Auf diese Weise würde das *Dashboard-System* als eine technische Gestaltungsform zur Kompensation von endogenen und exogenen Einflüssen bei der Einwilligung dienen können. Dabei würde das *Dashboard-System* als „*opacity tool*" und zugleich als „*transparency tool*" fungieren.

5. Ergebnis

Die Identitätsverwaltung mit der informierten freiwilligen Einwilligung unterliegt Verzerrungsfaktoren auf der endogenen und der exogenen Ebene, durch die ein Legititimationsdefizit bei der Einwilligung entstehen kann. Mit der vorliegend vertretenen Darstellung bedarf es der Kompensation dessen durch rechtliche oder technische Maßnahmen. Auf der technischen Ebene könnten aufgrund von verbreiteten Einwilligungsabfragen „*Reading Agents*" eingesetzt werden, mit denen der Betroffene einen Assistenten zur Risikobewertung und Entscheidungsfindung erhalten würde. Dabei könnten auch „*Rating*"-Systeme über das Vergleichsergebnis mit mehreren Datenschutzerklärungen hinzugezogen werden, die bei der Entscheidungsfindung unterstützend wirken. Ebenso könnten aufgrund der Verzerrungsfaktoren bei der Entscheidungsfindung „*Nudging*"-Strukturen zur „Steuerung der Selbststeuerung"[604] einbezogen werden, die zu einer Steigerung des Bewusstseins über endogene und exogene Faktoren führen könnten. Dafür wäre ein *Dashboard-System* geeignet, um die erforderliche Transparenz für die kontextspezifischen Einwilligungen über die personalen Identitäten herbeizuführen, und um eine risikobewusste Entscheidungsfindung zu ermöglichen. Maßgeblich dabei wäre eine iterative Aus-

603 4. Teil, B., IV.; zu einem „*anti-discrimination by design*" vgl. *Wischmeyer*, AöR 143 (2018), 1 (29).

604 *Zippelius*, Das Wesen des Rechts, 2012, S. 34.

gestaltung, damit für den Datenzyklus der personalen Identität die Kontrolle regelmäßig ausgeübt werden kann. Um dem Kontroll-Paradoxon gerecht zu werden, bedarf es eines ausgewogenen Verhältnisses zwischen der absoluten Kontrolle über die Einwilligung mit einer echten Wahlmöglichkeit und den darauffolgenden iterativen Einwilligungsmöglichkeiten. Damit könnte eine kontextspezifische absolute Kontrolle über die personale Identität, iterativ auf den Datenzyklus verteilt, ausgeübt werden, so dass eine Bewusstseinssteigerung für den Schutz der personalen Identität herbeigeführt wird.

Insgesamt wirkt sich die Gestaltung der Einwilligungsstruktur auf den anzuwendenden Stand der Technik im Identitätsverwaltungsmodell aus und sollte auf die Dienste und das Internet der Dinge übertragen werden. Ebenso könnten bei der technischen Gestaltung für die Identitätsverwaltung die Rechtfertigungsgründe gemäß Art. 6 Abs. 1 b) – f) DSGVO einbezogen werden. Sobald eine gerechtfertigte Datenverarbeitung erfolgt, könnten die Rechtfertigungsgründe transparent über das *Dashboard-System* hinsichtlich der generierten personalen Identitäten einsehbar sein. Folglich könnten die Rechtfertigungsgründe gemäß Art. 6 Abs. 1 b) – f) DSGVO ebenso zum Gegenstand des Identitätsverwaltungsmodells werden.

III. Identitätsverwaltung ohne aktive Handlung des Betroffenen, Art. 6 Abs. 1 b) – f) DSGVO

Die Rechtfertigung für die Datenverarbeitung im Rahmen der Identitätsverwaltung kann ohne aktive Handlung des Betroffenen erfolgen. Damit mangelt es zunächst an der Kontrolle für die Begründung der Rechtfertigung und die Kontrollmöglichkeit beschränkt sich auf die Kenntnisnahme der transparenten Datenschutzerklärung und ihre Einbeziehung in die Entscheidungsfindung. Demnach kann *ex post* zur Rechtfertigung ein gesteigerter Bedarf an Identitätsverwaltung bestehen, um das Kontrolldefizit zu einem späteren Zeitpunkt des Datenzyklus zu kompensieren.

Die Rechtfertigung gemäß Art. 6 Abs. 1 b) – d) DSGVO knüpft jeweils an der Erforderlichkeitsprüfung durch den Verantwortlichen in variierender Prüfungsintensität an. Indem die Erforderlichkeitsprüfung im Verbotsvorbehalt wurzelt, verlangt die Rechtfertigung mit der Erforderlichkeit

eine gewisse Alternativlosigkeit der Datenverarbeitung.[605] Mit der Rechtfertigungsprüfung durch den Verantwortlichen erfolgt eine implizite Risikobewertung in der Erforderlichkeit, da die konkreten Umstände der Identitätsverwaltung und der Zweck der Datenverarbeitung einbezogen werden müssen.[606] Etwa im Beschäftigtendatenschutzrecht kann gemäß Art. 88 DSGVO i. V. m. § 26 BDSG die Datenverarbeitung für die Durchführung der Beschäftigung gerechtfertigt sein, was die Begründung, die Durchführung und die Beendigung der Beschäftigung umfasst, wenn die Datenverarbeitung aufgrund der beschäftigungsspezifischen Interessen erforderlich ist.

Die Abgrenzung im Einzelnen, wann die Rechtfertigung über die Einwilligung oder die Erforderlichkeit zu erfolgen hat, richtet sich nach dem Vorliegen oder dem Fehlen eines Entscheidungsspielraumes für den Betroffenen. Sobald kein Entscheidungsspielraum zur Verfügung steht, spricht dies für die Erforderlichkeit der Datenverarbeitung, wohingegen beim Bestehen eines granularen Entscheidungsspielraumes die Rechtfertigung nach Art. 6 Abs. 1 a) DSGVO für vorzugswürdig gehalten wird.[607] Die Definitionsmacht über die Bestimmung, wann ein Entscheidungsspielraum beim Betroffenen besteht, obliegt dem Verantwortlichen, so dass die Erwägungen über die Bestimmung des geeigneten Rechtfertigungsgrundes für den Betroffenen undurchsichtig sind. Der Betroffene verbleibt mit der Feststellung über das Bestehen einer Einwilligungsmöglichkeit oder dem Fehlen dieser.

Die mit dem öffentlichen Interesse gerechtfertigte Datenverarbeitung bringt das Fehlen eines Entscheidungsspielraums besonders deutlich zum Ausdruck. Danach besteht kein Raum für die Freiwilligkeit der betroffenen Person, sondern wegen des öffentlichen Interesses oder der Ausübung öffentlicher Gewalt kann die Datenverarbeitung als erforderlich eingeordnet werden, Art. 6 Abs. 1 e) DSGVO. In dem *Dashcam*-Urteil des Bundesgerichtshofes[608] wurden aufgrund des überwiegenden Beweisinteresses des Staates an einer funktionierenden Zivilrechtspflege die *Dashcam*-Aufnahmen im Straßenverkehr auch ohne Einwilligung als gerechtfertigt angesehen. Die informationelle Selbstbestimmung trat in der Gesamtabwägung

605 *Buchner/Petri*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 6 DSGVO Rn. 15.
606 4. Teil, B., II., 2., a), bb).
607 www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/ (Zuletzt aufgerufen 20.06.2020).
608 BGH, Urt. v. 15.05.2018 – VI ZR 233/17.

zurück. Darin kommt deutlich zum Ausdruck, dass bei Bestehen eines öffentlichen Interesses die Wahlmöglichkeit des Betroffenen ausgeschlossen ist und die Rechtfertigung der Datenverarbeitung mit der Erforderlichkeit eintritt. Für die Identitätsverwaltung bedeutet dies, dass mit einer Rechtfertigung über das öffentliche Interesse gemäß Art. 6 Abs. 1 e) DSGVO die freiwillige Entscheidung und die Kontrollmöglichkeit des Betroffenen ausbleibt und diese zu einem späteren Zeitpunkt im Datenzyklus erfolgt. Demnach ist das Identitätsverwaltungsmodell nicht auf die Kontexte beschränkt, bei denen eine Einwilligungsmöglichkeit besteht, sondern erstreckt sich auf sämtliche Rechtfertigungsgründe. Die Kontrollmöglichkeit über die personalen Identitäten besteht dann *ex ante* zur Rechtfertigung auf der Ebene der Transparenz und *ex post* zur Rechtfertigung bei den Betroffenenrechten.

Eine vergleichbare Sachlage erscheint ebenso bei der Rechtfertigung über das berechtigte Interesse gemäß Art. 6 Abs. 1 f) DSGVO. Dieser Erlaubnistatbestand tritt in der Rechtsbeziehung zwischen Verbraucher und Unternehmer als ein verbreiteter Rechtfertigungsgrund[609] auf, da er aus der Perspektive des Verantwortlichen vorzugswürdig ist und in der Umsetzung allein die dokumentierte Begründung vom Verantwortlichen verlangt. Gemäß Art. 6 Abs. 1 f) DSGVO muss das berechtigte Interesse zugleich ein legitimes Interesse sein, welches im Einklang mit nationalem und europäischem Recht steht. Die Bestimmung des legitimen Interesses ist ebenso Gegenstand einer Abwägung, die unter Einbeziehung des risikobasierten Ansatzes erfolgt und einer eigenständigen Risikobewertung unterliegt.[610] Denn mit der Identifikation eines hohen Risikos bei der Datenverarbeitung geht ein gesteigertes Rechtfertigungsbedürfnis einher, welches zu einem Einwilligungserfordernis führen kann. Somit kommt die Rechtfertigung über das berechtigte Interesse allein bei solchen Datenverarbeitungen in Betracht, die mit einem geringen Risiko für die Rechte und Freiheiten natürlicher Personen verbunden sind. Weiter müssen die Datenverarbeitungen, die auf dem legitimen Interesse basieren, von der „vernünftigen Erwartung" des Betroffenen gedeckt sein, so dass unvorhersehbare und überraschende Datenverarbeitungen ausgeschlossen sind, EWG 47 S. 1. Die Voraussetzung für das Vorliegen der Datenverarbeitung im Rahmen der vernünftigen Erwartung lässt sich vergleichen mit der *contra*

609 *Herfurth*, ZD 2018, 514.

610 *Quelle*, European Journal of Risk Regulation 2018, 502 (515); *Art. 29 Data Protection Working Party*, WP 217, Opinion 6/2014 on the notion of legitimate interest of the data controller (9. April 2014), S. 33–37.

proferentem-Regel aus dem Recht der allgemeinen Geschäftsbedingungen gemäß § 305c Abs. 2 BGB, wonach Zweifel bei der Auslegung zu Lasten des Verwenders gehen. Übertragen auf die datenschutzrechtliche Rechtfertigung mit dem berechtigten Interesse würde die Rechtfertigung einer Datenverarbeitung außerhalb der vernünftigen Erwartung zu Lasten des Verantwortlichen gehen und möglicherweise einen sanktionsbewehrten Sachverhalt begründen.

Dennoch ist mit der Abwägungsverantwortung des Verantwortlichen eine erhebliche Gestaltungsmacht verbunden, die zu einer Verfestigung von Verhandlungsungleichgewichten und bestehenden Informationsasymmetrien beitragen kann. Denn die Abwägung erfolgt in der Vorbereitung zur Datenverarbeitung und nur das Abwägungsergebnis wird für den Betroffenen erkennbar, was die bestehende Informationsasymmetrie verstärkt. Folglich erlangen die Informationspflichten bei der Rechtfertigung mit dem berechtigten Interesse ebenso ein gesteigertes Gewicht, indem die Informationen der alleinige Anknüpfungspunkt für die Kontrolle durch den Betroffenen sind. Dabei können von den Informationspflichten die Benennung des berechtigten Interesses und darüber hinaus die Einbeziehung des Abwägungsvorgangs zur Begründung des berechtigten Interesses erfasst sein, was im Einzelnen aber umstritten ist.[611] Insgesamt kommt in der Rechtfertigung über das berechtigte Interesse wegen der vorangegangen Abwägung erneut der prozedurale Charakter im Datenschutzrecht zum Ausdruck.

Die Rechtfertigung der Datenverarbeitung für die Identitätsverwaltung kann ohne aktive Handlung durch den Betroffenen erfolgen. Die Rechtfertigung ergibt sich dabei aus der Erforderlichkeit, dem öffentlichen Interesse und dem berechtigten Interesse über die Datenverarbeitung. Jeweils obliegt die Entscheidung und Abwägung zur Identifikation des bestehenden Rechtfertigungsgrundes dem Verantwortlichen. Dabei tritt das *Konzept des Selbstdatenschutzes* aufgrund der fehlenden aktiven Handlung des Betroffenen zurück, verlangt aber gleichzeitig für die Wahrung der informationellen Selbstbestimmung eine restriktive Auslegung der Rechtfertigungsgrundlage.[612] Insgesamt kommt in diesen Rechtfertigungsgründen eine Verfestigung des bestehenden Verhandlungsungleichgewichts und der Informationsasymmetrie zum Ausdruck. Die Folge kann eine Steigerung der Marktmacht sein und langfristig kann die Rechtfertigung der Datenverar-

611 *Veil*, NJW 2018, 3337 (3339).

612 *Roßnagel*, in: Roßnagel/Abel (Hrsg.), Handbuch Datenschutzrecht, 2003, 3.4. Rn. 13.

beitung mit dem berechtigten Interesse zu einer marktbeherrschenden Stellung von Intermediären beitragen.

Den Rechtfertigungsgründen ohne Zutun des Betroffenen ist gemein, dass sie keine Grundlage für die aktive kontrollierte Identitätsverwaltung durch den Betroffenen ermöglichen. Vielmehr können durch die Datenverarbeitungen personale Identitäten generiert werden, die erst nach der Rechtfertigung auf der *ex post*-Ebene der Betroffenenrechte zum Gegenstand der Kontrolle werden können. Entsprechend ist in einem Identitätsverwaltungsmodell auf der Ebene der Transparenz über die Datenverarbeitung und anschließend der Transparenz über die generierten personalen Identitäten die Kontrolle einzuräumen, damit das Kontrolldefizit auf den Ebenen *ex ante* und *ex post* zur Rechtfertigung ausgeglichen werden kann.

IV. Zusammenfassung

Das Rechtfertigungserfordernis für die Identitätsverwaltung wurzelt in dem Verbot mit Erlaubnisvorbehalt und setzt das Vorliegen eines Rechtfertigungstatbestandes für die Verwaltung der personalen Identitäten voraus. Das Verbotsprinzip wird in seiner Funktionalität bei der Datenverarbeitung im Verhältnis zwischen Staat und Bürger deutlich, wonach eine Ermächtigungsgrundlage für die staatliche Datenverarbeitung gegeben sein muss. In diesem Subordinationsverhältnis können personale Identitäten ohne aktive Handlung durch den Betroffenen begründet werden. Gleichzeitig gilt das Verbotsprinzip für die Rechtsbeziehung zwischen Privaten ungeachtet dessen, ob es sich um eine P2C-, B2B-, B2C- oder C2C-Rechtsbeziehung handelt. Zwar lässt sich in der B2C-Rechtsbeziehung eine zum Subordinationsverhältnis vergleichbare Asymmetrie feststellen, jedoch kann die grundrechtliche Abwehrdimension gegenüber staatlichen Eingriffen schwerlich auf die Rechtsbeziehung Privater übertragen werden. Diese ist von der mittelbaren Drittwirkung der Grundrechte geprägt, durch die eine einfachrechtliche Kompensation von ungleichen Verhandlungspositionen erfolgen könnte.

Weiter könnte die paternalistische Schutzwirkung des Verbotsvorbehaltes in Frage gestellt werden, denn es konnte nachgewiesen werden, dass mit der Einwilligung keine Bestätigung oder Steigerung der informationellen Selbstbestimmung einhergeht. Vielmehr ist die Realität davon geprägt, dass die Einwilligung ohne umfassende Kenntnisnahme der Datenschutzerklärung erteilt wird und das Interesse des Betroffenen an unmittelbaren Gratifikationen überwiegt. Somit scheint mit dem Verbotsvorbehalt eine

vermeintliche Kontrollmöglichkeit über die rechtfertigende Einwilligung zu bestehen, mit der generierte personale Identitäten über den Datenzyklus hinweg vermeintlich kontrollierbar sind.

Auch aus verhaltensökonomischer Perspektive kann das Verbotsprinzip in seiner Wirkung angezweifelt werden, denn dieses lässt sich als eine Ausprägung des aus amerikanischer Perspektive vorherrschenden Vorsichtsprinzips in Europa[613] einordnen. Danach soll mit dem Vorsichtsprinzip grundsätzlich das Schadensrisiko vermieden werden, obwohl das datenschutzrechtliche Verbotsprinzip nicht zwingend zu einem gesteigerten Schutz für die informationelle Selbstbestimmung und damit zur Schadensminderung führt. Daraus könnte sich eine Beschränkung des Verbotsprinzips auf den öffentlich-rechtlichen Kontext ableiten lassen, so dass im privatrechtlichen Kontext die Datenverarbeitung der einfachrechtlichen Ausgestaltung unterliegen würde. Ferner kommt als weiche paternalistische Intervention die Implementierung eines Identitätsverwaltungsmodells in Betracht, mit dem das legitimatorische Defizit der Einwilligung kompensiert werden kann. Dabei könnte in rechtlicher und technischer Hinsicht ein *Dashboard-System* als Lösung fungieren.

Die Risiken aufgrund des legitimatorischen Defizits der Einwilligung durch die endogenen und exogenen Entscheidungsfaktoren können in einem *Dashboard-System* mit Transparenzanforderungen, Zugangsrechten und der rechtfertigenden Einwilligung gebündelt werden. Ebenso kommen *„reading agents"* für den Betroffenen in Frage, um die maßgeblichen Informationen für die Identitätsverwaltung aus den Datenschutzerklärungen extrahieren zu können. Weiter könnte das *Dashboard-System* leichte Anreizmechanismen in Gestalt von *„Nudging"* enthalten, da spiegelbildlich zu den Anreizmechanismen über die Einwilligungserteilung ein Schutzmechanismus für die personalen Identitäten erforderlich ist. Dieses paternalistische *„Nudging"* müsste mit der Prämisse ausgestaltet sein, dass die Privatheitspräferenzen und die kontextspezifischen Risiken gegenüber personalen Identitäten tatsächlich in der Entscheidungsfindung einbezogen werden. Damit müssten die Datenschutzerklärungen als Konzept neu definiert werden und möglicherweise Gegenstand einer *iterativen Verhandlung* werden. Auf diesem Wege würde der prozeduralisierten Rechtfertigung entsprochen werden und diese könnte in ein prozedural geprägtes Identitätsverwaltungsmodell überführt werden.

Sobald die Rechtfertigung ohne aktive Handlung durch den Betroffenen erfolgt, kommt ein eigenständiger rechtlicher Schutzmechanismus gegen-

613 *Kahneman*, Schnelles Denken, langsames Denken, 2012, S. 432.

über nachteiligen Bestimmungen in den Datenschutzerklärungen in Betracht, der parallel zu den Schutzregelungen im Recht der allgemeinen Geschäftsbedingungen ausgestaltet sein könnte. Dieser kann in einer datenschutzrechtlichen *contra proferentem*-Regel liegen, mit der die Spezifika der Informationsasymmetrien über ein differenziertes Regelungsregime für P2C-, B2B-, B2C- und C2C-Rechtsbeziehungen einbezogen werden. Damit könnte eine Kompensation des Verhandlungsungleichgewichtes und der Informationsasymmetrie erfolgen. Gerade bei der Rechtfertigung ohne aktive Handlung des Betroffenen erscheint eine Verfestigung des Ungleichgewichts möglich, so dass die Kontrolle *ex ante* aufgrund der Informationspflichten und *ex post* zur Rechtfertigung auf der Ebene der Betroffenenrechte erfolgen würde.

D. Ex post Rechtfertigung personaler Identitäten in der DSGVO

Die Identitätsverwaltung *ex post* zur Rechtfertigung verlangt zunächst einen Einblick des Betroffenen in die personalen Identitäten aus den Datenverarbeitungen, wozu das Auskunftsrecht gemäß Art. 15 DSGVO dient (I.). Mit der Kenntnis über die personalen Identitäten wird der Abgleich im Rahmen des Rechts auf informationelle Selbstbestimmung ermöglicht, was die Grundlage für die Entscheidung über das geeignete Betroffenenrecht zur Wiedererlangung der Kontrolle über die personalen Identitäten ist. Dies lässt sich insbesondere über das Recht auf Löschung gemäß Art. 17 DSGVO (II.) und das Recht auf Datenübertragbarkeit gemäß Art. 20 DSGVO vornehmen (III.). Weiter kann zu einem späteren Zeitpunkt des Datenzyklus der Bedarf nach Transparenz und Kontrolle bei einem Datenschutzverstoß (IV.) und dem Recht auf Kontrolle bei automatisierten Entscheidungen entstehen (V.). Als zeitlich letztes Recht des Betroffenen kommt die Geltendmachung eines gerichtlichen Rechtsbehelfs wegen eines materiellen oder immateriellen Schadens gemäß Art. 79 DSGVO in Betracht (VI.).

I. Auskunft als Zugangsrecht für die Identitätsverwaltung, Art. 15 DSGVO

Das Recht auf Auskunft ist in Art. 8 Abs. 2 S. 2 GRC primärrechtlich verankert und stellt die Voraussetzung zur informierten Ausübung der Betroffenenrechte dar. In dem Recht auf Auskunft gemäß Art. 15 DSGVO liegt

die Vorstufe in Gestalt der Informationsbeschaffung, mit der die Entscheidung über die Notwendigkeit der Ausübung eines Betroffenenrechts und die Entscheidung über die Wahl des geeigneten Betroffenenrechts ermöglicht werden. Dabei lässt sich das Auskunftsrecht zugleich als Zugangsrecht einordnen, wie es bereits die englischsprachige Überschrift des Art. 15 DSGVO als „*right of access by the data subject*" mit der Übersetzung des Begriffs „*access*" als Zugang[614] nahelegt. Mit dem Verständnis des Auskunftsrechts als Zugangsrecht erlangt dieses die Funktion eines Rechts zur absoluten Kontrolle der personalen Identitäten.

Die Voraussetzung für eine wirksame Identitätsverwaltung ist zunächst der Zugang zu den Daten im Rahmen der Auskunft, um anschließend *ex post* zur Rechtfertigung eine Entscheidung über die Ausübung der Betroffenenrechte vornehmen zu können. Auf diese Weise wird die Steuerungsmöglichkeit über die personalen Identitäten im Datenzyklus über Art. 15 DSGVO zurückerlangt und kann in regelmäßigen „angemessenen Abständen" ausgeübt werden, EWG 63 S. 1. Von dem Recht auf Auskunft sind die spiegelbildlichen Informationen aus den Informationspflichten gemäß Art. 12 DSGVO erfasst. Sie sollen dem Betroffenen der wirksamen Ausübung seiner Betroffenenrechte nach der Rechtfertigung dienen. Dabei hat der Verantwortliche eine Kopie der personenbezogenen Daten zur Verfügung zu stellen, woraus sich die Pflicht zur Bündelung der personenbezogenen Daten ableiten lässt, die bereits bei der Planung der technischen und organisatorischen Maßnahmen einzubeziehen ist. Die Ausübung des Auskunftsrechts verlangt zunächst die Authentifizierung des Betroffenen gemäß Art. 12 Abs. 6 DSGVO und umfasst, ob eine Datenverarbeitung stattgefunden hat und welche Daten verarbeitet wurden.

In einem Identitätsverwaltungsmodell mit der technischen Ausgestaltung eines *Dashboard-Systems* kann das Auskunftsrecht unmittelbar zwischen dem Betroffenen und Verantwortlichen wirken. Gleichzeitig ließe sich eine kontextspezifische Erweiterung in Erwägung ziehen, die den Zugang zu einer personalen Identität ermöglicht und diese in anderen Kontexten einsetzbar wäre. Dafür könnte das *Dashboard-System* als iterative Zu-

614 Die Übersetzung des Begriffs „*right of access*" entspricht einem Zugangsrecht. Demgegenüber ist in der deutschen Fassung der DSGVO von einem Auskunftsrecht die Rede, welches auch mit „*the right to information*" übersetzt werden oder dem „*right to be informed*" gleichgesetzt werden kann. Ebenso verwendet die Datenschutzaufsichtsbehörde in England den Begriff des „*right of access*", www.ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/ (Zuletzt aufgerufen 20.06.2020).

gangs- und Kontrollmöglichkeit mit der Maßgabe dienen, dass die tatsächliche Ausübung des Auskunftsrechts erleichtert wird. Dabei würde das Auskunftsrecht erweitert werden und zur Einräumung eines Zugangsrechts als Kontrollmöglichkeit führen.

Insgesamt offenbart sich das Auskunftsrecht als Transparenzerfordernis *ex post* zur Rechtfertigung und kann durch den Verantwortlichen auch als vertrauensbildende Maßnahme gegenüber dem Betroffenen eingesetzt werden. Denn mit der Kenntnis des Betroffenen über seine personalen Identitäten nach der Rechtfertigung, wird eine reale Kontroll- und Gestaltungsmöglichkeit eingeräumt, die die Bereitschaft zur Fortsetzung der Datenverarbeitung unter den bisherigen Datenverarbeitungsbedingungen steigern kann.

II. Löschungsrecht zur Identitätsverwaltung, Art. 17 DSGVO

Das Löschungsrecht für die Identitätsverwaltung ist als Gegenrecht zur Einwilligung und ihren Konsequenzen im Datenzyklus einzuordnen, da mit der Geltendmachung des Rechts die Datenverarbeitung und ihre Folgen im Datenzyklus der personalen Identität beendet werden können. Der Ursprung des Löschungsrechts geht zurück auf das *Google Spain*-Urteil des EuGHs[615], in dem ein Recht auf Vergessenwerden für den online-Kontext begründet wurde. Dieses Recht auf Vergessenwerden wurde nunmehr vom Bundesverfassunsgsgericht[616] für die nationalen Grundrechte anerkannt und konkretisiert.

Mit dem Recht auf Vergessenwerden aus Art. 17 DSGVO besteht *ex post* zur Rechtfertigung die Möglichkeit, dass ein bestehendes Legitimationsdefizit der Einwilligung mit der Löschungsmöglichkeit personaler Identitäten ausgeglichen wird. Ebenso kann ein vorangegangenes Kontrolldefizit durch die Löschung der Datensätze zur personalen Identität kompensiert und damit die Kontrolle zurückerlangt werden. Weiter können mit dem Recht auf Vergessenwerden und dem Recht auf Datenportabilität zu einem späteren Zeitpunkt im Datenzyklus die Wirkungsfolgen der endogenen und exogenen Entscheidungsfaktoren ausgeglichen werden.[617] Dazu gehört die Kompensation der Einwilligungsfolgen in den sozialen Medien,

615 EuGH, Urt. v. 13.05.2014 – C-131/12, Google Spain Sl ./. Gonzalez.

616 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.

617 *Hermstrüwer/Dickert*, Tearing the Veil of Privacy Law, 2013, S. 19 f.

die sich in Gestalt von Bewertungen oder Fehlbewertungen auf das Bild der personalen Identität aufgrund ihrer Dauerhaftigkeit auswirken und ein nachträgliches Interventionsinteresse begründen können.

Aus grundrechtlicher Perspektive geht es daher um ein *Recht auf Neubeginn* im online-Kontext, welches mit der Löschung von Kommentaren und Attributen zu personalen Identitäten im online-Kontext durch den Verantwortlichen realisiert wird. Inwieweit das Recht auf Vergessenwerden eine geeignete Kompensation darstellt und essentieller Bestandteil eines Identitätsverwaltungsmodells zu sein hat, soll im Folgenden analysiert werden. Dazu gehören die Einräumung einer Kontrollmöglichkeit für den Betroffenen durch das Recht auf Löschung (1.), die Durchführung der Löschpflichten durch den Verantwortlichen (2.), die mögliche Kompensation des Legitimationsdefizits mit einem Konzept der Informationsverjährung (3.) und einer abschließenden Bewertung (4.).

1. Kontrolle mit dem Recht auf Löschung, Art. 17 Abs. 1, Alt. 1 DSGVO

Der Betroffene hat das Recht gegenüber dem Verantwortlichen, die unverzügliche Löschung der ihn betreffenden personenbezogenen Daten zu verlangen und kann damit die Kontrolle über den Bestand der mit den Datensätzen verbundenen personalen Identitäten ausüben. Es geht bei dem Recht auf Löschung demnach um ein „Ur-Abwehrinstrument“[618] gegenüber dem Verantwortlichen als private oder staatliche Institution. Der Begriff des Löschens wurde gemäß § 3 Abs. 4 Nr. 5 BDSG a. F. definiert und umfasst das „Unkenntlichmachen gespeicherter personenbezogener Daten“. Demgegenüber bleibt der Begriff der Löschung in der DSGVO undefiniert und wird allein in der Legaldefinition der „Verarbeitung“ nach Art. 4 Nr. 2 DSGVO als das „Löschen oder die Vernichtung“ dem Vorgang der Verarbeitung personenbezogener Daten zugeordnet. Die Löschung der Daten werde insgesamt realisiert, wenn die personenbezogenen Daten unkenntlich gemacht werden, ohne dass dabei die Datenträger in physischer Hinsicht zerstört werden müssen.[619] Gleichwohl kann von dem Löschungsrecht der Informationsgehalt von Daten nur beschränkt erfasst werden, so dass sich die Frage nach dem Umfang und der Wirksamkeit des Löschungsrechts stellt.

618 *Spiecker gen. Döhmann*, KritV 2014, 28 (34).

619 *Laue/Nink/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis, 2019, § 4 Rn. 47.

Im *Google Spain*-Urteil des EuGHs wurde die Verantwortlichkeit der Typisierungen und Erkenntniserlangung beim Suchmaschinenbetreiber gesehen und entsprechend die Notwendigkeit der Einräumung einer Löschoption durch den Verantwortlichen festgestellt.[620] Die Löschoption würde nicht unbeschränkt gelten, sondern bedarf der Abwägung des Schutzes der informationellen Selbstbestimmung gemäß Art. 7, 8 GRC mit der Meinungsfreiheit oder dem Informationsinteresse, Art. 17 Abs. 3 a) DSGVO. Gleichwohl hat der EuGH das Recht auf Vergessenwerden im online-Kontext anerkannt, indem bestimmte Informationen nach der Interessenabwägung nicht mehr mit dem Namen in Verbindung gebracht werden dürfen.[621]

Die Ausübung des Rechts auf Vergessenwerden ermöglicht keine absolute Kontrolle über die Informationen, sondern nur die relative Kontrolle, da die Informationen allein gegenüber dem datenverarbeitenden Verantwortlichen gelöscht werden können und nicht gegenüber Dritten. Jedoch suggeriere das Recht auf Vergessenwerden die absolute Kontrolle und damit den Optimismus, dass eine vollständige Löschung der personenbezogenen Daten möglich sei, was auf der Rechtfertigungsebene wiederum zu einer gesteigerten Einwilligungsbereitschaft auch gegenüber sensiblen Informationen führen kann und das Kontroll-Paradoxon wirken könne.[622] Damit geht es bei dem Recht auf Löschung auch um die Vermeidung der Perpetuierung des Erinnerns dahingehend, dass das Nicht-Erinnern ausgelöst werden solle, was aber kaum realisierbar sei.[623] Erschwerend kommen die Ubiquität der Datenverarbeitung und die vielfältigen Rekombinationsmöglichkeiten hinzu, nach denen die Datensätze vermehrt dezentral gespeichert werden und das Recht auf Vergessenwerden kaum umfassend umgesetzt werden könne, zumal die Speicherung in Typisierungen durch den Verantwortlichen erfolge und der Betroffene davon keine Kenntnis erlangen könne.[624] Somit wirkt sich das Recht auf Löschung allein gegenüber den Datensätzen als Kontrollrecht aus, schließt aber einen damit verbundenen Informationsgehalt oder das Fortbestehen von gewonnenen Erkenntnissen aus früheren Datenverarbeitungen nicht aus. Folglich wirken sich die Relativität der Informationen und ihre eingeschränkte Kontrollier-

620 EuGH, Urt. v. 13.05.2014 – C-131/12, Google Spain Sl ./. Gonzalez, Rn. 28, 37–39.
621 EuGH, Urt. v. 13.05.2014 – C-131/12, Google Spain Sl ./. Gonzalez, Rn. 99.
622 *Hermstrüwer/Dickert*, Tearing the Veil of Privacy Law, 2013, S. 7 f.
623 *Spiecker gen. Döhmann*, KritV 2014, 28 (36).
624 *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 71 Fn. 267.

barkeit nicht nur auf der Ebene der Einwilligungsfolgen aus, sondern auch auf der Ebene des Rechts auf Vergessenwerden.

Der mit dem Recht auf Vergessenwerden intendierte Zweck, einen *Neubeginn* für die personale Identität zu gewährleisten, unterliegt Beschränkungen, da die Rechtsausübung zu einem eigenen Informationsgehalt über den Rechtsausübenden führen kann. Dies könne zu einer unerwünschten Perpetuierung von Informationen über diesen führen, dem sog. Streisand-Effekt.[625] Nach diesem Effekt erlangen Informationen, die als unerwünscht gelten und möglichst vermieden werden sollen, eine gesteigerte Aufmerksamkeit und werden auf diese Weise bekannter als voher. Insgesamt besteht demnach kein Schutz dahingehend, welche Erkenntnisse aus den Daten generiert werden und welches Bild von einer personalen Identität erstellt wird, worin die eingeschränkte Wirkkraft des Rechts auf Vergessenwerden liegt. Folglich ist mit der relativen Kontrolle über das Recht auf Löschung nach der Sprachgebung des Bundesverfassungsgerichts von einer „Chance auf Vergessen"[626] auszugehen und bedarf zudem eines Verhaltens, das von einem „Vergessenwollen" getragen ist.[627] Erschwerend kann hinzukommen, dass der Verantwortliche zwar die Löschung der personenbezogenen Daten vornimmt, aber die vorgenommenen Typisierungen der Daten durch den Verantwortlichen und die damit verbundenen Erkenntnisse bestehen bleiben, worin *Spiecker gen. Döhmann* ein Vollzugsdefizit des Rechts auf Vergessenwerden sieht.[628]

2. Löschpflichten durch den Verantwortlichen, Art. 17 Abs. 1, Alt. 2, Abs. 2 DSGVO

Die Löschpflichten durch den Verantwortlichen werden ausgelöst durch die Zweckerreichung, den Widerruf der Einwilligung, wenn ein Widerspruch gegen die Datenverarbeitung eingelegt wurde, wenn die Datenverarbeitung unrechtmäßig war oder wenn ein datenfreier Eintritt in die Volljährigkeit ermöglicht werden soll, Art. 17 Abs. 1 a) – f) DSGVO. Darin sind die Eigenschaften der Identitätsverwaltung durch Kontrollmöglichkeiten

625 *Ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 300 f.; *Spiecker gen. Döhmann*, KritV 2014, 28 (32).
626 BVerfG, Urt. v. 06.11.2019 – 1 BvR 16/13, Recht auf Vergessen I, Rn. 123; *Masing*, NJW 2012, 2305 (2308).
627 BVerfG, Urt. v. 06.11.2019 – 1 BvR 16/13, Recht auf Vergessen I, Rn. 123.
628 *Spiecker gen. Döhmann*, KritV 2014, 28 (40 f.).

mit dem Widerruf der Einwilligung, dem Widerspruch gegen die Datenverarbeitung und die Chance auf einen datenfreien *Neubeginn* mit der Volljährigkeit abgebildet, so dass die Löschpflichten in diesen Konstellationen mit technischen Maßnahmen durch den Verantwortlichen realisiert werden müssen. Diese beginnen bereits *ex ante* zur Rechtfertigung bei den technischen und organisatorischen Maßnahmen, die eine wirksame Realisierung der Datenlöschung umfassen müssen, denn „Computer kennen keine Gnade des Vergessens“[629]. Dazu gehört die separate Speicherung von Datensätzen zu den personalen Identitäten und den generierten Profilen durch Aussonderung, so dass eine wirksame Löschung umsetzbar ist (EWG 26 S. 3) und den Anforderungen der Identitätsverwaltung Rechnung getragen werden kann. Im Einzelnen kann es um die Löschung von Berechtigungen und Nutzungsprotokollen gehen, mit denen die Auswertung des Nutzungsverhaltens möglich ist.[630] Dies lässt sich technisch mit dem Einsatz eines „digitalen Radiergummis“[631], der in bestimmten Zeitabständen aktiv wird, realisieren. Ebenso könnte es um die Verneinung bestehender Datensätze gehen, so dass die ursprünglichen Informationen mit dem Zusatz einer Negation versehen werden.[632] Diese Methoden könnten etwa bei der Auswertung des Nutzungsverhaltens von Arbeitnehmern und den Zugriff auf bestimmte Datenbanken eingesetzt werden, um nach der Zweckerreichung die Profile zu löschen. Auch wäre im „*Smart Home*“ der Einsatz von derartigen Löschungstechniken denkbar, um die Betroffenen vor der umfassenden Profilerstellung zu schützen.

Insgesamt hat der Verantwortliche den Löschanspruch nicht absolut umzusetzen. Der Löschanspruch erstreckt sich allein auf den Verantwortlichen und nicht auf Dritte. Gleichwohl war in der Fassung des EU-Parlaments der Wortlaut vorgesehen, dass die „Löschung *aller* Querverweise auf die personenbezogenen Daten bzw. aller Kopien und Replikationen“ von Dritten umfasst sein sollen, Art. 17 Abs. 1 DSGVO-E. Dieser vorgesehene Wortlaut wurde jedoch aufgegeben. Somit befindet sich der Verantwortliche in einem Spannungsfeld zwischen dem Recht auf Vergessenwerden und der wirksamen Umsetzung des *Rechts auf Neubeginn*. Denn es lassen sich die Daten löschen, ohne dabei die Informationen und Erkenntnisse über die personale Identität zu erfassen.

---

629 *Steinmüller*, Information, Modell, Informationssystem, S. 43.
630 *Lehnert/Luther/Christoph u.a.*, Datenschutz mit SAP, 2018, S. 129, 133, 287 f.
631 *Kalabis/Selzer*, DuD 2012, 670 (672 f.).
632 *Haft*, Einführung in die Rechtsinformatik, 1977, S. 31.

Folglich kann sich die Löschpflicht allein auf eine mögliche Leistung des Verantwortlichen beziehen, wozu die Löschung der Daten gehört. Weiter könne sich aus der Löschpflicht eine von *Spiecker gen. Döhmann* vorgeschlagene Beweislastumkehrregelung ergeben, mit der ein „ersichtliches Bemühen" über die Löschmaßnahmen nachgewiesen werden müsse.[633] Dies steht im Einklang mit der in Art. 17 Abs. 2 DSGVO enthaltenen Wertung, dass eine Löschpflicht gegenüber Dritten nicht bestehen kann und nur solche Maßnahmen ergriffen werden müssen, die „unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten" möglich sind. Damit muss der Verantwortliche nachweisen, welche Maßnahmen zur Löschung möglich waren. Schließlich kommen die Einreden des Verantwortlichen gemäß Art. 17 Abs. 3 DSGVO in Betracht, die der Wirkkraft des Rechts auf Vergessenwerden gerade aufgrund von gesetzlichen Aufbewahrungspflichten oder der Meinungsfreiheit entgegenstehen können.

3. Kontrolle durch Informationsverjährung

Die Kontrollmöglichkeit aus dem Recht auf Vergessenwerden könnte in das bisher begründete Identitätsverwaltungsmodell mit dem von *Drackert* entwickelten Rechtsinstitut der Informationsverjährung erweitert werden. Die Informationsverjährung wird aus der Verjährungsdogmatik abgeleitet, wonach das Motiv, den Rechtsfrieden herbeizuführen, auf Informationen übertragen und ein Schutzmechanismus gegen die Verwendung veralteter Informationen geschaffen werden soll.[634] Darin kommt der Grundsatz *venire contra factum proprium* zum Ausdruck, dass der geschaffene Vertrauenstatbestand über die Verwendung der Informationen nicht überraschend durch Entkontextualisierung aufgehoben werden darf und vergessen gedachte Informationen doch noch zum Einsatz kommen können.

Wenn die Datenverarbeitung lange zurückliegt, könnten die Informationen nach einem bestimmten Zeitpunkt nicht mehr verwertbar sein. Wobei mit der Einrede der Informationsverjährung kein absolutes Verarbeitungsverbot einherginge, da Informationen relativ wirken und das Recht nur gegenüber dem Verantwortlichen geltend gemacht werden kann.[635] Die Einrede der Informationsverjährung könnte bei der Identitätsverwal-

633 *Spiecker gen. Döhmann*, KritV 2014, 28 (37).
634 *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 301.
635 *Ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 70 f.

tung gegen Datenverarbeitungen zu einer personalen Identität ausgeübt werden, die nicht mehr auf aktuellen Datensätzen basieren. Demnach wäre eine auf die Identitätsverwaltung konzipierte Informationsverjährung in Gestalt der Befristung von personalen Identitäten denkbar, die den Schutz kontextspezifischer personaler Identitäten zeitlich beschränkt und nach einem bestimmten Zeitraum die personale Identität neu begründet werden würde.

Die Befristung personaler Identitäten stünde im Gleichlauf zu einem iterativen Einwilligungskonzept mit einer technischen Unterstützung durch ein *Dashboard-System*, welches dafür eingesetzt werden könnte, bestehende aktive kontextspezifische personale Identitäten einzusehen, um die (automatische) Löschung der Identitäten vorzunehmen. Damit könnte der kontextübergreifenden Verbindung von personalen Identitäten und der Entkontextualisierung von personalen Identitäten begegnet werden.

Insgesamt könnte mit der Notwendigkeit einer Befristung bestimmter personaler Identitäten das Legitimationsdefizit der Einwilligung oder der Rechtfertigung ohne aktive Handlung ausgeglichen werden. Denn es besteht aus verhaltensökonomischer Perspektive die Möglichkeit, dass die Ausübung der Rechte „vergessen“[636] werde und die Asymmetrie zwischen Verantwortlichem und Betroffenen zu einem späteren Zeitpunkt der Datenverarbeitung eine Verstärkung erfährt. Zudem besteht für den Betroffenen die Schwierigkeit, die Verwendung veralteter Datensätze in einer neuen personalen Identität zu erkennen und entsprechend sein Einrederecht geltend zu machen. Vielmehr ist es wahrscheinlich, dass der Betroffene eine vage Vermutung über das Fortwirken veralteter Datensätze hat und dies aber für die Geltendmachung der Einrede selten ausreichen wird. Demnach ist das Rechtsinstitut der Informationsverjährung dem Grunde nach vielversprechend, stößt jedoch auf Umsetzungsschwierigkeiten und sollte für die Identitätsverwaltung in eine Befristung personaler Identitäten umgewandelt werden.

4. Bewertung

Die Identitätsverwaltung umfasst Löschungsrechte, die durch das Recht auf Vergessenwerden gemäß Art. 17 DSGVO und den Widerruf der Einwilligung gemäß Art. 7 Abs. 3, 17 Abs. 1 b) DSGVO ausgeübt werden können. Die Einwilligung und das Recht auf Löschung stehen damit in direk-

636 *Hermstrüwer/Dickert*, Tearing the Veil of Privacy Law, 2013, S. 23.

ter Verbindung und können sich einander dahingehend bedingen, dass die Kenntnis über eine „*default*"-Option mit dem Recht auf Vergessenwerden zu einer gesteigerten Einwilligungsbereitschaft führen könne.[637] Genauso könnte die Kenntnis über eine automatische Löschung der Daten zu einem leichtfertigeren Umgang mit der Erteilung von Einwilligungen führen, wohingegen die Ausübung des Rechts auf Vergessenwerden und die Einrede der Informationsverjährung eine aktive Handlung voraussetzen, und damit einer bewußten Enstscheidung unterliegen würden. Wenn aber das Recht auf Vergessenwerden selbst vergessen werde, müsste für die Wirksamkeit von Löschungsrechten eine Einbeziehung dieses Phänomens im Identitätsverwaltungsmodell erfolgen.

Dieses könnte in einer technischen Gestaltung durch sog. „*information hiding*"[638] zur Risikominimierung über die Erkenntnismöglichkeiten liegen, mit der eine Überführung in den Schutzmechanismus der Intransparenz vorgenommen werden kann. Von der Einwilligung könnte umfasst sein, dass nach der Datenverarbeitung für eine personale Identität konstituierende Informationen unabhängig von der Zweckerreichung gelöscht werden. Dabei geht es um die Verzerrung von Erkenntnismöglichkeiten auch durch das Hinzufügen von sog. *Dummydaten*[639], die zu einem Gesamtbild einer personalen Identität zusammengeführt werden, mit dem die Schutzdimensionen über die informationelle Selbstbestimmung wiederhergestellt werden können. Demnach würde eine Ausgestaltung des Identitätsverwaltungsmodells mit der „Kontrolle von Intransparenz" die *Big Data*-Phänomene einbeziehen, so dass mit der Identitätsverwaltung die informationelle Selbstbestimmung in einer schützenden Variante ausgeübt werden kann. Mit der kontrollierten Intransparenz über den Gesamtdatensatz könne die mögliche Erkenntnis aus einer falschen Schlussfolgerung bestehen,[640] die einen eigenständigen Schutzbedarf auslöst aber keinen abschließenden Schutz entfaltet. Damit sei eine „*Symphonie der Intransparenz*"[641] durch das Blockieren und Freigeben von Daten[642] und dem damit einhergehenden Differenzierungsmonopol beim Betroffenen als Bestandteil eines Identitätsverwaltungsmodells in Erwägung zu ziehen, um damit eine Steigerung der Kontrolle über die Daten und Erkenntnismög-

637 *Dies.*, Tearing the Veil of Privacy Law, 2013, S. 16.
638 *Buchmann*, DuD 2015, 510 (511).
639 *Ders.*, DuD 2015, 510 (511).
640 *Spiecker gen. Döhmann*, KritV 2014, 28 (35); zum kalkulierbaren Nichtwissen als Schutzgegenstand, *Albers*, Informationelle Selbstbestimmung, 2005, S. 115.
641 *Luhmann*, in: Baecker (Hrsg.), Die Kontrolle von Intransparenz, 2017, 96.
642 *Ders.*, in: Baecker (Hrsg.), Die Kontrolle von Intransparenz, 2017, 96 (101).

lichkeiten herbeizuführen. Dies verlangt Differenzierungsentscheidungen über die Zusammensetzung der Datensätze der personalen Identitäten durch den Betroffenen und ist als Bestandteil der Identitätsverwaltung einzuordnen.

Das Risiko falscher Erkenntnisse kann mit einem Recht auf Vergessenwerden oder mit dem Recht auf Berichtigung gemäß Art. 16 DSGVO ausgeglichen werden. Damit lässt sich der Datensatz zu einer personalen Identität berichtigen, Art. 16 S. 1 DSGVO, vervollständigen oder mit einer Erklärung ergänzen, Art. 16 S. 2 DSGVO, was zwar zu einer faktischen Mehrverarbeitung führen würde, aber mit dem Interesse der Richtigstellung zu rechtfertigen ist. Ebenso ist als Vorrecht zum Recht auf Vergessenwerden das Recht auf einschränkende Verarbeitung gemäß Art. 18 DSGVO einzuordnen, wonach das Begehren eines Löschanspruches zu weitgehend wäre und etwa für die Verteidigung von Rechtsansprüchen der Erhalt bestimmter Daten begehrt wird.

Neben der Informationsverjährung und Befristung von personalen Identitäten sollte ein Recht auf Vergessenwerden als „Chance auf Vergessen" im Identitätsverwaltungsmodell einbezogen werden. Gleichwohl besteht bei der Informationsverjährung die praktische Schwierigkeit für den Betroffenen, die Verwendung veralteter Datensätze für eine wirksame Rechtsausübung zu erkennen. Demnach sollte für ein Identitätsverwaltungsmodell die Befristung personaler Identitäten einbezogen werden, womit man den praktischen Umsetzungsschwierigkeiten eines Informationsverjährungsrechts begegnen kann. Weiter können in Anbetracht wirkender verhaltensökonomischer Verzerrungen über das Recht auf Vergessenwerden bewusste Differenzierungsentscheidungen über die Intransparenz zu einer Gestaltung personaler Identitäten im online-Kontext führen und das Recht auf Vergessenwerden würde als Steuerungsinstrument fungieren. Denn die Intransparenz und das Vergessen seien die Voraussetzung und Grundlage für den Prozess der Evolution und des Lernens,[643] welches sich auf die „Evolution der Identität" im Sinne eines Neubeginns übertragen lässt.

Das Recht auf Vergessen findet seine Erweiterung in Gestalt des Vergessens bei einem bestimmten Verantwortlichen durch das „Schwesterrecht"[644] der Datenübertragbarkeit gemäß Art. 20 DSGVO. Mit diesem Recht wird die Übertragung der Datensätze an einen neuen Verantwortlichen ermöglicht.

643 *Spiecker gen. Döhmann*, KritV 2014, 28 (34) mwN.
644 *Edwards/Veale*, Duke L. & Tech. Rev. 2017, 18 (72).

III. Datenübertragbarkeit zur Identitätsverwaltung, Art. 20 DSGVO

Das Recht auf Datenübertragbarkeit enthält mit dem Recht zur Übertragung der Datensätze über eine personale Identität die Grundlage für die Identitätsverwaltung. Mit diesem Recht wird einerseits die informationelle Selbstbestimmung gemäß Art. 7, 8 GRC geschützt und andererseits erfolgt die Stärkung des Betroffenen gegenüber dem ökonomischen Phänomen der „*lock in*"-Effekte, wonach Betroffene nur unter erschwerten Bedingungen den Dienst wechseln können.[645] Demnach soll mit dem Recht auf Datenübertragbarkeit ein „*empowerment*"[646] der Betroffenen erfolgen und zugleich der Wettbewerb zwischen den Diensten zur Bereitsstellung von Wechselmöglichkeiten gefördert werden, so dass Art. 20 DSGVO auch als „Nutzerschutzrecht" fungiere.[647] Denn mit der umfangreichen Nutzung eines Dienstes etwa in sozialen Netzwerken kann eine faktische Sogkraft einhergehen, in die mit dem Recht auf Datenübertragbarkeit interveniert werden kann. Gleichzeitig lässt sich mit dem Recht auf Datenübertragbarkeit ein Anreizmechanismus für den Markt schaffen, etwa um Mitarbeiterdaten von dem ursprünglichen Arbeitgeber zu einem neuen Arbeitgeber zu übertragen oder den Wechsel von beruflichen online-Netzwerken erleichtern zu können.

Mit dem Recht auf Datenübertragbarkeit soll somit eine „bessere Kontrolle über die eigenen Daten" mit „automatischen Mitteln" ermöglicht werden, mit denen der Betroffene die Daten in einem „strukturierten, gängigen, maschinenlesbaren und interoperablen Format" erhalten kann, EWG 68 S. 1. Damit wird dem Betroffenen die Kontrolle über die Kontextänderung eingeräumt, so dass das Recht ein Minus zum Recht auf Vergessenwerden darstellt. Da gegenüber dem ursprünglichen Verantwortlichen die Datensätze zur personalen Identität vergessen werden müssen, aber gegenüber dem neuen Verantwortlichen die Datensätze verfügbar sein sollen, unterliegen die Daten einer Wiederverwendbarkeit. Demnach soll zunächst das Kontrollrecht des Betroffenen dargestellt werden (1.), anschließend die Durchführung der Datenübertragbarkeit durch den Verantwortli-

645 *Veil*, in: Gierschmann/Schlender/Stentzel u.a. (Hrsg.), Kommentar Datenschutz-Grundverordnung, 2017, Art. 20 DSGVO Rn. 3.

646 *Art. 29 Data Protection Working Party*, WP 242, Guidelines on the right to data portability (5. April 2017), S. 5.

647 *Reinhardt*, AöR 142 (2017), 528 (557) spricht von faktischer Sogkraft; *Roßnagel/Richter/Nebel*, ZD 2013, 103 (107).

chen (2.) und schließlich die Datenübertragbarkeit als Grundlage der Identitätsverwaltung begründet werden (3.).

1. Kontrolle mit dem Recht auf Datenübertragbarkeit

Die Ausübung des Rechts auf Datenübertragbarkeit begründet gegenüber dem Verantwortlichen die Kontrolle zur Übertragung der Datensätze in einen anderen Kontext und ermöglicht die kontextbezogene Verwaltung der Datensätze zu personalen Identitäten. Die Kontrolle liegt in dem Recht auf Geltendmachung der Datenübertragbarkeit und in dem „qualifizierten Herausgabeanspruch der betroffenen Person bezüglich ihrer Daten“[648]. Dazu gehört, dass die betroffene Person die bereitgestellten Daten in einem strukturierten und maschinenlesbaren Format erhält. Gemäß Art. 20 Abs. 1 DSGVO sind von dem Recht solche Daten erfasst, die „bereitgestellt“ wurden und als „*user-generated content*“ gelten. Der Wortlaut „bereitgestellt“ setzt eine aktive Handlung voraus, so dass durch physische Bewegung entstandene passiv generierte Daten etwa von einem Fitnesstracker oder Profildaten möglicherweise nicht erfasst sind, wie es von *Janal*[649] vertreten wird.

Für die Identitätsverwaltung mit dem Recht auf Datenübertragbarkeit ist die vollständige Übertragbarkeit der Daten und Erkenntnisse erforderlich, um die Verwaltung der *Idem*- und *Ipse*-Anteile personaler Identitäten umfassend realisieren zu können. Folglich könnte mit der Einwilligung oder der Nutzung des Dienstes die mit dem Begriff „bereitgestellt“ geforderte aktive Handlung konsumiert sein, so dass alle kausal auf die Einwilligung folgenden Datenverarbeitungen von dem Recht auf Datenübertragung erfasst wären. Eine derartige Auslegung wäre zwar zum Schutz der personalen Identitäten wünschenswert, erscheint aber in Anbetracht des eindeutigen Wortlautes und Gesetzeszwecks, „*lock in*“-Effekte zu mindern, konstruiert. Demnach sind von Art. 20 Abs. 1 DSGVO die Übertragung der erhobenen Daten, Metadaten und Nutzungsdaten umfasst,[650] wohingegen die Transaktionsdaten, Daten mit gesetzlicher Speicherungspflicht gemäß Art. 6 Abs. 1 c) – f), Art. 9 Abs. 2 b) – j) DSGVO und Kommunikationsdaten mit Dritten vom Übertragungsrecht ausgeschlossen sein sol-

---

648 *Kühling/Sackmann*, Rechte an Daten, 20. November 2018, S. 21.
649 *Janal*, JIPITEC 2017, 59 (61) Rn. 8.
650 *Art. 29 Data Protection Working Party*, WP 242, Guidelines on the right to data portability (5. April 2017), S. 18 f.

len.[651] Demgegenüber wären die vom Verantwortlichen erlangten Erkenntnisse aus den Daten und die generierten Profile vom Recht auf Datenübertragbarkeit nicht erfasst, da sie nicht aktiv bereitgestellt wurden.

Gleichwohl ist dem Schutzzweck des Rechts auf Datenübertragbarkeit zu entnehmen, dass die vom Verantwortlichen erlangten Erkenntnisse ein Faktor für die Steigerung der „*lock in*"-Effekte sind, und demnach es dem Schutz der informationellen Selbstbestimmung entspräche, diese Erkenntnisse dem neuen Dienstanbieter „mitzugeben". Insgesamt ist aber der Wortlaut des Art. 20 DSGVO dahingehend eindeutig, dass sich das Recht auf die aktiv „bereitgestellten" Daten beschränkt. Zwar wird mit dem Recht auf Datenübertragbarkeit ein hohes Kontrollmaß über die personalen Identitäten geschaffen, da sich aber die Kontrolle auf die Datensätze im ursprünglichen Kontext bezieht, lässt sich die Kontrolle nicht auf die umfassenden personalen Identitäten in ihren *Ipse*-Anteilen ausweiten.

2. Datenübertragung durch den Verantwortlichen

Die Datenübertragung muss in organisatorischer und technischer Hinsicht durch den Verantwortlichen umgesetzt werden. Dazu gehört die Aussonderungsfähigkeit der zu dem Betroffenen gehörenden Daten von dem Gesamtdatensatz und spezifizierte Schnittstellen zur Übertragung der Datensätze über eine personale Identität an den neuen Verantwortlichen. Mit der Beschränkung des Rechts auf Datenübertragbarkeit auf die „bereitgestellten" personenbezogenen Daten ist eine differenzierte Strukturierung und Speicherung der Nutzer-, Transaktions- und Metadaten erforderlich, damit der Datenexport nach der Geltendmachung des Rechts auf Datenübertragbarkeit ermöglicht werden kann. Bei dem exportierenden Verantwortlichen müssen interoperable Formate zur Gewährleistung der Datenübertragbarkeit eingerichtet werden und der importierende Verantwortliche muss die technischen Bedingungen zur Annahme der Daten herstellen. Dabei wird in EWG 68 S. 2 der Verantwortliche dazu aufgefordert, interoperable Formate zu entwickeln, worin aber keine Verpflichtung erkennbar ist. Vielmehr liegt aufgrund des Wortlautes „sollen" ein Empfehlungscharakter in der Regelung, wozu es gehöre, sich mit dem importierenden Verantwortlichen in Verbindung zu setzen.[652] Eine weitere Be-

651 *Janal*, JIPITEC 2017, 59 f.

652 *Veil*, in: Gierschmann/Schlender/Stentzel u.a. (Hrsg.), Kommentar Datenschutz-Grundverordnung, 2017, Art. 20 DSGVO Rn. 55.

schränkung des umfassenden Übertragungsrechts liegt in dem technischen Machbarkeitsvorbehalt gemäß Art. 20 Abs. 2 a. E. DSGVO, EWG 68 S. 8. Danach könnte das Recht auf Datenübertragbarkeit eine Einschränkung erfahren, wenn die Bereitstellung und Übertragung der Datensätze mit unverhältnismäßigem Aufwand verbunden sind. Folglich erscheint es wünschenswert, wenn sich die bereits bestehenden Interoperabilitätsregelungen in der eIDAS-VO zur grenzüberschreitenden Identifizierung für die umfassende Übertragung der personalen Identitäten im Datenschutzrecht als Regelungsvorbild heranziehen ließen.

Die von dem Verantwortlichen gewählte Interoperabilitätsmethode kann in einer detaillierten Form zum Bestandteil der Informationspflichten gemäß Art. 13 Abs. 2 b) DSGVO werden, so dass bei der Löschung oder Sperrung des „*Accounts*" von dem Recht auf Datenübertragbarkeit Gebrauch gemacht werden kann. Damit könnte ein Anreiz für den Verantwortlichen geschaffen werden, um an einem hohen Interoperabilitätsniveau mitzuwirken und dieses transparent zu machen. Diese Umsetzung der Anforderungen nach Art. 20 DSGVO könnte zu einer wettbewerblichen Dynamik führen, in der Dienstanbieter mit der Gewährleistung eines ausdifferenzierten Datenübertragbarkeitssystems eine gesteigerte Nachfrage erfahren könnten. Gleichzeitig ist eine Beeinflussung des Wettbewerbes mit dem Verlangen eines Entgeltes für die Datenübertragbarkeit denkbar und wird als rechtlich nicht ausgeschlossen angesehen.[653] Gleichwohl wurde festgestellt, dass sich Verhalten an Gratifikationen orientiert,[654] so dass die Zahlung eines Entgeltes den Betroffenen von der Geltendmachung des Rechts auf Datenübertragbarkeit abhalten könnte. Demnach erscheint ein Anreizmechanismus für den Betroffenen mit monitären Gratifikationen, wie es etwa bei dem Wechsel von Finanzdienstleistern verbreitet ist, naheliegender. Folglich könnte etwa ein berufliches online-Netzwerk damit werben, dass bei einem Wechsel zu diesem eine bestimmte Gratifikation in Gestalt von Prämien erfolgt.

3. Datenübertragbarkeit als Grundlage der Identitätsverwaltung

Das Recht auf Datenübertragbarkeit fungiert durch die Kontrolle der Kontextänderung als Grundlage für die Identitätsverwaltung. Sobald sich zwi-

653 *Ders.*, in: Gierschmann/Schlender/Stentzel u.a. (Hrsg.), Kommentar Datenschutz-Grundverordnung, 2017, Art. 20 DSGVO Rn. 15, 44.

654 4. Teil, C., II., 1., d).

schen dem Verantwortlichen und dem Betroffenen das Machtungleichgewicht derart manifestiert hat, dass die Ausübung des Rechts auf Datenübertragbarkeit zu einer „*re-balance*“[655] zugunsten des Betroffenen führe, kann von einer zumindest partiellen Wiederherstellung der informationellen Selbstbestimmung ausgegangen werden. Damit würde das Recht auf Datenübertragbarkeit seine Funktion als Nutzerschutzrecht entfalten.

In Anbetracht der *Big Data*-Phänomene des Internets der Dinge erscheint die Interoperabilität aus der ökonomischen Perspektive wegen der gesteigerten Nutzbarkeit von Daten über mehrere Komponenten hinweg als Wettbewerbsvorteil.[656] Dies kann einerseits zu erneuten „*lock in*“-Effekten und andererseits zu einer Steigerung des Kontrollniveaus bei dem Betroffenen führen. Dieses Kontrollniveau lässt sich in dem *Dashboard-System* abbilden. So schlägt die Artikel-29-Gruppe vor, dass extrahierte Daten aus einem Datenset in ein „*Tool*“ übertragen werden sollen, mit dem die Zugangsverwaltung ermöglicht wird,[657] was über das *Dashboard-System* zur Identitätsverwaltung abgebildet werden könnte. Denn über das *Dashboard-System* lässt sich der Zugang zu den extrahierten Datensätzen einräumen, die im Rahmen des Rechts auf Datenübertragbarkeit von dem Betroffenen kontrolliert in einen anderen Kontext überführt werden.

Solch ein Konzept würde eine Bündelung der Funktionalitäten von Diensten umfassen und wäre vergleichbar mit Passwortmanagern, die als Assistenzsystem für die Verwaltung einer hohen Anzahl von Passwörtern zu diversen online-Kontexten dienen. Die von Intermediären angebotenen *Single Sign-On*-Lösungen gewährleisten bereits eine interoperable Übertragung personaler Identitäten über die Benutzerdaten. Mit der Klarnamenpflicht und dem damit verbundenen Vertrauensmaß schaffen *Facebook* und *Google* eine diensteübergreifende Identifizierungsmöglichkeit und bündeln die Funktion der Identifizierung.

In Anbetracht der Marktmacht über die generierten personalen Identitäten durch einen Intermediär erscheint die Öffnung gegenüber weiteren Identitätsverwaltungsdiensten vorzugswürdig. Entsprechend ist die Identitätsverwaltung mit staatlich zertifizierten Identitätsattributen denkbar, wie es etwa der elektronische Personalausweis vorsieht. Damit enthalten die *Idem*-Anteile einer personalen Identität im online-Kontext ein hohes Ver-

655 *Art. 29 Data Protection Working Party*, WP 242, Guidelines on the right to data portability (5. April 2017), S. 4.

656 *Kerber/Schweitzer*, JIPITEC 2017, 39 (42) Rn. 11.

657 *Art. 29 Data Protection Working Party*, WP 242, Guidelines on the right to data portability (5. April 2017), S. 16.

trauens- und Sicherheitsniveau, was sich auch auf den privaten Rechtsverkehr übertragen ließe.

In rechtlicher Hinsicht könnte eine Erweiterung des Rechts auf Datenübertragbarkeit durch die Umwandlung der Soll-Vorschrift des Art. 20 DSGVO, EWG 68 in eine Muss-Vorschrift mit der Aufhebung des technischen Machbarkeitsvorbehalts erfolgen. Ebenso wären auf der rechtlichen Gestaltungsebene entsprechende Nutzungsbedingungen mit den Interoperabilitätsanforderungen als wettbewerbsfördernder Vertragsbestandteil denkbar, so dass sich der Betroffene bei der Wahl des Dienstes an dem potentiellen Interoperabilitätsniveau orientieren könnte. Damit würden Kontrollmöglichkeiten über personale Identitäten eingerichtet und gesteigert werden, wie sie aus Art. 17, 20 DSGVO abgeleitet wurden.

Mit der Kontrollmöglichkeit aus dem Recht auf Datenübertragbarkeit verbleibt gerade bei einem hohen Interoperabilitätsmaß das Risiko eines Angriffes etwa auf die Integrität, Authentizität und Vertraulichkeit von Schnittstellen. Dies gilt besonders, wenn die Bestimmung der Verantwortlichkeiten im Rahmen der „systemischen Digitalisierung“[658] hinsichtlich der Zuständigkeit über die Vermeidung eines IT-Sicherheitsvorfalles erschwert sein kann.

Für ein Identitätsverwaltungsmodell könnte etwa das Risiko korrumpierter personaler Identitäten bestehen, welches in einem *Dashboard-System* mit entsprechenden IT-Sicherheitsmaßnahmen einzubeziehen wäre. Insbesondere könnte eine unmittelbare Verbindung von dargestellten personalen Identitäten mit dem Widerspruchsrecht gemäß Art. 21 DSGVO eine Lösung für den Schutz der informationellen Selbstbestimmung darstellen. Denn mit diesem Recht könnte die personale Identität in Gestalt eines Profils mit dem Zusatz „unwahr“ versehen werden, wodurch die Authentizität einer personalen Identität in Frage gestellt und dies für Dritte erkennbar gemacht werden würde. Damit könnte das auf Zugangsrechte beschränkte Identitätsverwaltungsmodell erweitert werden, so dass über die Daten hinaus die Erkenntnisse zur personalen Identität in relativer Hinsicht kontrollierbar werden.

4. Ergebnis

Das Recht auf Datenübertragbarkeit sollte hinsichtlich der bestehenden Soll-Vorschrift des Art. 20 DSGVO, EWG 68 in eine Muss-Vorschrift um-

658 *Spiecker gen. Döhmann*, CR 2016, 698 (703).

gewandelt werden, damit die verantwortlichen Stellen die Interoperabilität für einen Wechsel gewährleisten. Dabei könnte als Interoperabilitätsschnittstelle ein *Dashboard-System* fungieren, das den Zugang zu den Datensätzen über den *Ipse-* und *Idem*-Anteil personaler Identitäten ermöglicht. Hierbei wäre es *de lege ferenda* wünschenswert, wenn über die „bereitgestellten" Daten hinaus auch die Profile erfasst werden. Damit würde dem Betroffenen ein Recht eingeräumt werden, das ein echtes Gegengewicht zu Machtungleichgewichten darstellt und die Kontrolle über die Kontextänderung und damit verbundene Informations- und Erkenntnismöglichkeiten erleichtert. Dabei könnten für einen Wechsel etwa finanzielle Prämien durch den neuen Dienstanbieter in Aussicht gestellt werden. Somit enthält das Recht auf Datenübertragbarkeit nach derzeitiger Rechtslage eine wesentliche Grundlage für die Identitätsverwaltung im Hinblick auf die ermöglichte Kontextänderung.

IV. Kontrolle gegen automatisierte Entscheidungen, Art. 22 Abs. 2 DSGVO

Für die Identitätsverwaltung bedarf es neben der Kontrolle der Daten und Erkenntnisse über eine personale Identität der Kontrolle über das Ergebnis einer automatisierten Verarbeitung, die eine unmittelbare rechtliche Wirkung entfaltet. Von der automatisierten Entscheidung ist gemäß Art. 4 Nr. 4 DSGVO jegliche Form einer automatisierten Verarbeitung personenbezogener Daten zur Analyse oder Prognose von Aspekten bezüglich der Arbeitsleistung, der wirtschaftlichen Lage, der Gesundheit, der persönlichen Vorlieben oder Interessen, der Zuverlässigkeit oder des Verhaltens, des Aufenthaltsortes der betroffenen Person, soweit dies eine rechtliche Wirkung für den Betroffenen entfaltet, umfasst. Damit kann die personale Teilidentität, die auf der automatisierten Einzelentscheidung im Kontext des Arbeitsplatzes oder im Gesundheitskontext basiert, zum Gegenstand einer Entscheidung mit unmittelbarer rechtlicher Wirkung[659] werden, so dass es jeweils um den Schutz der kontextspezifischen personalen Teiliden-

659 Der Streit, ob positive rechtliche Wirkungen vom Wortlaut erfasst sind, wird von der Literatur (*Schulz*, in: Gola/Eichler/Franck u.a. (Hrsg.), Kommentar, Datenschutz-Grundverordnung, 2018, Art. 22 DSGVO Rn. 22; *Buchner*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 22 DSGVO Rn. 25) mit dem Argument des Wortlauts gemäß Art. 22 Abs. 1 DSGVO „*rechtliche Wirkung oder eine in ähnlicher Weise erhebliche Beeinträchtigung*" verneint. Dieser würde auf eine negative rechtliche Wirkung abstellen. Demgegenüber ließe

tität geht. Die mit der automatisierten Einzelentscheidung begründete Identität darf nicht dazu führen, dass die natürliche Person mit ihren Persönlichkeitsmerkmalen zum Objekt der Entscheidung gemacht wird. Folglich bedarf es einer weiteren Prüfung über die „besondere Richtigkeitsgewähr“[660] dieser automatisierten Entscheidung als generierte personale Identität, die den Wahrheitsgehalt der personalen Identität und den Schutz vor einer vom Algorithmus ausgelösten diskriminierenden Entscheidung umfasst, die sich in dem digitalen Identitätsbild manifestieren kann. Darin wird ein entscheidender Schutzbedarf bei der automatisierten Einzelentscheidung und der damit generierten personalen Identität gesehen.[661]

Auch an dieser Stelle kann die Kontrolle durch die Transparenz über die involvierte Logik des automatisierten Entscheidungsprozesses gemäß Art. 13 Abs. 2 f) DSGVO erfolgen. Ebenso ermöglicht die Rechtfertigung über die Einwilligung die Kontrolle des Betroffenen, die sich auf die systematische Stellung des Art. 22 DSGVO als spezifisches Betroffenenrecht[662] und der damit verbundenen Kontrollmöglichkeit erstreckt. Dagegen bedarf es der Einräumung einer weiteren Kontrollmöglichkeit für den Betroffenen bei der Rechtfertigung der automatisierten Entscheidung ohne aktive Handlung über den Vertragsabschluss oder eine Rechtsvorschrift etwa einer Kollektivvereinbarung, Art. 22 Abs. 2 a) – b) DSGVO. Weiter hat der Verantwortliche gemäß Art. 22 Abs. 3 DSGVO die erforderlichen Maßnahmen zur Wahrung der berechtigten Interessen des Betroffenen zu treffen, etwa durch einen einzurichtenden Anspruch auf Eingreifen in die automatisierte Einzelentscheidung. Gemäß EWG 71 S. 4 wäre dieser Anspruch des Betroffenen auf ein Eingreifen durch den Verantwortlichen iterativ auszugestalten und umfasst die Darlegung des eigenen Standpunkts, den Anspruch auf Erläuterung der Entscheidung und das Recht auf Anfechtung dieser Entscheidung. Aus diesem iterativen Konzept kann eine Verhandlungsstruktur abgeleitet werden, die eine Intervention in die automatisierte Entscheidung und die daraus generierte personale Identität er-

---

sich für die Annahme des Schutzes gegen positive rechtliche Wirkungen anführen, dass mit der automatisierten Entscheidung eine „neue“ auf dem Algorithmus basierende personale Identität generiert werden könne und eine gravierende Abweichung zur realen personalen Identität darstellen kann, vgl. *Brecht/Steinbrück/Wagner*, PinG 2018, 10.

660 *Albers*, Informationelle Selbstbestimmung, 2005., S. 535.

661 *Edwards/Veale*, Duke L. & Tech. Rev. 2017, 18 (48).

662 *Schulz*, in: Gola/Eichler/Franck u.a. (Hrsg.), Kommentar, Datenschutz-Grundverordnung, 2018, Art. 22 DSGVO Rn. 6.

möglicht. Das darin abgebildete Recht auf Begründung des Ergebnisses der automatisierten Entscheidung erscheint nach *Edwards/Vaele* nur als ein schwaches Recht, da dieses iterative Konzept als Soll-Vorschrift und nicht als Muss-Vorschrift geregelt ist.[663] Dennoch könnte EWG 71 S. 4 als Vorlage für ein *iteratives Verhandlungskonzept* herangezogen werden und als risikominimierende Maßnahme in der Datenschutz-Folgenabschätzung gemäß Art. 35 Abs. 3 a) DSGVO in die Gesamtrisikobewertung einfließen. Ebenso könnte das *iterative Verhandlungskonzept* in technischer Hinsicht in das *Dashboard-System* integriert werden, so dass die technische Komplexität der automatisierten Einzelentscheidung über die personale Identität transparent wird und sich die Maßnahmen zum Schutz des Betroffenen treffen lassen.

Weil mit der automatisierten Einzelentscheidung aufgrund der hohen Komplexität des Entscheidungsverfahrens gegenüber dem Betroffenen Einschüchterungseffekte[664] eintreten können, bedarf es der Wiederherstellung des Kontrollniveaus über die personale Identität aus der automatisierten Einzelentscheidung. Denn bei dieser generierten personalen Identität ist ein Kontrollverlust eingetreten, der kompensationsbedürftig ist. Diese Kompensation könnte durch das beschriebene *iterative Verhandlungsmodell* in einem *Dashboard-System* erfolgen, mit dem eine Angleichung zwischen personaler Identität aus der automatisierten Entscheidung und aus der informationellen Selbstbestimmung erfolgen würde.

V. Transparente Datenschutzverstöße als Bestandteil der Identitätsverwaltung, Art. 33 DSGVO

Nach der Rechtfertigung der Datenverarbeitung kann die Verletzung des Schutzes personenbezogener Daten direkten Handlungsbedarf bei dem Verantwortlichen oder Betroffenen auslösen. Dafür bedarf es der Transparenz über den Datenschutzverstoß, wie es in Art. 33, 34 DSGVO geregelt wird. Diese Regelungen gehören zu dem zweiten Abschnitt des vierten Kapitels, wonach die „Sicherheit personenbezogener Daten" geregelt wird, die bereits zu den Grundsätzen der Datenverarbeitung gehört, Art. 5 Abs. 1 f) DSGVO. Dazu gehören die Meldepflicht durch den Verantwortlichen gemäß Art. 33 DSGVO gegenüber der Aufsichtsbehörde und gemäß Art. 34 DSGVO bei einem hohen Risiko für die Rechte und Freiheiten na-

663 *Edwards/Veale*, Duke L. & Tech. Rev. 2017, 18 (50).
664 *Di Fabio*, Grundrechtsgeltung in digitalen Systemen, 2016, S. 47.

türlicher Personen gegenüber dem Betroffenen. Weiter hat der Betroffene gemäß Art. 77 Abs. 1, Art. 57 Abs. 1 f) DSGVO ein direktes Beschwerderecht bei der Aufsichtsbehörde, wenn die Ansicht eines mutmaßlichen Verstoßes gegen die Verordnung besteht.

Wann eine „Verletzung des Schutzes personenbezogener Daten" und damit der personalen Identitäten gegeben ist, wird gemäß Art. 4 Nr. 12 DSGVO legaldefiniert und umfasst „eine Verletzung der Sicherheit, die (…) zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt (…)". Für die Gewährleistung der *ex post* Transparenz einer Verletzung durch den Verantwortlichen ist der risikobasierte Ansatz über die Prognose des Schadens und der Eintrittswahrscheinlichkeit einzubeziehen,[665] da der Verletzungsbegriff das eingetretene Risiko umschreibt.

Für die Realisierung eines effektiven Schutzes ist die Schaffung der Transparenz über die Verletzung der personalen Identität maßgeblich. Dabei muss nicht zwingend ein materieller oder immaterieller Schaden vorliegen, sondern es genügt einer der in Art. 4 Nr. 12 DSGVO aufgelisteten Vorgänge. Insbesondere kann gemäß EWG 85 S. 1 der Kontrollverlust über die personenbezogenen Daten bereits eine Verletzung des Schutzes personenbezogener Daten bedeuten. Erst mit der Transparenz über diese neue Risikolage im Datenzyklus kann der Betroffene gemäß Art. 34 DSGVO, EWG 86 S. 2, basierend auf einer Empfehlung durch den Verantwortlichen, die notwendigen Vorkehrungen zum Schutz seiner personalen Identität treffen. Weiter sind Informationen über die „betroffenen Kategorien" personenbezogener Daten, die „ungefähre(n) Zahl der betroffenen personenbezogenen Datensätze" und die Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen an die Aufsichtsbehörde mitzuteilen, Art. 33 Abs. 3 a) 2. Hs., Art. 33 Abs. 3 d) DSGVO. Gleichzeitig unterliegt die Informationsmitteilungen dem Machbarkeitsvorbehalt des Verantwortlichen.[666]

Die Vorkehrungen des Betroffenen können konkret etwa zu einer Passwortänderung oder innerhalb der Identitätsverwaltung zu der Geltendmachung des Rechts auf Vergessenwerden oder des Rechts auf Datenübertragbarkeit führen. Mit dem Transparenzerfordernis aus Art. 33, 34 DSGVO

665 *Jandt*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 33 DSGVO Rn. 9.

666 *Martini*, in: Paal/Pauly/Ernst (Hrsg.), Kommentar, DS-GVO, 2018, Art. 33 DSGVO Rn. 47.

über die Verletzungen und der damit einhergehenden Schutzmöglichkeit des Betroffenen wird nachträglich zur Datenverarbeitung ein „vorbeugender Persönlichkeitsschutz“[667] gewährleistet. Hierin liegt erneut ein verfahrensrechtlich ausgestaltetes Schutzkonzept[668] *ex post* zur Rechtfertigung vor, welches in dem Identitätsverwaltungsmodell einzubeziehen wäre. Es könnten konkrete Handlungsoptionen etwa über ein *Dashboard-System* für den Betroffenen zum Schutz gegen korrumpierte personale Identitäten durch die Verletzung personenbezogener Daten eingeräumt und damit ein weiteres Schutzregime geschaffen werden. Insgesamt enthalten die Vorgaben der Art. 33, 34 DSGVO eine indirekte Kontrollmöglichkeit, die mit der *ex post* Transparenz zu einem späteren Zeitpunkt des Datenzyklus dem Betroffenen dienen können.

Darüber hinaus setzen Art. 33, 34 DSGVO die Dokumentation der Datenverarbeitung gemäß Art. 5 Abs. 2 DSGVO voraus, die die Vorbereitung der Datenverarbeitung und die fachliche Auseinandersetzung zur Maßnahmenfindung für den gesamten Datenverarbeitungsvorgang umfasst. Diese Dokumentation kann in der Zusammenarbeit mit der Aufsichtsbehörde gemäß Art. 31, 33 DSGVO hinsichtlich des Verstoßes gegen die Sicherheit personenbezogener Daten einbezogen werden. Hiermit wird ein kooperativer Austausch über die Ursachen des Sicherheitsverstoßes und die möglichen Abhilfemaßnahmen auch unter Offenlegung der Datenverarbeitungsvorgänge vorgenommen. Nach *Martini* werden die Strategien zur Einhaltung der datenschutzrechtlichen Vorgaben ebenso von der Dokumentationspflicht umfasst,[669] was in Anbetracht unternehmerisch motivierter Geschäftsgeheimnisse als weitgehend eingeordnet werden kann. Gleichzeitig wird damit die Verantwortungszuschreibung im Sinne des Konzeptes der „*Accountability*“ zur wirksamen Umsetzung der datenschutzrechtlichen Pflichten sichergestellt. Indem die Rechenschaftspflicht sich auch auf die Exkulpationsmöglichkeit gegenüber der Aufsichtsbehörde bezieht, aber in Anbetracht der praktischen Unmöglichkeit, jeden Schritt dokumentieren zu können, sei der Umfang der Dokumentationspflicht restriktiv auszulegen.[670] Eine Einschränkung der Dokumentationspflichten gilt ebenfalls, wenn der Verantwortliche gemäß Art. 42 DSGVO zertifiziert ist, da mit

667 *Ders.*, in: Paal/Pauly/Ernst (Hrsg.), Kommentar, DS-GVO, 2018, Art. 33 DSGVO Rn. 1.
668 *Ders.*, in: Paal/Pauly/Ernst (Hrsg.), Kommentar, DS-GVO, 2018, Art. 33 DSGVO Rn. 10.
669 *Ders.*, in: Paal/Pauly/Ernst (Hrsg.), Kommentar, DS-GVO, 2018, Art. 24 DSGVO Rn. 40.
670 *Veil*, ZD 2018, 9 (16).

der Zeritifizierung bereits der Nachweis und die Rechenschaft über die Umsetzung der zertifizierungsrelevanten Vorgaben erfolgt ist.

VI. Kontrolle durch gerichtlichen Rechtsbehelf, Art. 79 DSGVO

Als *ultima ratio* der Kontrolle nach der Rechtfertigung und bei einem Verstoß gegen die Datenschutzgrundverordnung kann die Durchsetzung möglicher Schadensersatzansprüche über den Gerichtsweg erfolgen. Die Kontrolle der personalen Identitäten lässt sich mit dem in Art. 79 Abs. 2 S. 2 DSGVO statuierten Wahlrecht über den Gerichtsort darstellen, da der Betroffene sich über den Gerichtsort mit einem für ihn günstigen Schutzregime informieren und den Ort der Klageeinreichung wählen kann, sog. „*forum shopping*". Der Betroffene hat ein Wahlrecht zwischen dem Gerichtsort, in dem der Verantwortliche seine Niederlassung hat und dem Gerichtsort, bei dem der Betroffene seinen Aufenthaltsort hat, Art. 79 Abs. 2 S. 1, 2 DSGVO.[671] Dieses Wahlrecht ist entscheidend, wenn der Ort der Niederlassung des Verantwortlichen und der Aufenthaltsort des Betroffenen auseinanderfallen und an dem jeweiligen Gerichtsort ein unterschiedliches Schutzniveau von den Gerichten entschieden wird.

Insofern wirkt sich in der Identitätsverwaltung die Wahl des Gerichtsortes aus, die sich auf das zu erzielende datenschutzrechtliche Schutzniveau der personalen Identitäten bezieht. Sobald der Betroffene die Verletzung seiner Rechte und Freiheiten gerichtlich geltend macht, würde das Schutzniveau der personalen Identitäten in der gerichtlichen Bewertung in gewissem Maße ebenfalls der Kontrolle des Betroffenen unterliegen. Demnach könnte zu einem Identitätsverwaltungsmodell die Transparenz über den hypothetischen Gerichtsort bei der konkreten Datenverarbeitung gehören.

671 Ebenso wurde ein Wahlrecht bei der Geltendmachung einer Verletzung von Persönlichkeitsrechten, die durch Inhalte auf der Webseite erfolgt sind, in der eDate-Entscheidung des EuGHs anerkannt. Demnach könne zwischen dem Gerichtsort, an dem der Zugang zur Webseite besteht, oder dem Gerichtsort, an dem der Urheber niedergelassen ist, oder dem Gerichtsort, in dem der Schwerpunkt der Interessen des Geschädigten liegt, gewählt werden; EuGH, Urt. v. 25.10.2011 – C-509/09 und C-161/10, eDate Advertising, Rn. 52.

VII. Zusammenfassung

Die Identitätsverwaltung *ex post* zur Rechtfertigung personaler Identitäten setzt chronologisch zunächst die Auskunftsmöglichkeit über die personalen Identitäten und ihren Status im Datenzyklus voraus. Dafür muss durch den Verantwortlichen der Zugang zu den personalen Identitäten gewährt werden, womit das Auskunftsrecht gemäß Art. 15 DSGVO des Betroffenen eine absolute Kontrollmöglichkeit über die personalen Identitäten nach der Rechtfertigung einräumt. Mit dem Auskunftsrecht wird die Transparenz *ex post* zur Rechtfertigung geschaffen und lässt sich als vertrauensbildende Maßnahme des Betroffenen einordnen.

Dem folgend, sind das Recht auf Vergessenwerden und das Recht auf Datenübertragung als Kernrechte eines Identitätsverwaltungsmodells anzusehen. Mit dem Recht auf Vergessenwerden wird eine Löschpflicht über die verarbeiteten personenbezogenen Daten ausgelöst, wobei die Annahme eines tatsächlichen Vergessens der personenbezogenen Daten ausgeschlossen werden muss, da die Erinnerungen und die aus der Datenverarbeitung generierten Erkenntnisse nicht zwingend umfasst sind. Somit wirkt das Recht auf Vergessen nur relativ, weshalb von einer „Chance des Vergessens" auszugehen ist. Auch beim Recht auf Vergessenwerden wirken verhaltensökonomische Verzerrungen, so dass es der Einbeziehung weiterer Schutzmechanismen über die Löschung der Daten hinaus bedarf. Das Konzept einer „*Symphonie der Intransparenz*" fungiert als ein solcher Schutzmechanismus, da mit der Löschung und Verzerrung von bestimmten Datensätzen der Erkenntnisgehalt über eine personale Identität verfälscht werden kann. Demnach dient die Intransparenz als Gestaltungs- und Steuerungsinstrument in einem Identitätsverwaltungsmodell, zumal für den Schutz des allgemeinen Persönlichkeitsrechts auf diesem Weg die „Evolution der Identität" und das *Recht auf Neubeginn* gewährleistet werden. Daneben lässt sich mit dem Recht auf Datenübertragbarkeit als Minus über das Löschungsrecht die personale Identität direkt verwalten, indem der Kontext einer personalen Identität geändert wird. Die Effektivität des Rechts könnte jedoch zweifelhaft werden, da die Gewährleistung technischer Schnittstellen durch den Verantwortlichen einer Soll-Vorschrift und dem technischen Machbarkeitsvorbehalt unterliegen, so dass *de lege ferenda* eine Muss-Vorschrift möglicherweise sogar mit Sanktionsvorbehalt wünschenswert ist und sich auf den Wettbewerb der Dienstanbieter positiv auswirken könnte. Damit würde sich die Funktion des Rechts auf Datenübertragbarkeit als Nutzerschutzrecht tatsächlich realisieren lassen.

Weiter ist bei Datenschutzverstößen gemäß Art. 33, 34 DSGVO die Transparenz dieser vorgesehen, die es dem Betroffenen ermöglicht, die geeigneten Maßnahmen zum Schutz seiner Rechte und Freiheiten zu treffen. Darin liegt eine Kontrollmöglichkeit des Betroffenen, die sich als ein Verfahren infolge der Informationen über den Datenschutzverstoß darstellt. Sobald der Betroffene der Ansicht ist, dass ein Verstoß gegen die Verordnung vorliegt, kommt neben dem Beschwerderecht gemäß Art. 77 Abs. 1 DSGVO die gerichtliche Geltendmachung gemäß Art. 79 Abs. 2 DSGVO in Frage, bei der der Betroffene ein Wahlrecht hat und die Identitätsverwaltung sich sogar auf die Entscheidung über den Ort des anzurufenden Gerichts erstreckt.

Insgesamt lassen sich die rechtlichen Anforderungen in ein *Dashboard-System* übertragen, mit dem eine iterative Zugangs- und Kontrollmöglichkeit *ex post* zur Rechtfertigung eingeräumt wird. Dabei könnten die personalen Identitäten zum Gegenstand von Löschoptionen, der kontrollierten Intransparenz und der Kontrolle über die kontextübergreifende Datenübertragung werden. Ebenso wären im gesamten Datenzyklus die Transparenz über den Status einer personalen Identität und ein mögliches Verletzungsrisiko in einem *Dashboard-System* zu gewährleisten. Damit könnte der Schutz von personalen Identitäten in ihrem *Ipse-* und *Idem*-Anteil erfolgen, welches mit einem iterativen Begründungskonzept aus dem Recht gegen die automatisierte Entscheidung gemäß EWG 71 S. 4 ermöglicht wird. Folglich würden die personalen Identitäten iterativ in einem *Dashboard-System* aktualisiert werden können.

E. Identitätsverwaltung im Telemedien- und Telekommunikationsgesetz

I. Identitätsverwaltung im Telemediengesetz

Die Identitätsverwaltung im Telemedienrecht erfolgt im Kontext der Telemediendienste. Davon erfasst sind Dienste, die über die bloße Signalübertragung hinaus einen Kommunikationsprozess zur Informationsübertragung begründen und darin der Schwerpunkt der Leistungserbringung liegt, § 3 Nr. 24 TKG.[672] Mit der Geltung der Datenschutzgrundverordnung ist von dieser ebenfalls der Schutz von personenbezogenen Informationsübertragungen erfasst, so dass der Anwendungsbereich des Telemedi-

672 *Kremer*, CR 2012, 438 (440 f.).

engesetzes hinter dem der Datenschutzgrundverordnung zurücktreten könnte. Hinzu kommt, dass an sich die künftige EPrivacy-VO den Schutz der Nutzung von Telemediendiensten umfassen sollte und wiederum die Regelungen der DSGVO verdrängen würde. Solange eine EPrivacy-VO jedoch noch nicht gilt, ist auf die DSGVO und die Fortgeltungsmaßgabe gemäß Art. 95 DSGVO abzustellen, wonach die Richtlinie für elektronische Kommunikation 2002/58/EG weiterhin neben der Datenschutzgrundverordnung Anwendung findet.[673] Folglich soll das Telemediengesetz weiterhin als anwendbar eingestuft werden und die Identitätsverwaltung aus diesem Blickwinkel der TMG-Regelungen einbezogen werden. Für die Identitätsverwaltung sind demnach die Datensätze über die personalen Teilidentitäten im Telemedienrecht relevant (1.), die Kontrollmöglichkeiten durch den Betroffenen (2.), die Identitätsverwaltung durch den Dienstanbieter (3.) und weiter soll ein abschließender Ausblick erfolgen (4.).

1. Personale Teilidentitäten im Telemedienrecht

Die personalen Teilidentitäten im Telemedienrecht lassen sich einem Nutzer zurechnen, wenn über einen Nutzungsvertrag die Datensätze freigeschaltet werden und sich damit die Nutzung auf den Nutzer zurückführen lässt. Dazu gehört die Verarbeitung von Datensätzen beim Einsatz des Telemediendienstes, die einen eigenständigen Erkenntnisgehalt mit sich bringen können. Dieser leitet sich aus den Bestandsdaten (a), den Nutzungsdaten (b) und Profildaten (c) ab.

a) Personale Teilidentität durch Bestandsdaten, § 14 Abs. 1 TMG

Die personale Teilidentität aus den Bestandsdaten bildet sich in ihren statischen und dynamischen Ausprägungen ab und führt zu einem eigenständigen Erkenntniswert. Von den Bestandsdaten sind diejenigen Daten erfasst, die für die Begründung, die inhaltliche Ausgestaltung oder die Änderung eines Vertragsverhältnisses zwischen dem Dienstanbieter und Nutzer erforderlich sind, § 14 Abs. 1 TMG. Demnach ist der Gegenstand der Bestandsdaten über die Vertragsauslegung zu ermitteln und ist begrenzt

673 *Schmitz*, in: Spindler/Schmitz (Hrsg.), Kommentar, TMG, 2018, Vor §§ 11 ff. TMG Rn. 23.

durch die Erforderlichkeit für die Vertragsgestaltung.[674] Zu den Bestandsdaten können die Identifizierungsdaten, Anschrift, E-Email-Adresse, Rufnummer und der Zweck des Vertrages, die Kenn- und Passwörter, der Vertragszeitraum, der Ort der Nutzung des Telemediendienstes, die Leistungsmerkmale und die Zahlungsart gehören.[675] Demnach generiert sich die personale Teilidentität aus den Bestandsdaten mit dem Vertragsschluss und wird mit der „strikten Erforderlichkeit" gerechtfertigt, so dass die Entstehung der personalen Teilidentität ohne eine aktive Handlung über den Vertragsschluss hinaus erfolgt und keine eigenständige Einwilligung[676] verlangt. Der damit verbundene Datenzyklus der personalen Teilidentität in ihrem überwiegenden *Idem*-Anteil ist auf den vertraglich bestimmten Zeitraum begrenzt und erfährt mit der Lösch- und Sperrpflicht am Vertragsende gemäß § 13 Abs. 4 S. 2 TMG eine zeitliche Begrenzung. Aus dieser temporären Ausgestaltung der personalen Teilidentität im Telemedienrecht und dem damit verbundenen Erkenntnisgehalt hat der Nutzer allein im Rahmen des Vertragsschlusses eine Kontrollmöglichkeit. Gleichwohl lässt sich die Kontrollmöglichkeit über die Transparenz des bestehenden Vertragsverhältnisses in einem *Dashboard-System* abbilden, womit für den Nutzer der statische *Idem*-Anteil der personalen Teilidentität sichtbar wird.

b) Personale Teilidentität durch Nutzungsdaten, § 15 Abs. 1 TMG

Im Telemedienrecht wird infolge der Nutzung des Dienstes durch die Datenverarbeitung eine personale Teilidentität über die Nutzungsdaten begründet. Die Nutzungsdaten umfassen solche Daten, mit denen die Inanspruchnahme der Telemediendienste ermöglicht wird und die Abrechnung erfolgt, § 15 Abs. 1 S. 2 TMG. Danach sind Identifikationsdaten, Angaben über den Zeitraum der Nutzung und der in Anspruch genommene Telemediendienst von den Nutzungsdaten erfasst[677] und gehören zur personalen Teilidentität in ihrem überwiegenden dynamischen *Ipse*-Anteil, § 15 Abs. 1 S. 2 Nr. 1–3 TMG. Weiter gehören die Log-in Daten, die statischen oder dynamischen IP-Adressen, die Kommunikationspartner, die abgerufenen Informationen und Downloads zu der personalen Teilidentität in ihrem *Ipse*-Anteil dazu. Die Verarbeitung dieser Daten ist gerechtfertigt,

674 *Ders.*, in: Spindler/Schmitz (Hrsg.), Kommentar, TMG, 2018, § 14 TMG Rn. 15.
675 *Ders.*, in: Spindler/Schmitz (Hrsg.), Kommentar, TMG, 2018, § 14 TMG Rn. 73.
676 *Ders.*, in: Spindler/Schmitz (Hrsg.), Kommentar, TMG, 2018, § 14 TMG Rn. 9.
677 *Ders.*, in: Spindler/Schmitz (Hrsg.), Kommentar, TMG, 2018, § 15 TMG Rn. 42.

wenn sie nach der Datenschutzrichtlinie „erforderlich" war, was nach dem *Breyer*-Urteil[678] des EuGHs nunmehr bei Maßnahmen zur Gewährleistung der Datensicherheit auch gilt.[679]

Folglich stellen die Nutzungsdaten die Grundlage für die Begründung einer personalen Teilidentität über das Nutzungsverhalten in dem Kontext des Telemediendienstes dar. Es handelt sich um eine dynamische zeitlich beschränkte personale Teilidentität, die so lange gilt bis der Zweck erreicht wurde und die Lösch- und Sperrpflichten wirken. Mit diesen Nutzungsdaten ist ein kontextabhängiger Erkenntnisgewinn aus dem Nutzungsverhalten möglich, über den der Nutzer durch die Rechtfertigung mit der Erforderlichkeit und damit ohne aktive Handlung keine Kontrolle ausüben kann. Im Gleichlauf zu den Bestandsdaten wäre für die Transparenz an den Nutzer daher die Einbeziehung der Nutzungsdaten in dem *Dashboard-System* wünschenswert.

c) Personale Teilidentität durch Nutzungsprofil, § 15 Abs. 3 TMG

Die personale Teilidentität kann aus einem pseudonymisierten Nutzungsprofil bestehen und zum Zweck der Werbung und der Marktforschung eingesetzt werden, § 15 Abs. 3 TMG. Dieses Nutzungsprofil lässt sich in ein kurzzeitiges Momentprofil, Kurzzeitprofil und Langzeitprofil unterscheiden, wobei die umfassende und langfristige Speicherung und Auswertung von Daten zu einem Langzeitprofil führt.[680] Mit jedem dieser Profiltypen wird ein kontextspezifisches Bild über die personale Teilidentität in ihrem *Ipse*-Anteil erstellt. Aus diesen Bildern lassen sich Erkenntnisse etwa über das Konsumverhalten, die Interessen und Aktivitäten der Nutzer ziehen, die auf algorithmischen Vermutungen und Korrelationen beruhen, so dass es sich um konstruierte Bilder einer personalen Teilidentität handelt. Zwar basiert diese personale Teilidentität auf einem Pseudonym, welches gemäß § 15 Abs. 3 S. 3 TMG mit dem Nutzer nicht zusammengeführt werden darf, jedoch den Schutz für die personale Identität gewährleistet. Denn in der Profilerstellung liegt ein Eingriff in die informationelle Selbstbestimmung. Dieser Eingriff ist einerseits von der Erforderlichkeit aus der Ver-

678 EuGH, Urt. v. 19.10.2016 – C-582/14, Breyer ./. BRD, Rn. 55, 60.

679 *Schmitz*, in: Spindler/Schmitz (Hrsg.), Kommentar, TMG, 2018, § 15 TMG Rn. 58 f.

680 *Ders.*, in: Spindler/Schmitz (Hrsg.), Kommentar, TMG, 2018, § 15 TMG Rn. 92–94.

tragsbeziehung heraus gerechtfertigt und andererseits unterliegt er einer teleologisch erweiternden Auslegung in Gestalt des Erfordernisses eines aktiven *opt-ins*. Damit genügt die konkludente Einwilligung nach den Vorgaben aus Art. 6 Abs. 1 a) DSGVO für ein rechtfertigendes *opt-in* zur Profilerstellung.[681]

Die personale Teilidentiät aus dem pseudonymisierten Nutzungsprofil unterliegt durch die Annahme des Erfordernisses eines aktiven *opt-ins* der relativen Kontrollmöglichkeit. Denn der Dienstanbieter setzt den Algorithmus für den Erkenntnisgewinn aus den Nutzungsdaten ein, womit die personale Teilidentität von dem Dienstanbieter begründet wird. Demnach besteht die Kontrolle nicht mehr über das erstellte Profil des Dienstanbieters und das damit verbundene Bild der personalen Teilidentität. Die Transparenz über die Logik für die Profilerstellung und die Risiken für die informationelle Selbstbestimmung könnten durch die pseudonymisierten Nutzungsprofile wiederum in dem *Dashboard-System* transparent gemacht werden, und damit der Kontrollmöglichkeit unterliegen.

d) Personale Teilidentität durch *Cookies*

Die personale Teilidentität wird auch durch den von Cookies generierten Datensatz[682] begründet. Die Cookies unterscheiden sich in Verfolgungs-Cookies zur Informationserlangung über das Nutzungsverhalten und in Dienste-Cookies zur Erbringung der Dienste. In beiden Varianten wird durch das Setzen von Cookies der Nutzer wiedererkannt. Sein vorheriges Nutzungsverhalten wird abrufbar und erlaubt über die statische oder dynamische IP-Adresse die Identifizierung des Nutzers.[683] Folglich ist mit Cookies die Erstellung einer personalen Teilidentität in ihrem *Ipse*-Anteil verbunden, die Erkenntnisse über das Nutzungsverhalten hinsichtlich der je-

681 *Ders.*, in: Spindler/Schmitz (Hrsg.), Kommentar, TMG, 2018, § 15 TMG Rn. 25, 36, 98.

682 Ebenso als digitale Identität einordnend, *Windley*, Digital Identity, 2005, S. 51 f. Zur Funtionsweise: Mit dem ersten Aufrufen einer Webseite, die Cookies verwendet, werden diese Informationen bei dem verwendeten Browser des Nutzers hinterlegt und beim nächsten Aufrufen der gleichen Webseite an den Server zurückgeschickt. Dieser erhält damit die Informationen über das Nutzungsverhalten auf dieser Webseite, welches die Verknüpfung von bereits beim ersten Aufrufen eingegebenen Informationen ermöglicht.

683 *Schmitz*, in: Spindler/Schmitz (Hrsg.), Kommentar, TMG, 2018, § 13 TMG Rn. 12 f.

weiligen Webseiten ermöglicht. Dies setzt voraus, dass der Nutzer nicht nur gemäß Art. 5 Abs. 3 S. 1 der RL 2002/58[684] vor Beginn des automatisierten Verfahrens der Cookie-Setzung unterrichtet wird, sondern nach dem Urteil des EuGHs eine wirksame Einwilligung durch aktives Verhalten vorliegen muss und ein vorangekreuztes Kästchen demnach für die Annahme einer Einwilligung unzureichend ist.[685] Dabei stützt sich der EuGH auf Art. 4 Nr. 11 und Art. 6 Abs. 1 a) DSGVO, die eine freiwillige und unmissverständliche Einwilligung voraussetzen.[686]

Insgesamt erfolgt die Wirkung der Cookies im Verborgenen („*Hidden Identifiers*")[687] und der Nutzer hat über die Inhalte der Cookies mit Ausnahme der Browser-Einstellung keine absolute oder relative Kontrollmöglichkeit. Die mit Cookies generierten personalen Teilidentitäten über den *Ipse*-Anteil befinden sich damit in der Sphäre des Dienstanbieters und entfalten dort ihre Wirkung hinsichtlich der Erkenntnis- und Werbemöglichkeiten. Eine Kompensation des Kontrolldefizits könnte durch Erweiterung des Unterrichtungserfordernisses zu einem späteren Zeitpunkt im Datenzyklus erfolgen. Hierbei könnte mit einem *Dashboard-System* ein erleichterter Zugang zu der personalen Teilidentität und der Kontrolle dieser ermöglicht werden. Damit lässt sich die Transparenz über die logische Struktur und das Bild der personalen Teilidentität aus den Cookies erstellen.

2. Kontrolle durch den Nutzer im Datenzyklus

Die personalen Teilidentitäten unterliegen der Kontrolle durch den Nutzer, wenn dieser eine Kontrollmöglichkeit im Datenzyklus erlangt. Das TMG als einfachrechtliche Konkretisierung der Datenschutzrichtlinie und der „Cookie"-Richtlinie[688] würde durch die *EPrivacy*-VO eine Konkretisie-

684 Europäische Richtlinie vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).

685 EuGH, Urt. v. 01.10.2019 – C-673/17, Rn. 54.

686 EuGH, Urt. v. 01.10.2019 – C-673/17, Rn. 61–63; nach deutscher Rechtslage wurde bislang für Verfolgungs-Cookies die Einwilligung gemäß § 13 Abs. 2 Nr. 2 TMG vorausgesetzt, *Schmitz*, in: Spindler/Schmitz (Hrsg.), Kommentar, TMG, 2018, § 13 TMG Rn. 19.

687 EWG 24 Datenschutzrichtlinie für elektronische Kommunikation.

688 Richtlinie (EU) vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der

rung erfahren. Solange diese noch nicht gilt, finden die Vorschriften der DSGVO Anwendung, so dass für die Unterrichtungspflichten wiederum Art. 12, 13 Abs. 2 f) DSGVO gerade im Hinblick auf die Profilerstellung klarstellend wirken und eine Kontrollmöglichkeit einräumen. Daneben kommt die Kontrollmöglichkeit durch die elektronische Einwilligung gemäß den Anforderungen § 13 Abs. 2 Nr. 1–3 TMG in Betracht. Demgegenüber unterliegen die personalen Teilidentitäten in ihren *Idem*- und *Ipse*-Anteilen, die auf den Bestandsdaten, Nutzungsdaten und den Dienste-Cookies basieren, der Rechtfertigung im Rahmen der Erforderlichkeit. Folglich kann der Nutzer seine Kontrollmöglichkeit erst zu einem späteren Zeitpunkt des Datenzyklus ausüben. Diese Kontrolle könnte etwa über das Widerrufsrecht gemäß § 13 Abs. 2 Nr. 4 TMG, die Beendigung der Nutzung gemäß § 13 Abs. 4 Nr. 1 TMG und das Recht auf Vergessenwerden gemäß Art. 17 DSGVO im Wege der europarechtskonformen Auslegung gegenüber den Nutzungsdaten und dem Nutzungsprofil ausgeübt werden. Neben dem Kontrollrecht über die Löschung kann die Sperrung der personalen Teilidentitäten gemäß §§ 13 Abs. 4 Nr. 2, 15 Abs. 4 TMG verfolgt werden.

Folglich ergeben sich aus dem TMG im Gleichlauf zur DSGVO durch die Informationspflichten, die Einwilligung und die Löschungsrechte für den Nutzer relative Kontrollmöglichkeiten über die personalen Teilidentitäten. Gleichwohl sind die personalen Teilidentitäten, die auf der Erforderlichkeit gemäß §§ 14, 15 Abs. 1, 3 TMG basieren, in einem Kontrollsystem bislang nicht integriert, so dass der Bedarf an der Einrichtung einer Kontrollmöglichkeit zu einem späteren Zeitpunkt der personalen Teilidentität in einem *Dashboard-System* besteht, indem die Transparenz über die entstandenen personalen Teilidentitäten hergestellt wird.

3. Identitätsverwaltung durch den Dienstanbieter

Die Identitätsverwaltung durch den Dienstanbieter erfolgt im Gleichlauf zu den Maßgaben nach der DSGVO *ex ante* zur Rechtfertigung der personalen Teilidentitäten. Danach hat der Dienstanbieter bei der Begründung des Dienstangebotes die technischen und organisatorischen Maßnahmen im Rahmen des wirtschaftlich Zumutbaren zum Schutz für die personenbezogenen Daten sicherzustellen und den Stand der Technik zu berück-

elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz.

sichtigen, § 13 Abs. 4, 7 S. 2 TMG.[689] Dabei bestehen in § 13 Abs. 6 TMG Vorgaben, mit denen der Dienstanbieter die Nutzung und Bezahlung anonym oder durch ein Pseudonym im Rahmen des technisch Zumutbaren zu ermöglichen hat, worin implizite Vorgaben für ein Identitätsverwaltungsmodell enthalten sind. Denn mit dem Pseudonym wird eine personale Teilidentität in ihrem *Idem*-Anteil geschaffen, die einen geringen Erkenntniswert mit sich bringt und durch den Nutzer kontrolliert werden kann. Zu diesem Schutzkonzept der personalen Teilidentitäten gehört, dass die Nicht-Verkettbarkeit der generierten personalen Teilidentitäten gewährleistet werden muss, wie es aus §§ 13 Abs. 4 Nr. 4, 15 Abs. 3 S. 3 TMG hervorgeht. Diese technischen und organisatorischen Maßnahmen durch den Dienstanbieter gehen als Ergebnis aus einer vorangegangen Risikobewertung hervor, bei der die Popularität eines Dienstes zu einer Steigerung der wirtschaftlichen Zumutbarkeitsgrenze führen und weitere Schutzpflichten für die personalen Teilidentitäten voraussetzen kann.

Insgesamt hätte der Dienstanbieter den Einschätzungsspielraum über die Gestaltung des Identitätsverwaltungsmodells unter Wahrung der Datenschutzprinzipien innerhalb des Dienstes, wozu der differenzierte Einsatz von Anonymisierungs- und Pseudonymisierungsmethoden, die Transparenz über den Dienst und die generierten personalen Teilidentitäten gehören. Schließlich ist dieses Transparenzkonzept zu einem späteren Zeitpunkt des Datenzyklus auf die Betroffenenrechte zu erweitern, was mit einem *Dashboard-System* umgesetzt werden kann.

4. Ausblick

Die Grundlagen für die Identitätsverwaltung aus dem Telemedienrecht sind vorübergehender Natur und würden von einer künftigen EPrivacy-VO verdrängt werden. Mit dieser Verordnung würde etwa die Einwilligung für die Rechtmäßigkeit der Kommunikation beim Einsatz elektronischer Dienste gemäß Art. 9 EPrivacy-VO-E geregelt werden, worin ein Gleichlauf zur DSGVO liegen würde. Ebenso sind Löschpflichten gemäß Art. 7 EPrivacy-VO-E vorgesehen, mit denen die Anonymisierung oder Löschung der Daten durch den Betreiber vorgesehen wäre.[690] Diesen Vorgaben übergeordnet können die Rechtsanforderungen und Technikanforde-

689 3. Teil, A., I., 5.–6.

690 Zu dem Entwurf im Einzelnen kritisch *Härting/Gössling*, CRi 2018, 6 (8).

rungen der NIS-Richtlinie[691] und des BSIG wirken, wenn es um den Schutz und die Realisierung von personalen Teilidentitäten und der Identitätsverwaltung im Kontext kritischer Infrastrukturen geht. Dabei wirkt sich neben den rechtlichen Anforderungen die technische Gestaltung deutlich auf das mögliche Nutzungsverhalten aus, indem das Schutzniveau über den Einsatz von Anonymisierungs- und Pseudonymisierungsmethoden die Entscheidung des Betroffenen für einen bestimmten Dienst beeinflussen kann. Ebenso könnte für die Stärkung des Nutzers eine Struktur des „*Nudgings*" eingesetzt werden, mit dem die Aufmerksamkeit auf die Schutzmöglichkeiten gelenkt wird. Dennoch beschränkt sich eine derartige Identitätsverwaltung auf den Zugang zu bestimmten personalen Teilidentitäten nach dem TMG, ohne die Erkenntnisdimension aus den Bestands- und Nutzungsdaten einzubeziehen. Diese Ebene ist der Identitätsverwaltung *de lege ferenda* vorbehalten, könnte jedoch in der technischen Gestaltung durch eine Transparenzsteigerung über ein *Dashboard-System* als ein Konzept des „*identity management by design*" erfolgen. Dieses könnte durch eine eigenständige Hardware- und Softwaregestaltung für die Identitätsverwaltung umgesetzt werden, so dass ein dem TMG und zukünftig der EPrivacy-VO unterliegender Kommunikationsdienst die Grundlage für die Identitätsverwaltung darstellen könnte. Dem stünde jedoch entgegen, dass der Anbieter eines solchen Dienstes als *Trusted Third Party* fungieren würde und bei einem Angriff die informationelle Selbstbestimmung von vielen Nutzern verletzt werden könnte. Folglich wäre ein *Dashboard-System* als Kommunikationsdienst derart auszugestalten, dass die Datensätze selbst bei dem ursprünglichen Dienstanbieter verbleiben würden, und auf Anfrage des Nutzers die aktuelle personale Teilidentität über eine Schnittstelle in einem *Dashboard-System* sichtbar wird. Diese personalen Teilidentitäten könnten im Sinne der dargestellten rechtlichen Kontrollmöglichkeiten beibehalten, modifiziert oder gelöscht werden. Im Ergebnis erscheint dabei ein *Dashboard-System* als Kommunikationsdienst für die Identitätsverwaltung naheliegend, jedoch müsste dieses nur zur Transparenz der personalen Identitäten über Schnittstellen beitragen, ohne dabei die personalen Identitäten zu speichern.

691 Richtlinie (EU) 2016/1148 des europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.

II. Identitätsverwaltung im Telekommunikationsgesetz

Die Identitätsverwaltung im Telekommunikationsrecht richtet sich nach den Datensätzen aus der Telekommunikation, mit denen Informationen über die personalen Teilidentitäten erlangt werden können. Gemäß dem *ISO-OSI-Schichtenmodell* betrifft dies im Telekommunikationsrecht die Signalübertragung und die mit dem Telekommunikationsdienst verbundenen Vertragsbeziehungen zum Teilnehmer. Demnach richtet sich die Identitätsverwaltung im Telekommunikationsrecht danach, ob der Anwendungsbereich des bereichsspezifischen Datenschutzrechts bei dem Vorliegen von elektronischen Informations- und Kommunikationsdiensten eröffnet ist. Dafür muss der Schwerpunkt des Dienstes in der Signalübertragung liegen und diese muss gegenüber der Inhaltsübermittlung im Vordergrund stehen, § 3 Nr. 24 TKG. Folglich sind die Signalübertragung und der vertragliche Rahmen für die Bestimmung der personalen Identität im Telekommunikationsrecht grundlegend. Gleichzeitig bedarf es der Einordnung von personalen Identitäten, die auf den Kommunikationsmöglichkeiten über das Internet, sog. *over the top*-Dienste (OTT-Dienste), beruhen. Als OTT-Dienste gelten solche Dienste, deren Inhalte und Anwendungsmöglichkeiten über das offene Internet erbracht werden. Diese OTT-Dienste sind aufgrund ihrer Funktionalität ohne die elektronische Signalübertragung ausgestattet und dienen der Inhaltsübertragung mittels einer Verbindungsstelle zwischen den Teilnehmern in einer „*Client-Server*"-Architektur.[692] Gleichwohl besteht eine Parallelität zwischen dem vom TKG geregelten Verhalten der Nutzung von Telekommunikationsdiensten und dem Nutzungsverhalten von OTT-Diensten, so dass die Kontrolle personaler Identitäten in OTT-Diensten ebenfalls nachvollzogen werden soll.

Insgesamt wird die personale Identität im Telekommunikationsrecht auf der unteren Schicht des *ISO-OSI-Modells* neben den Vertragsdaten eingeordnet und in den Ausprägungen der jeweiligen personalen Teilidentitäten herausgearbeitet (1.). Damit sollen die Kontrolle des Teilnehmers innerhalb des Datenzyklus (2.) und die Identitätsverwaltung durch den Anbieter (3.) verdeutlicht werden.

692 *Maier/Schaller*, ZD 2017, 373 (374).

1. Personale Teilidentitäten im Telekommunikationsrecht

Die personalen Teilidentitäten im Telekommunikationsrecht können mit den Bestandsdaten (a), den Verkehrsdaten (b) und den Standortdaten (c) begründet werden.

a) Personale Teilidentität durch Bestandsdaten, §§ 95, 3 Nr. 3 TKG

Die personale Teilidentität, die auf den Bestandsdaten basiert, setzt sich aus solchen Daten zusammen, die für die Begründung, die inhaltliche Ausgestaltung, Änderung oder Beendigung des Vertragsverhältnisses über einen Telekommunikationsdienst erforderlich sind, §§ 3 Nr. 3, 95 Abs. 1 S. 2 TKG. Dazu gehören im Gleichlauf zu den Bestandsdaten im TMG etwa der Name, Adresse und die Abrechnungsdaten, aus denen die personale Teilidentität mit ihrem *Idem*-Anteil im TKG-Kontext begründet wird und die von der entsprechenden personalen Teilidentität im TMG abweichen kann. Die Begründung dieser Teilidentität wird mit der Erforderlichkeit für die Vertragserfüllung gerechtfertigt und bedarf für die Weitergabe der Bestandsdaten an Dritte der Einwilligung des Teilnehmers. Für die Identifizierung bei der Nutzung eines im Voraus bezahlten Mobilfunkdienstes kann die Richtigkeit der Angaben durch die Überprüfung etwa des Personalausweises erfolgen, § 111 Abs. 1 S. 2 TKG. Damit wird das Vertrauen über die Richtigkeit der Angaben im Personalausweis auf den Telekommunikationsdienst erweitert, so dass die personale Teilidentität in ihrem *Idem*-Anteil über die Bestandsdaten ein hohes Vertrauensniveau auslösen und zugleich Anknüpfungspunkt für strafrechtliche Ermittlungen gegen den Anschlussinhaber sein kann.

Wegen des hohen Vertrauensniveaus über die Richtigkeit der Identitätsinformationen in den Bestandsdaten könnte diese personale Teilidentität in einem Identitätsverwaltungsmodell in Gestalt eines interoperablen „*Identity Ecosystem*“ eingesetzt werden. Demnach würde die personale Teilidentität über die Bestandsdaten in Kontexten mit dem gleichen Vertrauensniveau übertragbar sein und eine kontextübergreifende Identitätsverwaltung ermöglichen. Denn sobald einmal die Identifizierung eines Teilnehmers erfolgt, könnte es dem Grundsatz der Datenminimierung entsprechen, diese einmal generierte personale Teilidentität wiederzuverwerten.

b) Personale Teilidentität durch Verkehrsdaten, §§ 96, 3 Nr. 30 TKG

Die personale Identität, die auf den Verkehrsdaten basiert, umfasst die mit der Erbringung des Telekommunikationsdienstes verbundenen Datenverarbeitungen, § 3 Nr. 30 TKG. Dazu gehören die Verbindungsdaten, die IP-Adresse, die MAC-Adresse und die Kennung über die Berechtigung mit den Log-in-Daten, so dass der *Idem*-Anteil personaler Teilidentitäten von den Verkehrsdaten erfasst ist. Die Erhebung der Verkehrsdaten ist für den Zweck gemäß § 96 Abs. 1 TKG zum Aufbau und der Nutzung der Verbindung gerechtfertigt und zum Zwecke der Vermarktung durch die Einwilligung erforderlich, § 96 Abs. 3 S. 1 TKG. Die Verkehrsdaten sind in ihrem Erkenntnisgehalt dadurch gekennzeichnet, dass sie als eine zeitlich gebundene Momentaufnahme erscheinen und dynamisch sind. Sie sind damit abhängig von dem Nutzungsverhalten und können als verhaltensgeprägte personale Teilidentität in ihrem überwiegenden *Ipse*-Anteil eingestuft werden.

Gleichwohl kann die Speicherung der Verbindungsdaten für das sog. „*Abuse-Handling(s)*“[693] und der Strafverfolgung dienen. Damit können die personalen Teilidentitäten, basierend auf den Verkehrsdaten, einem Vergangenheitsbezug unterliegen und gleichzeitig in die Zukunft wirken. Darin liegt eine Parallele zu dem festgestellten Phänomen von Profilen als Ergebnis von dem in der Vergangenheit liegenden Verhalten, die ebenfalls eine personale Teilidentität begründen können. Dennoch muss zwischen solchen Profilen als *Ipse*-Anteile personaler Teilidentitäten differenziert werden, die zum Schutz des Teilnehmers aus Gründen der IT-Sicherheit eingesetzt werden und solchen Profilen, die aus ökonomischen Motiven für gezielte Werbemaßnahmen begründet werden. Erstere personale Teilidentität mit Vergangenheitsbezug wird bei der Grundrechtsabwägung gegenüber der informationellen Selbstbestimmung aufgrund eines übergeordneten Sicherheitsinteresses gerechtfertigt sein. Dagegen unterliegt die ökonomisch motivierte Profilbildung den Rechtfertigungsgründen aus Art. 6 Abs. 1 DSGVO.

c) Personale Teilidentität durch Standortdaten, §§ 98, 3 Nr. 19 TKG

Die personale Teilidentität aus Standortdaten ist ebenfalls mit dem Verhalten des Teilnehmers verbunden und besteht aus solchen Daten, die in

693 *Kühling/Schall/Biendl*, Telekommunikationsrecht, 2014, Rn. 639.

einem Telekommunikationsnetz erhoben und verwendet werden und den Standort des Endgeräts eines öffentlich zugänglichen Telekommunikationsdienstes angeben, §§ 98, 3 Nr. 19 TKG. Gleichwohl sind die Standortdaten ebenfalls gemäß Art. 4 Nr. 1 DSGVO als personenbezogene Daten und damit als Inhaltsdaten geschützt, so dass sie innerhalb des *ISO-OSI-Schichtenmodells* nicht auf der unteren Ebene der Signale einzuordnen sind. Dies stellt eine Anomalie im Telekommunikationsrecht dar. Gleichwohl soll im Folgenden die Darstellung in Übereinstimmung mit den Standortdaten als personenbezogene Daten und ihrem *Ipse*-Anteil der personalen Teilidentität erfolgen.

Insgesamt lässt sich mit den Standortdaten ein genaues Profil über das Bewegungsverhalten des Teilnehmers nachbilden, so dass die personale Teilidentität in ihrem *Ipse*-Anteil, basierend auf dem Bewegungsverhalten, einen umfangreichen Erkenntniswert über den Teilnehmer hinsichtlich der Dauer, Häufigkeit und des Zeitpunktes seines Aufenthaltes ermöglicht. Darin kann ein erheblicher Eingriff in die informationelle Selbstbestimmung liegen, so dass die unverzügliche Anonymisierung dieser Daten gemäß § 98 Abs. 1 S. 2 TKG vorgesehen ist und in anderen Fällen die entsprechende Einwilligung einzuholen wäre.[694] Weiter werden nach dem EWG 2 der EPrivacy-VO-E die Standortdaten als hochsensible Informationen eingeordnet, worin eine Anerkennung der umfangreichen Erkenntnismöglichkeiten aus kontextübergreifenden Datensätzen liegt. Folglich ist die erleichterte Ortung von Mobilfunktelefonen und der Standortverlauf durch Intermediäre, die über die Privatheitseinstellung deaktiviert werden können, ein Phänomen, welches in die Identitätsverwaltung aufgenommen und in einen eigenen Schutzmechanismus zu überführen wäre. Entsprechend werden in Art. 4 Abs. 3 c) EPrivacy-VO-E die Standortdaten als elektronische Kommunikationsmetadaten eingeordnet und stellen gleichzeitig die elektronischen Kommunikationsdaten gemäß Art. 4 Abs. 3 a) EPrivacy-VO-E dar. Diese müssen gemäß Art. 7 Abs. 2 EPrivacy-VO-E anonymisiert oder gelöscht werden und dürfen nur unter den Maßgaben des Art. 6 Abs. 2 EPrivacy-VO-E gespeichert werden, wenn die gesonderten Rechtfertigungsanforderungen vorliegen.

Das Phänomen der Speicherung von Standortdaten durch Intermediäre ist für die Teilnehmer in ihrer Tragweite nicht unmittelbar transparent. Dies betrifft etwa die Speicherung des Standortverlaufes, die der Nutzer bei einer Suchmaschine erst durch vertiefte Auseinandersetzung mit den Privatheitseinstellungen transparent und damit kontrollierbar macht.

694 *Dies.*, Telekommunikationsrecht, 2014, Rn. 641.

Demgegenüber ist nach § 98 Abs. 1 S. 2 TKG und Art. 7 Abs. 2 EPrivacy-VO-E vorgesehen, dass bei einer Speicherung die Einwilligung erteilt werden muss, die wiederum eine Transparenz über die Speicherung der Standortdaten voraussetzt. Insgesamt kann die personale Teilidentität aus den Standortdaten einer hohen Sensibilität unterliegen, so dass es zunächst der Transparenz über diese Teilidentität bedarf, um entsprechende Schutzmaßnahmen vornehmen zu können. In einem *Dashboard-System* ginge es um die Transparenz und den technischen Schutz der personalen Teilidentität, die auf den Standortdaten basiert. Damit würde dem Teilnehmer eine reale Kontrollmöglichkeit eingeräumt werden.

2. Kontrolle durch den Teilnehmer im Datenzyklus

Die Kontrolle über die personalen Teilidentitäten nach dem Telekommunikationsrecht erfolgt im Gleichlauf zu den Feststellungen im Telemedienrecht. Maßgeblich ist die Kontrollmöglichkeit über die personale Teilidentität mit der Einwilligung hinsichtlich der Standortdaten und der Vermarktung der Verkehrsdaten. Im Übrigen unterliegen die personalen Teilidentitäten, die auf den Bestandsdaten, Verkehrsdaten und den erforderlichen Standortdaten basieren, der Kontrolle durch die Informationspflichten gemäß § 93 TKG über die Verwendung der personenbezogenen Daten im Einzelnen. Auf dieser Grundlage kann die Einwilligung mit einer vorformulierten Einwilligungsklausel gemäß § 94 TKG als Kontrollmittel abgefragt werden. Zu einem fortgeschrittenen Zeitpunkt bei der Verarbeitung personenbezogener Daten kommen das Auskunftsrecht gemäß § 93 Abs. 1 S. 4 TKG und die Benachrichtigungspflicht bei der Verletzung des Schutzes personenbezogener Daten gemäß § 109a Abs. 1 S. 2 i.V.m. Abs. 2 TKG in Betracht. Damit kann der Teilnehmer nach der Rechtfertigung der Speicherung die Kontrolle über die personale Teilidentität im Rahmen der Transparenz ausüben.

Dagegen ist die Einordnung der Kontrollmöglichkeit über die personalen Teilidentitäten aus OTT-Diensten differenzierter. Bislang war unklar, ob die Kommunikation über das Internet unter das Tatbestandsmerkmal der Signalübertragung im Telekommunikationsrecht subsumierbar ist.[695] Nun hat der EuGH einen technischen Ansatz gewählt[696] und differenziert zwischen zweistufigen OTT-0-Diensten und einstufigen OTT-1-Diensten.

695 *Kühling/Schall*, CR 2015, 641; *Gersdorf*, K&R 2016, 91.
696 *Wüsthof*, N&R 2019, 275 (277–279).

Bei den zweistufigen OTT-0-Diensten wird die Signalübertragung in der zweiten Stufe angenommen, da etwa *SkypeOut* in einem ersten Schritt von einem Engerät innerhalb der Internetverbindung bis zum Gateway die Informationen überträgt und in einem zweiten Schritt aufgrund einer Zusammenschaltungsvereinbarung in das öffentliche Telefonnetz eine Signalübertragung erfolgt.[697] Demgegenüber wurde *Gmail* nicht als elektronischer Kommunikationsdienst mit Signalübertragung eingeordnet, da die Übertragung der Datenpakete über einen Dritten, nämlich den Internetbetreiber erfolgt, sog. OTT-1-Dienst.[698] Aus diesen technikbezogenen Differenzierungen ergibt sich für den Schutz personaler Identitäten, dass das rechtliche Schutzniveau von dem verwendeten Dienst abhängt. Gleichwohl wird der Schutz mit den zukünftigen Regelungen der Richtlinie zum Kodex für elektronische Kommunikation[699] und der EPrivacy-VO umfasst, so dass spezifische Regelungen zur Kontrollierbarkeit der personalen Teilidentitäten aus OTT-Diensten bevorstehen.

3. Identitätsverwaltung durch den Anbieter

Die Identitätsverwaltung könnte durch den Dienstanbieter im Gleichlauf zu den Anforderungen nach der DSGVO und dem TMG mit der Gewährleistung entsprechender technischer Schutzvorkehrungen erfolgen, die ebenfalls unter dem Wirtschaftlichkeitsvorbehalt gemäß § 107 Abs. 2 S. 4 TKG stehen. Im Hinblick auf die Verwaltung der personalen Teilidentitäten würde diese eine Separierung der Datensätze zu den Bestandsdaten, Verkehrsdaten und Standortdaten verlangen, damit diese in die Transparenz überführt werden können. Damit erlangt der Teilnehmer über die Kenntnis der generierbaren und generierten personalen Teilidentitäten eine Kontrollmöglichkeit, die über das *Dashboard-System* gewährleistet werden könnte. Neben der Kontrolle über die Transparenz der personalen Teilidentität und den Informationspflichten kommt die Kontrolle über die rechtfertigende Einwilligung in Betracht. Insgesamt wird die Identitätsverwaltung durch den Telekommunikationsanbieter mit der Transparenz, der Einwilligung und dem Auskunftsrecht ermöglicht, wobei die Anzahl der TKG-Kontexte für eine Einwilligung gering sein würde. Weiter unterliegt

697 EuGH, Urt. v. 05.06.2019 – C142/18, „Skype“, Rn. 34–38.
698 EuGH, Urt. v. 13.06. 2019 – C193/18, „Gmail“, Rn. 38.
699 Art. 2 Nr. 1 a. E. Richtlinie 2018/1972 über den europäischen Kodex für die elektronische Kommunikation.

etwa die personale Teilidentität über die Standortdaten dem Anonymisierungsvorbehalt, so dass der Anbieter die geeignete Anonymisierungsmethode zu bestimmen hätte und der Teilnehmer auf diesem Wege nicht über diese personale Teilidentität in Kenntnis gesetzt werden müsste.

4. Ausblick

Das Identitätsverwaltungsmodell lässt sich mit der personalen Teilidentität in ihrem *Ipse*-Anteil aus den Standortdaten nach dem Telekommunikationsgesetz erweitern. Dabei unterliegt diese verhaltensbezogene personale Teilidentität einem hohen Schutzbedarf, der im Telekommunikationsrecht für die elektronische Signalübertragung gilt, aber noch nicht die Kommunikation mit OTT-Diensten einbezieht. Der Schutz personaler Teilidentitäten aus OTT-Diensten unterliegt einer technischen Betrachtung des konkreten Dienstes und würde bei einem OTT-0-Dienst von dem Telekommunikationsrecht umfasst sein. Bei einem OTT-1-Dienst ist auf das künftige Regelungsregime aus der Richtlinie zum Kodex für elektronische Kommunikation und der EPrivacy-VO abzustellen.

Für ein Konzept der Identitätsverwaltung kann die personale Teilidentität über die Bestandsdaten, die mit einem Personalausweis abgeglichen werden, einen Anker über eine personale Teilidentität begründen, der über ein hohes Vertrauensmaß verfügt und sich möglicherweise kontextübergreifend einsetzen lässt. Demgegenüber ist aus der personalen Teilidentität aus den Verkehrsdaten und den Standortdaten ein enger Verhaltensbezug bei der Identitätsbildung festzustellen, so dass ein ausgeprägtes Transparenzbedürfnis zur Kontrolle der personalen Teilidentitäten in ihren *Ipse*-Anteilen besteht.

Insgesamt ist die Identitätsverwaltung nach dem TKG zwischen dem Telekommunikationsanbieter und Teilnehmer ausgestaltet, wohingegen die Kommunikation im Internet über den Intermediär, der eine Applikation zur Verfügung stellt, erfolgt. Für die Identitätsverwaltung kommt ebenfalls eine solche Applikation etwa in Gestalt eines *Dashboard-Systems* in Betracht, das vergleichbar wäre mit dem „*Mobile Payment*" über einen „*NFC-Badge*" („*Near Field Communication*"-Plakette)[700] zur Zahlung mit einer entsprechenden Applikation. Mit dieser Applikation würden die personalen Teilidentitäten in einem anderen Kontext einsetzbar werden und, ver-

700 *Steinacker/Krauß*, in: Bräutigam/Rücker, E-Commerce - Rechtshandbuch, 2016, 13. Teil, C. Rn. 2–9.

gleichbar mit der Funktionalität der Zahlung eines Geldbetrages in einem spezifischen Kontext, die wiederholte Verwendung personaler Teilidentitäten erfolgen. Dabei scheint eine hybride Schnittstellen-Struktur, mit der gleichzeitig die elektronische Kommunikation im online-Kontext kontrolliert werden könnte, ohne dass eine *Trusted Third Party* erforderlich wäre, für die informationelle Selbstbestimmung eine schonende technische Ausgestaltung zu sein.

III. Zusammenfassung

Aus dem TMG und TKG konnten die rechtlichen Grundlagen für ein Identitätsverwaltungsmodell herausgearbeitet werden. Dabei wurde die personale Identität aus der Datenschutzgrundverordnung um die personalen Teilidentitäten aus dem TMG und TKG erweitert, die aus den Bestandsdaten, Nutzungsdaten, Verkehrsdaten und Standortdaten zu einem eigenständigen Erkenntnisgehalt führen können. Die Kontrollmöglichkeit vor der Rechtfertigung beschränkt sich auf die Transparenz. Auch bei der Rechtfertigung erstreckt sich die Kontrolle über die Einwilligung auf die Verarbeitung der personenbezogenen Daten und implizit auf den mit ihnen verbundenen Erkenntnisgehalt, wobei für die Profile eine separate Einwilligung erforderlich sein sollte.

Nach der Rechtfertigung wird zu einem späteren Zeitpunkt im Datenzyklus mit den Nutzer- und Teilnehmerrechten durch das Auskunftsrecht der Zugang als absolute Kontrollmöglichkeit zur personalen Identität gewährt. Gleichzeitig handelt es sich um dienstabhängige Kontexte, ohne dass der Nutzer oder der Teilnehmer einen Gesamtüberblick über die personalen Teilidentitäten im online-Kontext hat. Dieser Gesamtüberblick kann über ein *Dashboard-System* hergestellt werden. Da auch bei diesem System die maßgebliche Kontrollmöglichkeit über die Transparenz und rechtfertigende Einwilligung erfolgt, könnte mit einem *Dashboard-System* eine Stärkung des Schutzes der informationellen Selbstbestimmung erfolgen. Dabei könnte das *Dashboard-System* als eine Applikation eingesetzt werden, die die Kontrolle der personalen Teilidentitäten und Kommunikation, vergleichbar mit dem „*Mobile Payment*“, ermöglicht, ohne dabei als *Trusted Third Party* zu fungieren.

F. Ergebnis: Identitätsverwaltung im IKT-Recht

Das Identitätsverwaltungsmodell nach der Datenschutzgrundverordnung umfasst *ex ante* zur Rechtfertigung die Kontrolle über den Datenzykyklus durch die Informationen zur Datenverarbeitung und die damit verbundenen Risiken. Dazu gehören zunächst die personenbezogenen Daten und das Identifizierungsrisiko der natürlichen Person.[701] Weiter unterliegt jede Datenverarbeitung der vorherigen Zweckfestlegung, auf der die Generierung der personalen Identität mit den personenbezogenen Daten möglich wird. Mit der Zweckfestlegung erfolgt zugleich die *Instruktion* für die Erkenntnismöglichkeiten über die personale Identität, was dem Betroffenen eine Kontrollmöglichkeit einräumt. Diese Kontrollmöglichkeit wird jedoch mit der Zweckänderung gemäß Art. 6 Abs. 4 DSGVO im Laufe des Datenzyklus eingebüßt und es wird ein neues Risiko für die Rechte und Freiheiten der natürlichen Person ausgelöst. Die Kontrollmöglichkeit beschränkt sich dabei allein auf die Informationen über die Zweckänderung. Weiter geht es *ex ante* zur Rechtfertigung um die Risikoallokation bei der Datenverarbeitung über die Informationspflichten und die Konkretisierung der Datenverarbeitungsgrundsätze. Mit diesen datenschutzrechtlichen Anforderungen vor der Datenverarbeitung besteht gerade über die Informationen eine erste Kontrollmöglichkeit für den Betroffenen. Gleichzeitig hat der Verantwortliche zur Gewährleistung der Identitätsverwaltung technische und organisatorische Maßnahmen vorzunehmen, die in einem „*identity management by design*"-Konzept münden können.[702]

Die Identitätsverwaltung erlangt bei der Rechtfertigung ihren Kerngehalt über die Kontrollmöglichkeit mit der Einwilligung. Es konnte nachgewiesen werden, dass die Einwilligung kognitiven Verzerrungsfaktoren unterliegt und die rationale Entscheidung darin besteht, dass der Betroffene in der Vorstellung einer rationalen Entscheidung handelt. Das damit verbundene Legitimationsdefizit über die rechtfertigende Einwilligung könnte mit einem „*layered approach*" über iterative Einwilligungen gelöst werden. Dies gilt in besonderem Maß, wenn die Rechtfertigung ohne eine aktive Handlung durch den Betroffenen erfolgt. Daher lässt sich in der technischen Realisierung an ein *Dashboard-System* denken, das einen Überblick über die Datenverarbeitung mit den verbundenen Betroffenenrechten schafft und die personalen Teilidentitäten zusammenführt, damit diese kontrollierbar werden. Es wäre denkbar, ein „*Nudging*"-System für den

701 4. Teil, A., I.
702 4. Teil, B.

Schutz der Rechte und Freiheiten des Betroffenen einzusetzen. Gleichwohl würde damit eine indirekte Beeinflussung der freiwilligen Entscheidungsfindung erfolgen, die zunächst intransparent wäre und keinen unmittelbaren Beitrag für einen gesteigerten Schutz der informationellen Selbstbestimmung bedeuten würde.[703]

Weiter kann die Identitätsverwaltung *ex post* zur Rechtfertigung zunächst über das Auskunftsrecht als Zugangsrecht zu den personalen Identitäten erfolgen. Auf dieser Grundlage wäre die Kontrollmöglichkeit insbesondere mit dem Recht auf Vergessenwerden und dem Recht auf Datenübertragbarkeit gegeben. Weiter kommt das Recht gegen automatisierte Entscheidungen und damit automatisiert generierte Bilder personaler Identitäten in Betracht. Dabei lässt sich aus dem EWG 71 S. 4 ein *iteratives Verhandlungssystem* zwischen Verantwortlichem und Betroffenen nachweisen, welches als Verfahren für eine dynamisch ausgestaltete Identitätsverwaltung in einem *Dashboard-System* herangezogen werden kann. Ebenso lassen sich die Risikolagen als Gegenstand der Identitätsverwaltung einbeziehen und der Verantwortliche kann mit der Einrichtung eines iterativen Verhandlungskonzeptes *ex ante* über die Datenschutzerklärung und *ex post* über die personale Identität mit ihren Attributen selbst die Risiken neu ordnen.[704]

Die Identitätsverwaltung, basierend auf dem TMG und dem TKG, unterliegt dem Vorbehalt, dass die zu der DSGVO komplemäntere EPrivacy-VO noch nicht in Kraft getreten ist und demnach die bereichsspezifischen Datenschutzregeln im TMG und TKG unter der Maßgabe der datenschutzrechtlichen Vorgaben nach der DSGVO fortgelten. Aus dem TMG geht eine personale Teilidentität aus den Bestandsdaten, den Nutzungsdaten, dem Nutzungsprofil und den „Cookies" hervor. Ebenso geht aus dem TKG jeweils eine personale Teilidentität aus Bestandsdaten, Verkehrsdaten und Standortdaten hervor, wobei letztere gemäß Art. 4 Nr. 1 DSGVO auch dem Anwendungsbereich der DSGVO unterliegen. Aus jeder dieser personalen Teilidentitäten lässt sich ein eigener Erkenntniswert ableiten, so dass die Transparenz darüber mit einem *Dashboard-System* zu einer Schutzsteigerung der informationellen Selbstbestimmung führen würde.[705] Innerhalb dieses *Dashboard-Systems* sind „*Nudges*" als Anstöße für eine risikobewusste Entscheidungsfindung des Betroffenen auf der Rechtfertigungsebene und *ex post* zur Rechtfertigung denkbar, ohne dass die „*Nudges*" die Ent-

703 4. Teil, C.
704 4. Teil, D.
705 4. Teil, E.

scheidungsfindung negativ beeinflussen oder gar eine nachteilige Wirkung auf den Betroffenen haben. Weiter sollte das *Dashboard-System* mit einem iterativen Verhandlungssystem ausgestaltet sein, welches bereits auf der Ebene der Informationspflichten in Gestalt von iterativ verhandelten Datenschutzerklärungen und auf der Ebene *ex post* zur Rechtfertigung durch das Zugangsrecht als Kontrollmöglichkeit wirken kann. Diese technische Gestaltung könnte durch eine *Trusted Third Party* erfolgen, vorzugswürdig erscheint jedoch ein mit Schnittstellen ausgestaltetes *Dashboard-System*, ohne den Datensatz der personalen Teilidentitäten zu speichern. Demnach könnte ein *Dashboard-System* derart ausgestaltet sein, dass ein Intermediär die Interoperabilität personaler Identitäten vergleichbar mit der Bezahlung im „*Mobile Payment*" über eine Schnittstelle ermöglicht. Dies würde einem „*Identity Ecosystem*" als eine Plattform für personale Identitäten mit einem gestuften Vertrauensniveau entsprechen. Damit lässt sich auch der Grundsatz der Datenminimierung wirksam realisieren, da die personalen Teilidentitäten einmalig gespeichert würden. Weiter handelt es sich jeweils bei den aus dem IKT-Recht abgeleiteten personalen Teilidentitäten um Agenten aus den Datensätzen, die der natürlichen Person zurechenbar sind. Zugleich kann diese Zurechnungsbeziehung in gradueller Intensität ausgestaltet sein und das Vertrauensniveau variieren, wenn etwa die ursprüngliche Identifizierung mit dem Personalausweis erfolgte.

Aus dem IKT-Recht konnten die einzelnen Datenverarbeitungen und personalen Teilidentitäten nachgewiesen werden, die nunmehr in eine funktionsfähige Einheit zusammengeführt und mit dem *Dashboard-System* für die Verwaltung transparent gemacht werden kann. Dahingehend fungiert die *Identitätsverwaltung als Metamethode*[706] und verlangt ein Verfahren, wie es aus den Phasen der Datenverarbeitung *ex ante* zur Rechtfertigung, der Rechtfertigung und *ex post* zur Rechtfertigung hergeleitet wurde. Damit fungiert die Identitätsverwaltung als ein Programm und ist eine *Metamethode* über die Gesamtheit der personalen Teilidentitäten. Dieses Programm kann in Gestalt eines *Dashboard-Systems* mit einer interoperablen Struktur umgesetzt werden. Darin läge neben einem normativen und administrativen Schutz auch ein technischer, der als Erweiterung zu einem möglicherweise rechtlich ausgeschöpften Schutzmechanismus[707] dient. Damit könnte sich die Wirksamkeit des IKT-Rechts zum Schutz der informationellen Selbstbestimmung in Gestalt der Identitäten auf einer überge-

706 2. Teil, B., III; 3. Teil, B., II., 2.

707 *Roßnagel*, in: Roßnagel/Abel (Hrsg.), Handbuch Datenschutzrecht, 2003, 3.4. Rn. 42.

ordneten Gestaltungsebene mit einem Meta-Programm als effektiv und das IKT-Recht hinsichtlich der Transparenz- und Einwilligungsanforderungen als durchsetzbares Recht erweisen. Wie das *Identitätsverwaltungsmodell auf der Metaebene als Verfahren* weiter differenziert werden kann, soll im 5. Teil durch Einbeziehung der *spieltheoretischen Perspektive* herausgearbeitet werden. Damit soll die Untersuchung um eine Perspektive erweitert werden und die Annahme eines Meta-Programms der Identitätsverwaltung mit einem *Dashboard-System* eine weitere Fundierung erfahren.