7.Teil: Gesamtergebnis

Es wurde ein Identitätsverwaltungsmodell begründet, welches die personale Identität im online-Kontext im Gleichlauf zum offline-Kontext schützen soll. Dafür wurde die Identitätsverwaltung in IKT-Systemen zunächst stipulativ als die Kontrolle einer natürlichen Person über die Begründung und Annahme von personalen Teilidentitäten definiert. Dies führte zu der Differenzierung zwischen einem statischen *Idem*-Anteil und einem dynamischen *Ipse*-Anteil der personalen Identität,[902] die gleichermaßen in das Identitätsverwaltungsmodell einbezogen wurden. Der Schutz dieser Anteile der personalen Identität unterliegt nach dieser Untersuchung der abwehrrechtlichen Dimension des Kombinationsgrundrechts gemäß Art. 7, 8 GRC, was die informationelle Selbstbestimmung der natürlichen Person über die Verwendung der personenbezogenen Daten umfasst.[903] Ebenso wurde das Konzept der Kontrolle über personale Identitäten aus dem allgemeinen Persönlichkeitsrecht gemäß Art. 2 Abs. 1 GG abgeleitet, wenn die innere Dimension der Persönlichkeitsentwicklung und die äußere Dimension der Selbstdarstellung auch in ihrem Gewährleistungsgehalt geschützt werden. Dabei wurde die kommunikative Dimension des allgemeinen Persönlichkeitsrechts herausgearbeitet, was sich in dem Recht auf informationelle Selbstbestimmung konkretisiert und den Schutz der Informationen und Erkenntnismöglichkeiten über eine personale Identität umfasst. Weiter lässt sich der datenbasierte Lebenszyklus einer personalen Identität mit dem *Recht auf Neubeginn* zeitlich beschränken, was seine einfachrechtliche Ausprägung im Recht auf Vergessenwerden gemäß Art. 17 DSGVO findet und die grundrechtliche Anforderung der Kontrolle über personale Teilidentitäten verdeutlicht.[904] Darin kommen die zeitgebundene und kontextspezifische Dynamik der personalen Identität in ihren *Idem*- und *Ipse*-Anteilen zum Ausdruck, die vom grundrechtlichen Schutz umfasst sind.

Weiter wurden auf dieser Basis die Anforderungen an die Identitätsverwaltung konkretisiert, indem einfachrechtliche Typologien als Grundlage für die Modellbildung herangezogen wurden. Dazu gehörten zunächst das

902 1. Teil, C., II., 2.
903 2. Teil, A., I.
904 2. Teil, A., II., 1.

Namensrecht und im elektronischen Rechtsverkehr die Signatur, die jeweils an den *Idem*-Anteil der personalen Identität anknüpfen. Demgegenüber konnte der dynamische *Ipse*-Anteil personaler Identitäten im elektronischen Rechtsverkehr mit der vertraulichen und sicheren Kommunikation über das De-Mail-G abgebildet werden.[905] Diese Ausprägungen der personalen Identität bedürfen in einem Identitätsverwaltungsmodell der Kontrolle, die in eine absolute Kontrolle über den Zugang zur personalen Identität und in eine relative Kontrolle über das Bild der personalen Identität differenziert wurde.[906] Insoweit kommt es bei dem Identitätsverwaltungsmodell darauf an, dass eine Kontrollierbarkeit über die Erkennntnisse zu einer personalen Identität geschaffen wird.[907] Diese Anforderungen an ein Identitätsverwaltungsmodell wurden auf das IKT-Recht übertragen.

Demnach sollte die soziotechnische Kontrollierbarkeit der personalen Identitäten mit ihren *Idem*- und *Ipse*-Anteilen über den Datenzyklus hinweg im IKT-Recht nachvollzogen werden. Dafür wurde die Identitätsverwaltung im Datenschutzrecht chronologisch *ex ante* zur Rechtfertigung, der Rechtfertigung und *ex post* zur Rechtfertigung abgeleitet. Es konnte nachgewiesen werden, dass für die Kontrolle durch den Betroffenen zunächst die Informationspflichten maßgeblich sind und der Bedarf nach Transparenz über die Risiken der Datenverarbeitung besteht.[908] Weiter dient die rechtfertigende Einwilligung ebenfalls der Kontrolle von personalen Identitäten, so dass die Einwilligungsentscheidung einer differenzierten Analyse unterlag und in Anbetracht der hohen Einwilligungsbereitschaft („*digital unconscious*“) auf verhaltensökonomische Verzerrungsfaktoren untersucht wurde.[909] Dabei wurde ein legitimatorisches Defizit über die Rechtfertigungswirkung der Einwilligung und der Rechtfertigung ohne aktive Handlung bei der Begründung personaler Identitäten festgestellt, welches zu einem Kompensationsbedarf mit den Betroffenenrechten führt.[910] Da jedoch die Betroffenenrechte nicht immer umfassend wahrgenommen werden, konnte eine umfassende Kompensation schwerlich angenommen werden.[911]

Ferner konnten in online-Kontexten die personalen Teilidentitäten, basierend auf den Bestands-, Nutzer-, Standort- und Verkehrsdaten, aufzei-

905 3. Teil, A., I., II.
906 3. Teil, C.
907 3. Teil, B., D.
908 4. Teil, B., II.
909 4. Teil, B., II.
910 4. Teil, C., II., III.
911 4. Teil, D.

gen, dass sie einen eigenständigen Erkenntnisgehalt über die personale Identität ermöglichen.[912] Für die Kontrolle dieser personalen Teilidentitäten wurde der Bedarf nach einem Identitätszugang im Rahmen der Informationspflichten und des Auskunftsrechts gemäß Art. 12, 15 DSGVO und der damit verbundenen Gewährleistung der *kontextuellen Integrität* von personalen Teilidentitäten abgeleitet. Ein Gesamtüberblick sollte dabei mit einem *Dashboard-System* geschaffen werden, denn darin liegt die Grundlage für ein Konzept des „*identity management by design*“[913].

Bei einem Ausgleich des Legitimationsdefizits gegenüber der informationellen Selbstbestimmung stellt sich die Frage nach einem kompensatorischen Mechanismus über die Betroffenenrechte hinaus. Dafür konnte mit der spieltheoretischen Modellierung eine weitere Perspektive eingeführt werden, mit der die datenschutzrechtliche Konstellation im Hinblick auf das Strategieverhalten der Spieler des Verantwortlichen und des Betroffenen untersucht wurde. Nach dieser spieltheoretischen Modellierung richtet sich das Strategieverhalten nach den bestehenden Informationsständen und den erzielbaren Auszahlungswerten. Wenn dabei das öffentliche Gut der persönlichen Informationen als „Verhandlungsmasse“ im Zentrum des Strategieverhaltens steht, bedarf es zum Schutz des öffentlichen Gutes der persönlichen Informationen eines möglichst schonenden Strategieverhaltens.[914] Dieses liegt in der kooperationsfördernden *TIT for TAT*-Strategie, die mit den Verfahrensprinzipien der Mediation begünstigt wird und das Potential zu einer dominierenden Strategie hat. Mit dem Mediationsverfahren wird dieser Rahmen geschaffen, in dem die Bilder personaler Identitäten unter den *Instruktionen* der Verfahrensprinzipien im „Schatten des Rechts“ verhandelbar werden.[915] Denn es konnte ein Konflikt zwischen dem Verantwortlichen und Betroffenen über den Schutz der persönlichen Informationen nachgewiesen werden, der einer Intervention bedarf. Diese Intervention wurde im Wettbewerbsrecht, welches Anreize für datenschutzkonforme Produkte und Dienste schaffen kann, und in einem Verfahren[916], welches mit einem technischen Mediationsagenten als Metakommunikation konkretisiert wurde,[917] aufgezeigt. Folglich wird in einem Identitätsverwaltungsmodell die Notwendigkeit einer mediativen Identi-

912 4. Teil, E.
913 4. Teil, B., VI.
914 5. Teil, A.
915 5. Teil, B., III.
916 5. Teil, B., IV.
917 5. Teil, C., III.

tätsverwaltung aufgezeigt, um die Verhandlung der Bilder personaler Identitäten in ihrem *Ipse*-Anteil zu ermöglichen.[918] Dabei geht es um die Intervention und um ein Gegengewicht zur Datenverarbeitung und Profilerstellung von Intermediären mit marktbeherrschender Stellung.

Insgesamt konnte gezeigt werden, dass die mediative Identitätsverwaltung dem Schutz des öffentlichen Gutes der persönlichen Informationen dient und ein technischer Mediationsagent als Interventionsmechanismus fungieren kann. Daneben konnte für die Gewährleistung des Modells der Identitätsverwaltung ein Paradigmenwechsel auf drei Ebenen abgeleitet werden, der aus dem Zugang zu den personalen Identitäten, der verhandlungsfähigen personalen Identität und einer dezentralen kontextbezogenen Identitätsverwaltung besteht.[919] Dafür soll etwa mit einem *Dashboard-System* die Transparenz über die kontextspezifischen personalen Teilidentitäten begründet und die Verwaltung dieser zur Gewährleistung der *kontextuellen Integrität* ermöglicht werden. Folglich stellt sich die Frage nach der Implementierung der Identitätsverwaltung auf der Mikro- und Makroebene, so dass der soziotechnische Regelungsbedarf (A.) und der prinzipienbasierte Ansatz (B.) mit einem abschließenden Ausblick (C.) dargestellt werden sollen.

A. Soziotechnischer Regelungsbedarf

Die grundrechtssichernde Implementierung eines technischen Mediationsagenten und einer Struktur für die mediative Identitätsverwaltung könnte einen regulatorischen Eingriff verlangen, bei dem der Anknüpfungspunkt zu bestimmen ist. Zum einen geht es auf der Mikroebene um die Implementierung eines „*mechanism by design*" in Gestalt des technischen Mediationsagenten und zum anderen geht es auf der Makroebene um einen Anreizmechanismus für Maßnahmen zum Ausgleich der Informationsasymmetrien gerade gegenüber Intermediären mit marktbeherrschender Stellung. Jeweils kann ein staatlicher regulatorischer Eingriff dazu dienen, die Technologieentwicklung, Gesamtstrukturen und schließlich das Verhalten des Einzelnen zu beeinflussen. Demgegenüber ist in ökonomischer Hinsicht ein „*Nudging*"-System denkbar, welches bei der Umsetzung rechtlicher Anforderungen durch den Verantwortlichen für den Selbstdatenschutz des Betroffenen unterstützend wirkt, ohne dabei freiheitsbeschrän-

---

918 5. Teil, C., IV., V.
919 6. Teil.

kende Wirkung zu entfalten. Als „*Nudges*" sind Konzepte denkbar, die neben einer vereinfachten bildlichen Darstellung der Risiken auch Warnungen über die Folgen der Einwilligungen enthalten können. Diese würden als (paternalistische) Anreize für eine risikobewusste Entscheidung wirken und sich als wenig invasiver Mechanismus günstig auf den Schutz des öffentlichen Gutes der persönlichen Informationen auswirken.

Ferner kommt *de lege ferenda* die Erweiterung der Schutzgüter im Produkthaftungsrecht gemäß § 1 Abs. 1 ProdHG auf den Schutz der persönlichen Informationen und damit der informationellen Selbstbestimmung in Betracht, womit die Hersteller gehalten wären, die Fehlerfreiheit bei der Entwicklung datenschutzkonformer Produkte zu gewährleisten. Dies würde sich wiederum auf den Wettbewerb mit datenschutzkonformen Produkten auswirken und die öffentliche Reputation, „*privacy by design*"-Produkte im Markt anzubieten, eine positive Marktdynamik für den „*Market for Lemons*"[920] und den Schutz personaler Identitäten im online-Kontext fördern. Gleichwohl würde es sich dabei um eine Marktentwicklung handeln, die den „*Market for Lemons*" nicht vollständig verdrängt, da Informationsasymmetrien nicht aufgelöst werden können. Insofern besteht der Bedarf an wettbewerbsrechtlichen Interventionsmechanismen gegenüber Intermediären mit marktbeherrschender Stellung fort, da der Markt allein, wie sich an dem *Cambridge Analytika-* und *Facebook*-Skandel zeigte,[921] kaum datenschutzkonforme Produkte hervorbringt.

Mit der rechtfertigenden Einwilligung als maßgebliche Kontrollhandlung über personale Identitäten geht ein soziotechnischer Regelungsbedarf einher, um verhaltensökonomische Verzerrungen und langfristige Erkenntnismöglichkeiten aus dem Datenzyklus kompensieren zu können. Dafür kommen erweiterte Transparenzpflichten gemäß Art. 13 DSGVO in Betracht, die etwa auf die verhaltensökonomischen Verzerrungen hinweisen würden, so dass eine Ergänzung dieser Norm in Frage kommt. Ebenso ist ein mit dem AGB-Recht vergleichbares Schutzregime denkbar, was zwischen Datenverarbeitungen im B2C-, B2B- und C2C-Verhältnis differenziert und eine *contra proferentem*-Regel für Zweifelsfälle vorsieht.[922] Daneben wäre die Einbeziehung der Risikobewertung durch den Verantwortlichen *de lege ferenda* als ausdrückliche Informationspflicht wünschenswert, damit eine risikobewusste Entscheidung von dem Betroffenen vorgenom-

920 4. Teil, B., IV., 2., a).
921 www.faz.net/aktuell/wirtschaft/diginomics/fragen-und-antworten-zu-facebook-und-cambridge-analytica-15505321.html (zuletzt aufgerufen 20.06.2020).
922 4. Teil, C., II., 2.

men werden kann. Dies lässt sich aus den Informationspflichten gemäß Art. 13 DSGVO und dem EWG 39 S. 5 ableiten, wonach Betroffene über die Risiken der Datenverarbeitung informiert und aufgeklärt werden sollen. Dafür müssten die maßgeblichen Risikokriterien, die im Rahmen der semi-quantitativen Risikobewertungsmethode bestimmt wurden, transparent gemacht werden.[923]

Weiter könnte eine spezifische Rechtsregel mit dem Inhalt, dass neben „*privacy by design*" ein „*identity management by design*" mit umfassenden Transparenzanforderungen eingesetzt werden müsste, verfolgt werden.[924] Es würde sich um eine konkretisierende Regelung des Art. 25 DSGVO handeln, die für eine effektive Wirkung über eine Soll-Vorschrift hinaus als Muss-Vorschrift ausgestaltet werden sollte. Diese könnte auch in dem EWG 78 S. 2 abgebildet werden. Darin käme die „techniksteuernde Funktion des Rechts"[925] zum Ausdruck und die Reputation über den Einsatz eines „*identity management by design*"-Konzeptes würde sich positiv auf die Wettbewerbsfähigkeit des Verantwortlichen auswirken können.

Ebenso kommt *de lege ferenda* eine Begründungspflicht in Frage, sollte der Verantwortliche bei umfangreichen Datenverarbeitungen kein Identitätsverwaltungskonzept vorsehen. Diese könnte vergleichbar mit der Begründungsanforderung aus § 253 Abs. 3 Nr. 1 ZPO ausgestaltet sein, wonach Angaben in einer Klageschrift über den Versuch einer Mediation oder außergerichtlichen Streitbeilegung vorzunehmen sind.[926] Darin würde ein einfachrechtlicher Anreiz liegen, der den Verantwortlichen dazu veranlasst, sich mit der Einbeziehung der Identitätsverwaltung ernsthaft auseinanderzusetzen und der Verantwortliche begründen müsste, warum ein Identitätsverwaltungskonzept nicht umgesetzt wurde.

B. Prinzipienbasierter Ansatz

Neben einer einfachrechtlichen Regelung zur Implementierung der Identitätsverwaltung könnte ebenso ein prinzipienbasierter Ansatz gewählt werden. Gegenüber den Rechtsnormen ermöglicht das Prinzip die Verfolgung eines generellen Regelungsziels und einen hohen Abstraktionsgrad.[927] Das

923 4. Teil, B., II., 2.
924 4. Teil, B., VI.
925 *Schallbruch*, Schwacher Staat im Netz, 2018, S. 182.
926 5. Teil, C., V.
927 *Zippelius*, Das Wesen des Rechts, 2012, S. 84.

Prinzip ist somit ein Gegengewicht zu einem Regelungsüberschuss, der seit dem Volkszählungsurteil dem Datenschutzrecht teilweise zugeschrieben wird.[928] Insoweit könnte die Einführung eines Prinzips dem Schutz der personalen Identitäten und der Identitätsverwaltung im online-Kontext dienen.

Zwar ist der prinzipienbasierte Ansatz von der angloamerikanischen Rechtskultur geprägt und wurde im Zusammenhang mit dem IT-Recht von *Easterbrook* in dem Aufsatz „*Cyberspace and the Law of the Horse*" zugespitzt.[929] Danach sollten nämlich generelle Prinzipien für das IT-Recht bestimmt werden, damit kontextspezifische detaillierte Rechtsregeln (etwa das „Pferderecht") für das damals neue IT-Recht unnötig werden. Entsprechend zeigen die Grundsätze der Datenverarbeitung in Art. 5 DSGVO die Wirksamkeit eines prinzipienorientierten Ansatzes, da diese Grundsätze sich auf das gesamte Datenschutzrecht erstrecken und kontextspezifisch umgesetzt werden müssen. Folglich wird die Innovationsoffenheit gewährleistet und kontextspezifische Detailregeln werden verdrängt. Weiter könne mit Prinzipien flexibler auf zeitlich bedingte neue Entwicklungen reagiert werden, womit zugleich eine Technologieoffenheit gewährleistet wäre.[930]

Das Regelungsziel, den Selbstdatenschutz mit der mediativen Identitätsverwaltung zu fördern, lässt sich auf prinzipieller Ebene abbilden. Indem die Kontrollmöglichkeiten des Betroffenen im IKT-Recht nachgewiesen wurden, erscheint eine hohe Abstraktion zum Schutz der personalen Identität folgerichtig. Gleichwohl bedarf es einer Erweiterung auf der technischen Gestaltungsebene, die den Zugang zu den personalen Identitäten und die Verhandlung der Bilder personaler Identitäten etwa mit einem *Dashboard-System* ermöglicht. Damit wird dem politischen und wirtschaftlichen Bestreben, die *digitale Souveränität* zu stärken, gefolgt und ein effektiver Schutzmechanismus zum eigenverantwortlichen Selbstdatenschutz begründet.

Erweiternd lässt sich die Identitätsverwaltung hinsichtlich der statischen *Idem*- und dynamischen *Ipse*-Anteile als Gegenstand der staatlichen Daseinsvorsorge einordnen, die bereits von *Schallbruch* für die elektronische Identifizierung angenommen wird.[931] Damit müsste dem Betroffenen

928 *Schallbruch*, Schwacher Staat im Netz, 2018, S. 226.
929 *Easterbrook*, U. Chi. Legal F. 1996, 207.
930 *Zippelius*, Das Wesen des Rechts, 2012, S. 107.
931 *Schallbruch*, Schwacher Staat im Netz, 2018, S. 234; ebenso *Hornung*, in: Roßnagel (Hrsg.), Wolken über dem Rechtsstaat?, 2015, 189 (206).

über den Datenzyklus hinweg prinzipiell eine dynamische Identitätsverwaltung ermöglicht werden, die ein umfassenderes, digitales Handeln gewährleisten würde. Dies würde den Schutz der informationellen Selbstbestimmung im offline-Kontext auf den online-Kontext spiegelbildlich übertragen. Folglich würde sich die staatliche Gewährleistungsverantwortung zur Grundrechtsausübung auf den online-Kontext mit einer dynamischen Identitätsverwaltungsmöglichkeit erstrecken.

Insgesamt könnte es sich um ein im IKT-Recht geltendes „*Prinzip der verhandlungsfähigen personalen Identität*" für den online-Kontext handeln, dem ein dynamisches und iteratives Schutzkonzept für personale Identitäten immanent ist. Dieses sollte mit den Anforderungen einer dezentralen Identitätsverwaltung erweitert werden und ebenso den Zugang zur personalen Identität ermöglichen. Weiter müsste die Verhandlungsfähigkeit der personalen Identität rechtlich und technisch gewährleistet werden. Dieses Prinzip würde dem Konzept der „regulierte(n) Selbstregulierung im Schatten des Rechts"[932] dienen, wenngleich die Effektivität eines solchen Prinzips von seiner tatsächlichen Anwendung abhängig sein würde. Damit besteht ebenso der Bedarf an der Sicherstellung einer effektiven Rechtsanwendung, die mit einem verhaltensökonomischen Anreizmechanismus umgesetzt werden sollte.

C. Ausblick

Die Identitätsverwaltung würde für eine Implementierung zunächst einen politischen Willen voraussetzen, damit eine rechtliche Regulierung folgen kann. Diese sollte nicht als Detailregelung ausgestaltet sein, sondern es würde ebenso wirksam ein Prinzip mit entsprechenden Anreizmechanismen eingeführt werden können. Weiter wäre ein solches Prinzip dazu geeignet, eine technische Gestaltungsprämisse auf der Hardware- und Software-Ebene für den online-Kontext zu schaffen. Hierbei kommt die Implementierung einer dezentralen und interoperablen Identitätsverwaltungsarchitektur in Betracht, mit der die Überführung personaler Teilidentitäten in verschiedene Kontexte ermöglicht wird. Gleichzeitig könnte die Implementierung auf der Softwareebene mit der Einrichtung eines technischen Mediationsagenten, der die Verfahrensprinzipien der Mediation umsetzt, erfolgen. Damit würde für eine Identitätsverwaltungsarchitektur die wesentliche Implementierungsebene zur effektiven Anwendung eines „*Prin-*

932 *Spiecker gen. Döhmann*, K&R 2017, 4 (6).

zips der verhandlungsfähigen personalen Identität" für den online-Kontext realisiert werden können.

Weiter würde mit der Implementierung einer Identitätsverwaltungsarchitektur eine Steigerung des Informationszugangs des Betroffenen zu den personalen Identitäten erfolgen und der Verantwortliche wäre dazu gehalten, diesen Zugang zu ermöglichen. Darin würde nicht nur eine Schutzsteigerung für das öffentliche Gut der persönlichen Informationen liegen, sondern auch die Pluralität personaler Identitäten für den online-Kontext im freiheitlich demokratischen Sinne gefördert werden. Folglich ließe sich sogar vertreten, dass es zur staatlichen Gewährleistungsverantwortung gehöre, die Pluralität der personalen Identitäten auch im online-Kontext sicherzustellen. Demnach lässt sich nicht nur die elektronische Identifizierung als Bestandteil der staatlichen Daseinvorsorge einordnen, sondern auch das *Prinzip der verhandlungsfähigen personalen Identität*.

Mit der Europäisierung des Datenschutzrechts erscheint hierbei jedoch eine nationale Regulierung wenig zielführend, so dass eine Erweiterung der Datenverarbeitungsgrundsätze gemäß Art. 5 DSGVO in Frage kommt. Damit würde ein Gegengewicht zu den Intermediären mit marktbeherrschender Stellung geschaffen werden, welches jedoch mit einem wirksamen Anreizmechanismus ergänzt werden müsste. Zudem wurzelt die prinzipielle Förderung einer dynamischen Identitätsverwaltung im online-Kontext in den grundrechtlichen und einfachrechtlichen Schutzvorgaben, weshalb ein Prinzip für den online-Kontext eine konsequente Erweiterung des bestehenden Schutzregimes bedeuten würde. Insofern ist für die Implementierung der Identitätsverwaltung zunächst der europäische Gesetzgeber gefragt und zugleich erscheint nach den hier gewonnenen Ergebnissen die Einbeziehung verhaltensökonomischer Erkenntnisse für wirksame Anreizmechanismen und für den Selbstdatenschutz wünschenswert.